Institut suisse de droit comparé
Schweizerisches Institut für Rechtsvergleichung
Istituto svizzero di diritto comparato
Swiss Institute of Comparative Law

# GUTACHTEN

# ÜBER DAS

# DATENSCHUTZRECHT

# IN AUSGEWÄHLTEN STAATEN

# (DEUTSCHLAND, ÖSTERREICH, ITALIEN, FRANKREICH, VEREINIGTES KÖNIGREICH, SPANIEN, BENELUX, SLOWENIEN, NORWEGEN, KANADA, USA)

**Avis 09-207**

Lausanne, den 19. November 2010

LHU/AA/AF/AP/KJD/MH/MM/SK/cf

*Class. ISDC: CA/* A,CND,D,E,F,GB,I,N,NL,SLO 65.1

**INHALTSÜBERSICHT UND INHALTSVERZEICHNIS**

# Inhaltsübersicht

# Inhaltsverzeichnis

**ZUSAMMENFASSUNG**

## ZUSAMMENFASSUNG

Auf eidgenössischer Ebene wird der Datenschutz seit dem 1. Juli 1993 durch das Bundesgesetz über den Datenschutz (Datenschutzgesetz, DSG; SR 235.1) geregelt. Nach der Revision von 2006 ist angesichts aktueller Revisionsprojekte im Rahmen der europäischen Zusammenarbeit aber auch angesichts der teilweisen Kritik und politischer Vorstösse eine **umfassende Evaluation** des Datenschutzgesetzes im Gang. Dabei geht es insbesondere um Effektivität, Effizienz und Wirksamkeit des Gesetzes. Die Evaluation soll aber auch einen internationalen Vergleich der Schweizerischen Regelung ermöglichen. Die vorliegende Analyse soll also einen Überblick über verschiedene Aspekte des Datenschutzes in verschiedenen Staaten ermöglichen und dabei insbesondere interessante Hinweise für die Schweiz anzeigen.

Die Analyse behandelt die Rechtslage in **10 verschiedenen Staaten**, mit einem klaren Fokus auf Europa. Dabei werden zunächst die vier grösseren Nachbarländer der Schweiz untersucht, aber auch das spanische Recht, das englische Recht als Vertreter der angelsächsischen Rechtsordnungen, das slowenische Recht als Beispiel einer mittel- und osteuropäischen Rechtsordnung, das holländische Recht als Beispiel einer Rechtsordnung der Benelux Länder sowie das kanadische Recht als aussereuropäische Rechtsordnung berücksichtigt. Zudem enthält die Analyse einige Ausführungen zu Regelungen in der USA im Bereich neuer Technologien.

Auf **internationaler Ebene** bestehen seit den 1980er Jahren sowohl im Rahmen der OECD (*OECD Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data*[1]*)* als auch im Rahmen des Europarates (*Europäischen Datenschutzkonvention*[2]*)* Instrumente, welche einen freien Informationsaustausch und einen Schutz der Betroffenen ermöglichen. Von ungleich grösserer Bedeutung sind für die untersuchten Rechtsordnungen (mit Ausnahme von Kanada und der USA) die Regelung im Rahmen des europäischen **Gemeinschaftsrechts**. Dabei hat in erster Linie die *Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr*[3] angesichts ihres Detaillierungsgrads eine umfassende Rechtsharmonisierung herbei geführt und auch über die Grenzen des EWR die Rechtsentwicklung beeinflusst, so insbesondere in Kanada. Um die Bedürfnisse des Datenschutzes der technologischen Entwicklung anzupassen, wurde 2002 die *Richtlinie 2002/58/EG*[4] *über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation* erlassen, welche telekommunikationsspezifische Regelungen zum Datenschutz enthält. Im Bereich der Telekommunikation bezweckt schliesslich die (in der politischen Diskussion allerdings umstrittene) *Richtlinie 2006/24/EG über die Vorratsspeicherung von Daten*[5] die Harmonisierung der Aufbewahrung von Daten und soll damit Ermittlung und Verfolgung schwerer Straftaten erleichtern.
Auf nationaler Ebene finden sich in allen untersuchten Rechtsordnungen (mit Ausnahme der USA) spezifische Datenschutzgesetze. So ist der Datenschutz in Deutschland auf Bundesebene im

---

1 http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html (15.11.2010).

2 http://conventions.coe.int/Treaty/GER/Treaties/Html/108.htm (15.11.2010).

3 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:DE:HTML (15.11.2010).

4 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:DE:PDF (15.11.2010).

5 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:DE:HTML (15.11.2010)

*Bundesdatenschutzgesetz* geregelt. Daneben existieren regionale Regelungen auf Länderebene (Landesdatenschutzgesetze), sowie Regelungen im Bereich der Telekommunikation im Telekommunikationsgesetz. In Österreich ist Datenschutz im „*Bundesgesetz über den Schutz personenbezogener Daten*" geregelt. In Italien besteht ein *Datenschutzgesetz*, in Frankreich sind die wesentlichen Regelungen in einem Gesetz „*Informatique et Libertés*" aus dem Jahre 1978 enthalten und als Kontrollstelle die *Commission Nationale de l'Informatique et des Libertés* arbeitet. In Grossbritannien beinhaltet die wichtigste Regelungen *the Data Protection Act 1998* wobei die Regeln nicht immer der kontinentalen Systematik entsprechen. Die Kontrolle der Einhaltung der Datenschutzregelungen wird durch den *Information Commissioner* ausgeübt. In Spanien die Grundlegende Regelung beinhaltet *Ley de Protección de Datos* aus dem Jahre 1999 und in Slovenien *Zakon o varstvu osebnih podatkov* das im Januar 2005 in Kraft trat. In Niederlanden ist es *Wet bescherming persoonsgegevens* und in Norwegen *Personopplysningsloven*. In Kanada bestehen auf Landesebene das *Loi sur la Protection des Renseignements Personnels* für den öffentlichen Sektor sowie das *Loi sur la Protection des Renseignements Personnels et les Documents éléctroniques* für den privaten Sektor, daneben haben verschiedene Provinzen ihre eigene Gesetzgebung.

**Grundsätze der Datenverarbeitung**

Bei den **Grundsätzen** der Datenverarbeitung finden sich in allen Rechtsordnungen (sowie auch in Frankreich) die Vorgaben von Art. 6 der Richtlinie 95/46/EG wieder, z.T. wörtlich (in Spanien), z.T. sinngemäss. So sind der Grundsatz der Datensicherheit (Ergreifen von angemessenen Massnahmen), Grundsätze von Rechtmässigkeit, Verhältnismässigkeit, Zweckbindung und Einwilligung durchgehend anerkannt. In der Ausgestaltung ergeben sich zwar einige Unterschiede, so wird z.B. in Deutschland anstelle auf Treu und Glaube auf die Gesetzmässigkeit der Verarbeitung abgestellt, oder in Grossbritannien findet sich keine ausdrückliche Erwähnung der Erkennbarkeit, sondern vielmehr eine Umsetzung der Vorschriften von Art. 7 Richtlinie 95/46/EG, oder das Prinzip der Sparsamkeit ist unterschiedlich ausgeprägt. Es bestehen aber keine Anhaltspunkte dafür, dass die Unterschiede bei der Umsetzung der Grundsätze einer fundamental anderen Haltung gegenüber dem Datenschutz entsprechen.

Unterschiede finden sich hingegen in der **Art der Regelung** bzw. im Anwendungsbereich. Dabei fällt einerseits auf, dass die sektorspezifische Gesetzgebung in den angelsächsischen Rechtssystemen eine viel grössere Bedeutung haben, was einen allgemeinen Quervergleich etwas erschwert. Es ist jedoch gerade im Hinblick auf die Umsetzung der Richtlinie 2002/58/EG zu beachten, dass auch in Kontinentaleuropa Datenschutzregeln in Spezialgesetzen verankert werde, was einen allgemeinen Quervergleich erschwert (s. unten). Ein weiterer Unterschied besteht im Anwendungsbereich der Datenschutzgesetzgebung. In Deutschland und in Kanada sind für öffentliche und private Datenbearbeitung verschiedene Gesetze anwendbar, in den meisten übrigen Staaten bestehen innerhalb desselben Gesetzes Sondervorschriften für den privaten oder den öffentlichen Sektor, z.B. zum Verfahren, zur Bewilligung von Datenbearbeitung, und zum Zugang zu Daten. In wieder anderen Staaten (Frankreich, Grossbritannien) wird grundsätzlich nicht zwischen öffentlicher und privater Datenbearbeitung differenziert.

Bei verschiedenen grundlegenden Instrumenten des Datenschutzes entsprechen sich die untersuchten Rechtsordnungen weitgehend. So ist das **Auskunftsrecht** (Art. 8 DSG; Art. 12 Richtlinie 95/46/EG) in allen Rechtsordnungen ein wesentlicher Teil des Schutzes von Betroffenen. Bei der Umsetzung liegen keine nennenswerten Unterschiede vor. Auch bei der **grenzüberschreitenden Bekanntgabe** und bei der Bekanntgabe **besonders schützenswerten Personendaten** finden sich kaum grundsätzliche Unterschiede, was darauf zurückzuführen ist, dass die Bestimmungen der Richtlinie hier relativ genau sind (Art. 8 und Art. 25 ff. Richtlinie 95/46/EG). Im Resultat bestehen für die grenzüberschreitende Bekanntgabe auch in Kanada ähnliche Regeln, auch wenn eine ausdrückliche gesetzliche Bestimmung fehlt. Bei den besonders schützenswerten Daten findet sich

hingegen in Kanada nicht eine den europäischen Bestimmungen entsprechende Regelung, wobei gewisse Sonderbestimmungen für Gesundheitsdaten durchaus spezifisch behandelt werden.

**Technologieentwicklung und Datenschutz**

Zu den Regelungen zum **Verhältnis von Technologieentwicklung** und Datenschutz finden sich hingegen beträchtliche Unterschiede zwischen den verschiedenen Staaten. Im Gemeinschaftsrecht bestehen Sonderreglungen für automatisierte Einzelentscheidungen (Art. 15 Richtlinie 95/46/EG) sowie zur elektronischen Kommunikation (Richtlinie 2002/58/EG). Nach der Richtlinie 2002/58/EG müssen Betreiber eines öffentlich zugänglichen elektronischen Kommunikationsdienstes geeignete technische und organisatorische Massnahmen ergreifen, um die Sicherheit seiner Dienste (inkl. Netzsicherheit) zu gewährleisten (Art. 4). Daneben bestehen restriktive Vorschriften zur Verarbeitung von Verkehrsdaten und deren Speicherung (Verarbeitung und Speicherung nur zur Gebührenabrechnung), sowie detaillierte Vorschriften zur Rufnummernanzeige des Anrufers, Standortdaten, Anrufweiterschaltung, Teilnehmerverzeichnissen und zu unerbetenen Nachrichten. Dabei geht es darum, die jeweiligen Operationen nur mit Zustimmung zu erlauben oder mindestens eine „opting out" zu ermöglichen. Die Umsetzung dieser Vorschriften erfolgte in verschiedenen Staaten im Datenschutzrecht (insbesondere in den UK und in Italien), in anderen Staaten in Spezialgesetzgebung (z.B. in Deutschland im Telekommunikationsgesetz vom 22. Juni 2004, BGBl 2004 Nr. 29, 1109, in Österreich im Telekommunikationsgesetz, BGBl 40/2003; und in Frankreich der *Code des postes et des communications électroniques*, Art. L34-1 ff.), so dass sie in der Analyse nicht eingehend berücksichtigt wurde. Für den vorliegenden Zusammenhang relevanter erscheinen die Staaten, welche im Bereich neuer Technologien über die gemeinschaftsrechtlichen Vorgaben hinausgehen.

Abgesehen von der Umsetzung der gemeinschaftsrechtlichen Vorgaben sehen verschiedene Staaten lediglich vor, dass die Regelungen (oft auf Initiative der Datenschutzinstanz) den technologischen Entwicklungen anzupassen sind, so z.B. in Frankreich und in Holland. In anderen Ländern wird in Bereichen mit technologischer Entwicklung auf Selbstregulierung („Code of Conducts, z.B. in Frankreich und dem Vereinigten Königreich) und / oder auf internationale Entwicklungen (z.B. in Spanien) verwiesen. In anderen Rechtsordnungen finden sich spezifischere Regelungen in bestimmten Bereichen. Im Rahmen des Datenschutzgesetzes finden sich z.B. ausdrückliche Regeln zur Biometrie (Slowenien) oder zur Verwendung mobiler personenbezogener Speicher- und Verarbeitungsmedien (Deutschland). Im Weiteren enthalten das deutsche, österreichische und slowenische Recht Vorschriften für Arten der Videoüberwachung. Nach deutschem Recht ist die **Beobachtung öffentlich zugänglicher Räume** mit optisch-elektronischen Einrichtungen nur dann zulässig, soweit sie zur Aufgabenerfüllung öffentlicher Stellen, zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Nach österreichischem Recht besteht eine Meldepflicht für die systematische, insbesondere fortlaufende Feststellung von Ereignissen, die ein bestimmtes Objekt oder eine bestimmte Person betreffen, durch technische Bildaufnahme- oder Bildübertragungsgeräte. Nach einer neuen Standardanwendung sind Videoüberwachungen in Banken, Juweliergeschäften, Trafiken und Tankstellen von der Meldepflicht ausgenommen, wenn sie sich innerhalb des Standards bewegen (soweit insbesondere die Aufzeichnungsdauer von 72 Stunden nicht überschritten wird). Mit einer Videoüberwachung dürfen jedoch nicht Ereignisse an Orten festgestellt werden, die zum höchstpersönlichen Lebensbereich eines Betroffenen zählen. Im Weiteren ist die Videoüberwachung zum Zweck der Mitarbeiterkontrolle an Arbeitsstätten untersagt. In Slowenien sehen die Vorschriften zur Videoüberwachung eine Hinweispflicht sowie eine erhöhte Sicherheitspflicht im Umgang mit den Daten vor.

Auch ausserhalb Europas hat die Entwicklung neuer Technologien einen Einfluss auf den Datenschutz. Dabei zeigen die zwei untersuchten Rechtsordnungen verschiedenartige Regelungsmuster. In Kanada geht man (wie in Europa, z.B. in Österreich) von der

**Technologieneutralität** der Regelungen des Datenschutzes aus, d.h. von deren Anwendbarkeit unabhängig der Form der Datensammlung und –aufbewahrung. Die technologische Entwicklung wird jedoch aufmerksam verfolgt, und es bestehen verschiedene Arbeitsgruppen und auch konkrete Untersuchungen zur Problematik des Datenschutzes im Zusammenhang mit neuen Technologien. Ein Bereich ist z.B. die Nutzung moderner Technologien zur Sicherung von Daten, ein anderes Beispiel die Untersuchung zur Datenschutzverletzung im Bereich elektronischer sozialer Netzwerke.
In den USA wurden Regelungen in den Staaten von Kalifornien und Massachusetts untersucht. In Massachusets wurde kürzlich ein neues Gesetz erlassen, welches für Datenbearbeitung ein regelrechtes **Informationssicherungsprogramm** verlangt. Dabei muss ein risiko-orientierter Ansatz verfolgt werden. Es bestehen besondere Vorschriften zum Schutz von Computernetzwerken und eine weitgehende Verpflichtung zur Verschlüsselung von elektronisch übermittelten und gespeicherten Informationen. „Privacy by design" wird damit zur allgemeinen Pflicht. In Kalifornien findet sich kein allgemeines Datenschutzgesetz, doch Regeln zu neuen Technologien finden sich einer Vielzahl von Gesetzen. Besondere Aufmerksamkeit widmet der Gesetzgeber dabei der Problematik des „*identity theft*", d.h. der Verwendung einer anderen Identität zu Täuschungszwecken. Neben Strafbestimmungen und Strafverfolgungsmassnahmen ermöglicht die Gesetzgebung den Betroffenen besondere Korrekturmechanismen. Ein anderer Bereich, in welchem eine Vielzahl von Bestimmungen bestehen, ist das Sammeln von Daten mit elektronischen Hilfsmitteln. Dabei wird das Sammeln teils sektorspezifisch (z.B. in der Automobilindustrie), teils eher allgemein (Aufnahmen in Privatsphäre) geregelt. Auch im Informatikbereich und in der Telekommunikation besteht eine Vielzahl sehr spezifischer Vorschriften. Trotz dieser Vielzahl gesetzlicher Grundlage beeinflussen aus unserer Sicht durchwegs ähnliche Grundsätze die Regelungen: das Sammeln und Speichern von Daten ist nur für bestimmte Zwecke oder / und mit dem Einverständnis der betroffenen Person zulässig, was darüber hinaus geht, ist verboten. Oft haben die Betreiber oder die Sammler besondere Hinweispflichten. Schliesslich findet sich vielerorts eine Schadenersatzpflicht.

**Rechte der Betroffenen**

Neben dem bereits erwähnten Informationsrecht, das auf Art. 12 der Richtlinie 95/46/EG zurückgeht, sehen alle Rechtsordnungen weitere, rechtlich durchsetzbare Ansprüche der Betroffenen vor. Diese richten sich in erster Linie an Einzelpersonen, wobei Organisationen zum Schutz der Betroffenen je nach allgemeiner Einstellung der Rechtsordnung zu deren Klageberechtigung durchaus eine Rolle spielen können. Neben der Anrufung in einem juristischen Verfahren hat die Aufsichtsbehörde in allen untersuchten Rechtsordnungen auch die Möglichkeit zum Führen von Untersuchungen auf eigene Initiative oder gestützt auf Hinweise von Drittpersonen.

Nach Art. 12 lit. b der Richtlinie 95/46/EG müssen die Mitgliedstaaten das Recht auf **Berichtigung, Löschung und Sperrung** garantieren. Diese drei Ansprüche sind denn auch weitgehend umgesetzt. Lediglich in Kanada beschränkt sich der Rechtsanspruch auf eine Berichtigung. Das im Schweizerischen Recht vorgesehene Instrument der Vermerkung besteht hingegen nicht in allen Rechtsordnungen, wobei in Deutschland, Grossbritannien, Kanada und Slowenien bestehen ähnliche Möglichkeiten bestehen (Gegendarstellung in Deutschland, Vermerkung im Vereinigten Königreich und in Kanada). Auch ein Recht auf Veröffentlichung oder mindestens Mitteilung ist nicht in allen Rechtsordnungen vorgesehenen. Verschiedene Rechtsordnungen (D, UK, A) sehen hingegen einen spezifischen Schadenersatzanspruch vor (so z.B. in Österreich ausdrücklich für immateriellen Schaden), wobei in den übrigen Rechtsordnungen möglicherweise die allgemeinen Schadenersatzbestimmungen anwendbar sind. Im öffentlichen Bereich bestehen im Wesentlichen dieselben Schutzmechanismen, wobei hier der Schutz bei gewissen Datensammlungen (z.B. im Zusammenhang mit Strafverfolgung) vermindert ist. Als besonderes Instrument ist der im deutschen Recht vorgesehene Anspruch auf Benachrichtigung von Stellen, welche die (unrechtmässig bearbeiteten) Daten erhalten haben zu erwähnen.

**Datenschutzbehörden**

Durch die Datenschutzgesetze werden immer auch die **Kontrollstellen** errichtet, die die Anwendung der von den Mitgliedstaaten zur Umsetzung der EU-Richtlinien erlassenen einzelstaatlichen Gesetze in ihrem Hoheitsgebiet zu überwachen. Diese Stellen nehmen die ihnen zugewiesenen Aufgaben in völliger Unabhängigkeit wahr. Die Ausgestaltung dieser Kontrollstelle ist sehr unterschiedlich. In einigen Staaten handelt es sich um eine Kollegialbehörde (so z.B. in Frankreich, Italien, Österreich, Spanien, Holland), in anderen um eine hierarchisch strukturierte Behörde (Deutschland, Grossbritannien, Kanada, Slowenien), Wahlorgan sind je nach Staat das Parlament, die Exekutive, oder Mischformen (in Frankreich), die Amtsdauer betragen in der Regel mindestens vier Jahre. Die Stellung innerhalb der Verwaltung kann sehr unterschiedlich sein (Parlament in Kanada, Justizministerium im Vereinigten Königreich, in Holland; keine Zuordnung in anderen Staaten), und auch beim Budget finden sich verschiedene Modalitäten, wobei in der Regel das Parlament das letzte Wort hat. Es findet sich somit strukturell kein einheitliches Modell.

Bei den **Funktionen der Behörde** finden sich in allen untersuchten Rechtsordnungen eine Spezialisierung – die Behörde hat in der Regel kaum andere Kompetenzen, ausser allenfalls das Recht auf Information über staatliche Aktivitäten allgemein. Allen Rechtsordnungen gemeinsam ist ebenfalls, dass die Datenschutzbehörde konsultative und informative Funktionen hat und mit weitreichenden Kompetenzen zur Informationsbeschaffung ausgestattet ist. Dies kann bis zur Einvernahme gewisser Personen im Rahmen von Untersuchungen gehen (z.B. in den UK und in Kanada), und die meisten Rechtsordnungen anerkennen der Behörde auch das Recht zur Anordnung von Bussen bei Nichtbefolgung von Informationsanfragen. Speziell zu erwähnen sind in diesem Zusammenhang die „*assessment notice*“ des englischen Rechts, welche weitgehende Auskunftspflichten begründen.

Bei den **Einwirkungsbefugnissen** finden sich wohl am meisten Unterschiede. In den meisten Rechtsordnungen kann die Behörde den Datenbearbeitern direkt bindende Anordnungen zur Datenbearbeitung erlassen (Sperrung, Löschung und Vernichtung von Daten), wenn auch diese Möglichkeit teilweise nur als vorläufige Massnahme bei Dringlichkeit (z.B. in Österreich, Frankreich) vorgesehen ist. In diesen Staaten hat somit die Aufsichtsbehörde eine gewisse Entscheidungsmacht und kann auch bindende Handlungsanweisungen anordnen. In anderen Staaten (Holland, Deutschland, Kanada mit Ausnahmen) sind diese Anordnungen den gerichtlichen Behörden vorbehalten, die Datenschutzbehörde muss sich dann in der Regel auf Handlungsempfehlungen beschränken. Sanktionsmöglichkeiten haben die Aufsichtsbehörde hingegen in allen untersuchten Rechtsordnungen mindestens im Rahmen einer Busse oder eines gerichtlichen Antrags. Einer indirekten Sanktion kommen öffentlich gemachte Berichte oder Berichte an übergeordnete Stellen gleich, welche z.B. in Deutschland, dem Vereinigten Königreich, in Kanada und in Italien vorgesehen sind. Besondere Sanktionsmechanismen finden sich in Deutschland und im Vereinigten Königreich. So kann die deutsche Aufsichtsbehörde über nicht-öffentliche Datenbearbeiter den Datenschutzbeauftragten abberufen. Im Vereinigten Königreich kann die Aufsichtsbehörde bei Eingeständnis einer Verletzung auf ein Strafverfahren verzichten und eine Kaution verlangen – ein Mechanismus, der dem englischen Strafverfahren entspricht. Die Palette an Sanktionsmöglichkeiten ist somit sehr breit.

**Vorschriften für Datenbearbeiter**

Die Anforderungen an die Datenarbeiter entsprechen sich in den Rechtsordnungen insofern, als dass überall eine allgemeine Sorgfalts- und Schutzpflicht besteht, wobei die Vorschriften mehr oder weniger detailliert sind. Die organisatorischen Vorschriften haben besonders in Kanada und in den USA eine besondere Bedeutung und sind oft gesetzlich konkretisiert, wobei sich auch in anderen Rechtsordnungen mehr und mehr eigentliche „Codes de conduite“ entwickeln. Eine freiwillige Zertifizierung (entsprechend Art. 11 DSG) ist hingegen lediglich in Deutschland und Frankreich vorgesehen. Übereinstimmend vorgesehen ist hingegen in allen Rechtsordnungen die Pflicht zur

Meldung von Datensammlungen, welche auch im Gemeinschaftsrecht vorgesehen ist (Art. 18 Richtlinie 1995/46/EG). Die Institution des Datenschutzbeauftragten ist hingegen weniger weit verbreitet und scheint im Vereinigten Königreich, Italien, Österreich und Slowenien nicht vorgesehen. Das Mittel der unaufgeforderten Mitteilung an Betroffene findet sich ebenfalls nur in einigen Rechtsordnungen (Frankreich, Italien, Österreich und Deutschland), und in verschiedener Ausgestaltung (periodische Mitteilung, Mitteilung nur bei Erhebung ohne Kenntnis der Person). Im Weiteren sind die Anforderungen an Datenbearbeiter jedoch hinsichtlich Detaillierungsgrad und Inhalt so unterschiedlich, dass sich ein Vergleich kaum machen lässt. So wird insbesondere auch auf eine Analyse der Delegationskompetenzen und ähnlichen Einzelheiten verzichtet.

**Schlussfolgerung (entspricht allgemeinen Schlussfolgerungen)**

Ein detaillierter Vergleich mit dem schweizerischen Recht ist im Rahmen dieser Analyse nicht möglich. Ganz allgemein scheint jedoch das Schweizerische Recht dem europäischen Standard weitgehend zu entsprechen und teilweise darüber hinauszugehen, insbesondere was die Rechte der Betroffenen sowie die Aktivitäten der Datenschutzbeauftragten betrifft. Keine analogen Regelungen finden sich jedoch (unseres Wissens) im Gebiet der **elektronischen Kommunikation und der modernen Technologien**, wo die Richtlinie 2002/58/EG, das amerikanische Recht sowie deutsche und österreichische Regelungen zur Videoüberwachung allenfalls Beispielscharakter haben könnten. Die weitere Entwicklung lässt zudem weitere Initiativen insbesondere auf dem Gebiet der „social networks“ erwarten.

Auch im Hinblick auf die **Kompetenzen der Aufsichtsbehörde** geht das schweizerische Recht eher weniger weit als andere Rechtsordnungen. Auch wenn sich hier die verschiedenen Rechtsordnungen erheblich unterscheiden ist doch darauf hinzuweisen, dass die Mehrheit von Staaten der Behörde weitreichende Entscheidbefugnisse einräumen. Es bestehen aber auch gewisse Bedenken hinsichtlich (Rechtsstaatlichkeit, Verfahrensgarantien), welche durchaus ernst zu nehmen sind.

# I. SACHVERHALT

## 1. Ausgangslage

Auf eidgenössischer Ebene wird der Datenschutz heute durch das Bundesgesetz über den Datenschutz (Datenschutzgesetz, DSG; SR 235.1) vom 19. Juni 1992, in Kraft seit dem 1. Juli 1993 und geändert mit Revision vom 24. März 2006, in Kraft seit dem 1. Januar 2008, geregelt. Es gilt für das Bearbeiten von Daten natürlicher und juristischer Personen durch Privatpersonen und Bundesorgane.

Das Gesetz wurde geschaffen, weil der Einsatz der modernen Informations- und Kommunikationstechnologien in fast allen Lebensbereichen und die enorme Intensivierung der Datenverarbeitung und -verbreitung in Gesellschaft, Wirtschaft und Staat die Risiken von Persönlichkeitsverletzungen stark anwachsen liessen. Das Privat- und Verwaltungsrecht boten in ihrer damaligen Form keinen ausreichenden Schutz gegen Verletzungen der Persönlichkeit, die auf Informationstätigkeiten beruhten.

Das DSG dient entsprechend dem Persönlichkeitsschutz derjenigen Personen, deren Daten bearbeitet werden (Art. 1 DSG) und damit der Gewährleistung der informationellen Selbstbestimmung (Art. 13 Abs. 2 BV). Konkret bezweckt es in erster Linie den Schutz vor missbräuchlicher Verwendung von Personendaten und die Gewährleistung der Kontrolle über die Verwendung ihrer Daten durch betroffene Personen. Das Gesetz enthält einen allgemeinen Teil, in dem allgemeine Datenbearbeitungsgrundsätze niedergelegt sind, die sowohl für die Organe des Bundes als auch für private Datenbearbeiter gelten. Ferner enthält das Gesetz je spezifische Bestimmungen für die Datenbearbeitung durch Privatpersonen (diesfalls als Ergänzung und Konkretisierung des Persönlichkeitsschutzes des Zivilgesetzbuchs) und für die Datenbearbeitung durch Bundesorgane. Die Datenbearbeitung durch kantonale Behörden ist grundsätzlich nicht Gegenstand des DSG; sie wird durch kantonales Datenschutzrecht geregelt (vorbehältlich Art. 37 DSG).

Das Datenschutzgesetz und seine Anwendung sind neben der Hervorhebung seines Gewinns für die Durchsetzung der Grundrechte immer wieder Gegenstand von Kritik. Wesentliche Kritikpunkte sind etwa die Folgenden:

- DSG als Hindernis für sinnvolle Zusammenarbeit zwischen verschiedenen Verwaltungsstellen und damit für kohärentes Verwaltungshandeln;
- DSG als übermässige Einschränkung wirtschaftlicher Tätigkeiten;
- Hohe administrative Belastung für die Datenbearbeiter im Vergleich zum Nutzen (mangelnde Effizienz);
- Ziel der Datenschutzgesetzgebung werden mit den vom Gesetz vorgesehenen Mechanismen nicht erreicht (mangelnde Wirksamkeit);
- Ausgestaltung einzelner Instrumente ist mit Mängeln behaftet (z.B. Registrierpflicht, Informationspflicht für Auslandübermittlungen);
- Vermehrte Notwendigkeit technologiebezogener Regelungen (z.B. Videoüberwachung) vor dem Hintergrund der Technologieneutralität als Konzept des DSG;
- Unabhängigkeit der Aufsichtsinstanz (EDÖB) nicht gewährleistet;
- Ressourcenmangel verhindert effektive Ausübung der Aufsicht;
- keine wirksamen Durchsetzungsmittel (keine Sanktionen des EDÖB; Zivilverfahren sind zu schwerfällig).

Anlässlich der Schengen-Assoziierung wurde kürzlich im Bereich des Datenschutzes von europäischen Experten der Stand der Umsetzung des Schengen Acquis in der Schweiz evaluiert. Im Rahmen dieser Evaluation wurden namentlich folgende Schlussfolgerungen gezogen:

- Die Datenschutzgesetzgebung ist aufgrund der föderalen Struktur der Schweiz komplex;
- die Unabhängigkeit des EDÖB sollte gestärkt werden;
- der EDÖB sollte über die erforderlichen Ressourcen verfügen.

Kürzlich genehmigte der Bundesrat die Übernahme des Rahmenbeschlusses der EU über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden. Im Moment sind Arbeiten für eine Teilrevision des DSG im Gange, soweit dies für die Umsetzung dieses Beschlusses notwendig ist. Betroffen ist die Datenbekanntgabe im Rahmen der Schengener Zusammenarbeit. Der Revisionsentwurf berücksichtigt ebenfalls die von der EU anlässlich der Evaluation der Schweiz abgegebenen Empfehlungen, wonach die Unabhängigkeit des EDÖB gestärkt werden müsse (insbesondere: die Wahl des EDÖB durch den Bundesrat soll neu der Genehmigung durch das Parlament bedürfen).

Ferner wurden im Jahr 2003 von der Geschäftsprüfungskommission des Nationalrats einzelne Fragen im Zusammenhang mit der Organisation des Datenschutzes innerhalb der Bundesverwaltung und im Jahr 2006 von der Eidgenössischen Finanzkontrolle der Mitteleinsatz des EDÖB für den Datenschutz in der Bundesverwaltung untersucht. Privatim (Vereinigung der schweizerischen Datenschutzbeauftragten) führte kürzlich eine Bevölkerungsumfrage durch, welche die Sensibilisierung der Bevölkerung für datenschutzrechtliche Fragestellungen zum Gegenstand hatte.

Eine Evaluation, bei der auch einzelne Aspekte des DSG betroffen sein werden, ist mit den Arbeiten zur Erfüllung des Po. Lustenberger (07.3682) gegenwärtig im Gange. Das Postulat verlangt die Prüfung, ob der Datenaustausch zwischen Bundes- und Kantonsstellen vereinfacht werden kann. Der Datenschutz soll insbesondere in Bereichen gelockert werden, in denen die Gefahr des Missbrauchs beim Bezug von staatlichen Leistungen am grössten ist: Sozialhilfe, Einbürgerungen, Steuerwesen, Sozialversicherungen. Zu untersuchen wird sein, inwiefern sich die Konzeption des Datenschutzes bewährt oder wo allenfalls Anpassungen nötig sind. Zudem wird das Zusammenspiel allgemeiner Datenschutzregeln und spezialgesetzlicher Vorschriften näher zu prüfen sein. Die Arbeiten werden – begleitet von einer Arbeitsgruppe – durch das BJ, teilweise aber auch durch externe Expertinnen und Experten geführt. Der Evaluationsbericht soll bis Juni 2010 vorliegen. Im Unterschied zur vorliegenden umfassenden Evaluation werden im Rahmen der Arbeiten zur Erfüllung des Po. Lustenberger bloss Teilaspekte des DSG evaluiert.

Schliesslich laufen im Moment diverse Arbeiten zur Umsetzung der Strategie des Bundesrates 2009 im Bereich Informationsgesellschaft Schweiz, und die EU-Kommission führt bis am 31. Dezember 2009 eine Umfrage zur EU-Datenschutzrichtlinie 95/46/EG durch.

## 2. Ziel der Evaluation

Das Datenschutzgesetz ist nunmehr seit über 16 Jahren in Kraft. Eine umfassende Evaluation des Gesetzes steht noch aus. Eine Evaluation scheint angesichts der Vielzahl der vom DSG Betroffenen (insb. sämtliche privaten Datenbearbeiter), der skizzierten Kritik, der Empfehlungen der EU-Experten im Rahmen der Schengen-Assoziierung sowie im Lichte von Art. 170 BV angezeigt. Der gegenwärtige Zeitpunkt ist für eine Evaluation geeignet, da die praktische Anwendung des Gesetzes im Wesentlichen gut eingespielt ist (ausgenommen die im Rahmen der Revision vom 24. März 2006 geänderten und neu geschaffenen Bestimmungen, die allenfalls später separat evaluiert werden können).

Ziel der Evaluation des DSG ist es, verschiedene Teilaspekte des Gesetzes hinsichtlich Effektivität, Wirksamkeit und Effizienz zu überprüfen und gegebenenfalls Vorschläge für Anpassungen (Vollzug und/oder gesetzliche Bestimmungen) zu machen. Angesichts des weiten Geltungsbereichs des DSG und der beschränkten personellen und finanziellen Ressourcen, die für die Evaluation zur Verfügung stehen, ist es unabdingbar, die Evaluation auf bestimmte Teilaspekte des Gesetzes zu fokussieren. Im

Vordergrund stehen dabei die Bekanntheit des Gesetzes und die Durchsetzungsmechanismen einerseits, das Aufsichtsorgan (EDÖB) andererseits.

# 3. Stellung des rechtsvergleichenden Gutachtens im Rahmen der Evaluation

Die Evaluation des Datenschutzgesetzes umfasst eine rechtsvergleichende Dokumentenanalyse, um die Situation in der Schweiz mit der Erfahrung umliegender Länder vergleichen zu können. Das Schweizerische Institut für Rechtsvergleichung wurde in diesem Rahmen mit der Analyse der Situation in zehn Staaten beauftragt. Das Gutachten soll einen Überblick über die Rechtslage in verschiedenartigen Staaten geben.

Neben den vier grösseren Nachbarländern der Schweiz werden das angelsächsische Recht, das spanische Recht, das solowenische Recht als Beispiel einer mittel- und osteuropäischen Rechtsordnung, das holländische Recht als Beispiel einer Rechtsordnung der Benelux Länder, das norwegische Recht als Beispiel einer skandinavischen und einer nicht-EU Rechtsordnung sowie das kanadische Recht als aussereuropäische Rechtsordnung berücksichtigt.

# II. FRAGESTELLUNG

## 1. An welchen Grundsätzen orientiert sich der Datenschutz im betreffenden Land (vgl. Art. 4 DSG)? Welchen Grundsätzen kommt ein besonderes Gewicht zu?

- Rolle der Zweckbindung der Datenbearbeitung
- Grundsätze Datenbearbeitung (Rechtmässigkeit, Treu und Glauben, Verhältnismässigkeit, Sparsamkeit)
- Erkennbarkeit/Transparenz, Einwilligung
- andere?
- Bearbeitung besonders schützenswerten Daten
- Datensicherheit
- Grenzüberschreitende Bekanntgabe
- Auskunftrecht (art. 8 DSG)
- Wie ist das Verhältnis von Technologieentwicklung und Datenschutzrecht geregelt? Ist das Gesetz technologieneutral ausgestaltet oder werden bestimmte Anwendungen explizit thematisiert? Welche technologiebezogenen Regelungen bestehen (z.B. Privacy by design, Automatisierte Einzelentscheidungen, Vorabkontrolle)?
- Y-a-t-il un régime différent pour le traitement effectué par des personnes privées et les traitements effectués par des autorités publiques (administrations) ?

## 2. Welche Durchsetzungsrechte für Betroffene sieht das heranzuziehende Land vor für Datenschutzanliegen? Wie sind diese ausgestaltet, (vgl. DSG Art. 15 Art. 25, Art. 27)?

### 2.1. Bei Datenbearbeitungen durch Private:

a. Sperrung

b. Berichtigung

c. Vernichtung

d. Vermerkung (entsprechend Art. 15 Abs. 2 DSG)

e. Mitteilung und Veröffentlichung

f. Andere?

g. Verfahren (Ausgestaltung, prozessuale Rechte wie Möglichkeit zur Sammelklage, etc.)

h. Abklärung durch den Datenschutzbeauftragten, wenn Dritte melden (kann er abklären? Muss er abklären?)

### 2.2. Bei Datenbearbeitungen durch den Behörden / Verwaltungen:

a. Unterlassung widerrechtlicher Bearbeitung

b. Beseitigung der Folgen widerrechtlicher Bearbeitungen

c. Feststellung der widerrechtlichen Bearbeitung

d. Vermerkung (entsprechend Art. 25 Abs 2 DSG)

e. Sperrung

f. Berichtigung

g. Vernichtung

h. Mitteilung und Veröffentlichung

i. Andere?

j. Verfahren (Ausgestaltung, prozessuale Rechte wie Möglichkeit zur Sammelklage, etc.)

k. Abklärung durch den Datenschutzbeauftragten, wenn Dritte melden (Kann er abklären? Muss er abklären?)

## 3. Ausgestaltung der nationalen Aufsichtsbehörde

### 3.1. Ausgestaltung Behörde (Zusammensetzung: forme de l'autorité – collège ou une personne/einstufig/zweistufig, etc, condition de nomination, fonctionnement, innerhalb/ausserhalb Verwaltung, etc.)

### 3.2. Wie wird die Unabhängigkeit gegenüber Verwaltung und Privatwirtschaft gewährleistet:

a. Wahl: Wahlorgan, Amtszeitregelung (Wiederwahl, unbeschränkt?), weitere Aspekte der Wahl

b. Administrative Zuordnung zu den übrigen nationalen Behörden

c. Gibt es Rechenschaftspflichten gegenüber anderen Behörden? (z.B. Tätigkeitsbericht an die Öffentlichkeit oder eine Behörde?) Haben andere Behörden Weisungsrechte gegenüber der DS-Aufsichtsbehörde?

d. Zuständigkeit und Mitspracherechte der Aufsichtsbehörde für die Zuteilung finanzieller Mittel an die Aufsichtsbehörde

e. Hinweise auf Regelungen über die Höhe der Ressourcen?

f. Weitere Aspekte der Unabhängigkeit

### 3.3. Zuständigkeitsbereich, insbesondere:

a. Zuständig für Bearbeitungen durch Private? Durch Behörden? Durch Behörden anderer Verwaltungseinheiten?

b. Zuständig nur für Datenschutz, oder auch für andere Aufgaben, z.B. Öffentlichkeitsprinzip, Informationsschutz?

c. Gibt es im betreffenden Land andere Datenschutzaufsichtsorgane (wie z.B. in der Schweiz in den Kantonen und den Gemeinden). Wie sind in diesem Fall die Kompetenzen abgegrenzt?

### 3.4. Aufgaben und Kompetenzen:

a. Beratung

b. Aufsicht I: Untersuchungsbefugnisse / Abklärungsrechte / Mittel der Informationsbeschaffung: Besuchsrecht/Inspektion, Recht auf Zugang zu Daten, Recht auf Einholung aller für die Erfüllung des Aufsichtauftrags erforderlichen Informationen, wie Herausgabe von Papieren; Pfändung, Zwangsmöglichkeit, weitere

c. Aufsicht II: Möglichkeiten vorheriger Kontrolle, Behörde als Bewilligungsinstanz bestimmter Bearbeitungen

d. Aufsicht III: Einwirkungsbefugnisse (wie Sperrung, Löschung oder Vernichtung von Daten oder das vorläufige oder endgültige Verbot einer Verarbeitung anzuordnen), Reaktions- und Sanktionsmöglichkeiten bei fehlbarem Verhalten: Handlungsempfehlungen, Handlungsanweisung, Busse aussprechen oder andere Sanktionsmöglichkeiten, Einschlagen des Gerichtswegs, weitere?

e. Information der Öffentlichkeit

f. Weitere Aufgaben und Kompetenzen? (Verfügungsrecht, Klagerecht, Anzeigebefugnis, oder Beschwerderecht)

Mitwirkungspflicht

### 3.5. Hinweise auf weitere Regelungen zur Organisation intern und extern

## 4. Welche Rolle wird den Organisationen zum Schutz der Betroffenen (wie z.B. Konsumenten- oder Patientenschutzorganisationen) zugewiesen?

- Werden diesen bestimmte Kompetenzen oder Rechte eingeräumt (z.B. Verbandsbeschwerde oder ähnliches, können sie subventioniert werden, weitere Kompetenzen oder Rechte)?
- In welcher Form wenden sich die Betroffenen an diese Organisationen?

## 5. Welche Aktivitäten der Datenbearbeiter sind in der Rechtsordnung vorgesehen (private und öffentliche); handelt es sich um „Kann-Vorschriften“ oder um Pflichten (soweit nicht unter 2.1 abgehandelt)?

- Datenschutzzertifizierung
- Meldung von Datensammlungen
- Anerkennung betrieblicher Datenschutzbeauftragter
- Datenbrief (periodische unaufgeforderte Mitteilung über Datenbearbeitungen an Betroffene)
- Selbstregulierung (code de conduite, BCR, …)
- Privacy by design
- weitere?

# III. ANALYSE

## A. ÜBERSICHT

### 1. Grundsätze des Datenschutzes

#### 1.1. Grundsätze 1

| | Datensicherheit | Zweckbindung | Rechtmässigkeit (R), Treu und Glauben (TG), Verhältnismässigkeit (V), Sparsamkeit (S) | Erkennbarkeit / Einwilligung | Auskunftsrecht |
|---|---|---|---|---|---|
| **Deutschland** | Ja | Ja | R, S, V | Ja | Ja |
| **Frankreich** | Ja | Ja | R, TG, V | Ja | Ja |
| **Grossbritannien** | Ja | Ja | R, TG, V, S | Einwilligung;<br>Erkennbarkeit als Grundgedanke, in spezifische Regeln umgesetzt | Ja |
| **Holland** | Ja | Ja | R, TG, V, S | Ja | Ja |
| **Italien** | Ja | Ja | R, V, S | Ja | Ja |
| **Kanada** | Ja | Ja | R, TG, V, S | Ja | Ja |

| | | | | | |
|---|---|---|---|---|---|
| **Österreich** | Ja | Ja | R, TG, V, S | Ja | Ja |
| **Slowenien** | Ja | Ja | Ja | Ja | Ja |
| **Spanien** | Ja | Ja | Ja | Ja | Ja |

## 1.2. Grundsätze 2

| | Unter-schiedliche Vorschriften für private und öffentliche Datenbearbeiter | Besondere Regeln für Bekannt-gabe besonders schützens-werter Daten | Vorschriften für Grenz-überschreitende Bekannt-gabe | Regelung zum Verhältnis zur Technologie-entwicklung |
|---|---|---|---|---|
| **Deutschland** | Ja | Ja | Ja | Ja |
| **Frankreich** | Nein | Ja | Ja | Nein, aber Vorschläge zur Anpassung durch Datenschutzkommission |
| **Grossbritannien** | Nein | Ja | Ja | Sonderregelungen in spezifischen Bereichen (Telemarketing, Internet) |
| **Holland** | Nur im Rechtsweg | Ja | Ja | Ja |
| **Italien** | Ja | Ja | Ja | z.T. Erarbeitung von Code of Conducts und Standards vorgesehen, im Bereich der elekt |

| | | | | |
|---|---|---|---|---|
| **Kanada** | Unterschiedliche gesetzliche Grundlage, ähnlich im Inhalt | Nein | Keine ausdrückliche Regelung, aber Verantwortlichkeit bei Weitergabe mit anderem Schutzniveau | Technologieneutral, aber Regelungen insbesondere zu elektronischen Dokumenten |
| **Österreich** | Gewisse Vorschriften auf private oder öffentliche Verwendungszwecke ausgerichtet | Ja | Ja | Technologieneutral, aber Sonderregeln in spezifischen Bereichen (Videoüberwachung) |
| **Slowenien** | Nur in Bewilligungssfragen | Ja | Ja | Ja |
| **Spanien** | Materiell ähnlich, aber öffentliche Datenbearbeiter haben gewisse Verweigerungsrechte (Zugang, Änderung); Sondervorschriften zum verwaltungsinternen Datenaustausch | Ja | Ja | Nein |

## 2. Durchsetzungsrechte

### 2.1. Verfahren

| | Rechtansprüche bei Datenschutzanliegen | Möglichkeit zur Sammelklage | Möglichkeit der Abklärung durch den Datenschutzbeauftragten bei Hinweisen von Dritten |
|---|---|---|---|
| **Deutschland** | Ja | Nein, aber ggf. Möglichkeit für Verbraucherschutzvereine, aus Unterlassungsklagengesetz zu klagen | Nach freiem Ermessen |

| | | | |
|---|---|---|---|
| **Frankreich** | Ja | Nein | Ja |
| **Grossbritannien** | Ja | Nicht audrücklich im Datenschutzgesetz vorgesehen | Ja |
| **Holland** | Ja | Nicht ausdrücklich im Datenschutzgesetz vorgesehen | Ja |
| **Italien** | Ja | Nicht vorgesehen | Ja |
| **Kanada** | Ja | Kein spezifischer Mechanismus, grundsätzlich möglich | Ja |
| **Österreich** | Ja | Nicht explizit im DS geregelt ; grundsätzlich nicht unmöglich | Ja (allgemeine Kontrollbefugnis auch ausserhalb des Beschwerde- und Ombudsmannverfahrens) |
| **Slowenien** | Ja | Nicht vorgesehen | Ja |
| **Spanien** | Ja | Nicht ausdrücklich vorgesehen | Ja |

## 2.2. Rechte bei Datenbearbeitung durch Private

| | Sperrung | Berichtigung | Vernichtung | Vermerkung | Mitteilung und Veröffentlichung | Andere |
|---|---|---|---|---|---|---|
| **Deutschland** | Ja | Ja | Ja | Gegendarstellung | Benachrichtigung der Stellen, an die die Daten weitergegeben wurden | Schadensersatz, Widerspruch gegen Verwendung |

| | | | | | | |
|---|---|---|---|---|---|---|
| **Frankreich** | Ja | Ja | Ja | Nein | Ja | n/a |
| **Grossbritannien** | Ja | Ja | Ja | Ja | Nicht audrück-lich im Daten-schutzge-setz vorge-sehen | Schadensersatz<br>Verbot zur Entscheidung aufgrund automatisierter Datenbearbeitung<br>Datenbearbeitungs verbot<br>Verbot zur Verwendung zu Marketingzwecken |
| **Holland** | Ja | Ja | Ja | Nein | Ja | n/a |
| **Italien** | Ja | Ja | Ja | Nein | Ja | n/a |
| **Kanada** | Nein | Ja | Nein | Ja | Ja | |
| **Österreich** | Ja | Ja | Ja | Nein | Nein | Widerspruchsrecht bei Vor-liegen überwiegender-schutzwürdiger Geheimhal-tungsinteressen, Anrufung und Beschwerde der DSK, Schadenersatz für immate-riellen Schaden |
| **Slowenien** | Ja | Ja | Ja | Teilweise ja | Ja | n/a |
| **Spanien** | Ja | Ja | Ja | Nein | Ja | n/a |

## 2.3. Rechte bei Datenbearbeitung durch Behörden

| | Unterlassung (U) / Beseitigung (B) / Feststellung (F) | Sperrung Berichtigung | Vernichtung | Vermerkung | Mitteilung und Veröffentlichung | Andere |
|---|---|---|---|---|---|---|
| **Deutschland** | U (Widerspruch gegen Verwendung) | Ja | Ja | Nein | Benachrichtigung der Stellen, an die die Daten weitergegeben wurden | Schadensersatz |
| **Frankreich** | U, B, F | Ja | Ja | Nein | Ja | n/a |
| **Grossbritannien** | U, B, F | Ja | Ja | Nicht audrücklich im Datenschutzgesetz vorgesehen | | |
| **Holland** | U, B, F | Ja | Ja | Nein | Ja | n/a |
| **Italien** | U, B, F | Ja | Ja | Nein | Ja | |
| **Kanada** | B, F | Ja | Nein | Ja | Ja | Schadenersatz |
| **Österreich** | U, B, F | Ja | Ja | Nein | Aufklärungspflicht | Schadenersatz und Genugtuung, Anrufung und Beschwerde an die DSK |

| | | | | | | |
|---|---|---|---|---|---|---|
| **Slowenien** | Ja | Ja | Ja | Teilweise ja | Ja | n/a |
| **Spanien** | Ja, reduzierter Schutz bei gewissen Datensammlungne (Sicherheit) | Ja | Ja | Nein | Ja | n/a |

# 3. Aufsichtsbehörde

## 3.1. Ausgestaltung

| **Ausgestaltung der Aufsichtsbehörde** | | | | | | |
|---|---|---|---|---|---|---|
| | Zusammensetzung (1 Person, mehrere, hierarchisch) | Wahlorgan | Amtszeitregelung | Administrative Zuordnung zu den übrigen Behörden | Rechenschaftspflichten gegenüber anderen Behörden | Zuteilung finanzieller Mittel an die Aufsichtsbehörde |
| **Deutschland** | Öffentlich :<br>Bundesdatenschutz-beauftragter und ca. 70 Mitarbeiter (hierarchisch) | Öffentlich :<br>Wahl durch Bundestag | Öffentlich :<br>5-jährige Amtszeit, einmalige Wiederwahl möglich | Öffentlich :<br>« beim » Bundesministerium des Inneren, | Öffentlich :<br>nicht weisungsgebunden, aber Rechts- und Dienstaufsicht (Regierung / Bundesministerium des Inneren) | Öffentlich :<br>Bundestag ; keine Mitspracherechte |
| | Nicht-öffentlich :<br>Landesbehörde oder Landesdatenschutz-beauftragter | Nicht-öffentlich :<br>abh. von Ausgestaltung | Nicht-öffentlich :<br>abh. von Ausgestaltung | Nicht-öffentlich :<br>abh. von Ausgestaltung | Nicht-öffentlich :<br>abh. von Ausgestaltung | Nicht-öffentlich :<br>abh. von Ausgestaltung |

| | | | | | | |
|---|---|---|---|---|---|---|
| **Frankreich** | 17 Personen, kollegial | 12 gewählte : je 2 durch Senat, Assemblée nationale, Assemblée générale du Conseil économique, social et environnemental, Cour de cassation, Conseil des Etats, Cour de Compte ; 5 ernannte Mitglieder (Dekret, Präsidenten der Assemblée nationale und des Senats) | 5 Jahre, einmal erneuerbar | Unabhängig und weisungsfrei | Jahresberichte an den Präsidenten, Premierminister und das Parlament, weisungsfrei | Aufrechnung auf Staatsaufhalt (Teil im Budget des Premierministers) |
| **Grossbritannien** | Information Commissioner und Information Commissioner's Office (hierarchisch) | Königin | Maximal fünf Jahre mit Verlängerungsmöglichkeit, dritte Amtsezeit nur unter besonderen Bedinungen | Justizministerium | Berichtet dem Parlament, nicht weisungsgebunden | Mittel werden vom Parlament bestimmt |

| | | | | | | |
|---|---|---|---|---|---|---|
| **Holland** | 1 Vorsteher und 2 weitere Mitglieder, Advisory board, Sekretariat | Ernennung durch „Royal decree“ auf Vorschlag des Justizministeriums | Ja. Vorsitzender auf 6 Jahre, Mitglieder auf 4 Jahre. Wiederwahl möglich | Ja, dem Justizministerium | Ja (Jahresberichte an das Justizministerium) | Zuteilung finanzieller Mittel durch das Justizministerium. |
| **Italien** | 4 Mitglieder (Kollegial) | Je 2 durch den Senat und durch die Abgeordnetenkammer | 4 Jahre<br>Einmalige Wiederwahl möglich | Keine Zuordnung, Koordinationspflicht. | Nein | Finanzministerium, dazu eigene Mittel. |
| **Kanada** | Hierarchisch (1 Commissioner) und Sekretariat | Parlament | 2 – 7 Jahre (je nach Staat) | z.T. Parlament, z.T. Ministerium | Parlament | z.T. Parlament, z.T. Ministerium (je nach Staat) |
| **Österreich** | unabhängige Kollegialbehörde mit gerichtsähnlicher Organisation; 6 Mitglieder | Wahl vom Bundespräsidenten auf Vorschlag der Bundesregierung | Fünf Jahre; Wiederbestellungen sind zulässig | Unabhängig und weisungsfrei | spätestens alle zwei Jahre Berichtserstellung über die Tätigkeit und Veröffentlichung | Im Budget des Bundeskanzleramtes ist ein Posten für die Datenschutzkommission vorgesehen. Das Budget des Bundeskanzleramtes wird vom Parlament beschlossen. |

| | | | | | | |
|---|---|---|---|---|---|---|
| **Slowenien** | Information Kommmisioner hierarchisch organisiert | Gewählt durch Parlament | Fünf Jahre, Wiederwahl möglich | Nein | Jahresbericht über die Tätigkeit ans Parlament, sonst kein Rechenschaftspflicht | Direkte Anschliessung an Staatsetat |
| **Spanien** | 1 Konsultativrat mit einem Direktor, Verwaltungsorgan | Regierung, mit Vorschlagsrechten / Vertretung des Parlaments (je 1 pro Kommer), des Justizministeriums, der Regionen und verschiedener anderer Organe (Universitäten, Konsumentenschutzorganisation, Handelskammer) | 4 Jahre | Nein | Jahresbericht an das Justizministerium, Mitteilung der Entscheidungen an den Ombudsman (Defensor del Pueblo) | Antrag an Regierung, Integration Staatsbudget |

## 3.2. Zuständigkeitsbereich und Kompetenzen

### 3.2.1. Zuständigkeit und Kompetenzen

| | Zuständig für private und öffentliche Datenbearbeiter? | Zuständig nur für Datenschutz? | Andere Datenschutz-aufsichtsorgane - Abgrenzung der Kompetenzen | Möglichkeit der Beratung<br>(wer beraten werden kann) | Möglich-keiten vorheriger Kontrolle | Information der Öffentlichkeit | Weitere Aufgaben und Kompetenzen |
|---|---|---|---|---|---|---|---|
| **Deutschland** | Öffentlich :<br>öffentliche Datenbearbeiter | Öffentlich :<br>Nein | Öffentlich : Landes-daten-schutzbeauf-tragte: Länderebene | Öffentlich:<br>Bundesdatenschutz-beauftragter: Bundesregierung, öffentliche Stellen des Bundes<br>Landesdatenschutz-beauftragter:<br>öffentliche Stellen der Länder | Ja | Ja | n/a |
| | Nicht-öffentlich :<br>private Datenbearbeiter | Nicht-öffentlich :<br>abh. von Ausgestaltung | Nicht-öffentlich :<br>Bundesdaten-schutzbeauftragter, abh. von Ausgestal-tung Landesdaten-schutzbeauftragte | Nicht-öffentlich:<br>betriebliche Beauftragte für Datenschutz und für die Datenver-arbeitung verant-wortliche Stellen | Ja | Ja | n/a |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Frankreich** | Ja | Ja | Keine | Oui. La CNIL peut être consultée par toute personne ou tout organisme public ou privé. | Ja | Ja | Ja |
| **Gross-britannien** | Ja | Auch andere Aufgaben | Keine | Ja. Individual members of the public, organisations and other government offices can request information and advice. | Ja | Ja | Ja |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Holland** | Ja | Ja | Keine | Ja. Citizens, customers, clients, employees, in short all persons in question whose personal data are being processed, can contact a data protection officer or the Data Protection Authority for information. The Dutch Data Protection Authority can also be asked to advice on proposals of law of decrees concerning data protection by the Dutch government. | Ja | Ja | Ja |
| **Italien** | Ja | Ja | Keine | Ja.<br>Giving opinion whenever required. | Ja | Ja | Ja |
| **Kanada** | Verschiedene Organe, zudem verschiedene Organa auf Landes und Provinzebene | Ja (im weiteren Sinn: inkl. Schutz der Privatsphäre) | Gemäss Kompetenz-verteilung im Bundes-staat (sachlich, territorrial) | Ja, öffentliche und private Datenbear-beiter | Nein | Ja | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Österreich** | Ja | Hauptsächlich | Nein (Datenschutzrat berät lediglich DSK) | Jedermann kann sich an die DSK mit Anfragen wenden. | Ja | Ja | Ja |
| **Slowenien** | Ja | Nein | Nein | Beratung als solches im Gesetz nicht vorgesehen, die Regelung schliesst aber nicht Beratung von allen Interesanten. | Ja | Ja | Ja |
| **Spanien** | Ja | Ja | Nein | Ja. Dans le cadre des fonctions de diffusion et information attribuées à l'AEPD, l'art. 37.1.e) de la LEPD dispose, en sens large, que l'AEPD "donnera aux **personnes** des renseignements sur leurs droits en matière de protection de données". | Ja. Les inspecteurs disposent de larges compétences leur permettant de collecter « toute information nécessaire pour accomplir leur tâche) | Ja | n/a |

### 3.2.2. Mittel der Informationsbeschaffung

| | Besuchrecht/ Inspektion | Recht auf Zugang zu Daten | Recht auf Einholung der Informationen | Recht auf Herausgabe | Pfändung | Zwangsmöglich-keit | Weitere |
|---|---|---|---|---|---|---|---|
| **Deutsch-land** | Öffentlich :<br>Ja | Öffentlich :<br>Ja | Öffentlich :<br>Ja | Öffentlich :<br>Nicht ausdrücklich geregelt | Öffentlich :<br>Nein | Öffentlich :<br>Nein | Öffentlich :<br>Mehrtätige Prüfung („Betriebs-prüfung“) |
| | Nicht-öffentlich :<br>Ja | Nicht-öffentlich :<br>Ja (Einsichts-recht) | Nicht-öffentlich :<br>Ja | Nicht-öffentlich :<br>nicht geregelt | Nicht-öffentlich :<br>Nein | Nicht-öffentlich :<br>Im Wege des Verwaltungs-zwangs nach Landesgesetz-gebung: Zwangsgeld, Ersatzvornahme, unmittelbarer Zwang | Nicht-öffentlich :<br>Nein |
| **Frankreich** | Ja, vorherige Information des Staatsanwalts nötig | Ja | Ja | Herausgabe von Kopien | Non | Busse ; andere Möglichkeiten nur durch Einschalten einer gerichtlichen Behöre | Administra-tive Sanktionen |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Gross-britannien** | Ja (assessment notice sowie gerichtlich angeordnete Durchsuchung) | Ja (assessment notice oder gerichtlich angeordnet) | Ja (information notice und assessment notice) | Ja (gerichtliche Anordnung nötig) | Ja (gerichtliche Anordnung nötig) | Durch gerichtlichen Zwang | Recht zur "Einvernahme" gewisser Personen im Rahmen der "assessment notice" |
| **Holland** | Ja | Nach allgemeinem Verwaltungsrecht. | Nach allgemeinem Verwaltungsrecht | Nach allgemeinem Verwaltungsrecht | Nein | Busse nur bei Fehlender Information | Keine |
| **Italien** | Ja (Art. 158 PDPC) | Ja. | Ja. | Ja. | Nicht vorgesehen. | Busse und Publikation der Entscheidung in der Zeitung, z.T. Freiheitsstrafe | Keine |
| **Kanada** | Ja | Ja | Ja | Ja | Ja | Nicht ausdrücklich | Anhörung von Auskunftsperfonen, Zeugeneinvernahme;<br>Zeugisverweigerungsrecht unterschiedlich |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Österreich** | Ja (§ 30 Abs. 4 DSG) | Ja (§ 30 Abs. 2 DSG) | Ja (§ 30 Abs. 2 DSG) | Ja (§ 30 Abs. 2 DSG) | Nicht ausdrücklich geregelt (siehe weitere: Anspruch auf Kopien) | Nein<br>(aus verfassungs-rechtlichen Gründen; Weigerung hat auch keine eigene strafrechtl. Sanktionen; aber in der Praxis kooperieren fast alle Auftraggeber, um die Anschuldigungen zu entkräften) | Recht auf Erstellung von Kopien von Daten und Anwendungen ; Recht auf Unterstützung durch Datenverarbeiter |
| **Slowenien** | Ja (Art. 53 PDPA) | Ja. | Ja. | Ja. | Nein. | Nicht vorgesehen. | Keine. |
| **Spanien** | Oui | Oui | Oui | Oui | Non | Oui, dans les cas d'infractions graves. | Immobilisa-tion (art. 49 LEPD et art. 121 du Décret royal 1720/2007, du 21 décembre 2007).) |

### 3.2.3. Einwirkungsbefugnisse der Aufsichtsbehörde

| | Einwirkungsbefugnisse | | | | Reaktions- und Sanktionsmöglichkeiten bei fehlbarem Verhalten | | | |
|---|---|---|---|---|---|---|---|---|
| | Sperrung von Daten | Löschung von Daten | Vernichtung von Daten | Vorläufiges oder endgültiges Verbot einer Verarbeitung | Handlungsempfehlungen und Handlungsanweisung | Einschlagen des Gerichtswegs | Busse | Weitere |
| **Deutschland** | Öffentlich:<br>Nein (gerichtliche Anordnung auf Antrag der Betroffenen) | Öffentlich:<br>Nein (gerichtliche Anordnung auf Antrag der Betroffenen) | Öff.:<br>Nein | Öffentlich:<br>Nein (gerichtliche Anordnung auf Antrag der Betroffenen) | Öffentlich:<br>Vorschläge zur Verbesserung | Öffentlich:<br>Strafrechtliche Anzeige bei Vorsatz möglich | Öffentlich:<br>Ja | Öffentlich:<br>Beanstandung bei übergeordneter Stelle; Empfehlung an die Bundesregierung; Aufnahme in Tätigkeitsbericht |
| | Nicht-öffentlich:<br>Nein (gerichtliche Anordnung auf Antrag der Betroffenen) | Nicht-öffentlich:<br>Nein (gerichtliche Anordnung auf Antrag der Betroffenen) | Nicht-öff.:<br>Nein (gerichtliche Anordnung auf Antrag der Betrof- | Nicht-öffentlich:<br>Ja | Nicht-öffentlich:<br>Anordnung von Massnahmen zur Beseitigung einer Verletzung | Nicht-öffentlich:<br>Strafrechtliche Anzeige möglich | Nicht-öffentlich:<br>Ja | Nicht-öffentlich:<br>Information der betroffenen Personen und der Gewerbeaufsichtsbehörde |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | fenen) | | | | | Abberufung des Daten-schutzbe-auftragten |
| **Frankreich** | Ja, bei Drin-glichkeit (3 Monate) | Oui, même si ce n'est pas exprés-sement prévu par la loi | Oui, même si ce n'est pas exprésse-ment prévu par la loi | Oui | Oui | Strafanzeige und direktes Einschlagen des Gerichtswegs | Oui | Verwarnung |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Gross-britannien** | Ja (Enforcement Notice) | Ja (Enforcement Notice) | Ja (Enforcement Notice) | May be possible although not specifically authorised by the relevant legislation | Ja : issue **undertakings** committing an authority to a particular course of action to improve its compliance;<br>•issue **practice recommendations** specifying steps the public authority should take to ensure conformity to the codes; | Ja<br>(Alternative : Kaution bei Eingeständnis des Verstosses) | Ja | •issue **decision notices** detailing the outcome of the ICO's investigation to publically highlight particular issues with an authority's handling of a specific request;<br>•report to Parliament on freedom of information issues of concern |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Holland** | Nein. Only the court can, upon request of the data subject, order blocking the data. | Nein. The Dutch Only the court can, upon request of the data subject, order eradication of data | Nein. Only the court can, upon request of the data subject, order destruction of data. | Nein. Only the court can, upon request of the data subject, prohibit processing of data. | Im Rahmen eines Untersuchungsberichts | Ja | Ja | Information der Betroffenen |
| **Italien** | Ja | Ja | Ja | Ja | Ja | Ja | Ja | Publikation in Zeitungen<br>Bericht an Parlement und Regierung. |
| **Kanada** | Im Rahmen der Handlungsanweisungen in gewissen Provinzen möglich | Im Rahmen der Handlungsanweisungen in gewissen Provinzen möglich) | Im Rahmen der Handlungsanweisungen in gewissen Provinzen möglich | Im Rahmen der Handlungsanweisungen in gewissen Provinzen möglich | Ja (Verbindlichkeit je nach Provinz unterschiedlich) | Ja | In Alberta und Britisch Columbia | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Österreich** | Ja, bei Gefahr im Verzug durch Bescheid (§ 30 Abs. 6a DSG) | Ja, gegen öffentliche Datenan-wender (§ 40 Abs. 4 DSG) | Ja, gegen öffentliche Datenan-wender (§ 40 Abs. 4 DSG) | Ja, bei Gefahr im Verzug durch Bescheid (§ 30 Abs. 6a DSG) | Ja (§ 30 Abs. 6 DSG) | DSK kann in schwerwiegen-den Fällen eine Feststellungs-klage vor Zivil-gericht erheben (§ 32 Abs. 5 DSG) | Nein | Soweit ersichtlich nein |
| **Slowenien** | Ja (Art. 54 PDPA) | Ja | Ja | Ja | Ja | Ja | Ja | Prohibition of the transfer of PD to third countries |
| **Spanien** | Oui | Oui | Oui | Oui | Oui | Oui | Oui | Non |

## 4. Rolle der Organisationen zum Schutz der Betroffenen

| | Kompetenzen | Anrufung durch Betroffene |
|---|---|---|
| **Deutschland** | Verbraucherschutzvereine: ggf. Möglichkeit für Unterlas-sungsklage nach Unterlassungsklagengesetz | n/a |
| **Frankreich** | Verbraucherschutzvereine | Pas de forme spécifique |
| **Grossbritannien** | n/a | n/a |
| **Holland** | n/a | n/a |
| **Italien** | n/a | n/a |
| **Kanada** | Allgemeine Klagekompetenz | Keine spezifische Form |
| **Österreich** | Keine spezifischen Kompetenzen | Keine spezifische Form |
| **Slowenien** | n/a | n/a |

| | | |
|---|---|---|
| **Spanien** | Keine spezifischen Kompetenzen | n/a |

## 5. Aktivitäten der privaten und öffentlichen Datenbearbeitern

| | Datenschutz-zertifizierung | Meldung von Datensammlun-gen | Anerkennung / Ernennung eines betrieblichen Datenschutz-beauftragten | Periodische unaufge-forderte Mitteilung über Datenbearbei-tungen an Betroffene | Code de conduite | Weitere vorgesehene Aktivitäten |
|---|---|---|---|---|---|---|
| **Deutschland** | Vorgesehen, aber noch nicht umgesetzt | Ja | Ja | Nein | n/a | Pflicht zur Benachrichtigung des Betroffenen, wenn ihn betreffende Daten ohne seine Kenntnis erhoben werden |
| **Frankreich** | Ja | Ja | Ja | Ja | Ja | |
| **Gross-britan-nien** | Nein | Nur Mitteilung einer Beschreibung der durchgefürten Datenverarbeitung | Nein | Nein | Ja | Keine |
| **Holland** | Nein | Ja | Ja | Nein | Ja | |
| **Italien** | Nein | Ja | Nein | Ja | Ja | |
| **Kanada** | Nein | Nein | Ja | Nein | Ja | |

| | | | | | | |
|---|---|---|---|---|---|---|
| **Österreich** | Ja | Ja | Nein | Ja | Keine Angaben | Pflichten des Dienstleisters: Daten nur im Rahmen des Auftrages verwenden ; Subkontrahierungsverbot ; Schaffung technischer Voraussetzungen für die überprüfungsmassnahmen ; Herausgabe-, Aufbewahrungs- und Vernichtungspflichten ; Informationspflichten (alle § 11 DSG) ; Pflichten des Auftraggebers: Informationspflicht an Betroffene (§ 24 DSG); besondere Informationspflicht bei unrechtsmässiger Datenverwendung (§ 24 ABs. 2a DSG); Pflicht zur Offenlegung der Identität des Auftraggebers (§ 25 DSG) |
| **Slowenien** | Nein | Ja | Nein | Nein | Betriebsintern | Special obligation concerning sectoral arrangements |
| **Spanien** | Nein | Ja | Ja | Nein | Vorgesehen | n/a |

# B. LÄNDERBERICHTE

## 1. Deutschland

### 1.1. Grundsätze des Datenschutzes

Der Datenschutz ist in Deutschland auf Bundesebene im Bundesdatenschutzgesetz[6] (BDSG) geregelt. Daneben existieren regionale Regelungen auf Länderebene (Landesdatenschutzgesetze).

#### 1.1.1. Rolle der Zweckbindung der Datenbearbeitung

Der Grundsatz der **Zweckbindung** der Datenbearbeitung gilt sowohl für die Datenbearbeitung durch öffentliche als auch durch nicht-öffentliche Stellen. Allerdings variieren die Anforderungen der Zweckbindung je nachdem, ob es sich um eine öffentliche oder eine nicht-öffentliche Stelle handelt.

**- Öffentliche Stellen -**

Nach § 14 Abs. 1 des Bundesdatenschutzgesetzes ist das Speichern, Verändern oder Nutzen personenbezogener Daten nur zulässig, wenn es zur Erfüllung der in der Zuständigkeit der verantwortlichen Stelle liegenden Aufgaben erforderlich ist und es für die **Zwecke** erfolgt, für die die Daten erhoben worden sind. Das Speichern, Verändern oder Nutzen personenbezogener Daten für **andere Zwecke** ist nach § 14 Abs. 2 BDSG nur zulässig, wenn:

- eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt,
- der Betroffene eingewilligt hat,
- offensichtlich ist, dass es im Interesse des Betroffenen liegt, und kein Grund zu der Annahme besteht, dass er in Kenntnis des anderen Zwecks seine Einwilligung verweigern würde,
- Angaben des Betroffenen überprüft werden müssen, weil tatsächliche Anhaltspunkte für deren Unrichtigkeit bestehen,
- die Daten allgemein zugänglich sind oder die verantwortliche Stelle sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Zweckänderung offensichtlich überwiegt,
- es zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer Gefahr für die öffentliche Sicherheit oder zur Wahrung erheblicher Belange des Gemeinwohls erforderlich ist,
- es zur Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Vollstreckung oder zum Vollzug von Strafen oder Massnahmen im Sinne des § 11 Abs. 1 Nr. 8 des Strafgesetzbuchs[7] oder von Erziehungsmassregeln oder Zuchtmitteln im Sinne des Jugendgerichtsgesetzes oder zur Vollstreckung von Bussgeldentscheidungen erforderlich ist,
- es zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person erforderlich ist oder
- es zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Zweckänderung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismässigem Aufwand erreicht werden kann.

---

6 Bundesdatenschutzgesetz (BDSG) in der Fassung der Bekanntmachung vom 14. 01.2003 (BGBl. I 2003 S. 66), zuletzt geändert durch Artikel 1 des Gesetzes vom 14.08.2009 (BGBl. I 2009, S. 2814).

7 Massregeln der Sicherung und Besserung, Verfall, Einziehung und Unbrauchbarmachung.

Personenbezogene Daten, die ausschliesslich zu Zwecken der **Datenschutzkontrolle**, der **Datensicherung** oder zur Sicherstellung eines **ordnungsgemässen Betriebes** einer Datenverarbeitungsanlage gespeichert werden, dürfen nur für diese Zwecke verwendet werden, § 14 Abs. 4 BDSG.

**- Nicht-öffentliche Stellen -**

Die **Erhebung, Speicherung, Veränderung oder Übermittlung** personenbezogener Daten oder ihre Nutzung als Mittel durch nicht-öffentliche Stellen für die Erfüllung eigener Geschäftszwecke ist nach § 28 Abs. 1 S. 1 BDSG zulässig:

- wenn es für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist,
- soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt, oder
- wenn die Daten allgemein zugänglich sind oder die verantwortliche Stelle sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung gegenüber dem berechtigten Interesse der verantwortlichen Stelle offensichtlich überwiegt.

Bei der Erhebung der Daten sind die **Zwecke**, für die sie verarbeitet oder genutzt werden sollen, **konkret festzulegen**, § 28 Abs. 1 S. 2 BDSG. Die Übermittlung oder Nutzung für einen **anderen Zweck** ist nach § 28 Abs. 2 BDSG zulässig, wenn:

- dies nach den oben genannten Voraussetzungen erlaubt ist
- soweit es zur
    - Wahrung berechtigter Interessen eines Dritten oder
    - zur Abwehr öffentlicher Gefahren für die staatliche oder öffentliche Sicherheit oder zur Verfolgung von Straftaten

  erforderlich ist und kein Grund zur Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung oder Nutzung hat, oder
- wenn es im Interesse einer Forschungseinrichtung zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Zweckänderung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismässigem Aufwand erreicht werden kann.

Sollen die Daten für Zwecke des **Adresshandels** oder der **Werbung** verarbeitet oder genutzt werden, so ist dies nur zulässig, soweit der Betroffene eingewilligt hat und im Falle einer nicht schriftlich erteilten Einwilligung die verantwortliche Stelle dem Betroffenen den Inhalt der Erklärung schriftlich bestätigt (ausser bei elektronischer Erklärung), § 28 Abs. 3 S. 1, 3a BDSG. Darüber hinaus ist die Verarbeitung oder Nutzung personenbezogener Daten nach § 28 Abs. 3 S. 2 BDSG zulässig, soweit es sich um **listenmässig** oder sonst zusammengefasste Daten über Angehörige einer Personengruppe handelt, die sich auf die Zugehörigkeit des Betroffenen zu dieser Personengruppe, seine Berufs-, Branchen- oder Geschäftsbezeichnung, seinen Namen, Titel, akademischen Grad, seine Anschrift und sein Geburtsjahr beschränken, und die Verarbeitung oder Nutzung erforderlich ist

- für Zwecke der Werbung für eigene Angebote der verantwortlichen Stelle, die diese Daten mit Ausnahme der Angaben zur Gruppenzugehörigkeit beim Betroffenen § 28 Abs. 1 S. 1 Ziff. 1 BDSG[8] oder aus allgemein zugänglichen Adress-, Rufnummern-, Branchen oder vergleichbaren Verzeichnissen erhoben hat,
- für Zwecke der Werbung im Hinblick auf die berufliche Tätigkeit des Betroffenen und unter seiner beruflichen Anschrift oder
- für Zwecke der Werbung für Spenden, die nach § 10b Absatz 1 und § 34g des Einkommensteuergesetzes steuerbegünstigt sind.

**Dritte**, denen diese Daten übermittelt werden, dürfen diese nur für den Zweck verwenden, zu dessen Erfüllung die Daten übermittelt wurden, es sei denn, die oben genannten Voraussetzungen liegen vor, § 28 Abs. 5 BDSG.

Das **geschäftsmässige** Erheben, Speichern, Verändern oder Nutzen personenbezogener Daten zum **Zweck der Übermittlung**, insbesondere wenn dies der **Werbung**, der Tätigkeit von Auskunfteien oder dem Adresshandel dient, ist nach § 29 Abs. 1 BDSG zulässig, wenn:

- kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Erhebung, Speicherung oder Veränderung hat,
- die Daten aus allgemein zugänglichen Quellen entnommen werden können oder die verantwortliche Stelle sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Erhebung, Speicherung oder Veränderung offensichtlich überwiegt, oder
- die Voraussetzungen des § 28a Abs. 1 oder Abs. 2 BDSG erfüllt sind[9]; Daten im Sinne von § 28a Abs. 2 S. 4 BDSG dürfen nicht erhoben oder gespeichert werden.

---

[8] Datenerhebung, die für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist.

[9] **§ 28a Datenübermittlung an Auskunfteien**

(1) [1]Die Übermittlung personenbezogener Daten über eine Forderung an Auskunfteien ist nur zulässig, soweit die geschuldete Leistung trotz Fälligkeit nicht erbracht worden ist, die Übermittlung zur Wahrung berechtigter Interessen der verantwortlichen Stelle oder eines Dritten erforderlich ist und

1. die Forderung durch ein rechtskräftiges oder für vorläufig vollstreckbar erklärtes Urteil festgestellt worden ist oder ein Schuldtitel nach § 794 der Zivilprozessordnung vorliegt,
2. die Forderung nach § 178 der Insolvenzordnung festgestellt und nicht vom Schuldner im Prüfungstermin bestritten worden ist,
3. der Betroffene die Forderung ausdrücklich anerkannt hat,
4. a) der Betroffene nach Eintritt der Fälligkeit der Forderung mindestens zweimal schriftlich gemahnt worden ist,

b) zwischen der ersten Mahnung und der Übermittlung mindestens vier Wochen liegen,

c) die verantwortliche Stelle den Betroffenen rechtzeitig vor der Übermittlung der Angaben, jedoch frühestens bei der ersten Mahnung über die bevorstehende Übermittlung unterrichtet hat und

d) der Betroffene die Forderung nicht bestritten hat oder

5. das der Forderung zugrunde liegende Vertragsverhältnis aufgrund von Zahlungsrückständen fristlos gekündigt werden kann und die verantwortliche Stelle den Betroffenen über die bevorstehende Übermittlung unterrichtet hat.

[2]Satz 1 gilt entsprechend, wenn die verantwortliche Stelle selbst die Daten nach § 29 verwendet.

(2) [1]Zur zukünftigen Übermittlung nach § 29 Abs. 2 dürfen Kreditinstitute personenbezogene Daten über die Begründung, ordnungsgemässe Durchführung und Beendigung eines Vertragsverhältnisses betreffend ein Bankgeschäft nach § 1 Abs. 1 Satz 2 Nr. 2, 8 oder Nr. 9 des Kreditwesengesetzes an Auskunfteien übermitteln, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der

Dabei ist § 28 Absatz 1 Satz 2 und Absatz 3 bis 3b (s.o.) anzuwenden, § 29 Abs. 1 S. 2 BDSG.

Die **Übermittlung** im Rahmen der oben genannten Zwecke nach § 29 Abs. 1 BDSG ist nach § 29 Abs. 2 BDSG zulässig, wenn:

- der Dritte, dem die Daten übermittelt werden, ein berechtigtes Interesse an ihrer Kenntnis glaubhaft dargelegt hat und
- kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat.

§ 28 Absatz 3 bis 3b (s.o.) gilt entsprechend. Für die Verarbeitung oder Nutzung der übermittelten Daten gelten nach § 29 Abs. 4 BDSG die Regelungen des § 28 Abs. 4 (Widerspruch des Betroffenen, s.u.) und 5 BDSG.

Personenbezogene Daten, die ausschliesslich zu Zwecken der **Datenschutzkontrolle**, der **Datensicherung** oder zur Sicherstellung eines **ordnungsgemässen Betriebes** einer Datenverarbeitungsanlage gespeichert werden, dürfen nur für diese Zwecke verwendet werden, § 31 BDSG.

### 1.1.2. Grundsätze Datenbearbeitung

Das BDSG folgt dem Grundsatz des sog. „**Verbotes mit Erlaubnisvorbehalt**“. Demnach sind die Erhebung, Verarbeitung und Nutzung von Daten verboten, es sei denn, dies ist durch das BDSG oder eine andere Rechtsvorschrift ausdrücklich erlaubt oder gestattet (**Rechtmässigkeit**) oder der Betroffene hat seine Einwilligung dazu erklärt, § 4 Abs. 1 S. 1 BDSG. Nach § 3a BDSG gilt der Grundsatz der **Datenvermeidung** und der **Datensparsamkeit**.

Statt der früheren Bestimmung, dass durch nicht-öffentliche Stellen erhobene Daten nach **Treu und Glauben** erhoben werden müssen, gilt nunmehr auch für diese der **gesetzliche Erlaubnisvorbehalt** (gesetzliche Grundlage oder Einwilligung).

Der Grundsatz der **Verhältnismässigkeit** findet im Bundesdatenschutzgesetz selbst keine Erwähnung, ist aber nach der Ansicht des Bundesverfassungsgerichts grundsätzlich zu beachten, wenn der Staat durch Gesetz in das Recht auf informationelle Selbstbestimmung eingreift:

> *„Einschränkungen dieses Rechts auf “informationelle Selbstbestimmung" sind nur im überwiegenden Allgemeininteresse zulässig. Sie bedürfen einer verfassungsgemässen gesetzlichen*

---

Übermittlung gegenüber dem Interesse der Auskunftei an der Kenntnis der Daten offensichtlich überwiegt. [2]Der Betroffene ist vor Abschluss des Vertrages hierüber zu unterrichten. [3]Satz 1 gilt nicht für Giroverträge, die die Einrichtung eines Kontos ohne Überziehungsmöglichkeit zum Gegenstand haben. [4]Zur zukünftigen Übermittlung nach § 29 Abs. 2 ist die Übermittlung von Daten über Verhaltensweisen des Betroffenen, die im Rahmen eines vorvertraglichen Vertrauensverhältnisses der Herstellung von Markttransparenz dienen, an Auskunfteien auch mit Einwilligung des Betroffenen unzulässig.

(3) [1]Nachträgliche Änderungen der einer Übermittlung nach Absatz 1 oder Absatz 2 zugrunde liegenden Tatsachen hat die verantwortliche Stelle der Auskunftei innerhalb von einem Monat nach Kenntniserlangung mitzuteilen, solange die ursprünglich übermittelten Daten bei der Auskunftei gespeichert sind. [2]Die Auskunftei hat die übermittelnde Stelle über die Löschung der ursprünglich übermittelten Daten zu unterrichten.

*Grundlage, die dem rechtsstaatlichen Gebot der Normenklarheit entsprechen muss. Bei seinen Regelungen hat der Gesetzgeber ferner den Grundsatz der **Verhältnismässigkeit** zu beachten."*[10]

### 1.1.3. Erkennbarkeit/Transparenz, Einwilligung

Der Grundsatz der **Erkennbarkeit** gilt für die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen nach § 6b BDSG. Ausserdem gilt der Grundsatz bei dem Einsatz „mobiler personenbezogener Speicher- und Verarbeitungsmedien" wie Chipkarten. Es muss für den Betroffenen eindeutig erkennbar sein, wenn ein Kommunikationsvorgang (z.B. Lesevorgang bei kontaktlosen Chipkarten) auf dem Speichermedium eine Datenverarbeitung auslöst, § 6c Abs. 3 BDSG.

Wie bereits dargestellt, ist die Erhebung, Verarbeitung und Nutzung von Daten nur zulässig, wenn dies ist durch das BDSG oder eine andere Rechtsvorschrift ausdrücklich erlaubt oder gestattet oder der Betroffene hat seine **Einwilligung** dazu erklärt hat, § 4 Abs. 1 S. 1 BDSG. Der Betroffene ist auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung sowie, soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen, auf die Folgen der Verweigerung der Einwilligung hinzuweisen. Die Einwilligung bedarf der Schriftform, sofern nicht aufgrund besonderer Umstände eine andere Form angemessen ist (§ 4a Abs. 1 BDSG). Soweit **besondere Arten personenbezogener Daten** (s.u.) erhoben, verarbeitet oder genutzt werden, muss sich die Einwilligung darüber hinaus ausdrücklich auf diese Daten beziehen (§ 4a Abs. 3 BDSG).

### 1.1.4. Bearbeitung besonders schützenswerter Daten

Das BDSG kennt besondere Vorschriften für sogenannte **besondere Arten personenbezogener Daten**. Dazu gehören nach § 3 Abs. 9 BDSG Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben.

**- Öffentliche Stellen -**

Besondere personenbezogene Daten dürfen nach § 13 Abs. 2 BDSG nur **erhoben** werden, wenn:

1. eine Rechtsvorschrift dies vorsieht oder aus Gründen eines wichtigen öffentlichen Interesses zwingend erfordert,
2. der Betroffene eingewilligt hat,
3. dies zum Schutz lebenswichtiger Interessen des Betroffenen oder eines Dritten erforderlich ist, sofern der Betroffene aus physischen oder rechtlichen Gründen ausserstande ist, seine Einwilligung zu geben,
4. es sich um Daten handelt, die der Betroffene offenkundig öffentlich gemacht hat,
5. dies zur Abwehr einer erheblichen Gefahr für die öffentliche Sicherheit erforderlich ist,
6. dies zur Abwehr erheblicher Nachteile für das Gemeinwohl oder zur Wahrung erheblicher Belange des Gemeinwohls zwingend erforderlich ist,

---

[10] Bundesverfassungsgericht, Urteil vom 15.12.1983, 1 BvR 209/83 u. a., Neue Juristische Wochenschrift 1984, S. 419-428, Leitsatz 2.

7. dies zum Zweck der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder Behandlung oder für die Verwaltung von Gesundheitsdiensten erforderlich ist und die Verarbeitung dieser Daten durch ärztliches Personal oder durch sonstige Personen erfolgt, die einer entsprechenden Geheimhaltungspflicht unterliegen,
8. dies zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Erhebung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismässigem Aufwand erreicht werden kann oder
9. dies aus zwingenden Gründen der Verteidigung oder der Erfüllung über- oder zwischenstaatlicher Verpflichtungen einer öffentlichen Stelle des Bundes auf dem Gebiet der Krisenbewältigung oder Konfliktverhinderung oder für humanitäre Massnahmen erforderlich ist.

Das **Speichern, Verändern oder Nutzen** besonderer Arten personenbezogener Daten für andere Zwecke ist nach § 14 Abs. 5 S. 1 BDSG nur zulässig, wenn:

- die Voraussetzungen vorliegen, die eine Erhebung dieser Daten zulassen würden oder
- dies zur Durchführung wissenschaftlicher Forschung erforderlich ist, das öffentliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Zweckänderung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismässigem Aufwand erreicht werden kann.

Bei der **Abwägung** ist im Rahmen des öffentlichen Interesses das wissenschaftliche Interesse an dem Forschungsvorhaben besonders zu berücksichtigen, § 14 Abs. 5 S. 2 BDSG.

**- Nicht-öffentliche Stellen -**

Das **Erheben, Verarbeiten** und **Nutzen** von besonderen Arten personenbezogener Daten durch nicht-öffentliche Stellen für **eigene Geschäftszwecke** ist nach § 28 Abs. 6 BDSG zulässig, wenn

- der Betroffene eingewilligt hat,
- dies zum Schutz lebenswichtiger Interessen des Betroffenen oder eines Dritten erforderlich ist, sofern der Betroffene aus physischen oder rechtlichen Gründen ausserstande ist, seine Einwilligung zu geben,
- es sich um Daten handelt, die der Betroffene offenkundig öffentlich gemacht hat,
- dies zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung überwiegt, oder
- dies zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Erhebung, Verarbeitung und Nutzung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismässigem Aufwand erreicht werden kann.

Das **Erheben** solcher Daten ist ausserdem nach § 28 Abs. 7 BDSG zulässig, wenn dies zum Zweck der **Gesundheitsvorsorge**, der medizinischen Diagnostik, der Gesundheitsversorgung oder Behandlung oder für die Verwaltung von Gesundheitsdiensten erforderlich ist und die Verarbeitung dieser Daten durch

**ärztliches Personal** oder durch sonstige Personen erfolgt, die einer entsprechenden Geheimhaltungspflicht unterliegen.

Für einen **anderen Zweck** dürfen die besonderen Arten personenbezogener Daten nur unter den oben genannten Voraussetzungen (mit Ausnahme der wissenschaftlichen Forschung) **übermittelt** und **genutzt** werden, § 28 Abs. 8 BDSG. Die Übermittlung und Nutzung ist auch zulässig, wenn dies zur Abwehr von erheblichen Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten von erheblicher Bedeutung erforderlich ist.

**Organisationen**, die politisch, philosophisch, religiös oder gewerkschaftlich ausgerichtet sind und **keinen Erwerbszweck** verfolgen, dürfen besondere Arten personenbezogener Daten ihrer **Mitglieder** oder von Personen, die im Zusammenhang mit deren **Tätigkeitszweck** regelmässig Kontakte mit der Organisation unterhalten erheben, verarbeiten oder nutzen, soweit dies für die Tätigkeit der Organisation erforderlich ist, § 28 Abs. 9 BDSG.

### 1.1.5. Datensicherheit

Nach § 9 BDSG haben öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, die **technischen und organisatorischen Massnahmen** zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind Massnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Dazu erläutert die Anlage zu § 9: Werden personenbezogene Daten **automatisiert verarbeitet** oder **genutzt**, ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Massnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind,

1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (**Zutrittskontrolle**),
2. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (**Zugangskontrolle**),
3. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschliesslich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (**Zugriffskontrolle**),
4. zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (**Weitergabekontrolle**),
5. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (**Eingabekontrolle**),

6. zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (**Auftragskontrolle**),
7. zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (**Verfügbarkeitskontrolle**),
8. zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Eine Massnahme nach den Ziffern 2 bis 4 ist insbesondere die Verwendung von dem Stand der Technik entsprechenden **Verschlüsselungsverfahren**.

Nach § 9a BDSG können zur Verbesserung des **Datenschutzes** und der **Datensicherheit** können Anbieter von Datenverarbeitungssystemen und -programmen und datenverarbeitende Stellen ihr Datenschutzkonzept sowie ihre technischen Einrichtungen durch unabhängige und zugelassene Gutachter **prüfen und bewerten lassen** sowie das Ergebnis der Prüfung veröffentlichen. Die näheren Anforderungen an die Prüfung und Bewertung, das Verfahren sowie die Auswahl und Zulassung der Gutachter sollen durch ein besonderes Gesetz geregelt werden.[11]

### 1.1.6. Grenzüberschreitende Bekanntgabe

Für die **Übermittlung** personenbezogener Daten an Stellen in anderen **EU-Mitgliedstaaten**, in anderen **EWR-Staaten** oder an Organe und Einrichtungen der **Europäischen Gemeinschaften** gelten nach § 4b BDSG die gleichen Vorschriften wie für die Datenübermittlung an deutsche öffentliche (§ 15 Abs. 1 BDSG) und nicht-öffentliche (§ 16 Abs. 1 BDSG) Stellen sowie die Vorschriften für die Datenverarbeitung durch nicht-öffentlicheStellen (§§ 28 - 30a BDSG), soweit die Übermittlung im Rahmen von Tätigkeiten erfolgt, die ganz oder teilweise in den Anwendungsbereich des Rechts der Europäischen Gemeinschaften fallen.

Die Übermittlung an die genannten Stellen, die **ausserhalb** dieser Tätigkeiten erfolgt, sowie **sonstige ausländische** oder **über- oder zwischenstaatliche** Stellen, unterliegt zunächst den gleichen Anforderungen, § 4b Abs. 2 S. 1 BDSG. Sie **unterbleibt** jedoch, soweit der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat, insbesondere wenn bei den genannten Stellen ein angemessenes Datenschutzniveau nicht gewährleistet ist, § 4b Abs. 2 S.2 BDSG.[12]

Die **Angemessenheit des Schutzniveaus** wird unter Berücksichtigung aller Umstände beurteilt, die bei einer Datenübermittlung von Bedeutung sind. Das umfasst **insbesondere** die Art der Daten, die Zweckbestimmung, die Dauer der geplanten Verarbeitung, das Herkunfts- und das Endbestimmungsland, die für den betreffenden Empfänger geltenden Rechtsnormen sowie die für ihn geltenden Standesregeln und Sicherheitsmassnahmen, § 4b Abs. 3 BDSG.

---

[11] Ein solches Gesetz wurde jedoch bislang nicht verabschiedet, vergleiche die Information auf der Homepage des Bundesdatenschutzbeauftragten, online abrufbar unter: http://www.bfdi.bund.de/cln_134/DE/Themen/GrundsaetzlichesZumDatenschutz/Einzelfragen/Artikel/Datenschutzaudit.html (04.08.2010).

[12] Diese Beschränkung gilt nicht, wenn die Übermittlung zur Erfüllung eigener Aufgaben einer öffentlichen Stelle des Bundes aus zwingenden Gründen der Verteidigung oder der Erfüllung über- oder zwischenstaatlicher Verpflichtungen auf dem Gebiet der Krisenbewältigung oder Konfliktverhinderung oder für humanitäre Massnahmen erforderlich ist, § 4b Abs. 2 S. 3 BDSG.

Darüber hinaus ist nach § 4c Abs. 1 BDSG die Übermittlung von Daten im Rahmen von Tätigkeiten, die ganz oder teilweise in den Anwendungsbereich des Rechts der Europäischen Gemeinschaften fallen, an **andere** als die oben genannten **Stellen** zulässig, auch wenn ein angemessenes **Datenschutzniveau nicht gewährleistet** ist, sofern:

1. der Betroffene seine Einwilligung gegeben hat,
2. die Übermittlung für die Erfüllung eines Vertrags zwischen dem Betroffenen und der verantwortlichen Stelle oder zur Durchführung von vorvertraglichen Massnahmen, die auf Veranlassung des Betroffenen getroffen worden sind, erforderlich ist,
3. die Übermittlung zum Abschluss oder zur Erfüllung eines Vertrags erforderlich ist, der im Interesse des Betroffenen von der verantwortlichen Stelle mit einem Dritten geschlossen wurde oder geschlossen werden soll,
4. die Übermittlung für die Wahrung eines wichtigen öffentlichen Interesses oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen vor Gericht erforderlich ist,
5. die Übermittlung für die Wahrung lebenswichtiger Interessen des Betroffenen erforderlich ist oder
6. die Übermittlung aus einem Register erfolgt, das zur Information der Öffentlichkeit bestimmt ist und entweder der gesamten Öffentlichkeit oder allen Personen, die ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offen steht, soweit die gesetzlichen Voraussetzungen im Einzelfall gegeben sind.

Bei **Nichterfüllung** der genannten **Anforderungen** kann die zuständige Aufsichtsbehörde einzelne Übermittlungen oder bestimmte Arten von Übermittlungen personenbezogener Daten **genehmigen**, wenn die verantwortliche Stelle ausreichende Garantien hinsichtlich des Schutzes des Persönlichkeitsrechts und der Ausübung der damit verbundenen Rechte vorweist, § 4c Abs. 2 S. 1 BDSG.

### 1.1.7. Auskunftsrecht

**- Öffentliche Stellen -**

Nach § 19 Abs. 1 BDSG kann der Betroffene von öffentlichen Stellen unentgeltlich (§ 19 Abs. 7 BDSG) Auskunft über die zu seiner Person gespeicherten **Daten** (auch die Herkunft der Daten), die **Empfänger** oder Kategorien von Empfängern, an die die Daten weitergegeben werden, und den **Zweck** der Speicherung verlangen. Dazu soll der Betroffene in seinem Antrag die Art der personenbezogenen Daten, über die Auskunft erteilt werden soll, näher bezeichnen. Sind die Daten weder automatisiert noch in automatisierten Dateien gespeichert, erhält er nur Auskunft, wenn er Angaben macht, die das Auffinden der Daten ermöglichen, und der für die Auskunftserteilung notwendige Aufwand nicht ausser Verhältnis zum Informationsinteresse des Betroffenen steht. Verfahren und Form der Auskunftserteilung stehen im Ermessen der verantwortlichen Stelle.[13]

Bezieht sich die Auskunftserteilung auf die Übermittlung personenbezogener Daten an **Verfassungsschutzbehörden**, den **Bundesnachrichtendienst**, den **Militärischen Abschirmdienst** und, soweit die

---

[13] Dies gilt nach Abs. 2 jedoch nicht für personenbezogene Daten, die nur gespeichert sind, weil sie aufgrund gesetzlicher, satzungsmässiger oder vertraglicher Aufbewahrungsvorschriften nicht gelöscht werden dürfen, oder ausschliesslich Zwecken der Datensicherung oder der Datenschutzkontrolle dienen und eine Auskunftserteilung einen unverhältnismässigen Aufwand erfordern würde.

Sicherheit des Bundes berührt wird, andere Behörden des Bundesministeriums der Verteidigung, ist sie nur mit **Zustimmung** dieser Stellen zulässig (§ 19 Abs. 3 BDSG).

Auskunft wird nach § 19 Abs. 4 BDSG **nicht erteilt**, wenn das Interesse des Betroffenen an der Auskunftserteilung zurücktreten muss, weil:

- sie die ordnungsgemässe Erfüllung der in der Zuständigkeit der verantwortlichen Stelle liegenden Aufgaben gefährden würde,
- sie die öffentliche Sicherheit oder Ordnung gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde oder
- die Daten oder die Tatsache ihrer Speicherung nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen,

Eine **Begründung der Ablehnung** ist nicht notwendig, wenn durch die Mitteilung der tatsächlichen und rechtlichen Gründe, auf die die Entscheidung gestützt wird, der mit der Auskunftsverweigerung verfolgte Zweck gefährdet würde. Der Betroffene ist in diesem Fall darauf hinzuweisen, dass er sich an den **Bundesbeauftragten für Datenschutz und Informationssicherheit** wenden kann, § 19 Abs. 5 BDSG. Wird dem Betroffenen keine Auskunft erteilt, so ist sie auf sein Verlangen dem Bundesbeauftragten für Datenschutz und Informationssicherheit zu erteilen, soweit nicht die jeweils zuständige oberste Bundesbehörde im Einzelfall feststellt, dass dadurch die Sicherheit des Bundes oder eines Landes gefährdet würde. Die Mitteilung des Bundesbeauftragten an den Betroffenen darf keine Rückschlusse auf den Erkenntnisstand der verantwortlichen Stelle zulassen, sofern diese nicht einer weitergehenden Auskunft zustimmt, § 19 Abs. 6 BDSG.

**- Nicht-öffentliche Stellen -**

Nicht-öffentliche Stellen haben nach § 34 Abs. 1 BDSG dem Betroffenen auf Verlangen Auskunft zu erteilen über die zu seiner Person **gespeicherten Daten** (auch bezüglich der Herkunft der Daten), den **Empfänger** oder die Kategorien von Empfängern, an die die Daten weitergegeben werden, und den **Zweck** der Speicherung.

Der Betroffene soll die Art der personenbezogenen Daten, über die Auskunft erteilt werden soll, näher bezeichnen. Werden die personenbezogenen Daten **geschäftsmässig zum Zweck der Übermittlung** gespeichert, ist Auskunft über die Herkunft und die Empfänger auch dann zu erteilen, wenn diese Angaben nicht gespeichert sind. Die Auskunft über die Herkunft und die Empfänger kann verweigert werden, soweit das Interesse an der Wahrung des **Geschäftsgeheimnisses** gegenüber dem Informationsinteresse des Betroffenen überwiegt.

Eine Stelle, die geschäftsmässig personenbezogene Daten zum **Zweck der Übermittlung** speichert, hat dem Betroffenen auf Verlangen Auskunft über die zu seiner Person gespeicherten Daten zu erteilen, auch wenn sie weder automatisiert verarbeitet werden noch in einer nicht automatisierten Datei gespeichert sind, § 34 Abs. 3 BDSG. Dem Betroffenen ist auch Auskunft zu erteilen über Daten, die gegenwärtig noch **keinen Personenbezug** aufweisen, bei denen ein solcher aber im Zusammenhang mit der Auskunftserteilung von der verantwortlichen Stelle hergestellt werden soll, sowie Daten, die verantwortliche Stelle nicht speichert, aber zum Zweck der Auskunftserteilung **nutzt**. Die Auskunft über die Herkunft und die Empfänger kann **verweigert** werden, soweit das Interesse an der Wahrung des Geschäftsgeheimnisses gegenüber dem Informationsinteresse des Betroffenen überwiegt.

Eine Pflicht zur Auskunftserteilung besteht gemäss § 34 Abs. 7 BDSG nicht, wenn:

- die Daten nur deshalb gespeichert sind, weil sie aufgrund gesetzlicher, satzungsmässiger oder vertraglicher Aufbewahrungsvorschriften nicht gelöscht werden dürfen oder ausschliesslich der Datensicherung oder der Datenschutzkontrolle dienen und eine Benachrichtigung einen unverhältnismässigen Aufwand erfordern würde,
- die Daten nach einer Rechtsvorschrift oder ihrem Wesen nach, namentlich wegen des überwiegenden rechtlichen Interesses eines Dritten, geheim gehalten werden müssen,
- die Speicherung oder Übermittlung für Zwecke der wissenschaftlichen Forschung erforderlich ist und eine Benachrichtigung einen unverhältnismässigen Aufwand erfordern würde,
- die zuständige öffentliche Stelle gegenüber der verantwortlichen Stelle festgestellt hat, dass das Bekanntwerden der Daten die öffentliche Sicherheit oder Ordnung gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde,
- die Daten für eigene Zwecke gespeichert sind und
    - aus allgemein zugänglichen Quellen entnommen sind und eine Benachrichtigung wegen der Vielzahl der betroffenen Fälle unverhältnismässig ist, oder
    - die Benachrichtigung die Geschäftszwecke der verantwortlichen Stelle erheblich gefährden würde, es sei denn, dass das Interesse an der Benachrichtigung die Gefährdung überwiegt.

Die Auskunft ist gemäss 34 Abs. 8 BDSG **unentgeltlich**. Werden die personenbezogenen Daten geschäftsmässig zum Zweck der Übermittlung gespeichert, kann der Betroffene einmal je Kalenderjahr eine unentgeltliche Auskunft in Textform verlangen. Für jede weitere Auskunft kann ein **Entgelt** verlangt werden, wenn der Betroffene die Auskunft gegenüber Dritten zu wirtschaftlichen Zwecken nutzen kann. Das Entgelt darf über die durch die Auskunftserteilung entstandenen unmittelbar zurechenbaren Kosten nicht hinausgehen. Ein Entgelt kann nicht verlangt werden, wenn besondere Umstände die Annahme rechtfertigen, dass Daten unrichtig oder unzulässig gespeichert werden, oder .die Auskunft ergibt, dass die Daten nach § 35 Abs. 1 BDSG zu berichtigen oder nach § 35 Abs. 2 S. 2 Ziff. 1 BDSG zu löschen sind.

Ist die Auskunftserteilung nicht unentgeltlich, ist dem Betroffenen nach 34 Abs. 9 BDSG die Möglichkeit zu geben, sich im Rahmen seines Auskunftsanspruchs persönlich Kenntnis über die ihn betreffenden Daten zu verschaffen.

### 1.1.8. Verhältnis von Technologieentwicklung und Datenschutz

Das BDSG enthält Sonderregelungen für den Einsatz automatisierter Einzelentscheidungen, die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen, und die Verwendung mobiler personenbezogener Speicher- und Verarbeitungsmedien.

§ 6a BDSG befasst sich mit **automatisierten Einzelentscheidungen**. Entscheidungen, die für den Betroffenen eine rechtliche Folge nach sich ziehen oder ihn erheblich beeinträchtigen, dürfen **nicht ausschliesslich** auf eine automatisierte Verarbeitung personenbezogener Daten gestützt werden, die der Bewertung einzelner Persönlichkeitsmerkmale dienen. Eine ausschliesslich auf eine automatisierte Verarbeitung gestützte Entscheidung liegt insbesondere dann vor, wenn keine **inhaltliche Bewertung** und darauf gestützte Entscheidung durch eine natürliche Person stattgefunden hat. Dies gilt nicht, wenn die Entscheidung im Rahmen des Abschlusses oder der Erfüllung eines Vertragsverhältnisses oder eines sonstigen Rechtsverhältnisses ergeht und dem Begehren des Betroffenen stattgegeben wurde oder die Wahrung der berechtigten Interessen des Betroffenen durch geeignete Massnahmen gewährleistet ist und die verantwortliche Stelle dem Betroffenen die Tatsache des Vorliegens einer solchen Entscheidung

mitteilt sowie auf Verlangen die wesentlichen Gründe dieser Entscheidung mitteilt und erläutert. Das Recht des Betroffenen auf Auskunft nach den §§ 19, 34 BDSG erstreckt sich auch auf den logischen Aufbau der automatisierten Verarbeitung der ihn betreffenden Daten.

§ 6b betrifft die **Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen**. Diese ist nur zulässig, soweit sie zur Aufgabenerfüllung öffentlicher Stellen, zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Der Umstand der Beobachtung und die verantwortliche Stelle sind durch geeignete Massnahmen erkennbar zu machen. Die **Verarbeitung oder Nutzung** erhobenen Daten ist zulässig, wenn sie zum Erreichen des verfolgten **Zwecks** erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Für einen **anderen Zweck** dürfen sie nur verarbeitet oder genutzt werden, soweit dies zur **Abwehr von Gefahren** für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten erforderlich ist. Die Daten sind unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen.

Nach § 6c muss eine Stelle, die ein **mobiles personenbezogenes Speicher- und Verarbeitungsmedium** (z.B. Chipkarten) ausgibt oder ein Verfahren zur automatisierten Verarbeitung personenbezogener Daten, das ganz oder teilweise auf einem solchen Medium abläuft, auf das Medium aufbringt, ändert oder hierzu bereithält, muss den Betroffenen über ihre Identität und Anschrift, in allgemein verständlicher Form über die Funktionsweise des Mediums einschliesslich der Art der zu verarbeitenden personenbezogenen Daten, darüber, wie er seine Rechte auf Auskunft, Berichtigung, Löschung, Sperrung und Widerspruch ausüben kann, und über die bei Verlust oder Zerstörung des Mediums zu treffenden Massnahmen unterrichten, soweit der Betroffene nicht bereits Kenntnis erlangt hat. Die Stelle hat dafür Sorge zu tragen, dass die zur Wahrnehmung des Auskunftsrechts erforderlichen Geräte oder Einrichtungen in angemessenem Umfang zum unentgeltlichen Gebrauch zur Verfügung stehen. Kommunikationsvorgänge, die auf dem Medium eine Datenverarbeitung auslösen, müssen für den Betroffenen eindeutig erkennbar sein.

Weder dem Datenschutzbeauftragten noch den Aufsichtsbehörden wurden in diesem Zusammenhang besondere Zuständigkeiten eingeräumt.

### 1.1.9. Unterschiedliche Regelungen für Datenbearbeitung durch Private / Behörden?

Das Bundesdatenschutzgesetz gilt für die Datenbearbeitung durch **öffentliche Stellen** des Bundes[14] und der Länder[15] sowie durch **nicht-öffentliche Stellen**[16]. Dabei gelten für die Datenbearbeitung durch

---

[14] Öffentliche Stellen des Bundes sind die Behörden, die Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen des Bundes, der bundesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie deren Vereinigungen ungeachtet ihrer Rechtsform. Als öffentliche Stellen gelten die aus dem Sondervermögen Deutsche Bundespost durch Gesetz hervorgegangenen Unternehmen, solange ihnen ein ausschliessliches Recht nach dem Postgesetz zusteht, § 2 Abs. 1 BDSG.

[15] Soweit der Datenschutz nicht durch Landesgesetz geregelt ist und soweit sie Bundesrecht ausführen oder als Organe der Rechtspflege tätig werden und es sich nicht um Verwaltungsangelegenheiten handelt, § 1 Abs. 2 Ziff. 2 BDSG. Öffentliche Stellen der Länder sind die Behörden, die Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen eines Landes, einer Gemeinde, eines Gemeindeverbandes und sonstiger der Aufsicht des Landes unterstehender juristischer Personen des öffentlichen Rechts sowie deren Vereinigungen ungeachtet ihrer Rechtsform, § 2 Abs. 2 BDSG.

öffentliche und nicht-öffentliche Stellen teilweise unterschiedliche Regeln. Die einzelnen Unterschiede werden an relevanter Stelle erläutert.

## 1.2. Durchsetzungsrechte der Datenschutzanliegen für Betroffene

### 1.2.1. Datenbearbeitungen durch Private

#### *1.2.1.1. Sperrung*

Nach § 35 Abs. 3 BDSG tritt die **Sperrung** an die **Stelle der Löschung** von Daten (vgl. unten cc) Vernichtung), wenn der Löschung gesetzliche, satzungsmässige oder vertragliche Aufbewahrungsfristen entgegenstehen, Grund zu der Annahme besteht, dass durch eine Löschung schutzwürdige Interessen des Betroffenen beeinträchtigt würden, oder eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismässig hohem Aufwand möglich ist.

Personenbezogene Daten sind nach § 35 Abs. 4 BDSG ferner zu sperren, wenn ihre Richtigkeit vom Betroffenen **bestritten** wird und sich weder die Richtigkeit noch die Unrichtigkeit feststellen lässt.

Nach § 35 Abs. 4a darf die Tatsache der Sperrung **nicht übermittelt** werden. Diese Regelung erklärt sich aus dem Kontext der Änderung des BDSG durch die Aufnahme der Regelungen § 28a „Datenübermittlung an Auskunfteien“ und § 28b „Scoring“ (Zulässigkeit der Ermittlung eines Wahrscheinlichkeitswerts für ein bestimmtes zukünftiges Verhalten zum Zwecke der Entscheidung, Durchführung oder Beendigung eines Vertragsverhältnisses mit dem Betroffenen). Absatz 4a bezieht sich in diesem Zusammenhang auf Sperrungen, die auf ein strittiges Datum hinweisen. Die Mitteilung einer Sperre könnte vom empfangenden Dritten leicht dahingehend missverstanden werden, dass der Betroffene nicht nur nicht zahlt, sondern auch noch ein schwieriger Kunde ist. Die Mitteilung könnte somit einen negativen Eindruck über den Betroffenen hinterlassen und deshalb zu einer für ihn negativen Entscheidung führen.[17]

Gesperrte Daten dürfen **ohne Einwilligung** des Betroffenen nur **übermittelt** oder **genutzt** werden, wenn es zu wissenschaftlichen Zwecken, zur Behebung einer bestehenden Beweisnot oder aus sonstigen im überwiegenden Interesse der verantwortlichen Stelle oder eines Dritten liegenden Gründen unerlässlich ist und die Daten hierfür übermittelt oder genutzt werden dürften, wenn sie nicht gesperrt wären, § 35 Abs. 8 BDSG.

#### *1.2.1.2. Berichtigung*

**Unrichtige** personenbezogene Daten sind zu berichtigen, § 35 Abs. 1 BDSG.

#### *1.2.1.3. Vernichtung*

Personenbezogene Daten **können jederzeit** gelöscht werden, es sei denn, dass der Löschung gesetzliche, satzungsmässige oder vertragliche Aufbewahrungsfristen entgegenstehen, Grund zu der Annahme besteht, dass durch eine Löschung schutzwürdige Interessen des Betroffenen beeinträchtigt würden,

---

16 Nicht-öffentliche Stellen sind natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts. Nimmt eine nicht-öffentliche Stelle hoheitliche Aufgaben der öffentlichen Verwaltung wahr, ist sie insoweit öffentliche Stelle, § 2 Abs. 4 BDSG.

17 Vergleiche die Begründung zum Gesetzentwurf der Bundesregierung: Entwurf eines Gesetzes zur Änderung des Bundesdatenschutzgesetzes vom 30. Juli 2008, S. 41, online abrufbar unter http://beck-aktuell.beck.de/sites/default/files/rsw/upload/Beck_Aktuell/Entwurf_BDSG_Regierung.pdf (05.08.2010).

oder eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismässig hohem Aufwand möglich ist, § 35 Abs. 2 S. 2, Abs. 3 BDSG.

Personenbezogene Daten **sind** nach § 35 Abs. 2 S. 2 BDSG zu löschen,

- wenn ihre Speicherung unzulässig ist,
- es sich um Daten über die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit, Sexualleben, strafbare Handlungen oder Ordnungswidrigkeiten handelt und ihre Richtigkeit von der verantwortlichen Stelle nicht bewiesen werden kann,
- sie für eigene Zwecke verarbeitet werden, sobald ihre Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist, oder
- sie geschäftsmässig zum Zweck der Übermittlung verarbeitet werden und eine Prüfung jeweils am Ende des vierten, soweit es sich um Daten über erledigte Sachverhalte handelt und der Betroffene der Löschung nicht widerspricht, am Ende des dritten Kalenderjahres beginnend mit dem Kalenderjahr, das der erstmaligen Speicherung folgt, ergibt, dass eine länger währende Speicherung nicht erforderlich ist.

#### *1.2.1.4. Vermerkung*

Grundsätzlich sind personenbezogene Daten nach § 35 Abs. 4 BDSG zu **sperren**, wenn ihre Richtigkeit vom Betroffenen **bestritten** wird und sich weder die Richtigkeit noch die Unrichtigkeit feststellen lässt. Nach § 35 Abs. 6 BDSG müssen personenbezogene Daten, die unrichtig sind oder deren Richtigkeit bestritten wird, bei der geschäftsmässigen Datenspeicherung zum Zweck der Übermittlung jedoch **nicht berichtig, gesperrt** oder **gelöscht** werden, wenn sie aus **allgemein zugänglichen** Quellen entnommen und zu Dokumentationszwecken gespeichert sind. Auf Verlangen des Betroffenen ist diesen Daten jedoch für die Dauer der Speicherung **seine Gegendarstellung** beizufügen. Die Daten dürfen nicht ohne diese Gegendarstellung übermittelt werden. Dies gilt nicht für Daten über die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit, Sexualleben, strafbaren Handlungen oder Ordnungswidrigkeit, deren Richtigkeit von der verantwortlichen Stellen nicht bewiesen werden kann (§ 35 Abs. 2 S. 2 Ziff. 2 BDSG).

#### *1.2.1.5. Mitteilung und Veröffentlichung*

Von der Berichtigung unrichtiger Daten, der Sperrung bestrittener Daten sowie der Löschung oder Sperrung wegen Unzulässigkeit der Speicherung sind die Stellen zu **verständigen**, denen im Rahmen einer Datenübermittlung diese Daten zur Speicherung **weitergegeben** wurden, wenn dies keinen unverhältnismässigen **Aufwand** erfordert und schutzwürdige **Interessen** des Betroffenen nicht entgegen stehen, § 35 Abs. 7 BDSG.

#### *1.2.1.6. Andere*

Das BDSG enthält eine **Schadensersatzregelung**. Fügt eine verantwortliche Stelle dem Betroffenen durch eine nach diesem Gesetz oder nach anderen Vorschriften über den Datenschutz unzulässige oder unrichtige Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten einen Schaden zu, ist sie oder ihr Träger dem Betroffenen zum Schadensersatz verpflichtet, § 7 BDSG. Die Ersatzpflicht entfällt, soweit die verantwortliche Stelle die nach den Umständen des Falles gebotene Sorgfalt beachtet hat.

Ausserdem kann der Betroffene nach § 35 Abs. 5 BDSG der Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten **widersprechen**. Diese dürfen dann nicht für eine automatisierte Verarbeitung oder Verarbeitung in nicht automatisierten Dateien erhoben, verarbeitet oder genutzt werden, soweit eine Prüfung ergibt, dass das **schutzwürdige Interesse** des Betroffenen wegen seiner besonderen persönlichen Situation das Interesse der verantwortlichen Stelle an dieser Erhebung, Verarbeitung oder Nutzung überwiegt. Dies gilt jedoch nicht, wenn eine Rechtsvorschrift die Stelle zur Erhebung, Verarbeitung oder Nutzung **verpflichtet**.

#### *1.2.1.7. Verfahren*

Für Streitigkeiten, die die Berichtigung, Sperrung oder Löschung von Daten nach § 35 BDSG betreffen, sind grundsätzlich die **Zivilgerichte** zuständig. Damit gilt für das Verfahren die Zivilprozessordnung. Eine Ausnahme gilt für Auseinandersetzungen im Rahmen von Arbeitsverhältnissen, für die die **Arbeitsgerichte** zuständig sind. Für Streitigkeiten bezüglich der Überwachung durch die Aufsichtsbehörden sind die **Verwaltungsgerichte** zuständig. Wird im Hauptsacheverfahren die Löschung von personenbezogenen Daten begehrt, kommt dies als vorläufige Massnahme im Verfahren des **einstweiligen Rechtsschutzes** in Betracht.[18]

**Sammelklagen** bedürfen für ihre Zulässigkeit einer näheren gesetzlichen Regelung,[19] die im Bereich des Datenschutzes nicht existiert. Sind Verletzungen datenschutzrechtlicher Informationspflichten als verbraucherschutzgesetzwidrige Praktiken nach § 2[20] des **Unterlassungsklagengesetzes**[21] anzusehen, so sind nach §§ 3 f. des Gesetzes qualifizierte **Verbraucherschutzvereine**, rechtsfähige Vereine zur Förderung gewerblicher Interessen und Handelskammern aktivlegitimiert. Zwar sind Datenschutzorganisationen in dem Gesetz nicht ausdrücklich aufgeführt, ihre Anerkennung ist jedoch nicht ausgeschlossen.[22]

#### *1.2.1.8. Abklärung durch Datenschutzbeauftragen bei Meldung durch Dritte*

Nach § 38 Abs. 1 S. 8 i.V.m. § 21 BDSG kann sich Jedermann an die Aufsichtsbehörde wenden, wenn er der Ansicht ist, bei der Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten durch nicht-öffentliche Stellen in seinen Rechten verletzt worden zu sein. Dritte, die nicht in eigenen Rechten verletzt wurden, können die Aufsichtsbehörde damit grundsätzlich nicht anrufen. Allerdings kann die Aufsichtsbehörde als Kontrollstelle anlassunabhängig tätig werden (§ 38 Abs. 1 S. 1 BDSG).[23] Damit steht es ihr frei, Meldungen von Dritten nachzugehen. Eine Pflicht hierzu besteht jedoch nicht.

---

18 A. Dix in Simitis, Bundesdatenschutzgesetz (Kommentar), 6. Auflage, Baden-Baden 2006, § 35 N. 82.

19 M. Vollkommer, Zöller Zivilprozessordnung (Kommentar), 28. Auflage, Köln 2010, § 60 N. 3a.

20 Abs. 1: „Wer in anderer Weise als durch Verwendung oder Empfehlung von Allgemeinen Geschäftsbedingungen Vorschriften zuwiderhandelt, die dem Schutz der Verbraucher dienen (Verbraucherschutzgesetze), kann im Interesse des Verbraucherschutzes auf Unterlassung in Anspruch genommen werden. Werden die Zuwiderhandlungen in einem geschäftlichen Betrieb von einem Angestellten oder einem Beauftragten begangen, so ist der Unterlassungsanspruch auch gegen den Inhaber des Betriebs begründet."

21 Gesetz über Unterlassungsklagen bei Verbraucherrechts- und anderen Verstößen (Unterlassungsklagengesetz - UKlaG) in der Fassung der Bekanntmachung vom 27. August 2002 (BGBl. I S. 3422, ber. S. 4346), zuletzt geändert durch Art. 3 G zur Einführung einer Musterwiderrufsinformation für Verbraucherdarlehensverträge, zur Änd. der Vorschriften über das Widerrufsrecht bei Verbraucherdarlehensverträgen und zur Änd. des Darlehensvermittlungsrechts vom 24. 7. 2010 (BGBl. I S. 977).

22 J. Bizer, Datenschutzrechtliche Informationspflichten, Datenschutz und Datensicherheit 2005, S. 451, 456.

23 Vgl. R. Hillebrand-Beck in in Rossnagel, Handbuch für Datenschutz, München 2003, S. 833 N. 64.

## 1.2.2. Datenbarbeitungen durch Behörde

### *1.2.2.1. Unterlassung widerrechtlicher Bearbeitung*

Personenbezogene Daten dürfen nach § 20 Abs. 5 BDSG nicht für eine automatisierte Verarbeitung oder Verarbeitung in nicht automatisierten Dateien erhoben, verarbeitet oder genutzt werden, soweit der Betroffene dieser bei der verantwortlichen Stelle **widerspricht** und eine Prüfung ergibt, dass das **schutzwürdige Interesse** des Betroffenen wegen seiner besonderen persönlichen Situation das Interesse der verantwortlichen Stelle an dieser Erhebung, Verarbeitung oder Nutzung überwiegt. Dies gilt jedoch nicht, wenn eine Rechtsvorschrift zur Erhebung, Verarbeitung oder Nutzung verpflichtet.

### *1.2.2.2. Beseitigung der Folgen widerrechtlicher Bearbeitung*

Regelungen zur **Beseitigung der Folgen widerrechtlicher Bearbeitung** entsprechend dem schweizerischen Datenschutzgesetz gibt es **nicht**. Ist die Erhebung der Daten unzulässig, so sind die Daten grundsätzlich zu **löschen** (s.u.).

### *1.2.2.3. Feststellung der widerrechtlichen Bearbeitung*

Regelungen zur **Feststellung der widerrechtlichen Bearbeitung** entsprechend dem schweizerischen Datenschutzgesetz gibt es **nicht**. Ist die Erhebung der Daten unzulässig, so sind die Daten grundsätzlich zu **löschen** (s.u.).

### *1.2.2.4. Vermerkung*

Regelungen zur **Vermerkung** entsprechend dem schweizerischen Datenschutzgesetz gibt es für öffentliche Stellen **nicht**. Wird die Richtigkeit personenbezogener Daten, die automatisiert verarbeitet oder in nicht automatisierten Dateien gespeichert sind, bestritten und lässt sich weder die Richtigkeit noch die Unrichtigkeit feststellen, so sind diese zu **sperren**, § 20 Abs. 4 BDSG.

### *1.2.2.5. Sperrung*

Nach § 20 Abs. 2 BDSG tritt die **Sperrung** an die **Stelle der Löschung** von Daten (vgl. unten gg) Vernichtung), wenn einer Löschung gesetzliche, satzungsmässige oder vertragliche **Aufbewahrungsfristen entgegenstehen**, Grund zu der Annahme besteht, dass durch eine Löschung schutzwürdige **Interessen des Betroffenen beeinträchtigt** würden, oder eine Löschung wegen der besonderen Art der Speicherung **nicht** oder nur mit unverhältnismässig hohem Aufwand möglich ist.

Personenbezogene Daten, die **automatisiert verarbeitet** oder in nicht automatisierten Dateien gespeichert sind, sind ferner zu sperren, soweit ihre Richtigkeit vom Betroffenen **bestritten** wird und sich weder die Richtigkeit noch die Unrichtigkeit feststellen lässt, § 20 Abs. 4 BDSG.

Personenbezogene Daten, die **weder automatisiert verarbeitet** noch in nicht automatisierten Dateien gespeichert sind, sind nach § 20 Abs. 6 BDSG zu sperren, wenn die Behörde im **Einzelfall** feststellt, dass ohne die Sperrung schutzwürdige Interessen des Betroffenen beeinträchtigt würden und die Daten für die Aufgabenerfüllung der Behörde nicht mehr erforderlich sind.

Gesperrte Daten dürfen **ohne Einwilligung** des Betroffenen nach § 20 Abs. 7 BDSG nur **übermittelt oder genutzt** werden, wenn es zu wissenschaftlichen Zwecken, zur Behebung einer bestehenden Beweisnot oder aus sonstigen im überwiegenden Interesse der verantwortlichen Stelle oder eines Dritten liegenden Gründen unerlässlich ist und die Daten hierfür übermittelt oder genutzt werden dürften, wenn sie nicht gesperrt wären.

#### *1.2.2.6. Berichtigung*

**Unrichtige** personenbezogene Daten sind zu berichtigen, § 20 Abs. 1 BDSG. Wird festgestellt, dass personenbezogene Daten, die weder automatisiert verarbeitet noch in nicht automatisierten Dateien gespeichert sind, unrichtig sind, oder wird ihre Richtigkeit von dem Betroffenen **bestritten**, so ist dies in geeigneter Weise **festzuhalten**.

#### *1.2.2.7. Vernichtung*

Personenbezogene Daten, die automatisiert verarbeitet oder in nicht automatisierten Dateien gespeichert sind, sind zu **löschen**, wenn ihre **Speicherung unzulässig** ist oder ihre Kenntnis für die verantwortliche Stelle zur Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist, § 20 Abs. 2 BDSG.

#### *1.2.2.8. Mitteilung und Veröffentlichung*

Von der Berichtigung unrichtiger Daten, der Sperrung bestrittener Daten sowie der Löschung oder Sperrung wegen Unzulässigkeit der Speicherung sind nach § 20 Abs. 8 BDSG die Stellen zu **verständigen**, denen im Rahmen einer Datenübermittlung diese Daten zur Speicherung **weitergegeben wurden**, wenn dies keinen unverhältnismässigen Aufwand erfordert und schutzwürdige Interessen des Betroffenen nicht entgegenstehen.

#### *1.2.2.9. Andere*

Das BDSG enthält eine **Schadensersatzregelung**. Fügt eine verantwortliche Stelle dem Betroffenen durch eine nach diesem Gesetz oder nach anderen Vorschriften über den Datenschutz unzulässige oder unrichtige Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten einen Schaden zu, ist sie oder ihr Träger dem Betroffenen zum Schadensersatz verpflichtet, § 7 BDSG. Die Ersatzpflicht entfällt, soweit die verantwortliche Stelle die nach den Umständen des Falles gebotene Sorgfalt beachtet hat.

Im Rahmen der **automatisierten Datenverarbeitung** durch eine **öffentliche** Stelle ist ihr Träger dem Betroffenen **unabhängig** von einem Verschulden zum **Schadensersatz** verpflichtet, wenn die Stelle dem Betroffenen durch eine nach dem BDSG oder nach anderen Vorschriften über den Datenschutz unzulässige oder unrichtige automatisierte Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten einen Schaden zugefügt hat, § 8 BDSG. Bei einer schweren Verletzung des Persönlichkeitsrechts ist dem Betroffenen der Schaden, der nicht Vermögensschaden ist, angemessen in Geld zu ersetzen. Die Ansprüche sind insgesamt auf einen Betrag von 130 000 Euro begrenzt. Ist aufgrund desselben Ereignisses an mehrere Personen Schadensersatz zu leisten, der insgesamt den Höchstbetrag von 130 000 Euro übersteigt, so verringern sich die einzelnen Schadensersatzleistungen in dem Verhältnis, in dem ihr Gesamtbetrag zu dem Höchstbetrag steht. Sind bei einer automatisierten Verarbeitung mehrere Stellen speicherungsberechtigt und ist der Geschädigte nicht in der Lage, die speichernde Stelle festzustellen, so haftet jede dieser Stellen.

#### *1.2.2.10. Verfahren*

Sind die gesetzlichen Voraussetzungen erfüllt, so steht dem Betroffenen ein **subjektives Recht** auf die Berichtigung, Sperrung oder Löschung seiner Daten zu. Dieses kann er **gerichtlich** durchsetzen. Welches Gericht für die Klage zuständig ist, richtet sich nach der die Daten verarbeitenden Behörde. In Betracht kommen das **Verwaltungsgericht**, das **Sozialgericht** oder das **Finanzgericht**. Wird im Hauptverfahren die Löschung von personenbezogenen Daten begehrt, kann eine Sperrung der Daten als **vorläufige Massnahme** im Verfahren nach § 123 der Verwaltungsgerichtsordnung in Betracht kommen.[24]

Soweit besondere Rechtsnormen **Verbänden** keine Beteiligungs- und Verfahrensrechte einräumen, können sie sich **nicht** zum Sachwalter ihrer Mitglieder oder der Allgemeinheit aufschwingen und in zulässiger Weise Klage erheben.[25] Die Möglichkeit für **Sammelklagen** besteht nicht.

#### *1.2.2.11. Abklärung durch Datenschutzbeauftragten, wenn Dritte melden*

An den Datenschutzbeauftragten kann sich nur wenden, wer der Ansicht ist, dass er bei der Erhebung, Verarbeitung oder Nutzung **seiner** personenbezogenen Daten durch öffentliche Stellen in seinen Rechten verletzt worden ist. Für die Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten durch Gerichte des Bundes gilt dies nur, soweit diese in Verwaltungsangelegenheiten tätig werden, § 21 BDSG. Allerdings kann der Bundesdatenschutzbeauftragte in seiner Kontrolltätigkeit auf eigenes Ermessen hin tätig werden,[26] somit auch, wenn er von einem nicht betroffenen Dritten von Verstössen gegen das Bundesdatenschutzgesetz erfährt.

## 1.3. Nationale Aufsichtsbehörde

In Deutschland existieren für öffentliche und nicht-öffentliche datenverarbeitende Stellen **getrennte** Aufsichtsbehörden:

Der **Bundesbeauftragte für den Datenschutz** und die Informationsfreiheit (Bundesdatenschutzbeauftragter) kontrolliert bei den **öffentlichen Stellen** des Bundes die Einhaltung der Vorschriften des BDSG und anderer Vorschriften über den Datenschutz, § 24 Abs. 1 BDSG.

Die **Aufsichtsbehörde** nach § 38 BDSG kontrolliert die Ausführung des BDSG und anderer Vorschriften über den Datenschutz durch **nicht-öffentliche Stellen**, soweit diese die automatisierte Verarbeitung personenbezogener Daten oder die Verarbeitung oder Nutzung personenbezogener Daten in oder aus nicht automatisierten Dateien regeln. Sie berät und unterstützt die Beauftragten für Datenschutz und die verantwortlichen Stellen mit Rücksicht auf deren typische Bedürfnisse. Da die Aufsichtsbehörden auf Länderebene angesiedelt sind, variiert die Ausgestaltung der Behörden zum Teil erheblich von Bundesland zu Bundesland. Mit Hinblick auf den Rahmen dieses Gutachtens musste daher eine Beschränkung der Darstellung erfolgen.

---

[24] O. Mallmann in Simitis, Bundesdatenschutzgesetz (Kommentar), 6. Auflage, Baden-Baden 2006, § 20 N. 106.

[25] C. Sennekamp, Verwaltungsprozessrecht VwVfG - VwGO (Kommentar), 1. Auflage, Baden-Baden 2006, § 42 VwGO N. 51.

[26] Vgl. H. Heil in Rossnagel, Handbuch für Datenschutz, München 2003, S. 766 N. 48.

### 1.3.1. Zusammensetzung, Ernennung und Eingliederung der Behörde

#### *1.3.1.1. Bundesdatenschutzbeauftragter*

Der Bundesdatenschutzbeauftrage steht in einem öffentlich-rechtlichen Amtsverhältnis. Die Dienststelle des Bundesdatenschutzbeauftragen ist „beim“ **Bundesministerium des Inneren** eingerichtet, § 22 Abs. 5 BDSG. Bei der Führung seiner Dienststelle wird er unterstützt und vertreten vom Leitenden Beamten. Die Dienststelle des Bundesdatenschutzbeauftragen gliedert sich in acht Fachreferate, den Bereich Zentrale Aufgaben und die Pressestelle. Der Mitarbeiterstab des Bundesdatenschutzbeauftragen umfasst zur Zeit etwa 70 Personen.[27] Die Fachreferate umfassen die folgenden Bereiche[28]:

- Grundsatzangelegenheiten; nicht-öffentlicher Bereich
- Rechtswesen, Finanzen, Arbeitsverwaltung, Verteidigung, Zivildienst, Auswärtiger Dienst, Innere Verwaltung (z.B. Ausländerrecht)
- Sozialwesen, Mitarbeiter- datenschutz
- Wirtschaft, Gesundheitswesen, Verkehr, Postdienste, Statistik
- Polizei, Nachrichtendienste
- Technologischer Datenschutz, Informationstechnik, Datensicherheit
- Europäische und Internationale Angelegenheiten, Innere Verwaltung (z.B. Meldewesen), Strafrecht, Aufarbeitung der Stasi-Unterlagen, Meldewesen
- Telekommunikations-, Tele- und Mediendienste; Projektgruppe Elektronische Gesundheitskarte (PG eGK)
- Informationsfreiheit

Der Bundesdatenschutzbeauftragte wird auf Vorschlag der Bundesregierung durch den **Deutschen Bundestag** (mit absoluter Mehrheit) gewählt und vom Bundespräsidenten ernannt. Die Amtszeit beträgt fünf Jahre, eine einmalige Wiederwahl ist zulässig, § 22 Abs. 1 und 3 BDSG.

Kandidaten für das Amt des Bundesdatenschutzbeauftragten müssen das 35. Lebensjahr vollendet haben und die **Befähigung zur Bekleidung öffentlicher Ämter** besitzen. Die Befähigung zum Richteramt ist nicht notwenig. Weitere Qualifikationsvoraussetzungen bestehen nicht. Dies wird mit der Vielseitigkeit der Aufgaben und der Tatsache begründet, dass das Amt des Bundesdatenschutzbeauftragten nicht mit Weisungs- oder Eingriffsbefugnissen gegenüber den von ihm kontrollierten Stellen ausgestattet ist.[29]

Neben dem Bundesdatenschutzbeauftragten existieren auf der Ebene der Länder die **Datenschutzbeauftragten der Länder**. Diese überwachen die Einhaltung der **Landesdatenschutzgesetze**. Diese gelten für die Behörden, Einrichtungen und sonstigen öffentlichen Stellen des Landes, die Gemeinden und Gemeindeverbände sowie für die sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts und deren Vereinigungen (öffentliche Stellen), soweit diese personenbezogene Daten verarbeiten. Die Rechtsstellung der Landesdatenschutzbeauftragten (mit Ausnahme von Schleswig-Holstein) enspricht im Wesentlichen der des Bundesdatenschutzbeauftragten. Ihre organisatorische Einbindung variiert jedoch:

- Zuweisung zum Innenministerium (wie auf Bundesebene) z.B. in Baden-Württemberg

---

[27] Informationen von der Homepage des Bundesdatenschutzbeauftragten, abrufbar unter http://www.bfdi.bund.de/cln_136/DE/Dienststelle/Aufgaben/Aufgaben_node.html (03.11.2010).

[28] Siehe das Organigramm der Dienststelle des Bundesdatenschutzbeauftragten, abrufbar unter http://www.bfdi.bund.de/cln_136/sid_E20700F2DC07EE9ADC7397EB4B7268AF/DE/Dienststelle/Organisation/organisation_node.html (04.11.2010).

[29] P. Gola in: Gola/Schomerus, Bundesdatenschutzgesetz Kommentar, 9. Auflage, München 2007, § 22 N. 4.

- Zuweisung zur jeweiligen Volksvertretung (Landesparlaments) z.B. in Rheinland-Pfalz
- „Unabhängiges Landeszentrum für Datenschutz“ in Form einer rechtsfähigen Anstalt des öffentlichen Rechts in Schleswig-Holstein.

Die Amtszeit der Landesbeauftragten liegt, je nach Bundesland, zwischen fünf bis acht Jahren oder ist auf die Dauer der Legislaturperiode beschränkt. Die Volksvertretung des jeweiligen Landes ist entweder direkt mit der Wahl des Landesdatenschutzbeauftragten betraut oder wirkt daran durch Zustimmung oder Ablehnung der Bestellung durch die Landesregierung mit.[30]

#### *1.3.1.2. Aufsichtsbehörde*

Die **Aufsichtsbehörde** nach § 38 BDSG kontrolliert die Ausführung des BDSG und anderer Vorschriften über den Datenschutz durch **nicht-öffentliche Stellen**, soweit diese die automatisierte Verarbeitung personenbezogener Daten oder die Verarbeitung oder Nutzung personenbezogener Daten in oder aus nicht automatisierten Dateien regeln. Sie berät und unterstützt die Beauftragten für Datenschutz und die verantwortlichen Stellen mit Rücksicht auf deren typische Bedürfnisse.

Die Aufsichtsbehörden sind auf Länderebene angesiedelt und dort teilweise beim jeweiligen Innenministerium[31], beim Landesverwaltungsamt[32] oder beim Landesdatenschutzbeauftragten (s.o.)[33] angesiedelt.[34] Eine Wahl erfolgt nur dann, wenn die Funktion der Aufsichtsbehörde durch den Landesdatenschutzbeauftragten wahrgenommen wird. In Bayern erfolgt die Prüfung der Datenverarbeitung im rechnischen Bereich durch den TÜV (), der berechtigt ist, für seine Tätigkeit bei der überprüften Stelle Gebühren zu erheben. Die Erhebung von Gebühren für die Aufsichtstätigkeit ist auch in einigen anderen Bundesländern zugelassen.[35]

### 1.3.2. Gewährleistung der Unabhängigkeit

#### *1.3.2.1. Bundesdatenschutzbeauftragter*

Der Bundesdatenschutzbeauftrage ist in der Ausübung seines Amtes **unabhängig** und nur dem Gesetz unterworfen. Er steht in einem öffentlich-rechtlichen **Amtsverhältnis eigener Art**, ist also weder Beamter auf Zeit noch Anstellter. Die **Rechtsaufsicht** obliegt der Bundesregierung, § 22 Abs. 4 BDSG. Er untersteht der **Dienstaufsicht**[36] des Bundesministeriums des Inneren, § 22 Abs. 5 BDSG. Die Fachaufsicht entfällt. Er unterliegt bei seiner Amtstätigkeit weder den Weisungen des Bundesministers des Innern, noch kann er wegen einzelner Amtshandlungen zur Rechenschaft gezogen, namentlich nicht entlassen oder versetzt werden.[37]

---

30 Gola, op.cit., § 22 N. 14.

31 So z.B. in Baden-Württemberg (Innenministerium, Referat Datenschutz).

32 Z.B. Landesverwaltungsamt Sachsen-Anhalt.

33 Z.B. Landesbeauftragter für Datenschutz und Informationsfreiheit Nordrhein-Westfalen.

34 Siehe Anhang V der Broschüre „Bundesdatenschutzgesetz - Text und Erläuterung“ des Bundesdatenschutzbeauftragten, online abrufbar unter http://www.bfdi.bund.de/cae/servlet/contentblob/416312/publicationFile/58836/INFO1_Maerz2009.pdf (05.08.2010).

35 Gola, op.cit., § 38 N. 29.

36 Regelung rein dienstrechtlicher Fragen wie Besoldung, Versorgung, Urlaub, Dienstzeit etc., vgl. Gola op.cit, § 22 N. 12.

37 Gola, op.cit., § 22 N. 10.

Der Haushalt der Dienststelle ist Bestandteil des Haushalts des BMI, und die Mitarbeiter der Dienststelle sind Angehörige dieses Ministeriums.[38] Nach § 22 Abs. 5 BDSG ist ihm für die Erfüllung seiner Aufgaben die notwendige **Personal- und Sachausstattung** zur Verfügung zu stellen, sie ist im Einzelplan des Bundesministeriums des Inneren in einem eigenen Kapitel auszuweisen. Nach dem Bundeshaushalt 2010 stehen **1.800 T€** zur Verfügung des Bundesbeauftragten für Datenschutz und Informationsfreiheit.[39] Mitspracherechte für die Zuteilung finanzieller Mittel etc. stehen dem Bundesdatenschutzbeauftragten nicht zu.

Der Bundesdatenschutzbeauftragte kann nach § 23 Abs. 1 BDSG nur auf sein **eigenes Verlangen** entlassen werden oder auf Vorschlag der Bundesregierung, wenn Gründe vorliegen, die bei einem **Richter auf Lebenszeit** aus dem Dienst rechtfertigen. Er darf nach Abs. 2 neben seinem Amt kein anderes besoldetes Amt, **kein Gewerbe und keinen Beruf ausüben** und weder der Leitung noch dem Aufsichtsrat oder dem Verwaltungsrat eines auf Erwerb gerichteten Unternehmens noch einer Regierung oder einer gesetzgebenden Körperschaft des Bundes oder eines Landes angehören. Er darf auch nicht gegen Entgelt aussergerichtliche **Gutachten** abgeben, § 23 Abs. 2 BDSG. Er hat dem Bundesministerium des Innern Mitteilung zu machen über **Geschenke**, die er in Bezug auf sein Amt erhält. Das Ministerium entscheidet über die Verwendung der Geschenke, § 23 Abs. 3 BDSG.

Darüber hinaus ist der Bundesdatenschutzbeauftragte über ihm amtlich bekanntgewordene betreffen, zur **Verschwiegenheit** verpflichtet. Er darf auch nach seiner Amtszeit nicht ohne Genehmigung des Bundesministeriums des Inneren vor Gericht oder aussergerichtlich aussagen oder Erklärungen abgeben. Dies berührt jedoch nicht die gesetzliche Pflicht, Straftaten anzuzeigen und bei Gefährdung der freiheitlichen demokratischen Grundordnung für deren Erhaltung beizutreten, § 23 Abs. 5 BDSG.

#### *1.3.2.2. Aufsichtsbehörde*

Bezüglich der Unabhängigkeit der Aufsichtsbehörden gegenüber anderen Behörden bestehen unterschiedliche landesrechtliche Regelungen. So können die Aufsichtsbehörden:

- vorbehaltlos in ministerielle Weisungsstränge eingegliedert sein,[40]
- der Fachaufsicht[41] oder
- der Rechtsaufsicht[42]

---

38 Gola, op.cit., § 22 N. 12.

39 Bundeshaushaltsplan, Einzelplan 06, Bundesministerium des Inneren, S. 6, online abrufbar unter http://www.bundesfinanzministerium.de/bundeshaushalt2010/pdf/epl06.pdf (05.08.2010).

40 Z.B. in Baden-Würtemberg nach § 1 Verordnung der Landesregierung über die zuständige Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich (Datenschutzzuständigkeitsverordnung – DSZuVO) vom 10. Januar 1978 (GBl. S. 78) oder das bei der der Regierung von Mittelfranken eingerichtete Landesamt für Datenschutzaufsicht nach §1Abs. 1 Bayerische Datenschutzverordnung (DSchV) vom 1. März 1994 (GVBl S. 153), zuletzt geändert durch § 1 Vierte VO zur Änd. der DatenschutzVO vom 10. 2. 2009 (GVBl S. 22).

41 Unter Anderem § 25 S. 2 Bremisches Datenschutzgesetz (BremDSG) vom 4. März 2003 (Brem.GBl. S. 85), zuletzt geändert durch Art. 15 BeamtenrechtsneuregelungsG vom 22. 12. 2009 (Brem.GBl. 2010 S. 17), § 22 Abs. 1 S. 3 Hamburgisches Datenschutzgesetz (HmbDSG) vom 5. Juli 1990 (HmbGVBl. S. 133, ber. S. 165, 226), zuletzt geändert durch Art. 10 G zur Neuregelung des hamburgischen Beamtenrechts vom 15. 12. 2009 (HmbGVBl. S. 405).

42 Z.B. § 33 Abs. 1 S. 2 Gesetz zum Schutz personenbezogener Daten in der Berliner Verwaltung (Berliner Datenschutzgesetz – BlnDSG) in der Fassung vom 17. Dezember1990 (GVBl.1991 S. 16, ber. S. 54), zuletzt geändert durch Art. II G zur Änd. des Allgemeinen Sicherheits- und OrdnungsG und des Berliner DatenschutzG vom 30. 11. 2007 (GVBl. S. 598), § 38 S. 2 Schleswig-Holsteinisches Gesetz zum Schutz

unterliegen.[43] Aufgrund der Vielzahl der bestehenden Gestaltungsmöglichkeiten würde jedoch es den Rahmen dieses Gutachtens sprengen, auf diese im Einzelnen einzugehen.

Das System der Datenschutzkontrolle über nicht-öffentliche Stellen in Deutschland entspricht laut dem Urteil des EuGH[44] im Vertragsverletzungsverfahren der Europäischen Kommission gegen Deutschland nicht den Anforderungen der EU-Datenschutzrichtlinie[45]. Der Gerichtshof kam zu dem Ergebnis, dass die Bundesrepublik Deutschland gegen ihre Verpflichtungen aus Art. 28 Abs. 1 Unterabs. 2 der Richtlinie verstoßen habe, indem sie die für die Überwachung der Verarbeitung personenbezogener Daten durch nichtöffentliche Stellen und öffentlich-rechtliche Wettbewerbsunternehmen zuständigen Kontrollstellen in den Bundesländern staatlicher Aufsicht unterstellt und damit das Erfordernis, dass diese Stellen ihre Aufgaben „in völliger Unabhängigkeit“ wahrnehmen, falsch umgesetzt habe.[46]

Die Höhe der Ressourcen **variiert** von Bundesland zu Bundesland. Beispielsweise verzeichnet der Haushaltsplan für das Land Nordrhein-Westfalen[47] für das Jahr 2010 für den Datenschutzbeauftragten Einnahmen in Höhe von 29,1 T€ und Ausgaben in Höhe von 3.033,8 T€, das Bundesland Hamburg[48] 22 T€ an Einnahmen und 1.261T€ an Ausgaben. **Mitspracherechte** bezüglich der finanziellen Mittel bestehen nicht.

### 1.3.3. Zuständigkeitsbereich

#### *1.3.3.1. Bundesdatenschutzbeauftragter*

Der Bundesdatenschutzbeauftragte ist zuständig für die Kontrolle der **öffentlichen Stellen** des Bundes, § 24 Abs. 1 BDSG. Die **Bundesgerichte** unterliegen der Kontrolle des Bundesbeauftragen nur, soweit sie in Verwaltungsangelegenheiten tätig werden, § 24 Abs. 3 BDSG. Daneben hat der Bundesdatenschutzbeauftragte auch **bestimmte nicht-öffentliche Stellen** zu beraten und zu kontrollieren. Hierbei handelt es sich um die Telekommunikations- und die Postdienstunternehmen sowie um private Unternehmen, die unter das Sicherheitsüberprüfungsgesetz fallen, § 24 Abs. 2 BDSG und § 23 Sicherheitsüberprüfungsgesetz. Als Bundesbeauftragter für Datenschutz und Informationsfreiheit ist er ausserdem für die Kontrolle nach dem Informationsfreiheitsgesetz zuständig, § 12 Abs. 2 Informationsfreiheitsgesetz.

---

personenbezogener Informationen (Landesdatenschutzgesetz - LDSG -) vom 9. Februar 2000 (GVOBl. Schl.-H. S. 169), zuletzt geändert durch Art. 12 G zur Neuregelung des Beamtenrechts in Schleswig-Holstein vom 26. 3. 2009 (GVOBl. Schl.-H. S. 93).

43 Für weitere Nachweise siehe Th. Petri in Simitis, Bundesdatenschutzgesetz (Kommentar), 6. Auflage, Baden-Baden 2006, § 38 N. 10.

44 EuGH, Urteil vom 09.03.2010, C-518/07, online abrufbar unter http://curia.europa.eu/jurisp/cgi-bin/form.pl?lang=DE&Submit=rechercher&numaff=C-518/07 (04.11.2020).

45 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, Amtsblatt Nr. L 281 vom 23.11.1995, S. 31ff.

46 Zwar bezog sich das Urteil lediglich auf die Aufsicht über nicht-öffentliche Stellen, die Argumentation des Gerichtshofs trifft jedoch auch auf die Aufsicht über öffentliche Stellen zu (vergl. Gola, op.cit., § 22 N. 12 und § 38 N. 31.

47 Abrufbar unter http://www.landtag.nrw.de/haushalt/cd-fm-0310/daten/pdf/2010/hh03/kap000.pdf (06.08.2010).

48 Abrufbar unter http://www.hamburg.de/contentblob/806940/data/einzelplan2.pdf (06.08.2010).

#### *1.3.3.2. Aufsichtsbehörde*

Die Aufsichtsbehörde ist zuständig für die Kontrolle der Ausführung des BDSG und anderer Vorschriften über den Datenschutz durch **nicht-öffentliche Stellen**, soweit diese die automatisierte Verarbeitung personenbezogener Daten oder die Verarbeitung oder Nutzung personenbezogener Daten in oder aus nicht automatisierten Dateien regeln. Sie berät und unterstützt die Beauftragten für Datenschutz und die verantwortlichen Stellen mit Rücksicht auf deren typische Bedürfnisse, § 38 BDSG. Ausserdem leistet sie den Aufsichtsbehörden anderer Mitgliedstaaten der Europäischen Union auf Ersuchen ergänzende Hilfe (Amtshilfe).

Die Aufsichtsbehörden existieren nur auf Landesebene, es gibt keine Bundesaufsichtsbehörde. Daneben existieren der Bundes- sowie die Landesbeauftragten für Datenschutz und Informationsfreiheit, die für die Kontrolle der öffentlichen datenverarbeitenden Stellen zuständig sind und teilweise in **Personalunion** mit der Aufsichtsbehörde existieren.

### 1.3.4. Aufgaben und Kompetenzen

#### *1.3.4.1. Bundesdatenschutzbeauftragter*

Der Bundesdatenschutzbeauftragte **berichtet** dem Deutschen Bundestag und der Öffentlichkeit über wesentliche Entwicklungen des Datenschutzes. Er erstellt **Gutachten** und **Berichte**. Auf Anfrage des Bundestages oder der Bundesregierung, **berät** und erteilt er der Bundesregierung und den öffentlichen Stellen des Bundes, soweit sie nicht als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen, **Empfehlungen** in Fragen des Datenschutzes, § 26 Abs. 1-3 BDSG.

Der Bundesdatenschutzbeauftragte kontrolliert des Weiteren bei den öffentlichen Stellen des Bundes die Einhaltung der Vorschriften des Bundesdatenschutzgesetzes und anderer Vorschriften über den Datenschutz, § 24 Abs. 1 BDSG. Dazu legt das BDSG keine definitiven **Formen für die Kontrolle** fest und beschränkt sich nicht auf die üblichen Informationsmittel des Auskunfts-, Akteneinsichts- und Zutrittsrechts, sondern verpflichtet die kontrollierten Stellen allgemein und umfassend zur Unterstützung. Die wichtigste Form der durchgeführten Kontrollen ist die umfassende Prüfung einer verantwortlichen Stelle durch ein Prüfteam von meinst zwei bis vier Mitgliedern während eines mehrtägigen Zeitraums. Eine solche Prüfung ist mit der Betriebsprüfung durch die Steuerbehörde vergleichbar. In der Regel werden solche Kontrollen vorher angekündigt, dies ist jedoch nicht verpflichtend. Bei der Kontrolle wird der Bundesdatenschutzbeauftragte wird auf eigene Initiative, nach Anrufung durch eine Betroffene Person (§ 21 BDSG) oder auf Ersuchen des Deutschen Bundestags, des Petitionsausschusses, des Innenausschusses oder der Bundesregierung tätig (§ 26 Abs. 2 S. 2 BDSG).[49]

Nach § 4c Abs. 2 S. 2 BDSG ist der Bundesdatenschutzbeauftragt zuständig für die Genehmigung von einzelnen **Übermittlungen** oder bestimmte Arten der Übermittlung personenbezogener Daten durch **Post- und Telekommunikationsunternehmen** an **ausländische Stellen**, die sich nicht in anderen Mitgliedsstaaten der Europäischen Union oder in anderen Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum befinden und nicht Organe oder Einrichtungen der Europäischen Gemeinschaft sind. Die Genehmigung kann erfolgen, wenn die Stelle ausreichende Garantien hinsichtlich des Schutzes des Persönlichkeitsrechts und der Ausübung der damit verbundenen Rechte vorweist.

Der Bundesbeauftragte teilt das Ergebnis seiner Kontrolle der öffentlichen Stelle mit. Mit der Mitteilung kann er **Vorschläge** zur Verbesserung des Datenschutzes, insbesondere zur Beseitigung von festgestellten Mängeln bei der Verarbeitung oder Nutzung personenbezogener Daten verbinden, § 24 Abs. 5 BDSG.

---

[49] Vgl. Heil in Rossnagel, op. cit., S. 766 N. 48.

Stellt er **Verstösse** gegen das BDSG oder gegen andere Vorschriften über den Datenschutz oder sonstige Mängel bei der Verarbeitung oder Nutzung personenbezogener Daten fest, so **beanstandet** er dies:

- bei der Bundesverwaltung gegenüber der zuständigen obersten Bundesbehörde,
- beim Bundeseisenbahnvermögen gegenüber dem Präsidenten,
- bei den aus dem Sondervermögen Deutsche Bundespost durch Gesetz hervorgegangenen Unternehmen, solange ihnen ein ausschliessliches Recht nach dem Postgesetz zusteht, gegenüber deren Vorständen,
- bei den bundesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie bei Vereinigungen solcher Körperschaften, Anstalten und Stiftungen gegenüber dem Vorstand oder dem sonst vertretungsberechtigten Organ und unterrichtet gleichzeitig die zuständige Aufsichtsbehörde

und fordert die betroffene Stelle unter Setzung einer Frist zur Stellungnahme auf, § 24 Abs. 1 BDSG. Die Beanstandung durch den Bundesdatenschutzbeauftragten stellt **keine verbindliche Weisung** dar. Wirkung kann sie also nur dann entfalten, wenn sie einer weisungsberechtigten Stelle zugeht, sie überzeugt und diese sie umsetzt, indem sie die Daten verarbeitende Stelle anweist, den beanstandeten Sachverhalt zu korrigieren.

Es liegt im Ermessen des Bundesdatenschutzbeauftragten, von einer Beanstandung **abzusehen** oder auf eine Stellungnahme der betroffenen Stelle zu **verzichten**, insbesondere wenn es sich um unerhebliche oder inzwischen beseitigte Mängel handelt, § 24 Abs. 2 BDSG.

Wenn die Beanstandung **nicht** zur **Behebung** des Verstosses oder zur **Beseitigung** des Mangels führt, steht es dem Bundesdatenschutzbeauftragten frei (sofern der Gegenstand der Beanstandung es rechtfertigt), sich nach § 26 Abs. 3 S. 1 BDSG an die **Bundesregierung** zu wenden und ihr im Rahmen der Empfehlungen zur Verbesserung des Datenschutzes Vorschläge zu machen. Ausserdem kann er den Fall in seinen **Tätigkeitsbericht** aufnehmen und dort seine Rechtsauffassung darlegen. Letzteres hat sich in der Vergangenheit als nützlich erwiesen, weil der Tätigkeitsbericht sehr eingehend in den Ausschüssen erörtert wird und gelegentlich zu Streitfragen auch Stellung genommen worden ist. In besonders gelagerten Fällen kann sich der Bundesbeauftragte auch nach § 26 Abs. 2 S. 3 BDSG jederzeit schriftlich an den Deutschen Bundestag wenden. Nach § 26 Abs. 1 S. 2 BDSG berichtet der Bundesdatenschutzbeauftragte ausserdem der Öffentlichkeit über wesentliche Entwicklungen des Datenschutzes.

**Einwirkungs**- oder **Sanktionsbefugnisse** stehen dem Bundesdatenschutzbeauftragten **nicht** zu. Allerdings ist der Bundesdatenschutzbeauftragte nach § 23 Abs. 5 S. 7 BDSG befugt, bei Kenntnisnahme von Verstössen gegen das Bundesdatenschutzgesetz, die nach §§ 43, 44 Abs. 1 BDSG eine Straftat darstellen, **Anzeige** zu erstatten.

Die öffentlichen Stellen des Bundes sind nach § 24 Abs. 4 BDSG verpflichtet, den Bundesdatenschutzbeauftragten und seine Beauftragten bei der Erfüllung ihrer Aufgaben zu **unterstützen**. Ihnen ist dabei insbesondere:

- Auskunft zu ihren Fragen sowie Einsicht in alle Unterlagen, insbesondere in die gespeicherten Daten und in die Datenverarbeitungsprogramme, zu gewähren, die im Zusammenhang mit der Kontrolle stehen,
- jederzeit Zutritt in alle Diensträume zu gewähren.

Diese Aufzählung hat jedoch nur **exemplarischen** Charakter. Zu den weiteren Befugnissen gehört i.a. die Überprüfung der praktischen Funktion aller Schutzvorkehrungen an Ort und Stelle.

**Ausnahmen** gelten dabei für Verfassungsschutzbehörden, den Bundesnachrichtendienst, den Militärischen Abschirmdienst und, soweit die Sicherheit des Bundes berührt wird, andere Behörden des Bundesministeriums der Verteidigung, die Behörden der Staatsanwaltschaft und der Polizei sowie öffentliche Stellen der Finanzverwaltung, soweit sie personenbezogene Daten in Erfüllung ihrer gesetzlichen Aufgaben im Anwendungsbereich der Abgabenordnung zur Überwachung und Prüfung speichern. Diese gewähren die Unterstützung **nur dem Bundesbeauftragten** selbst und den von ihm schriftlich besonders Beauftragten. Im **Einzelfall** kann die oberste Bundesbehörde, wenn die Auskunft oder Einsicht die Sicherheit des Bundes oder eines Landes gefährden würde, feststellen, dass die in der obigen Aufzählung dargestellten Unterstützungshandlungen **nicht zu gewähren** sind, § 24 Abs. 4 BDSG.

#### *1.3.4.2. Aufsichtsbehörde*

Die Aufsichtsbehörde berät die betrieblichen **Beauftragten für Datenschutz** (siehe unten) und die **verantwortlichen Stellen** mit Rücksicht auf deren typische Bedürfnisse, § 38 Abs. 1 S. 2 BDSG. Sie Aufsichtsbehörde **kontrolliert** die nicht-öffentlichen Stellen, soweit diese die automatisierte Verarbeitung personenbezogener Daten oder die Verarbeitung oder Nutzung personenbezogener Daten in oder aus nicht automatisierten Dateien regeln. Stellt die Aufsichtsbehörde einen Verstoss gegen dieses Gesetz oder andere Vorschriften über den Datenschutz fest, so ist sie befugt, die Betroffenen hierüber zu **unterrichten**, den Verstoss bei den für die Verfolgung oder Ahndung zuständigen Stellen **anzuzeigen** sowie bei schwerwiegenden Verstössen die **Gewerbeaufsichtsbehörde** zur Durchführung gewerberechtlicher Massnahmen zu unterrichten, § 38 Abs. 1 BDSG.

Die von der Aufsichtsbehörde mit der Kontrolle beauftragten Personen sind nach § 38 Abs. 4 BDSG befugt, soweit es zur Erfüllung der der Aufsichtsbehörde übertragenen Aufgaben erforderlich ist, während der Betriebs- und Geschäftszeiten Grundstücke und Geschäftsräume der Stelle zu **betreten** und dort **Prüfungen** und **Besichtigungen** vorzunehmen. Sie können **geschäftliche Unterlagen** sowie die gespeicherten personenbezogenen Daten und die Datenverarbeitungsprogramme einsehen. Der Auskunftspflichtige hat diese Massnahmen zu dulden.

Die zuständige Aufsichtsbehörde kann nach § 4c Abs. 2 BDSG einzelne **Übermittlungen** oder bestimmte Arten der Übermittlung personenbezogener Daten **an ausländische** Stellen, die sich nicht in anderen Mitgliedsstaaten der Europäischen Union oder in anderen Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum befinden und nicht Organe oder Einrichtungen der Europäischen Gemeinschaft sind, **genehmigen**. Die Genehmigung kann nur erfolgen, wenn die Stelle ausreichende **Garantien** hinsichtlich des Schutzes des Persönlichkeitsrechts und der Ausübung der damit verbundenen Rechte vorweist.

Die Aufsichtsbehörde kann ausserdem zur Sicherstellung dieses Gesetzes und anderer Vorschriften über den Datenschutz Massnahmen zur **Beseitigung festgestellter Verstösse** bei der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten oder technischer oder organisatorischer Mängel **anordnen**. Bei **schwerwiegenden Verstössen** oder Mängeln, insbesondere solchen, die mit einer besonderen Gefährdung des Persönlichkeitsrechts verbunden sind, kann sie die Erhebung, Verarbeitung oder Nutzung oder den Einsatz einzelner Verfahren **untersagen**, wenn die Verstösse oder Mängel entgegen der Anordnung und trotz der Verhängung eines **Zwangsgeldes** nicht in angemessener Zeit beseitigt werden. Sie kann die **Abberufung** des Beauftragten für den Datenschutz verlangen, wenn er die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit nicht besitzt, § 38 Abs. 5 BDSG.

Die der Kontrolle unterliegenden Stellen sowie die mit deren Leitung beauftragten Personen haben der Aufsichtsbehörde auf Verlangen die für die Erfüllung ihrer Aufgaben erforderlichen **Auskünfte** unverzüglich zu erteilen, § 38 Abs. 3 BDSG. Der Auskunftspflichtige kann die Auskunft auf solche Fragen **verwei-**

**gern**, deren Beantwortung ihn selbst oder einen Angehörigen der Gefahr strafgerichtlicher Verfolgung oder eines Verfahrens nach dem Gesetz über Ordnungswidrigkeiten aussetzen würde.

Die Aufsichtsbehörden sind nach § 38 Abs, 1 S. 8 i.V.m. § 23 Abs. 1 S. 4 und § 44 Abs. 2 BDSG befugt, bei Kenntnisnahme von Verstössen gegen das Bundesdatenschutzgesetz, die nach §§ 43, 44 Abs. 1 BDSG eine Straftat darstellen, **Anzeige** zu erstatten.

Daneben veröffentlicht die Aufsichtsbehörde alle zwei Jahre einen Tätigkeitsbericht, § 38 Abs. 1 S. 7 BDSG.

## 1.4. Rolle der Organisationen zum Schutz der Betroffenen

Das BDSG kennt **keine** besonderen Kompetenzen oder Rechte für Verbraucherschutzorganisationen. Wie bereits festgestellt, kommen Verbraucherschutzorganisationen nach §§ 3f. UKlaG ein **Klagerecht** zu, wenn sich Verletzungen datenschutzrechtlicher Organisationspflichten durch nicht-öffentliche Stellen als **verbraucherschutzgesetzwidrige Praktiken** nach § 2 UKlaG darstellen.

Zu der Form, in der sich die Betroffenen an diese Organisationen wenden, bestehen unseres Wissens **keine gesetzlichen Vorschriften**.

## 1.5. Mögliche und vorgeschriebene Aktivitäten der Datenbearbeiter (private und öffentliche)

### 1.5.1. Datenschutzzertifizierung

Das BDSG sieht in § 9a einen sog. „**Datenschutzaudit**“ vor: Zur Verbesserung des Datenschutzes und der Datensicherheit können Anbieter von Datenverarbeitungssystemen und -programmen und datenverarbeitende Stellen ihr Datenschutzkonzept sowie ihre technischen Einrichtungen durch **unabhängige** und **zugelassene Gutachter** prüfen und bewerten lassen sowie das Ergebnis der Prüfung **veröffentlichen**. Es ist vorgesehen, dass die näheren Anforderungen an die Prüfung und Bewertung, das Verfahren sowie die Auswahl und Zulassung der Gutachter durch ein besonderes Gesetz geregelt werden. Ein solches Gesetz wurde jedoch bisher nicht erlassen (s.o.). Es handelt sich um eine Kann-Vorschrift.

### 1.5.2. Meldung von Datensammlungen

Nach § 4d Abs. 1 BDSG sind **Verfahren automatisierter Verarbeitungen** sind vor ihrer Inbetriebnahme von nicht-öffentlichen verantwortlichen Stellen der zuständigen **Aufsichtsbehörde** und von öffentlichen verantwortlichen Stellen des Bundes sowie von den Post- und Telekommunikationsunternehmen dem **Bundesbeauftragten** für den Datenschutz und die Informationsfreiheit nach Massgabe von § 4e BDSG zu melden. Es handelt sich um eine Muss-Vorschrift.

Die Meldepflicht **entfällt** jedoch nach § 4d Abs. 2 und 3 BDSG, wenn die Stelle einen Datenschutzbeauftragten bestellt hat (siehe dort) oder wenn die verantwortliche Stelle personenbezogene Daten für eigene Zwecke erhebt, verarbeitet oder nutzt, hierbei in der Regel höchstens neun Personen ständig mit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten beschäftigt und entweder eine Einwilligung des Betroffenen vorliegt oder die Erhebung, Verarbeitung oder Nutzung für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldver-

hältnisses mit dem Betroffenen erforderlich ist. Diese Ausnahmen greifen jedoch nach § 4d Abs. 4 BDSG **nicht**, wenn es sich **um automatisierte Verarbeitungen** handelt, in denen geschäftsmässig personenbezogene Daten von der jeweiligen Stelle zum Zweck der Übermittlung, der anonymisierten Übermittlung oder der Markt- oder Meinungsforschung gespeichert werden.

Soweit automatisierte Verarbeitungen **besondere Risiken** für die Rechte und Freiheiten der Betroffenen aufweisen, unterliegen sie der **Prüfung vor Beginn** der Verarbeitung (Vorabkontrolle, s.u.), § 4d Abs. 5 BDSG

Sofern Verfahren automatisierter Verarbeitungen **meldepflichtig** sind, sind nach § 4e Abs. 1 BDSG folgende **Angaben** zu machen:

- Name oder Firma der verantwortlichen Stelle,
- Inhaber, Vorstände, Geschäftsführer oder sonstige gesetzliche oder nach der Verfassung des Unternehmens berufene Leiter und die mit der Leitung der Datenverarbeitung beauftragten Personen,
- Anschrift der verantwortlichen Stelle,
- Zweckbestimmungen der Datenerhebung, -verarbeitung oder -nutzung,
- eine Beschreibung der betroffenen Personengruppen und der diesbezüglichen Daten oder Datenkategorien,
- Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können,
- Regelfristen für die Löschung der Daten,
- eine geplante Datenübermittlung in Drittstaaten,
- eine allgemeine Beschreibung, die es ermöglicht, vorläufig zu beurteilen, ob die technischen und organisatorischen Massnahmen, die getroffen wurden, um die Ausführung der Vorschriften dieses Gesetzes zu gewährleisten, zur Gewährleistung der Sicherheit der Verarbeitung angemessen sind.

### 1.5.3. Bestellung betrieblicher Datenschutzbeauftragter

Nach § 4f Abs. 1 BDSG sind öffentliche und nicht-öffentliche Stellen, die personenbezogene Daten **automatisiert** verarbeiten **verpflichtet**, einen Datenschutzbeauftragten zu bestellen. Nicht-öffentliche Stellen müssen dies spätestens innerhalb eines Monats nach Aufnahme ihrer Tätigkeit tun. Dies gilt auch, wenn personenbezogene Daten auf **andere Weise** erhoben, verarbeitet oder genutzt werden und damit in der Regel mindestens 20 Personen beschäftigt sind. Eine **Ausnahme** gilt jedoch für Stellen, die in der Regel höchstens neun Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen. Soweit nicht-öffentliche Stellen automatisierte Verarbeitungen vornehmen, die einer **Vorabkontrolle** unterliegen, oder personenbezogene Daten geschäftsmässig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung automatisiert verarbeiten, haben sie unabhängig von der Anzahl der mit der automatisierten Verarbeitung beschäftigten Personen einen Beauftragten für den Datenschutz zu bestellen.

Zu den Aufgaben des Beauftragten für Datenschutz gehört es nach § 4g Abs. 1 BDSG, auf die **Einhaltung** des BDSG und anderer Vorschriften über den Datenschutz **hinzuwirken**. Dazu kann er sich in Zweifelsfällen an die für die Datenschutzkontrolle bei der verantwortlichen Stelle zuständige Behörde wenden. Er kann die **Beratung** durch die Aufsichtsbehörde nach § 38 Abs. 1 S. 2 BDSG in Anspruch nehmen. Insbesondere muss er:

- die **ordnungsgemässe Anwendung** der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden sollen, überwachen; zu diesem Zweck ist er

über Vorhaben der automatisierten Verarbeitung personenbezogener Daten rechtzeitig zu unterrichten,
- die bei der Verarbeitung personenbezogener Daten **tätigen Personen** durch geeignete Massnahmen mit den Vorschriften des BDSG und anderen Vorschriften über den Datenschutz und mit den jeweiligen besonderen Erfordernissen des Datenschutzes **vertraut machen**.

Auf Antrag macht der Beauftragte für Datenschutz die der Aufsichtsbehörde im Rahmen der Meldepflicht nach § 4d BDSG übermittelten Informationen für Jedermann verfügbar, § 4g Abs. 2 S. 2 BDSG.[50]

Der Beauftragte für den Datenschutz ist nach § 4f Abs. 3 BDSG dem Leiter der öffentlichen oder nicht-öffentlichen Stelle unmittelbar zu unterstellen. Er ist in Ausübung seiner Fachkunde auf dem Gebiet des Datenschutzes **weisungsfrei**. Er darf wegen der Erfüllung seiner Aufgaben nicht benachteiligt werden. Die öffentlichen und nicht-öffentlichen Stellen haben den Beauftragten für den Datenschutz nach § 4f Abs. 5 BDSG bei der Erfüllung seiner Aufgaben zu **unterstützen** und ihm insbesondere, soweit dies zur Erfüllung seiner Aufgaben erforderlich ist, Hilfspersonal sowie Räume, Einrichtungen, Geräte und Mittel zur Verfügung zu stellen. Betroffene können sich jederzeit an den Beauftragten für den Datenschutz wenden.

### 1.5.4. Datenbrief (periodische unaufgeforderte Mitteilung über Datenbearbeitung an Betroffene)

Es gibt keine Regelungen über **periodische** unaufgeforderte Mittelungen an Betroffene. Nach § 19a BDSG haben **öffentliche Stellen** den Betroffenen zu unterrichten, wenn ihn betreffende Daten **ohne seine Kenntnis** erhoben werden. Eine Pflicht zur Benachrichtigung besteht jedoch nicht, wenn der Betroffene auf andere Weise Kenntnis von der Speicherung oder der Übermittlung erlangt hat, die Unterrichtung des Betroffenen einen unverhältnismässigen Aufwand erfordert oder die Speicherung oder Übermittlung der personenbezogenen Daten durch Gesetz ausdrücklich vorgesehen ist. In Fällen, in denen die Auskunft an den Betroffenen nach § 19 Abs. 2-4 BDSG verweigert werden könnte, ist auch die Unterrichtung nicht erforderlich.

**Nicht-öffentliche** Stellen haben den Betroffenen nach § 33 BDSG zu benachrichtigen, wenn erstmals personenbezogene Daten für eigene Zwecke ohne Kenntnis des Betroffenen gespeichert werden. Werden personenbezogene Daten geschäftsmässig zum Zweck der Übermittlung ohne Kenntnis des Betroffenen gespeichert, ist der Betroffene von der erstmaligen Übermittlung und der Art der übermittelten Daten zu benachrichtigen. Der Betroffene ist auch über die Kategorien von Empfängern zu unterrichten, soweit er nach den Umständen des Einzelfalles nicht mit der Übermittlung an diese rechnen muss. Eine Pflicht zur Benachrichtigung besteht jedoch nicht, wenn:

- der Betroffene anders Kenntnis von der Speicherung oder Übermittlung erlangt hat,
- die Daten nur deshalb gespeichert sind, weil sie aufgrund gesetzlicher, satzungsmässiger oder vertraglicher Aufbewahrungsvorschriften nicht gelöscht werden dürfen oder ausschliesslich der

---

[50] Dies gilt nach § 4f Abs. 3 S. 1 BDSG nicht für Verfassungsschutzbehörden, den Bundesnachrichtendienst, den Militärischen Abschirmdienst und, soweit die Sicherheit des Bundes berührt wird, andere Behörden des Bundesministeriums der Verteidigung, die Behörden der Staatsanwaltschaft und der Polizei sowie öffentliche Stellen der Finanzverwaltung, soweit sie personenbezogene Daten in Erfüllung ihrer gesetzlichen Aufgaben im Anwendungsbereich der Abgabenordnung zur Überwachung und Prüfung speichern.

Datensicherung oder der Datenschutzkontrolle dienen und eine Benachrichtigung einen unverhältnismässigen Aufwand erfordern würde,
- die Daten nach einer Rechtsvorschrift oder ihrem Wesen nach, namentlich wegen des überwiegenden rechtlichen Interesses eines Dritten, geheim gehalten werden müssen,
- die Speicherung oder Übermittlung durch Gesetz ausdrücklich vorgesehen ist,
- die Speicherung oder Übermittlung für Zwecke der wissenschaftlichen Forschung erforderlich ist und eine Benachrichtigung einen unverhältnismässigen Aufwand erfordern würde,
- die zuständige öffentliche Stelle gegenüber der verantwortlichen Stelle festgestellt hat, dass das Bekanntwerden der Daten die öffentliche Sicherheit oder Ordnung gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde,
- die Daten für eigene Zwecke gespeichert sind und
    - aus allgemein zugänglichen Quellen entnommen sind und eine Benachrichtigung wegen der Vielzahl der betroffenen Fälle unverhältnismässig ist, oder
    - die Benachrichtigung die Geschäftszwecke der verantwortlichen Stelle erheblich gefährden würde, es sei denn, dass das Interesse an der Benachrichtigung die Gefährdung überwiegt,
- die Daten geschäftsmässig zum Zweck der Übermittlung gespeichert sind und
    - aus allgemein zugänglichen Quellen entnommen sind, soweit sie sich auf diejenigen Personen beziehen, die diese Daten veröffentlicht haben, oder
    - es sich um listenmässig oder sonst zusammengefasste Daten handelt

  und eine Benachrichtigung wegen der Vielzahl der betroffenen Fälle unverhältnismässig ist,
- aus allgemein zugänglichen Quellen entnommene Daten geschäftsmässig für Zwecke der Markt- oder Meinungsforschung gespeichert sind und eine Benachrichtigung wegen der Vielzahl der betroffenen Fälle unverhältnismässig ist.

### 1.5.5. Selbstregulierung

Eine innerbehördliche bzw. innerbetriebliche Selbstkontrolle der verantwortlichen Stellen erfolgt durch die oben dargestellten Beauftragten für Datenschutz.

### 1.5.6. Privacy by design

Es bestehen keine Regelungen betreffend Privacy by design.

# 2. Österreich

## 2.1. Grundsätze des Datenschutzes

Der Datenschutz ist in Österreich im „Bundesgesetz über den Schutz personenbezogener Daten" geregelt; das sogenannte „Datenschutzgesetz" trat im Jahr 2000 in Kraft (**DSG 2000**).[51] Durch die Datenschutz-RL der EU[52] wurde ein vollkommen neues Datenschutzrecht erforderlich.[53]

Im Jahr 2010 wurde eine wichtige Novelle zum DSG in Kraft gesetzt (**DSG-Novelle 2010**).[54] Vorherige Versuche, neue Novellen politisch umzusetzen, waren an negativen Stellungnahmen von Experten und aus der Praxis gescheitert. Insbesondere ging es dabei um die Frage, ob der Grundrechtsschutz auch für juristische Personen (weiter) gelten soll und ob verpflichtend ein betrieblicher Datenschutzbeauftragter eingeführt werden sollte. Die DSG-Novelle 2010 sieht nun beides nicht vor, was ihre Umsetzung politisch erleichterte.

Die wichtigsten **Neuerungen der DSG-Novelle 2010** sind kurz gefasst folgende: Zurechnung der Tätigkeit eines Ermittlungsdienstleisters zum Auftraggeber; Erleichterungen im internationalen Datenverkehr (weitestgehend Gleichstellung der EWR-Staaten mit EU-Mitgliedsstaaten); Präzisierung und Stärkung der verfahrensrechtlichen Durchsetzungsvorschriften; ausdrückliche Regelung der Videoüberwachung (Abschnitt 9a DSG) und allgemeines Auskunftsrecht bei Videoaufzeichnungen. Eine neue Verordnung für das Registrierungsverfahren ist zum 1.1.2012 geplant.

Wichtige Grundlinie der DSG-Novelle 2010 war zudem die Betonung der Selbstverantwortung der datenschutzrechtlichen Auftraggeber. Dies kommt in einer neuen Informationspflicht bei Datenmissbrauch („*Data Breach Notification Duty*"[55]) und in einem neuen vollelektronischen Registrierungsverfahren zum Ausdruck. Die Verantwortung für die inhaltliche Richtigkeit einer Meldung im Register wurde in Richtung auf den Auftraggeber verlagert. Es wurde aber auch die Aufsicht über die Auftraggeber verschärft.

Daneben bestehen **Landesdatenschutzgesetze**, und zwar für die Verwendung manueller Daten, die in Angelegenheiten verarbeitet werden, die in die Gesetzgebungskompetenz der Länder fallen.

Der Bundesgesetzgeber war der Meinung, dass (spätestens) mit der Novelle 2010 die Datenschutz-RL der EU vollständig umgesetzt ist; eine Ausnahme betraf nur die durch die Länder verarbeiteten

---

51 BGBl. I 1999/165.

52 Richtlinie 95/46/EG.

53 Siehe Mayer-Schönberger/Brandl, Datenschutzgesetz 2000, 2. Auflage, Linde : Wien 2006, S. 22, 47. Die Autoren sind sehr kritisch, ob mit der Version des DSG aus dem Jahr 2006 wirklich alle Bestimmungen der RL umgesetzt wurden. Es wird angeraten, stets zusätzlich den Text der Richtlinie zu konsultieren. Nach Ansicht des Bundesgesetzgebers ist die RL mit 2010 vollständig umgesetzt (mit einer Ausnahme, siehe sogleich im Text). Eine genauere, wissenschaftliche Auseinandersetzung mit dem Stand der Richtlinienumsetzung in Österreich scheint nach wie vor zu fehlen bzw. ist dem ISDC nicht zugänglich.

54 BGBl. I 2009/133.

55 Diese Pflicht gibt es angeblich sonst nur noch in Deutschland und sonst bisher nicht in Europa.

manuellen Daten. Aufgrund des Fehlens einer Verfassungsmehrheit konnte der Bundesgesetzgeber aber die Zuständigkeit in diesem Bereich nicht verändern und dieser Bereich verbleibt, auch nach Ansicht des Bundesgesetzgebers, in einem **nicht richtlinienkonformen** Zustand.[56]

### 2.1.1. Zweckbindung

Die Datenermittlung muss im Rahmen von festgelegten, eindeutigen und rechtmäßigen **Zwecken** erfolgen und die Weiterverwendung darf nicht in einer mit diesen Zwecken unvereinbaren Weise stattfinden (§ 6 DSG). Die Weiterverwendung für wissenschaftliche oder statistische Zwecke ist nach Massgabe der §§ 46 und 47 DSG zulässig. Die verwendeten Daten müssen für den Zweck der Datenanwendung wesentlich sein und dürfen nicht über diesen Zweck hinausgehen. Dabei müssen sie so verwendet werden, dass sie im Hinblick auf den Verwendungszweck im Ergebnis sachlich richtig und, wenn nötig, auf den neuesten Stand gebracht sind. Sie dürfen nur solange in personenbezogener Form aufbewahrt werden, als dies für die Erreichung der Zwecke, für die sie ermittelt wurden, erforderlich ist. Eine längere Aufbewahrungsdauer kann sich aus besonderen gesetzlichen, insbesondere archivrechtlichen Vorschriften ergeben.[57]

### 2.1.2 Grundsätze Datenbearbeitung

Das Grundrecht auf Datenschutz steht ganz am Beginn des DSG und steht im Rang einer Verfassungsbestimmung. Jedermann hat, insbesondere auch im Hinblick auf die Achtung seines Privat- und Familienlebens, Anspruch auf **Geheimhaltung** der ihn betreffenden personenbezogenen Daten, soweit ein schutzwürdiges Interesse daran besteht. Das Bestehen eines solchen Interesses ist ausgeschlossen, wenn Daten infolge ihrer allgemeinen Verfügbarkeit oder wegen ihrer mangelnden Rückführbarkeit auf den Betroffenen einem Geheimhaltungsanspruch nicht zugänglich sind.

Soweit die Verwendung von personenbezogenen Daten nicht im lebenswichtigen Interesse des Betroffenen oder mit seiner Zustimmung erfolgt, sind **Beschränkungen** des Anspruchs auf Geheimhaltung nur zur Wahrung überwiegender berechtigter Interessen eines anderen zulässig, und zwar bei Eingriffen einer staatlichen Behörde nur auf Grund von Gesetzen, die aus den in Art. 8 Abs. 2 der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten (EMRK), BGBl. Nr. 210/1958, genannten Gründen notwendig sind. Derartige Gesetze dürfen die Verwendung von Daten, die ihrer Art nach **besonders schutzwürdig** sind, nur zur Wahrung wichtiger öffentlicher Interessen vorsehen und müssen gleichzeitig angemessene Garantien für den Schutz der Geheimhaltungsinteressen der Betroffenen festlegen. Auch im Falle zulässiger Beschränkungen darf der Eingriff in das Grundrecht jeweils nur in der gelindesten, zum Ziel führenden Art vorgenommen werden.

Das DSG geht grundsätzlich vom **Verbotsprinzip** aus. Das bedeutet, die Verwendung von personenbezogenen Daten ist grundsätzlich verboten, falls nicht die mehrstufige Zulässigkeitsprüfung im Rahmen der §§ 6 bis 9 DSG ein positives Resultat ergibt. § 6 enthält in Form eines Katalogs die **wesentlichsten Grundsätze**, die bei Prüfung der Zulässigkeit der Datenanwendung zu beachten sind (insbesondere Treu und Glauben, Zweck, s. oben, 2.1.1.). § 6 ist eng an die DS-RL angelehnt. § 7

---

[56] Erläuternder Abschlussbericht zur DSG-Novelle 2010; abgedruckt bei Pollirer/Weiss/Knyrim, Datenschutzgesetz in der Fassung der Novelle 2010, Manz : Wien 2010, S. 12.

[57] Zu allem § 6 Abs. 1 DSG.

enthält die **konkrete Frage** nach der gesetzlichen Zuständigkeit oder der rechtlichen Befugnis des Auftraggebers zur Durchführung der bestimmten Datenanwendung sowie die Forderung, dass die schutzwürdigen Geheimhaltungsinteressen der Betroffenen nicht verletzt werden dürfen. Für die **nicht sensiblen Daten** enthält § 8 eine Generalklausel sowie einzelen Beispiele, nach denen schutzwürdige Interessen des betroffenen nicht verletzt sind. Für die **sensiblen Daten** enthält § 9 dagegen eine taxative (erschöpfende) Aufzählung der zulässigen Verwendungsfälle.

Der allgemeinste Grundsatz des österreichischen Datenschutzrechtes ist, dass Daten nur nach **Treu und Glauben** und auf rechtmäßige Weise verwendet werden dürfen (§ 6 DSG). Wichtig für die nähere Bestimmung des Grundsatzes von Treu und Glauben sind vor allem die Bestimmungen des 4. Abschnittes des DSG über die Pulizität der Datenverwendung. Aus dem Gebot der Verwendung in rechtmässiger Weise ergibt sich unter anderem auch, dass der Auftraggeber eine ausreichende rechtliche Befugnis bzw. Zuständigkeit für jene Art der Benützung von Daten, die er mit seiner Datenanwendung bewzeckt, besitzen muss.

### 2.1.3. Erkennbarkeit/Transparenz, Einwilligung

Die Frage der Erkennbarkeit, Transparenz und der Einwilligung wird im Rahmen der Interessensabwägung berücksichtigt (s. 2.1.2., 2.1.4.).

### 2.1.4. Bearbeitung besonders schützenswerter Daten

Daten dürfen nur verarbeitet werden, soweit der Zweck und Inhalt der Datenanwendung von den gesetzlichen Zuständigkeiten oder rechtlichen Befugnissen des **konkreten Auftraggebers** gedeckt sind und die **schutzwürdigen Geheimhaltungsinteressen** der Betroffenen nicht verletzen.[58] Die zulässige Datenübermittlung erfordert drei Voraussetzungen: die Daten müssen aus einer gemäss § 7 Abs. 1 DSG zulässigen Datenanwendung stammen (1.), der Empfänger muss dem Übermittelnden seine ausreichende gesetzliche Zuständigkeit oder rechtliche Befugnis - soweit diese nicht ausser Zweifel steht - im Hinblick auf den Übermittlungszweck glaubhaft machen (2.) und die schutzwürdigen Geheimhaltungsinteressen des Betroffenen dürfen nicht durch den Zweck und Inhalt der Übermittlung verletzt werden (3.).[59] Die Zulässigkeit einer Datenverwendung setzt voraus, dass die dadurch verursachten Eingriffe in das Grundrecht auf Datenschutz nur im erforderlichen Ausmass und mit den gelindesten zur Verfügung stehenden Mitteln erfolgen und dass die Grundsätze des § 6 DSG eingehalten werden.[60]

Die schutzwürdigen Geheimhaltungsinteressen des Betroffenen dürfen bei der Verwendung der Daten nicht verletzt werden. Dabei ist zu unterscheiden, ob es sich um sensible[61] oder nicht-sensible[62] Daten handelt.

---

58 § 7 Abs. 1 DSG.

59 § 7 Abs. 2 DSG.

60 § 7 Abs. 3 DSG.

61 § 9 DSG: Schutzwürdige Geheimhaltungsinteressen werden bei der Verwendung sensibler Daten ausschließlich dann nicht verletzt, wenn eine der folgenden Konstellationen vorliegt: wenn der Betroffene die Daten offenkundig selbst öffentlich gemacht hat (1), die Daten in nur indirekt personenbezogener Form verwendet werden (2), sich die Ermächtigung oder Verpflichtung zur Verwendung aus gesetzlichen Vorschriften ergibt, soweit diese der Wahrung eines wichtigen öffentlichen Interesses dienen (3), die Verwendung durch Auftraggeber des öffentlichen Bereichs in

### 2.1.5. Datensicherheit

Die Datensicherheit muss durch Massnahmen für alle Organisationseinheiten eines Auftraggebers oder Dienstleisters gewährleistet werden und das Datengeheimnis eingehalten werden.[63]

### 2.1.6. Grenzüberschreitende Bekanntgabe

Die **grenzüberschreitende Bekanntgabe** ist grundsätzlich dann genehmigungsfrei, wenn die Übermittlung und Überlassung der Daten an einen Empfänger im europäischen Wirtschaftsraum, welcher dem Recht der Europäischen Gemeinschaften unterworfen ist oder an einen Empfänger in einem Drittstaat mit angemessenem Datenschutz erfolgt (§ 12 DSG).[64] Fällt die Übermittlung und Überlassung der Daten nicht unter § 12 DSG, muss gemäss § 13 DSG eine Genehmigung der

---

Erfüllung ihrer Verpflichtung zur Amtshilfe geschieht (4), Daten verwendet werden, die ausschließlich die Ausübung einer öffentlichen Funktion durch den Betroffenen zum Gegenstand haben (5), der Betroffene seine Zustimmung zur Verwendung der Daten ausdrücklich erteilt hat, wobei ein Widerruf jederzeit möglich ist und die Unzulässigkeit der weiteren Verwendung der Daten bewirkt (6), die Verarbeitung oder Übermittlung zur Wahrung lebenswichtiger Interessen des Betroffenen notwendig ist und seine Zustimmung nicht rechtzeitig eingeholt werden kann (7), die Verwendung der Daten zur Wahrung lebenswichtiger Interessen eines anderen notwendig ist (8), die Verwendung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen des Auftraggebers vor einer Behörde notwendig ist und die Daten rechtmäßig ermittelt wurden (9), Daten für private Zwecke gemäß § 45 oder für wissenschaftliche Forschung oder Statistik gemäß § 46, zur Benachrichtigung oder Befragung des Betroffenen gemäß § 47 oder im Katastrophenfall gemäß § 48a verwendet werden (10), die Verwendung erforderlich ist, um den Rechten und Pflichten des Auftraggebers auf dem Gebiet des Arbeits- oder Dienstrechts Rechnung zu tragen, und sie nach besonderen Rechtsvorschriften zulässig ist, wobei die dem Betriebsrat nach dem Arbeitsverfassungsgesetz zustehenden Befugnisse im Hinblick auf die Datenverwendung unberührt bleiben (11), die Daten zum Zweck der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder -behandlung oder für die Verwaltung von Gesundheitsdiensten erforderlich ist, und die Verwendung dieser Daten durch ärztliches Personal oder sonstige Personen erfolgt, die einer entsprechenden Geheimhaltungspflicht unterliegen (12), nicht auf Gewinn gerichtete Vereinigungen mit politischem, philosophischem, religiösem oder gewerkschaftlichem Tätigkeitszweck Daten, die Rückschlüsse auf die politische Meinung oder weltanschauliche Überzeugung natürlicher Personen zulassen, im Rahmen ihrer erlaubten Tätigkeit verarbeiten und es sich hierbei um Daten von Mitgliedern, Förderern oder sonstigen Personen handelt, die regelmäßig ihr Interesse für den Tätigkeitszweck der Vereinigung bekundet haben; diese Daten dürfen, sofern sich aus gesetzlichen Vorschriften nichts anderes ergibt, nur mit Zustimmung der Betroffenen an Dritte weitergegeben werden (13).

62 § 8 Abs. 1 DSG: Schutzwürdige Geheimhaltungsinteressen sind bei Verwendung nicht-sensibler Daten in vier Konstellationen nicht verletzt, nämlich wenn eine ausdrückliche gesetzliche Ermächtigung oder Verpflichtung zur Verwendung der Daten besteht (1), der Betroffene der Verwendung seiner Daten zugestimmt hat (wobei ein Widerruf jederzeit möglich ist und die Unzulässigkeit der weiteren Verwendung der Daten bewirkt) (2), lebenswichtige Interessen des Betroffenen die Verwendung erfordern (3) oder wenn überwiegende berechtigte Interessen des Auftraggebers oder eines Dritten die Verwendung erfordern (4). Abs. 4 sieht eine besondere und strengere Regelung für Daten über gerichtlich oder verwaltungsbehördlich strafbare Handlungen oder Unterlassungen vor.

63 §§ 14 und 15 DSG.

64 Abs. 1 und 2 DSG. Abs. 3-5 erläutern weitere zulässige Konstellationen.

Datenschutzkommission eingeholt werden. Die betroffene Person hat das Recht jederzeit **Auskunft** über die zu ihrer Person verarbeitenden Daten zu erhalten.[65]

### 2.1.7. Auskunft

Jedermann hat, soweit ihn betreffende **personenbezogene Daten** zur automationsunterstützten Verarbeitung oder zur Verarbeitung in manuell, dh. ohne Automationsunterstützung geführten Dateien bestimmt sind, nach Maßgabe gesetzlicher Bestimmungen das **Recht auf Auskunft** darüber, wer welche Daten über ihn verarbeitet, woher die Daten stammen, und wozu sie verwendet werden, insbesondere auch, an wen sie übermittelt werden, und das **Recht auf Richtigstellung** unrichtiger Daten und das Recht auf Löschung unzulässigerweise verarbeiteter Daten (§ 1 DSG).

### 2.1.8. Verhältnis von Datenschutz und Technologieentwicklung

Das österreichische DSG ist grundsätzlich **technologieneutral** ausgestaltet. Die automatisierten Einzelentscheidungen und die Informationsverbundsysteme[66] stellen besondere Verwendungsarten von Daten dar und sind deshalb spezifisch in § 49 und § 50 DSG geregelt. Im Bereich neuer Technologien enthält das Gesetz zum teil spezifische Vorschriften, so im Bereich der Videoüberwachung[67] (2.9.1.1.). Als weiteres Beispiel zum Verhältnis von Datenschutz und Technologieentwicklung wird kurz die Behandlung von Google Street View behandelt (2.9.1.2.).

#### *2.1.8.1. Videoüberwachung*

Videoüberwachung im Sinne des österreichischen DSG bezeichnet die systematische, insbesondere fortlaufende **Feststellung von Ereignissen**, die ein bestimmtes Objekt (überwachtes Objekt) oder eine bestimmte Person (überwachte Person) betreffen, durch technische Bildaufnahme- oder Bildübertragungsgeräte.

Mit der Novelle zur StMV (Standard- und Musterverordnung) 2004[68] wurde eine neue **Standard-anwendung** (sogenannte SA032, "Videoüberwachung") geschaffen. Damit sind Videoüberwachungen in Banken, Juweliergeschäften (sowie im Handel mit Antiquitäten und Kunstgegenständen, Gold- und Silberschmiede), Trafiken und Tankstellen von der Meldepflicht ausgenommen, wenn sie sich innerhalb des Standards bewegen (insbesondere betreffend der überwachten Bereiche und der Aufzeichnungsdauer von 72 Stunden). Mit dem Standard "Videoüberwachung" wird schließlich auch die Überwachung von "bebauten Privatgrundstücken (samt Hauseingang und Garage)" von der Meldepflicht ausgenommen, wenn der Standard nicht verlassen wird (soweit insbesondere die Aufzeichnungsdauer von 72 Stunden nicht überschritten wird).

---

65 § 26 Abs. 1 DSG. Dasselbe gilt für Personengemeinschaften. Die diesbezüglichen Ausnahmen und Bedingungen sind in Abs. 2 ff. geregelt.

66 § 4 Ziff. 13 DSG erläutert den Begriff „Informationsverbundsystem“ folgendermassen: „die gemeinsame Verarbeitung von Daten in einer Datenanwendung durch mehrere Auftraggeber und die gemeinsame Benützung der Daten in der Art, dass jeder Auftraggeber auch auf jene Daten im System Zugriff hat, die von den anderen Auftraggebern dem System zur Verfügung gestellt wurden.“

67 Siehe zu allem §§ 50a-50e DSG.

68 BGBl. II Nr. 152/2010.

Für Videoüberwachung gelten die §§ 6 und 7 DSG, insbesondere der Verhältnismäßigkeitsgrundsatz (§ 7 Abs. 3). **Rechtmäßige Zwecke** einer Videoüberwachung sind jedoch (vorbehaltlich des § 50a Abs. 5) nur der Schutz des überwachten Objekts oder der überwachten Person oder die Erfüllung rechtlicher Sorgfaltspflichten, jeweils einschließlich der Beweissicherung. Persönlichkeitsrechte nach § 16 Allgemeinem Bürgerlichem Gesetzbuch bleiben unberührt.

Ein Betroffener ist durch eine Videoüberwachung dann nicht in seinen **schutzwürdigen Geheimhaltungsinteressen** (§ 7 Abs. 2 Z 3) verletzt, wenn (1.) diese im lebenswichtigen Interesse einer Person erfolgt, oder (2.) Daten über ein Verhalten verarbeitet werden, das ohne jeden Zweifel den Schluss zulässt, dass es darauf gerichtet war, öffentlich wahrgenommen zu werden, oder (3.) er der Verwendung seiner Daten im Rahmen der Überwachung ausdrücklich zugestimmt hat.

Ein Betroffener ist darüber hinaus durch eine Videoüberwachung ausschließlich dann nicht in seinen **schutzwürdigen Geheimhaltungsinteressen** (§ 7 Abs. 2 Z 3) verletzt, wenn sie nicht im Rahmen der Vollziehung hoheitlicher Aufgaben erfolgt und (1.) bestimmte Tatsachen die Annahme rechtfertigen, das überwachte Objekt oder die überwachte Person könnte das Ziel oder der Ort eines gefährlichen Angriffs werden, oder (2.) unmittelbar anwendbare Rechtsvorschriften des Völker- oder des Gemeinschaftsrechts, Gesetze, Verordnungen, Bescheide oder gerichtliche Entscheidungen dem Auftraggeber spezielle Sorgfaltspflichten zum Schutz des überwachten Objekts oder der überwachten Person auferlegen, oder (3.) sich die Überwachung in einer bloßen Echtzeitwiedergabe von das überwachte Objekt/die überwachte Person betreffenden Ereignisse erschöpft, diese also weder gespeichert (aufgezeichnet) noch in sonst einer anderen Form weiterverarbeitet werden (Echtzeitüberwachung), und sie zum Zweck des Schutzes von Leib, Leben oder Eigentum des Auftraggebers erfolgt.

Mit einer Videoüberwachung nach den zuvor festgehaltenen Bedingungen dürfen nicht Ereignisse an Orten festgestellt werden, die zum **höchstpersönlichen Lebensbereich** eines Betroffenen zählen. Weiters ist die Videoüberwachung zum Zweck der **Mitarbeiterkontrolle** an Arbeitsstätten untersagt.

**Schutzwürdige Geheimhaltungsinteressen** Betroffener sind auch dann **nicht verletzt**, wenn durch Videoüberwachung aufgezeichnete Daten über eine Verwendung entsprechend den gerade erklärten Bedingungen hinaus in folgenden Fällen übermittelt werden: (1.) an die zuständige Behörde oder das zuständige Gericht, weil beim Auftraggeber der begründete Verdacht entstanden ist, die Daten könnten eine von Amts wegen zu verfolgende gerichtlich strafbare Handlung dokumentieren, oder (2.) an Sicherheitsbehörden zur Ausübung der diesen durch andere Gesetze eingeräumten Befugnisse, auch wenn sich die Handlung oder der Angriff nicht gegen das überwachte Objekt oder die überwachte Person richtet. Die Befugnisse von Behörden und Gerichten zur Durchsetzung der Herausgabe von Beweismaterial und zur Beweismittelsicherung sowie damit korrespondierende Verpflichtungen des Auftraggebers bleiben unberührt.

Mit einer Videoüberwachung gewonnene Daten von Betroffenen dürfen nicht automationsunterstützt mit anderen Bilddaten abgeglichen und nicht nach sensiblen Daten als Auswahlkriterium durchsucht werden.

Videoüberwachungen unterliegen der Meldepflicht. Im Regelfall unterliegen sie der **Vorabkontrolle** (§ 18 Abs. 2).

Bestimmungen zur **Vorabkontrolle** lassen sich in § 18 Abs. 2 und § 20 finden. Wenn bei der Videoüberwachung unter Umständen (auch) strafrechtlich relevante Daten aufgezeichnet werden, darf eine Videoüberwachungsanlage erst nach Abschluss des Registrierungsverfahrens in Betrieb genommen werden bzw. erst dann, wenn sich das Datenverarbeitungsregister innerhalb von zwei

Monaten nach Einlangen der Meldung nicht geäußert hat (Vorabkontrollverfahren). Es gibt keinen Bestandschutz für Altanlagen

Der Auftraggeber einer Videoüberwachung hat diese geeignet zu kennzeichnen. Aus der Kennzeichnung hat jedenfalls der Auftraggeber eindeutig hervorzugehen, es sei denn, dieser ist den Betroffenen nach den Umständen des Falles bereits bekannt. Die Kennzeichnung hat örtlich derart zu erfolgen, dass jeder potentiell Betroffene, der sich einem überwachten Objekt oder einer überwachten Person nähert, tunlichst die Möglichkeit hat, der Videoüberwachung auszuweichen.

Abweichend von den allgemeinen Bestimmungen ist dem **Auskunftswerber**, nachdem dieser den Zeitraum, in dem er möglicherweise von der Viedo-Überwachung betroffen war, und den Ort möglichst genau benannt und seine Identität in geeigneter Form nachgewiesen hat, **Auskunft** über die zu seiner Person verarbeiteten Daten **durch Übersendung einer Kopie** der zu seiner Person verarbeiteten Daten in einem üblichen technischen Format zu gewähren. Alternativ kann der Auskunftswerber eine **Einsichtnahme** auf Lesegeräten des Auftraggebers verlangen, wobei ihm auch in diesem Fall die Ausfolgung einer Kopie zusteht. Die übrigen Bestandteile der Auskunft (verfügbare Informationen über die Herkunft, Empfänger oder Empfängerkreise von Übermittlungen, Zweck, Rechtsgrundlagen sowie allenfalls Dienstleister) sind auch im Fall der Überwachung schriftlich zu erteilen, wenn nicht der Auskunftswerber einer mündlichen Auskunftserteilung zustimmt.

In dem Fall, dass eine Auskunft wegen überwiegender berechtigter Interessen Dritter oder des Auftraggebers nicht in der beschriebenen Form erteilt werden kann, hat der Auskunftswerber Anspruch auf eine schriftliche Beschreibung seines von der Überwachung verarbeiteten Verhaltens oder auf eine Auskunft unter Unkenntlichmachung der anderen Personen. In Fällen der Echtzeitüberwachung ist ein Auskunftsrecht ausgeschlossen.

Sollte eine **betroffene Person** der Ansicht sein, eine Videoüberwachungsanlage ist nicht datenschutzkonform in Betrieb, so kann sie Schritte unternehmen. Sie kann sich mit einer Eingabe (§ 30 DSG) an die **Datenschutzkommission** wenden und damit ein Kontroll- und Ombudsmannverfahren einleiten. Ziel des Verfahrens ist es, den rechtmäßigen Zustand herzustellen. Dazu erhebt die Datenschutzkommission den Sachverhalt und zieht daraus rechtliche Schlüsse. Dies kann darin bestehen, dass nichts weiter zu veranlassen ist (wenn zB eine Attrappe in Gebrauch ist oder eine Aufzeichnung der Bilddaten nicht stattfindet), dass zur Meldung aufgefordert wird (im Falle der Aufzeichnung der Bilddaten; auch unter Androhung einer Verwaltungsstrafe nach § 52 Abs. 2 Z 1 bzw. Z 3 DSG 2000) oder dass aufgefordert wird, die Kamera(s) zu entfernen (für den Fall, dass diese jedenfalls nicht zulässig ist). Sollte eine Meldung eingebracht werden, wird im anschließenden Meldeverfahren geprüft, ob die Anlage zulässig ist. Der Einschreiter im Verfahren nach § 30 DSG 2000 hat nach Abs. 7 den Anspruch, darüber informiert zu werden, wie mit seiner Eingabe verfahren wurde. Eine Eingabe nach § 30 DSG 2000 sollte den Sachverhalt genau beschreiben, möglichst unter Beigabe von Beweismitteln wie Fotos etc. sowie die Kontaktdaten des mutmaßlichen Betreibers der Videoüberwachungsanlage enthalten. Dieser wird im Lauf des Verfahrens mit den Vorwürfen konfrontiert (wobei die **Anonymität des Einschreiters** gewahrt bleibt, wenn dafür besondere Gründe vorliegen - z.B. Arbeitgeber-Arbeitnehmer-Verhältnis; Mieter-Vermieter-Verhältnis).[69]

---

[69] So der Ratgeber der Datenschutzkommission auf http://www.dsk.gv.at/site/6355/default.aspx (Stand November 2010).

#### *2.1.8.2. Google Street-View in Österreich*

Aufgrund von öffentlich sowie gegenüber der österreichischen Datenschutzkommission abgegebenen Erklärungen von Google über die Ermittlung von W-LAN Daten im Zuge der Datensammlung für "Google Street View" hat die Datenschutzkommission am 21. Mai 2010 ein amtliches Prüfverfahren zur Klärung des Sachverhalts eingeleitet.

Bis zu dieser Klärung die Weiterführung der gesamten Datenanwendung "Google Street View" untersagt, sodass derzeit[70] keine der im Zusammenhang mit Google Street View in Österreich bereits ermittelten Daten weiter verarbeitet werden dürfen und keine neuen Daten in Österreich ermittelt werden dürfen.

Zur Klärung des Sachverhalts wurde Google Inc., USA, als registrierter Auftraggeber der Datenanwendung "Google Street View" im amtswegigen Prüfverfahren aufgefordert, bis zum 7. Juni 2010 eine genaue technische Beschreibung der Datenermittlungsvorgänge vorzulegen, sowie einen ausführlichen Fragebogen zu beantworten, dessen Inhalt im Wege der „Art. 29 Gruppe“ auch mit den anderen unabhängigen Datenschutz-Kontrollstellen der EU-Mitgliedstaaten koordiniert wurde.

Sobald die von Google eingeforderten Auskünfte eingelangt und geprüft wurden und insbesondere mehr Klarheit darüber besteht, ob tatsächlich personenbezogene Daten ermittelt wurden, die in der Meldung an das Datenverarbeitungsregister nicht enthalten sind, wird die Datenschutzkommission über weitere Schritte entscheiden.[71]

### 2.1.9. Private und öffentliche Datenverwendung

Das österreichische DSG unterscheidet nicht ausdrücklich zwischen **staatlichen** und **privaten** Datenbearbeitern. Das DSG unterscheidet zwischen **Auftraggeber** und **Dienstleister**.[72] Es gibt jedoch Bestimmungen im DSG, welche entweder nur auf private oder nur auf staatliche Datenbearbeiter

---

70 September 2010.

71 So die Information unter http://www.dsk.gv.at/site/6733/default.aspx (September 2010).

72 Unter „**Auftraggeber**“ wird gemäss § 4 Ziff. 4 DSG folgendes verstanden: „natürliche oder juristische Personen, Personengemeinschaften oder Organe einer Gebietskörperschaft beziehungsweise die Geschäftsapparate solcher Organe, wenn sie allein oder gemeinsam mit anderen die Entscheidung getroffen haben, Daten zu verwenden (Z 8), unabhängig davon, ob sie die Daten selbst verwenden (Z 8) oder damit einen Dienstleister (Z 5) beauftragen. Sie gelten auch dann als Auftraggeber, wenn der mit der Herstellung eines Werkes beauftragte Dienstleister (Z 5) die Entscheidung trifft, zu diesem Zweck Daten zu verwenden (Z 8), es sei denn dies wurde ihm ausdrücklich untersagt oder der Beauftragte hat auf Grund von Rechtsvorschriften oder Verhaltensregeln über die Verwendung eigenverantwortlich zu entscheiden. „**Dienstleister**“ werden gemäss § 4 Ziff. 5 DSG wie folgt definiert: „natürliche oder juristische Personen, Personengemeinschaften oder Organe einer Gebietskörperschaft beziehungsweise die Geschäftsapparate solcher Organe, wenn sie Daten nur zur Herstellung eines ihnen aufgetragenen Werkes verwenden.“

Anwendung finden.[73] In § 5 DSG ist definiert, was unter öffentlichen und was unter privaten Auftraggebern verstanden wird.

## 2.2. Durchsetzungsrechte der Datenschutzanliegen für Betroffene

### 2.2.1. Datenbearbeitung durch Private

Das Grundrecht auf Datenschutz ist mit **unmittelbarer Drittwirkung** ausgestattet. Das bedeutet, dass ein Betroffener im Privatrechtsverkehr direkt mit Klage beim (zivilen) Landesgericht gegen einen Auftraggeber vorgehen kann.

#### *2.2.1.1 Sperrung, Berichtigung, Vernichtung usw.*

Die Rechte auf Sperrung, Berichtigung, Vernichtung ergeben sich soweit ersichtlich aus dem DSG (§ 27-29 DSG). Zu den weiteren Ansprüchen siehe unten zur Datenbearbeitung durch öffentliche Bearbeiter.

Ein Recht auf „Vermerkung" kennt das DSG in der in der Schweiz vorgesehenen Form soweit ersichtlich nicht.

Neu seit dem Jahr 2010 findet sich eine Informationspflicht bei Datenmissbrauch („*Data Breach Notification Duty*"[74], § 24 DSG).

Der Auftraggeber einer Datenanwendung hat aus Anlaß der Ermittlung von Daten die Betroffenen in geeigneter Weise über den Zweck der Datenanwendung, für die die Daten ermittelt werden, und über Namen und Adresse des Auftraggebers, zu **informieren**, sofern diese Informationen dem Betroffenen nach den Umständen des Falles nicht bereits vorliegen.

Im Jahr 2010 wurde eine Informationspflicht bei Kenntniss vom Datenmissbrauch durch den Datenbearbeiter eingeführt: Wird dem Auftraggeber bekannt, dass Daten aus einer seiner Datenanwendungen systematisch und schwerwiegend unrechtmäßig verwendet wurden und den Betroffenen Schaden droht, hat er darüber unverzüglich die Betroffenen in geeigneter Form zu **informieren**. Diese Verpflichtung besteht nicht, wenn die Information angesichts der Drohung eines nur geringfügigen Schadens der Betroffenen einerseits oder der Kosten der Information aller Betroffenen andererseits einen unverhältnismäßigen Aufwand erfordert (§ 24a Abs. 2 DSG).

#### *2.2.1.2. Andere: Schadenersatz*

Aus dem DSG ergibt sich auche in **Schadenersatzanspruch** (§ 33 DSG). Ein Auftraggeber oder Dienstleister, der Daten **schuldhaft** entgegen den Bestimmungen des DSG verwendet, hat dem Betroffenen den **erlittenen Schaden** nach den allgemeinen Bestimmungen des bürgerlichen Rechts zu ersetzen. Werden durch die öffentlich zugängliche Verwendung der in § 18 Abs. 2 Z 1 bis 3 genannten Datenarten schutzwürdige Geheimhaltungsinteressen eines Betroffenen in einer Weise verletzt, die einer Eignung zur **Bloßstellung** gemäß § 7 Abs. 1 des Mediengesetzes, BGBl. Nr. 314/1981, gleichkommt, so gilt diese Bestimmung auch in Fällen, in welchen die öffentlich zugängliche

---

[73] Wie z.B. die besondere Verwendung von Daten für **private Zwecke** in § 45 und für publizistische Tätigkeiten in § 48 DSG nur für Privatpersonen ausgestaltet sind und die besondere Verwendung von Daten für wissenschaftliche Forschung in § 46 und die Verwendung im Katastrophenfall in § 48a nur die öffentlichen Auftraggeber betrifft.

[74] Diese Pflicht gibt es angeblich sonst nur noch in Deutschland und sonst bisher nicht in Europa.

Verwendung **nicht** in Form der **Veröffentlichung** in einem Medium geschieht. Der Anspruch auf angemessene Entschädigung für die **erlittene Kränkung** (immaterieller Schaden) ist gegen den Auftraggeber der Datenverwendung geltend zu machen. Der Auftraggeber und der Dienstleister haften auch für das **Verschulden ihrer Leute**, soweit deren Tätigkeit für den Schaden ursächlich war. Der Auftraggeber kann sich von seiner **Haftung befreien**, wenn er nachweist, daß der Umstand, durch den der Schaden eingetreten ist, ihm und seinen Leuten nicht zur Last gelegt werden kann. Dasselbe gilt für die **Haftungsbefreiung des Dienstleisters**. Für den Fall eines **Mitverschuldens** des Geschädigten oder einer Person, deren Verhalten er zu vertreten hat, gilt § 1304 Allgemeines Bürgerliches Gesetzbuch.

#### *2.2.1.3 Verfahren*

Ansprüche wegen Verletzung der Rechte einer Person oder Personengemeinschaft auf **Geheimhaltung, Richtigstellung oder Löschung** gegen einen privatrechtlichen Auftraggeber sind auf dem **Zivilrechtsweg** geltend zu machen. Handelt es sich um eine gesetzeswidrige Datenverwendung, hat der Betroffenen Anspruch auf **Unterlassung** und **Beseitigung** des Zustandes. Zur Sicherung der Ansprüche auf Unterlassung können **einstweilige Verfügungen** erlassen werden.

Gegen Rechtsträger, die in **Formen des Privatrechts** eingerichtet sind, ist das Grundrecht auf Datenschutz (mit **Ausnahme des Rechtes auf Auskunft)** auf dem **Zivilrechtsweg** geltend zu machen. In allen übrigen Fällen und für das Reht auf Auskunft ist die **Datenschutzkommission** (DSK) zur Entscheidung zuständig (§ 1 Abs.5 DSG).

Für den öffentlichen Bereich ist die DSK zur Gänze zuständig.

Es handelt sich um die sogenannte **Teilung des Rechtsschutzinstrumentariums**, die seit längerem im österreichen Recht verankert ist.

In § 5 DSG ist die Definition des **öffentlichen und privaten Bereichs** geregelt: Datenanwendungen sind dem öffentlichen Bereich zuzurechnen, wenn sie für Zwecke eines Auftraggebers des öffentlichen Bereichs durchgeführt werden. Auftraggeber des öffentlichen Bereichs sind alle Auftraggeber, die in Formen des öffentlichen Rechts eingerichtet sind, insbesondere auch als Organ einer Gebietskörperschaft, oder soweit sie trotz ihrer Einrichtung in Formen des Privatrechts in Vollziehung der Gesetze tätig sind. Alle anderen Auftraggeber gelten als Auftraggeber des privaten Bereichs.

#### *2.2.1.4 Abklärungen durch die Datenschutzkommission*

Bei begründetem Verdacht einer schwerwiegenden Datenschutzverletzung durch einen privatrechtlichen Auftraggeber hat die **Datenschutzkommission** die Pflicht eine Feststellungsklage nach der Zivilprozessordnung zu erheben. Bezieht sich eine zulässige Klage auf eine meldepflichtige Datenanwendung, kann das Gericht die Datenschutzkommission um Überprüfung der Richtigstellung des Registers und Überprüfung der Erfüllung der Meldepflicht ersuchen. [75]

### 2.2.2 Datenbearbeitungen durch Behörden

Die Rechte des Betroffenen sind weitestgehend identisch, egal ob es sich um eine Privatperson oder um eine Behörde als Datenbearbeiter handelt.

---

[75] Zu allem § 32 DSG.

Die Rechte des Betroffenen sind in §§ 16 und den §§ 26-29 DSG und der Rechtsschutz in §§ 30-34 DSG geregelt. Der Betroffene hat folgende Rechte: **Einsichtsrecht** ins Datenverarbeitungsregister (§ 16 Abs. 2), **Auskunftsrecht** (§ 26), Recht auf **Richtigstellung** oder **Löschung** (§ 27), **Widerspruchsrecht** beim Vorliegen von überwiegender schutzwürdiger Geheimhaltungsinteressen (§ 28) und eingeschränkte Rechte bei der Verwendung nur indirekt personenbezogener Daten (§ 29).

Wir gehen davon aus, dass dies den Rechten auf Unterlassung, Beseitigung, Feststellung, Sperrung, Berichtigung, Vernichtung und Mitteilung nach dem Schweizer DSG weitestgehend entspricht. Im Einzelnen gestaltet sich dies wie folgt:

#### *2.2.2.1 Unterlassung, Beseitigung, Berichtigung, Löschung*

Jeder Auftraggeber hat unrichtige oder entgegen den Bestimmungen dieses Bundesgesetzes verarbeitete Daten richtigzustellen oder zu löschen, und zwar aus eigenem, sobald ihm die Unrichtigkeit von Daten oder die Unzulässigkeit ihrer Verarbeitung bekannt geworden ist, oder auf begründeten Antrag des Betroffenen. Der Pflicht zur Richtigstellung unterliegen nur solche Daten, deren Richtigkeit für den Zweck der Datenanwendung von Bedeutung ist. Die Unvollständigkeit verwendeter Daten bewirkt nur dann einen Berichtigungsanspruch, wenn sich aus der Unvollständigkeit im Hinblick auf den Zweck der Datenanwendung die Unrichtigkeit der Gesamtinformation ergibt. Sobald Daten für den Zweck der Datenanwendung nicht mehr benötigt werden, gelten sie als unzulässig verarbeitete Daten und sind zu löschen, es sei denn, daß ihre Archivierung rechtlich zulässig ist und daß der Zugang zu diesen Daten besonders geschützt ist. Die Weiterverwendung von Daten für einen anderen Zweck ist nur zulässig, wenn eine Übermittlung der Daten für diesen Zweck zulässig ist (§ 27 DSG).

Sofern die Verwendung von Daten nicht gesetzlich vorgesehen ist, hat jeder Betroffene das Recht, **gegen die Verwendung** seiner Daten wegen Verletzung überwiegender schutzwürdiger Geheimhaltungsinteressen, die sich aus seiner besonderen Situation ergeben, beim Auftraggeber der Datenanwendung **Widerspruch** zu erheben. Der Auftraggeber hat bei Vorliegen dieser Voraussetzungen die Daten des Betroffenen binnen acht Wochen aus seiner Datenanwendung zu **löschen** und allfällige Übermittlungen zu **unterlassen** (§ 28 DSG).

#### *2.2.2.2. Andere: Schadenersatz*

Für einen Schadenersatzanspruch gegen den Rechtsträger einer Behörde sind die Zivilgericht zuständig (§ 33 Abs. 4 DSG). Zu weiteren Einzelheiten zum Schadenersatz siehe oben zu den privaten Datenbearbeitern (2.2.1.2).

#### *2.2.2.3. Verfahren*

Der Rechtsschutz des Betroffenen besteht aus der Möglichkeit, die **Kontrollbefugnisse** der Datenschutzkommission anzurufen (§ 30). Jedermann kann sich wegen einer behaupteten Verletzung seiner Rechte oder ihn betreffender Pflichten eines Auftraggebers oder Dienstleisters mit einer Eingabe an die **Datenschutzkommission** wenden. Die Datenschutzkommission kann im Fall eines begründeten Verdachtes auf Verletzung der Rechte und Pflichten Datenanwendungen überprüfen. Hiebei kann sie vom Auftraggeber oder Dienstleister der überprüften Datenanwendung insbesondere

alle notwendigen **Aufklärungen** verlangen und **Einschau** in Datenanwendungen und diesbezügliche Unterlagen begehren.

Ein Betroffener kann eine **Beschwerde** an die Datenschutzkommission richten (§ 31 DSG). Die Datenschutzkommission erkennt über Beschwerden von Personen oder Personengemeinschaften, die behaupten, in ihrem **Recht auf Auskunft** nach § 26 oder nach § 50 Abs. 1 dritter Satz oder in ihrem **Recht auf Darlegung einer automatisierten Einzelentscheidung** nach § 49 Abs. 3 verletzt zu sein, soweit sich das Auskunftsverlangen (der Antrag auf Darlegung oder Bekanntgabe) nicht auf die Verwendung von Daten für Akte im Dienste der Gesetzgebung oder der Gerichtsbarkeit bezieht. Die Datenschutzkommission erkennt weiters über Beschwerden von Personen oder Personengemeinschaften, die behaupten, in ihrem **Recht auf Geheimhaltung** (§ 1 Abs. 1) oder in ihrem **Recht auf Richtigstellung oder auf Löschung** (§§ 27 und 28) verletzt zu sein, sofern der Anspruch nicht nach § 32 Abs. 1 vor einem **Gericht** geltend zu machen ist oder sich gegen ein Organ im Dienste der Gesetzgebung oder der Gerichtsbarkeit richtet.

Die Datenschutzkommission kann begleitende Massnahmen im Beschwerdeverfahren anordnen (§ 31a).

#### *2.2.2.4. Verletzung ausländischen Rechts*

Eingaben nach § 30, Beschwerden nach § 31, Klagen nach § 32 und Schadenersatzansprüche nach § 33 DSG können nicht nur auf die Verletzung von österreichischem Recht, sondern **auch** von **datenschutzrechtlichen** Vorschriften eines **Mitgliedsstaates** der Europäischen Union oder eines anderen Vertragsstaates des Europäischen Wirtschaftsraums gegründet werden.[76]

## 2.3. Nationale Aufsichtsbehörde

### 2.3.1. Zusammensetzung, Ernennung und Eingliederung der Behörde

Zur Wahrung des Datenschutzes sind (neben der Zuständigkeit des Bundeskanzlers und der ordentlichen Gerichte) die **Datenschutzkommission** und der **Datenschutzrat** berufen.[77]

Die **Datenschutzkommission** ist eine unabhängige Kollegialbehörde und eine **gerichtsähnliche Organisation**. Sie besteht aus sechs Mitgliedern, welche alle rechtskundig sein müssen. Sie hat sich eine Geschäftsordnung zu geben, in der eines ihrer Mitglieder mit der Führung der laufenden Geschäfte zu betrauen ist (geschäftsführendes Mitglied). Diese Betrauung umfasst auch die Erlassung von verfahrensrechtlichen Bescheiden und von Mandatsbescheiden im Registrierungsverfahren. Inwieweit einzelne fachlich geeignete Bedienstete der Geschäftsstelle der Datenschutzkommission zum Handeln für die Datenschutzkommission oder das geschäftsführende Mitglied ermächtigt werden, bestimmt die Geschäftsordnung.[78] Die Geschäftsordnung normiert vordergründig die Abgrenzung der Befugnisse des Vorsitzenden, des geschäftsführenden Mitglieds und der anderen Mitglieder der Kommission.

---

[76] § 34 Abs. 2-4 DSG.

[77] § 35 Abs. 1 DSG.

[78] § 38 Abs. 1 DSG.

Die Datenschutzkommission ist bei Anwesenheit aller sechs Mitglieder beschlussfähig. Das **richterliche Mitglied** führt den Vorsitz. Für einen gültigen Beschluss der Datenschutzkommission ist die Zustimmung der Mehrheit der abgegebenen Stimmen notwendig. Bei Stimmengleichheit gibt die Stimme des Vorsitzenden den Ausschlag. Stimmenthaltung ist unzulässig. Beschlüsse der Datenschutzkommission werden vom Vorsitzenden ausgefertigt.[79]

Beim Bundeskanzleramt ist ein **Datenschutzrat** eingerichtet.[80] § 42 Abs. 1-4 DSG erklären die Zusammensetzung des Datenschutzrates. Dem Datenschutzrat gehören an:

1. Vertreter der **politischen Parteien**: Von der im Hauptausschuss des Nationalrates am stärksten vertretenen Partei sind vier Vertreter, von der am zweitstärksten vertretenen Partei sind drei Vertreter und von jeder anderen im Hauptausschuss des Nationalrates vertretenen Partei ist ein Vertreter in den Datenschutzrat zu entsenden, wobei es allein auf die Stärke im Zeitpunkt der Entsendung ankommt. Bei Mandatsgleichheit zweier Parteien im Hauptausschuss ist die Stimmenstärke bei der letzten Wahl zum Nationalrat ausschlaggebend;
2. je ein Vertreter der **Bundeskammer** für Arbeiter und Angestellte und der Wirtschaftskammer Österreich;
3. zwei Vertreter der **Länder**;
4. je ein Vertreter des **Gemeindebundes** und des **Städtebundes**;
5. ein vom Bundeskanzler zu ernennender Vertreter des **Bundes**.

Die in Ziffer 3-5 genannten Vertreter sollen **berufliche Erfahrung** auf dem Gebiet der Informatik und des Datenschutzes haben. Für jedes Mitglied ist ein Ersatzmitglied namhaft zu machen. Dem Datenschutzrat können Mitglieder der Bundesregierung oder einer Landesregierung sowie Staatssekretäre und weiters Personen, die zum Nationalrat nicht wählbar sind, nicht angehören.

### 2.3.2. Gewährleistung der Unabhängigkeit

Die **Datenschutzkommission** besteht aus sechs Mitgliedern, die auf Vorschlag der Bundesregierung vom Bundespräsidenten für die Dauer von fünf Jahren bestellt werden. Wiederbestellungen sind zulässig. Die Mitglieder müssen rechtskundig sein. Ein Mitglied muss dem Richterstand angehören. Die Vorbereitung des Vorschlages der Bundesregierung für die Bestellung der Mitglieder der Datenschutzkommission obliegt dem Bundeskanzler. Er hat dabei Bedacht zu nehmen auf einen Dreiervorschlag des Präsidenten des Obersten Gerichtshofs für das richterliche Mitglied, auf einen Vorschlag der Länder für zwei Mitglieder (Beschluss der Landeshauptleutekonferenz), auf einen Dreiervorschlag der Bundeskammer für Arbeiter und Angestellte für ein Mitglied, und auf einen Dreiervorschlag der Wirtschaftskammer Österreich für ein Mitglied. Alle vorgeschlagenen Personen sollen Erfahrung auf dem Gebiet des Datenschutzes besitzen. Ein Mitglied ist aus dem Kreise der

---

79 § 39 Abs. 1-3 und 5 DSG.

80 § 41 Abs. 1 DSG.

rechtskundigen Bundesbediensteten vorzuschlagen. Die Mitglieder der Datenschutzkommission üben diese Funktion neben ihnen sonst obliegenden beruflichen Tätigkeiten aus.[81]

Die Datenschutzkommission übt ihre Befugnisse auch gegenüber den obersten Organen der Vollziehung, wie die Bundesregierung, der Bundeskanzler, die übrigen Bundesminister, die Landesregierung, aus.[82]

Die Mitglieder der Datenschutzkommission sind in **Ausübung** ihres Amtes unabhängig und an keine Weisungen gebunden.[83] Mit anderen Worten ist die Datenschutzkommission als **Kollegialbehörde mit richterlichem Einschlag** in ihrer Funktion als entscheidendes Organ sowie in anderen Funktionen (§ 30 Abs. 6 und 6a) **weisungsfrei**. Die in der Geschäftsstelle der Datenschutzkommission tätigen Bediensteten unterstehen fachlich nur den Weisungen des Vorsitzenden oder des geschäftsführenden Mitglieds der Datenschutzkommission.[84]

Für die Unterstützung in der Geschäftsführung der Datenschutzkommission hat der Bundeskanzler eine **Geschäftsstelle einzurichten** und die notwendige Sach- und Personalausstattung bereitzustellen. Er hat das Recht, sich jederzeit über alle Gegenstände der Geschäftsführung der Datenschutzkommission beim Vorsitzenden und dem geschäftsführenden Mitglied zu unterrichten. Die Datenschutzkommission ist vor Erlassung von Verordnungen anzuhören, die auf der Grundlage dieses Bundesgesetzes ergehen oder sonst wesentliche Fragen des Datenschutzes unmittelbar betreffen. Die Datenschutzkommission hat spätestens alle zwei Jahre einen Bericht über ihre Tätigkeit zu erstellen und in geeigneter Weise zu veröffentlichen. Der Bericht ist dem Bundeskanzler zur Kenntnis zu übermitteln.[85]

Die Mitglieder gehören dem Datenschutzrat solange an, bis sie dem Bundeskanzler schriftlich ihr **Ausscheiden** mitteilen oder, mangels einer solchen Mitteilung, von der entsendenden Stelle (Abs. 1) dem Bundeskanzler ein anderer Vertreter namhaft gemacht wird. Mitglieder der Vertreter der politischen Parteien scheiden außerdem aus, sobald der Hauptausschuss neu gewählt wurde, und sie nicht neuerlich entsendet werden. Die Tätigkeit der Mitglieder des Datenschutzrates ist zudem ehrenamtlich.[86]

Der Datenschutzrat gibt sich mit Beschluss eine **Geschäftsordnung**. Er hat aus seiner Mitte einen Vorsitzenden und zwei stellvertretende Vorsitzende zu wählen. Die Funktionsperiode des Vorsitzenden und der stellvertretenden Vorsitzenden dauert fünf Jahre. Wiederbestellungen sind zulässig. Die Geschäftsführung des Datenschutzrates obliegt dem Bundeskanzleramt. Der Bundeskanzler hat das hierfür notwendige Personal zur Verfügung zu stellen. Bei ihrer Tätigkeit für den Datenschutzrat sind

---

81 § 36 Abs. 1-3a DSG.
82 § 35 Abs. 2 DSG.
83 § 37 Abs. 1 DSG.
84 § 37 Abs. 2 DSG.
85 § 38 Abs. 2-4 DSG.
86 § 42 Abs. 5 und 6 DSG.

die Bediensteten des Bundeskanzleramtes fachlich an die Weisungen des Vorsitzenden des Datenschutzrates gebunden.[87]

Für Beratungen und **Beschlussfassungen** im Datenschutzrat ist die Anwesenheit von mehr als der Hälfte seiner Mitglieder erforderlich. Zur Beschlussfassung genügt die einfache Mehrheit der abgegebenen Stimmen. Bei Stimmengleichheit gibt die Stimme des Vorsitzenden den Ausschlag. Stimmenthaltung ist unzulässig. Die Beifügung von Minderheitenvoten ist zulässig. Der Datenschutzrat kann aus seiner Mitte ständige oder nichtständige Arbeitsausschüsse bilden, denen er die Vorbereitung, Begutachtung und Bearbeitung einzelner Angelegenheiten übertragen kann. Er ist auch berechtigt, die Geschäftsführung, Vorbegutachtung und die Bearbeitung einzelner Angelegenheiten einem einzelnen Mitglied (Berichterstatter) zu übertragen. Jedes Mitglied des Datenschutzrates ist verpflichtet, an den Sitzungen - ausser im Fall der gerechtfertigten Verhinderung - teilzunehmen. Ist ein Mitglied an der Teilnahme verhindert, hat es hiervon unverzüglich das Ersatzmitglied zu verständigen. Mitglieder der Datenschutzkommission, die dem Datenschutzrat nicht angehören, sind berechtigt, an den Sitzungen des Datenschutzrates oder seiner Arbeitsausschüsse teilzunehmen. Ein Stimmrecht steht ihnen jedoch nicht zu. Die Beratungen in der Sitzung des Datenschutzrates sind, soweit er nicht selbst anderes beschließt, vertraulich. Die Mitglieder des Datenschutzrates, die anwesenden Mitglieder der Datenschutzkommission und die zur Sitzung zugezogenen Sachverständigen sind zur Verschwiegenheit über alle ihnen ausschließlich aus ihrer Tätigkeit im Datenschutzrat bekanntgewordenen Tatsachen verpflichtet, sofern die Geheimhaltung im öffentlichen Interesse oder im Interesse einer Partei geboten ist.[88]

Die Datenschutzkommission (DSK) hat sich eine Geschäftsordnung zu geben, in der eines ihrer Mitglieder mit der **Führung der laufenden Geschäfte** zu betrauen ist (geschäftsführendes Mitglied). Dieses geschäftsführende Mitglied hat die Entscheidungsbefugnis über finanzielle Ausgaben. Auch dieses geschäftsführende Mitglied der Datenschutzkommission ist in Ausübung seines Amtes unabhängig und an keine Weisungen gebunden. Auch die in der Geschäftsstelle der Datenschutzkommission tätigen Bediensteten unterstehen fachlich nur den Weisungen des Vorsitzenden oder des geschäftsführenden Mitglieds der Datenschutzkommission. Ein Budget im formellen Sinne gibt es innerhalb der Datenschutzkommission nicht. Das Gesetz sieht lediglich vor, dass für die Unterstützung in der Geschäftsführung der Datenschutzkommission (DSK) der Bundeskanzler eine Geschäftsstelle einzurichten hat und die notwendige Sach- und Personalausstattung bereitstellen muss. Die Datenschutzkommission meldet folglich ihren **notwendigen, finanziellen Bedarf** direkt dem Bundeskanzler. Im Budget des Bundeskanzleramtes ist ein Posten für die Datenschutzkommission vorgesehen. Das Budget des Bundeskanzleramtes wird vom Parlament beschlossen. Benötigt die Datenschutzkommission mehr Mittel, als im Budget des Bundeskanzleramtes veranschlagt sind, ist den allgemeinen Regeln für die Budgetüberschreitung zu folgen. Die Budgetüberschreitung wäre direkt vom Bundeskanzler zu beantragen.

### 2.3.3. Zuständigkeitsbereich

Die Datenschutzkommission ist sowohl für Datenbearbeitungen von Privatpersonen, als auch von öffentlichen Behörden zuständig.

---

87 § 43 DSG.

88 § 44 Abs. 3-8 DSG.

Die **Datenschutzkommission** erkennt über **Beschwerden** von Personen oder Personengemeinschaften, die behaupten, in ihrem Recht auf Auskunft (nach § 26 oder nach § 50 Abs. 1 dritter Satz) oder in ihrem Recht auf Darlegung einer automatisierten Einzelentscheidung (nach § 49 Abs. 3) **verletzt** zu sein, soweit sich das Auskunftsverlangen (der Antrag auf Darlegung oder Bekanntgabe) nicht auf die Verwendung von Daten für Akte im Dienste der Gesetzgebung oder der Gerichtsbarkeit bezieht. Die Datenschutzkommission erkennt weiter über Beschwerden von Personen oder Personengemeinschaften, die behaupten, in ihrem Recht auf Geheimhaltung (§ 1 Abs. 1) oder in ihrem Recht auf Richtigstellung oder auf Löschung (§§ 27 und 28) **verletzt** zu sein, sofern der Anspruch nicht (nach § 32 Abs. 1) vor einem **Gericht** geltend zu machen ist oder sich gegen ein Organ im Dienste der Gesetzgebung oder der Gerichtsbarkeit richtet.[89] Die Datenschutzkommission ist hauptsächlich zuständig für den Datenschutz. Um den Datenschutz zu gewährleisten und zur Wiederherstellung des rechtmässigen Zustandes, kann sie auch Strafanzeige erstatten und Klage erheben.[90]

Der **Datenschutzrat** berät die Bundesregierung und die Landesregierungen auf deren Ersuchen in rechtspolitischen Fragen des Datenschutzes. Zur Erfüllung dieser Aufgabe kann der Datenschutzrat Fragen von grundsätzlicher Bedeutung für den Datenschutz in Beratung ziehen. Dem Datenschutzrat ist Gelegenheit zur **Stellungnahme zu Gesetzesentwürfen** der Bundesministerien zu geben, soweit diese datenschutzrechtlich von Bedeutung sind. Auftraggeber des öffentlichen Bereichs haben ihre Vorhaben dem Datenschutzrat zur Stellungnahme zuzuleiten, soweit diese datenschutzrechtlich von Bedeutung sind. Der Datenschutzrat hat das Recht, von Auftraggebern des öffentlichen Bereichs Auskünfte und Berichte sowie die Einsicht in Unterlagen zu verlangen, soweit dies zur datenschutzrechtlichen Beurteilung von Vorhaben mit wesentlichen Auswirkungen auf den Datenschutz in Österreich notwendig ist. Der Datenschutzrat hat zudem das Recht, von der Datenschutzkommission Auskünfte und Berichte sowie Einsicht in Unterlagen zu verlangen. Er kann Auftraggeber des privaten Bereichs oder auch ihre gesetzliche Interessenvertretung zur Stellungnahme zu Entwicklungen von allgemeiner Bedeutung auffordern, die aus datenschutzrechtlicher Sicht Anlass zu Bedenken, zumindest aber Anlass zur Beobachtung geben. Er kann seine Beobachtungen, Bedenken und allfälligen Anregungen zur Verbesserung des Datenschutzes in Österreich der Bundesregierung und den Landesregierungen mitteilen, sowie über Vermittlung dieser Organe den gesetzgebenden Körperschaften zur Kenntnis bringen.[91]

### 2.3.4. Aufgaben und Kompetenzen

Allgemein kann gesagt werden, dass der ausserhalb des förmlichen Beschwerdeverfahrens liegenden Kontrollbefugnisse der Datenschutzbehörde **grosse Bedeutung** zukommt. § 30 DSG regelt die **Kontrollbefugnisse** der Datenschutzkommission: Jedermann kann sich wegen einer behaupteten Verletzung seiner Rechte oder ihn betreffender Pflichten eines Auftraggebers oder Dienstleisters nach diesem Bundesgesetz mit einer Eingabe an die Datenschutzkommission wenden (Abs. 1). Die Datenschutzkommission kann im Fall eines begründeten Verdachtes auf Verletzung der im Abs. 1 genannten Rechte und Pflichten Datenanwendungen überprüfen. Hierbei kann sie vom Auftraggeber oder Dienstleister der überprüften Datenanwendung insbesondere alle notwendigen Aufklärungen

---

89 § 31 Abs. 1 und 2 DSG.

90 § 30 Abs. 6 DSG.

91 § 41 Abs. 2 DSG.

verlangen und Einsicht in Datenanwendungen und diesbezügliche Unterlagen begehren. Sofern sich eine zulässige Eingabe oder ein begründeter Verdacht auf eine meldepflichtige Datenanwendung (Datei) bezieht, kann die Datenschutzkommission die Erfüllung der Meldepflicht überprüfen.

Datenanwendungen, die der **Vorabkontrolle** gemäß § 18 Abs. 2 DSG unterliegen, dürfen auch ohne Vorliegen eines Verdachts auf rechtswidrige Datenverwendung überprüft werden. Dies gilt auch für jene Bereiche der Vollziehung, in welchen ein Auftraggeber des öffentlichen Bereichs die grundsätzliche Anwendbarkeit der §§ 26 Abs. 5 und 27 Abs. 5 in Anspruch nimmt (Abs. 3). Zum Zweck der Einsicht ist die Datenschutzkommission nach Verständigung des Inhabers der Räumlichkeiten und des Auftraggebers (Dienstleisters) berechtigt, Räume, in welchen Datenanwendungen vorgenommen werden, zu betreten, Datenverarbeitungsanlagen in Betrieb zu setzen, die zu überprüfenden Verarbeitungen durchzuführen sowie Kopien von Datenträgern in dem für die Ausübung der Kontrollbefugnisse unbedingt erforderlichen Ausmaß herzustellen. Der Auftraggeber (Dienstleister) hat die für die Einsicht notwendige Unterstützung zu leisten. Die Kontrolltätigkeit ist unter möglichster Schonung der Rechte des Auftraggebers (Dienstleisters) und Dritter auszuüben.

Informationen, die der Datenschutzkommission oder ihren Beauftragten bei der Kontrolltätigkeit zukommen, dürfen ausschließlich für die Kontrolle im Rahmen der Vollziehung datenschutzrechtlicher Vorschriften verwendet werden. Dazu zählt auch die Verwendung für Zwecke der gerichtlichen Rechtsverfolgung durch den Einschreiter oder die Datenschutzkommission nach § 32. Im Übrigen besteht die Pflicht zur Verschwiegenheit auch gegenüber Gerichten und Verwaltungsbehörden, insbesondere Abgabenbehörden; dies allerdings mit der Maßgabe, dass dann, wenn die Einsicht den Verdacht einer strafbaren Handlung nach dem DSG, bestimmter strafbarer Handlungen nach dem Strafgesetzbuches oder eines Verbrechens mit einer Freiheitsstrafe, deren Höchstmaß fünf Jahre übersteigt, ergibt, Anzeige zu erstatten ist und hinsichtlich solcher Verbrechen und Vergehen auch Ersuchen nach § 76 der Strafprozessordnung, zu entsprechen ist.

Zur Herstellung des rechtmäßigen Zustandes kann die Datenschutzkommission **Empfehlungen** aussprechen, für deren Befolgung erforderlichenfalls eine angemessene Frist zu setzen ist. Wird einer solchen Empfehlung innerhalb der gesetzten Frist nicht entsprochen, so kann die Datenschutzkommission je nach der Art des Verstoßes von Amts wegen insbesondere Strafanzeige (nach §§ 51 oder 52 DSG) erstatten, bei schwerwiegenden Verstößen durch Auftraggeber des privaten Bereichs Klage vor dem zuständigen Gericht gemäß § 32 Abs. 5 DSG erheben oder bei Verstößen von Auftraggebern, die Organe einer Gebietskörperschaft sind, das zuständige oberste Organ befassen. Dieses Organ hat innerhalb einer angemessenen, jedoch zwölf Wochen nicht überschreitenden Frist entweder dafür Sorge zu tragen, dass der Empfehlung der Datenschutzkommission entsprochen wird, oder der Datenschutzkommission mitzuteilen, warum der Empfehlung nicht entsprochen wurde. Die Begründung darf von der Datenschutzkommission der Öffentlichkeit in geeigneter Weise zur Kenntnis gebracht werden, soweit dem nicht die Amtsverschwiegenheit entgegensteht (Abs. 6). Liegt durch den Betrieb einer Datenanwendung eine **wesentliche unmittelbare Gefährdung** schutzwürdiger Geheimhaltungsinteressen der Betroffenen (Gefahr im Verzug) vor, so kann die Datenschutzkommission die Weiterführung der Datenanwendung mit Bescheid (gemäß § 57 Abs. 1 des Allgemeinen Verwaltungsverfahrensgesetzes 1991 – AVG) untersagen. Wenn dies technisch möglich, im Hinblick auf den Zweck der Datenanwendung sinnvoll und zur Beseitigung der Gefährdung ausreichend scheint, kann die Weiterführung auch nur teilweise untersagt werden. Wird einer Untersagung nicht sogleich Folge geleistet, ist Strafanzeige nach § 52 Abs. 1 Z 3 DSG zu erstatten. Nach

Rechtskraft einer Untersagung nach diesem Absatz ist ein Berichtigungsverfahren nach § 22a Abs. 2 formlos einzustellen. Die Datenanwendung ist im Umfang der Untersagung aus dem Register zu streichen (Abs. 6a). Der Einschreiter ist darüber zu informieren, wie mit seiner Eingabe verfahren wurde (Abs. 7).

Im Falle einer eingereichten Beschwerde, kommen der **Datenschutzkommission** gemäss § 31 Abs. 5-8 DSG folgende Aufgaben und Kompetenzen zu: Die der Datenschutzkommission durch § 30 Abs. 2 bis 4 eingeräumten Kontrollbefugnisse kommen ihr auch in Beschwerdeverfahren nach Abs. 1 und 2 gegenüber dem Beschwerdegegner zu. Ebenso besteht auch hinsichtlich dieser Verfahren die Verschwiegenheitspflicht (nach § 30 Abs. 5) (Abs. 5). Im Fall der Einbringung einer zulässigen Beschwerde nach Abs. 1 oder 2 ist ein auf Grund einer Eingabe nach § 30 Abs. 1 über denselben Gegenstand eingeleitetes Kontrollverfahren durch eine entsprechende Information (§ 30 Abs. 7) zu beenden. Die Datenschutzkommission kann aber dennoch auch während der Anhängigkeit des Beschwerdeverfahrens von Amts wegen nach § 30 Abs. 2 vorgehen, wenn ein begründeter Verdacht einer über den Beschwerdefall hinausgehenden Verletzung datenschutzrechtlicher Verpflichtungen besteht. § 30 Abs. 3 bleibt unberührt (Abs. 6). Soweit sich eine Beschwerde nach Abs. 1 oder 2 als berechtigt erweist, ist ihr Folge zu geben und die Rechtsverletzung festzustellen. Ist eine festgestellte Verletzung im Recht auf Auskunft (wie in Abs. 1) einem Auftraggeber des privaten Bereichs zuzurechnen, so ist diesem auf Antrag zusätzlich die – allenfalls erneute – Reaktion auf das Auskunftsbegehren nach § 26 Abs. 4, 5 oder 10 in jenem Umfang aufzutragen, der erforderlich ist, um die festgestellte Rechtsverletzung zu beseitigen. Soweit sich die Beschwerde als nicht berechtigt erweist, ist sie abzuweisen (Abs. 7). Ein Beschwerdegegner, gegen den wegen Verletzung in Rechte nach den §§ 26 bis 28 Beschwerde erhoben wurde, kann bis zum Abschluss des Verfahrens vor der Datenschutzkommission durch Reaktionen gegenüber dem Beschwerdeführer (gemäß § 26 Abs. 4 oder § 27 Abs. 4) die behauptete Rechtsverletzung nachträglich beseitigen. Erscheint der Datenschutzkommission durch derartige Reaktionen des Beschwerdegegners die Beschwerde als gegenstandslos, so hat sie den Beschwerdeführer dazu zu hören. Gleichzeitig ist er darauf aufmerksam zu machen, dass die Datenschutzkommission das Verfahren formlos einstellen wird, wenn er nicht innerhalb einer angemessenen Frist begründet, warum er die ursprünglich behauptete Rechtsverletzung zumindest teilweise nach wie vor als nicht beseitigt erachtet. Wird durch eine derartige Äußerung des Beschwerdeführers die Sache ihrem Wesen nach geändert (§ 13 Abs. 8 AVG), so ist von der Zurückziehung der ursprünglichen Beschwerde und der gleichzeitigen Einbringung einer neuen Beschwerde auszugehen. Auch dies falls ist das ursprüngliche Beschwerdeverfahren formlos einzustellen und der Beschwerdeführer davon zu verständigen. Verspätete Äußerungen sind nicht zu berücksichtigen (Abs. 8).

§ 31a regelt die möglichen **begleitendenden Maßnahmen im Beschwerdeverfahren**: Sofern sich eine zulässige Beschwerde nach § 31 Abs. 2 auf eine meldepflichtige Datenanwendung (Datei) bezieht, kann die Datenschutzkommission die Erfüllung der Meldepflicht überprüfen und erforderlichenfalls nach den §§ 22 (Richtigstellung des Registers und Rechtsnachfolge) und 22a (Verfahren zur Überprüfung der Erfüllung der Meldepflicht) vorgehen (Abs. 1). Macht der Beschwerdeführer im Rahmen einer Beschwerde nach § 31 Abs. 2 eine wesentliche Beeinträchtigung seiner schutzwürdigen Geheimhaltungsinteressen durch die Verwendung seiner Daten glaubhaft, so kann die Datenschutzkommission nach § 30 Abs. 6a vorgehen (Abs. 2). Ist in einem Verfahren nach § 31 Abs. 2 die Richtigkeit von Daten strittig, so ist vom Beschwerdegegner bis zum Abschluss des Verfahrens ein Bestreitungsvermerk anzubringen. Erforderlichenfalls hat dies die Datenschutzkommission auf Antrag

des Beschwerdeführers mit Mandatsbescheid anzuordnen (Abs. 3). Beruft sich ein Auftraggeber des öffentlichen Bereichs bei einer Beschwerde wegen Verletzung des Auskunfts-, Richtigstellungs- oder Löschungsrechts gegenüber der Datenschutzkommission auf die §§ 26 Abs. 5 oder 27 Abs. 5, so hat diese nach Überprüfung der Notwendigkeit der Geheimhaltung die geschützten öffentlichen Interessen in ihrem Verfahren zu wahren. Kommt sie zur Auffassung, dass die Geheimhaltung von verarbeiteten Daten gegenüber dem Betroffenen nicht gerechtfertigt war, ist die Offenlegung der Daten mit Bescheid aufzutragen. Gegen diese Entscheidung der Datenschutzkommission kann die belangte Behörde Beschwerde an den Verwaltungsgerichtshof erheben. Wurde keine derartige Beschwerde eingebracht und wird dem Bescheid der Datenschutzkommission binnen acht Wochen nicht entsprochen, so hat die Datenschutzkommission die Offenlegung der Daten gegenüber dem Betroffenen selbst vorzunehmen und ihm die verlangte Auskunft zu erteilen oder ihm mitzuteilen, welche Daten bereits berichtigt oder gelöscht wurden. Die ersten beiden Sätze gelten in Verfahren nach § 30 sinngemäß (Abs. 4).

Die Datenschutzkommission hat folgende **Informationspflicht gegenüber der Öffentlichkeit**: Entscheidungen der Datenschutzkommission von grundsätzlicher Bedeutung für die Allgemeinheit sind von der Datenschutzkommission unter Beachtung der Erfordernisse der Amtsverschwiegenheit in geeigneter Weise zu veröffentlichen.[92]

## 2.4. Rolle der Organisationen zum Schutz der Betroffenen

Die wichtigsten Datenschutzbehörden in Österreich sind die Datenschutzkommission (DSK)[93] und der Datenschutzrat (DSR)[94]. Daneben existieren jedoch auch noch **private Datenschutzorganisationen** in Österreich, wie Arge Daten[95] – eine österreichische Gesellschaft für Datenschutz, VIBE.AT[96] – ein Verein für Internet-Benutzer Österreichs und der Verein Quintessenz[97] – ein Verein, welcher sich für den Datenschutz einsetzt. ITA[98] – das Institut der Technikfolgenabschätzung und Systemanalyse der Österreichischen Akademie der Wissenschaften – befasst sich ebenfalls mit Fragen bezüglich des Datenschutzes.

Die Kompetenzen der Datenschutzkommission und des Datenschutzrates wurden bereits oben behandelt (siehe 1.3.4). Die Datenschutzkommission hat jedoch noch eine weitere Kompetenz. Sie hat nämlich, wenn ein Einschreiter (§ 30 Abs. 1) es verlangt und es zur Wahrung der nach diesem Bundesgesetz geschützten Interessen einer größeren Zahl von natürlichen Personen geboten ist, einem Rechtsstreit auf Seiten des Einschreiters als **Nebenintervenient** (§§ 17 ff ZPO) beizutreten.[99]

---

92 § 39 Abs. 4 DSG.
93 http://www.dsk.gv.at
94 http://www.datenschutzrat.gv.at
95 http://www.argedaten.at
96 http://www.vibe.at
97 http://www.quintessenz.at
98 http://www.itas.fzk.de
99 § 32 Abs. 6 DSG.

Den privaten Datenschutzorganisationen kommen keine gesetzlichen Rechte und Kompetenzen im Bereich des Datenschutzes zu. Sie haben keine gesetzlich verankerte Möglichkeit der Verbandsbeschwerde. Subventionszahlungen müssen in Österreich derzeit nicht öffentlich gemacht werden.

Es konnte nicht festgestellt werden, in welchen verschiedenen Formen sich die Betroffenen an die Organisationen wenden.

## 2.5. Mögliche und vorgeschriebene Aktivitäten der Datenbearbeiter (private und öffentliche)

Das österreichische Datenschutzgesetz unterscheidet im Bereich der Datenbearbeiter zwischen **Auftraggeber**[100] und **Dienstleister**[101].

Neben den bereits erwähnten Pflichten des **Auftraggebers** wie die Auskunftspflicht gegenüber dem Betroffenen (§ 26 Abs. 1), der Pflicht unrichtige und gesetzeswidrig verarbeitete Daten richtigzustellen oder zu löschen (§ 27 Abs. 1) und der Pflicht zur Leistung von Schadenersatz bei schuldhafter gesetzeswidriger Datenverwendung (§ 33 Abs. 1), gibt es eine Reihe weiterer Pflichten für den Auftraggeber. Den Auftraggeber trifft die Pflicht bei jeder Datenanwendung dafür zu sorgen, dass die allgemeinen Grundsätze eingehalten werden.[102] Wenn der Auftraggeber bei der Datenanwendung einen Dienstleister beauftragen will, hat er die Prüfungspflicht gegenüber dem Dienstleister, ob dieser berechtigt ist jenes Gewerbe auszuüben.[103] Die beabsichtigte Heranziehung eines Dienstleisters durch einen Auftraggeber des öffentlichen Bereichs im Rahmen einer Datenanwendung, die der Vorabkontrolle gemäß § 18 Abs. 2 unterliegt, ist der Datenschutzkommission mitzuteilen, es sei denn, dass die Inanspruchnahme des Dienstleisters auf Grund ausdrücklicher gesetzlicher Ermächtigung erfolgt oder als Dienstleister eine Organisationseinheit tätig wird, die mit dem Auftraggeber oder einem diesem übergeordneten Organ in einem Über- oder Unterordnungsverhältnis steht.[104] Soweit der Datenverkehr mit dem Ausland nicht gemäß § 12 genehmigungsfrei ist, hat der Auftraggeber vor der Übermittlung oder Überlassung von Daten in das Ausland die Pflicht eine Genehmigung der Datenschutzkommission (§§ 35 ff) einzuholen. Die Datenschutzkommission kann die Genehmigung an die Erfüllung von Bedingungen und Auflagen binden.[105]

---

100 § 4 Ziff. 4 DSG : natürliche oder juristische Personen, Personengemeinschaften oder Organe einer Gebietskörperschaft beziehungsweise die Geschäftsapparate solcher Organe, wenn sie allein oder gemeinsam mit anderen die Entscheidung getroffen haben, Daten zu verwenden (Z 8), unabhängig davon, ob sie die Daten selbst verwenden (Z 8) oder damit einen Dienstleister (Z 5) beauftragen. Sie gelten auch dann als Auftraggeber, wenn der mit der Herstellung eines Werkes beauftragte Dienstleister (Z 5) die Entscheidung trifft, zu diesem Zweck Daten zu verwenden (Z 8), es sei denn dies wurde ihm ausdrücklich untersagt oder der Beauftragte hat auf Grund von Rechtsvorschriften oder Verhaltensregeln über die Verwendung eigenverantwortlich zu entscheiden.

101 § 4 Ziff. 5 DSG : natürliche oder juristische Personen, Personengemeinschaften oder Organe einer Gebietskörperschaft beziehungsweise die Geschäftsapparate solcher Organe, wenn sie Daten nur zur Herstellung eines ihnen aufgetragenen Werkes verwenden (Z 8).

102 § 6 Abs. 2 DSG.

103 § 10 Abs. 1 DSG.

104 § 10 Abs. 2 DSG.

105 § 13 Abs. 1 DSG.

Für alle Organisationseinheiten, die Daten verwenden, muss der Auftraggeber **Massnahmen zur Gewährleistung der Datensicherheit** treffen. Er ist verpflichtet sicherzustellen, dass die Daten vor zufälliger oder unrechtmäßiger Zerstörung und vor Verlust geschützt sind, dass ihre Verwendung ordnungsgemäß erfolgt und dass die Daten Unbefugten nicht zugänglich sind.[106] Zur Gewährleistung der Datensicherheit kann folgendes erforderlich sein: 1. die Aufgabenverteilung bei der Datenverwendung zwischen den Organisationseinheiten und zwischen den Mitarbeitern ausdrücklich festzulegen, 2. die Verwendung von Daten an das Vorliegen gültiger Aufträge der anordnungsbefugten Organisationseinheiten und Mitarbeiter zu binden, 3. jeder Mitarbeiter über seine nach diesem Bundesgesetz und nach innerorganisatorischen Datenschutzvorschriften einschließlich der Datensicherheitsvorschriften bestehenden Pflichten zu belehren, 4. die Zutrittsberechtigung zu den Räumlichkeiten des Auftraggebers oder Dienstleisters zu regeln, 5. die Zugriffsberechtigung auf Daten und Programme und der Schutz der Datenträger vor der Einsicht und Verwendung durch Unbefugte zu regeln, 6. die Berechtigung zum Betrieb der Datenverarbeitungsgeräte festzulegen und jedes Gerät durch Vorkehrungen bei den eingesetzten Maschinen oder Programmen gegen die unbefugte Inbetriebnahme abzusichern, 7. Protokoll zu führen, damit tatsächlich durchgeführte Verwendungsvorgänge, wie insbesondere Änderungen, Abfragen und Übermittlungen, im Hinblick auf ihre Zulässigkeit im notwendigen Ausmaß nachvollzogen werden können, 8. eine Dokumentation über die nach Z 1 bis 7 getroffenen Maßnahmen zu führen, um die Kontrolle und Beweissicherung zu erleichtern. Diese Maßnahmen müssen unter Berücksichtigung des **Standes der Technik** und der bei der Durchführung erwachsenden Kosten ein Schutzniveau gewährleisten, das den von der Verwendung ausgehenden Risiken und der Art der zu schützenden Daten angemessen ist.[107] Sofern gesetzlich nicht ausdrücklich anderes angeordnet ist, sind Protokoll- und Dokumentationsdaten drei Jahre lang aufzubewahren. Davon darf in jenem Ausmaß abgewichen werden, als der von der Protokollierung oder Dokumentation betroffene Datenbestand zulässigerweise früher gelöscht oder länger aufbewahrt wird.[108] Datensicherheitsvorschriften sind so zu erlassen und zur Verfügung zu halten, dass sich die Mitarbeiter über die für sie geltenden Regelungen jederzeit informieren können.[109]

Jeder **Auftraggeber** hat, soweit in den Abs. 2 und 3 nicht anderes bestimmt ist[110], vor Aufnahme einer Datenanwendung eine **Meldung an die Datenschutzkommission** mit dem in § 19 festgelegten Inhalt

---

106 § 14 Abs. 1 DSG.

107 § 14 Abs. 2 DSG.

108 § 14 Abs. 5 DSG.

109 § 14 Abs. 6 DSG.

110 § 17 Abs. 2 und 3 DSG: (2) Nicht meldepflichtig sind Datenanwendungen, die 1. ausschließlich veröffentlichte Daten enthalten oder 2. die Führung von Registern oder Verzeichnissen zum Inhalt haben, die von Gesetzes wegen öffentlich einsehbar sind, sei es auch nur bei Nachweis eines berechtigten Interesses oder 3. nur indirekt personenbezogene Daten enthalten oder 4. von natürlichen Personen ausschließlich für persönliche oder familiäre Tätigkeiten vorgenommen werden (§ 45) oder 5. für publizistische Tätigkeit gemäß § 48 vorgenommen werden oder 6. einer Standardanwendung entsprechen: Der Bundeskanzler kann durch Verordnung Typen von Datenanwendungen und Übermittlungen aus diesen zu Standardanwendungen erklären, wenn sie von einer großen Anzahl von Auftraggebern in gleichartiger Weise vorgenommen werden und angesichts des Verwendungszwecks und der verarbeiteten Datenarten die Gefährdung schutzwürdiger Geheimhaltungsinteressen der Betroffenen unwahrscheinlich ist. In der Verordnung sind für jede Standardanwendung die zulässigen Datenarten, die Betroffenen- und Empfängerkreise und die Höchstdauer der zulässigen Datenaufbewahrung festzulegen.

zum Zweck der **Registrierung im Datenverarbeitungsregister** zu erstatten. Diese Meldepflicht gilt auch für Umstände, die nachträglich die Unrichtigkeit und Unvollständigkeit einer Meldung bewirken (Änderungsmeldung). Für manuelle Dateien besteht eine Meldepflicht nur, soweit die Inhalte zumindest einen der Tatbestände des § 18 Abs. 2 Z 1 bis 3 erfüllen.[111]

Der Auftraggeber hat insoweit die **Pflicht** auf die **Vorabkontrolle** der Datenschutzkommission zu **warten**, bevor er meldepflichtige Datenanwendungen aufnimmt, welche sensible Daten enthalten, strafrechtlich relevante Daten (im Sinne des § 8 Abs. 4) enthalten, die Auskunftserteilung über die Kreditwürdigkeit der Betroffenen zum Zweck haben oder in Form eines Informationsverbundsystems durchgeführt werden sollen.[112] Der Auftraggeber ist verpflichtet einer Aufforderung zur **Nachmeldung** der Datenschutzkommission infolge Mangelhaftigkeit einer registrierten Meldung nachzukommen, andernfalls wird der Betrieb der Datenanwendung untersagt und Anzeige erstattet.[113]

Auftraggeber einer **Standardanwendung** haben die **Pflicht** jedermann auf Anfrage **mitzuteilen**, welche Standardanwendungen sie tatsächlich vornehmen. Sie sind zudem verpflichtet nicht-meldepflichtige Datenanwendungen der Datenschutzkommission bei Ausübung ihrer Kontrollaufgaben (gemäß § 30) offenzulegen.[114]

Zudem besteht eine **Informationspflicht** des Auftraggebers aus Anlass der Ermittlung von Daten die Betroffenen in geeigneter Weise über den Zweck der Datenanwendung, für die die Daten ermittelt werden und über Namen und Adresse des Auftraggebers zu informieren, sofern diese Informationen dem Betroffenen nach den Umständen des Falles nicht bereits vorliegen. Darüber hinausgehende Informationen sind in geeigneter Weise zu geben, wenn dies für eine Verarbeitung nach Treu und Glauben erforderlich ist. Dies gilt insbesondere dann, wenn gegen eine beabsichtigte Verarbeitung oder Übermittlung von Daten ein Widerspruchsrecht des Betroffenen gemäß § 28 besteht oder es für den Betroffenen nach den Umständen des Falles nicht klar erkennbar ist, ob er zur Beantwortung der an ihn gestellten Fragen rechtlich verpflichtet ist, oder Daten in einem Informationsverbundsystem verarbeitet werden sollen, ohne dass dies gesetzlich vorgesehen ist. Wird dem Auftraggeber bekannt, dass Daten aus einer seiner Datenanwendungen systematisch und schwerwiegend unrechtmäßig verwendet wurden und den Betroffenen Schaden droht, hat er darüber unverzüglich die Betroffenen in geeigneter Form zu informieren. Diese Verpflichtung besteht nicht, wenn die Information angesichts der Drohung eines nur geringfügigen Schadens der Betroffenen einerseits oder der Kosten der

---

(3) Weiter sind Datenanwendungen für Zwecke 1. des Schutzes der verfassungsmäßigen Einrichtungen der Republik Österreich oder 2. der Sicherung der Einsatzbereitschaft des Bundesheeres oder 3. der Sicherstellung der Interessen der umfassenden Landesverteidigung oder 4. des Schutzes wichtiger außenpolitischer, wirtschaftlicher oder finanzieller Interessen der Republik Österreich oder der Europäischen Union oder 5. der Vorbeugung, Verhinderung oder Verfolgung von Straftaten, von der Meldepflicht ausgenommen, soweit dies zur Verwirklichung des Zweckes der Datenanwendung notwendig ist.

111 § 17 Abs. 1 DSG.

112 § 18 Abs. 2 DSG.

113 § 22a Abs. 4 DSG.

114 § 23 DSG.

Information aller Betroffenen andererseits einen unverhältnismäßigen Aufwand erfordert. Keine Informationspflicht besteht bei nicht-meldepflichtigen Datenanwendungen.[115]

Ferner trifft den Auftraggeber die Pflicht zur **Offenlegung seiner Identität** bei Übermittlungen und bei Mitteilungen an Betroffene, sodass den Betroffenen die Verfolgung ihrer Rechte möglich ist. Bei meldepflichtigen Datenanwendungen ist in Mitteilungen an Betroffene die **Registernummer** des Auftraggebers anzuführen. Werden Daten aus einer Datenanwendung für Zwecke einer vom Auftraggeber verschiedenen Person verwendet, ohne dass diese ihrerseits ein Verfügungsrecht über die verwendeten Daten und damit die Eigenschaft eines Auftraggebers in Bezug auf die Daten erlangt, dann ist bei Mitteilungen an den Betroffenen neben der Identität der Person, für deren Zwecke die Daten verwendet werden, auch die Identität des Auftraggebers anzugeben, aus dessen Datenanwendung die Daten stammen. Handelt es sich hierbei um eine meldepflichtige Datenanwendung, ist die Registernummer des Auftraggebers beizufügen. Diese Pflicht trifft sowohl den Auftraggeber als auch denjenigen, in dessen Namen die Mitteilung an den Betroffenen erfolgt.[116]

**Weitere Pflichten** des Auftraggebers lassen sich wie folgt aufzählen: Ab dem Zeitpunkt der Kenntnis von einem Auskunftsverlangen darf der Auftraggeber Daten über den Auskunftswerber innerhalb eines Zeitraums von vier Monaten und im Falle der Erhebung einer Beschwerde gemäß § 31 an die Datenschutzkommission bis zum rechtskräftigen Abschluss des Verfahrens nicht vernichten.[117] Wurden im Sinne des Abs. 1 richtiggestellte oder gelöschte Daten vor der Richtigstellung oder Löschung übermittelt, so hat der Auftraggeber die Empfänger dieser Daten hiervon in geeigneter Weise zu verständigen, sofern dies keinen unverhältnismäßigen Aufwand, insbesondere im Hinblick auf das Vorhandensein eines berechtigten Interesses an der Verständigung, bedeutet und die Empfänger noch feststellbar sind.[118] Sofern die Verwendung von Daten nicht gesetzlich vorgesehen ist, hat jeder Betroffene das Recht, gegen die Verwendung seiner Daten wegen Verletzung überwiegender schutzwürdiger Geheimhaltungsinteressen, die sich aus seiner besonderen Situation ergeben, beim Auftraggeber der Datenanwendung Widerspruch zu erheben. Der Auftraggeber hat bei Vorliegen dieser Voraussetzungen die Daten des Betroffenen binnen acht Wochen aus seiner Datenanwendung zu löschen und allfällige Übermittlungen zu unterlassen.[119] Die Datenschutzkommission kann im Fall eines begründeten Verdachtes auf Verletzung der im Abs. 1 genannten Rechte und Pflichten Datenanwendungen überprüfen. Hierbei kann sie vom Auftraggeber oder Dienstleister der überprüften Datenanwendung insbesondere alle notwendigen Aufklärungen verlangen und Einsicht in Datenanwendungen und diesbezügliche Unterlagen begehren.[120] Soweit sich eine Beschwerde nach Abs. 1 oder 2 als berechtigt erweist, ist ihr Folge zu geben und die Rechtsverletzung festzustellen. Ist eine festgestellte Verletzung im Recht auf Auskunft (Abs. 1) einem Auftraggeber des privaten Bereichs zuzurechnen, so ist diesem auf Antrag zusätzlich die – allenfalls erneute – Reaktion auf das Auskunftsbegehren nach § 26 Abs. 4, 5 oder 10 in jenem Umfang aufzutragen, der erforderlich ist, um die festgestellte Rechtsverletzung zu beseitigen.[121] Es besteht auch eine **Pflicht** des Auftraggebers des privaten Bereichs zur **Stellungnahme** zu Entwicklungen von allgemeiner Bedeutung bei Aufforderung

---

115 § 24 DSG.
116 § 25 DSG.
117 § 26 Abs. 7 DSG.
118 § 27 Abs. 8 DSG.
119 § 28 Abs. 1 DSG.
120 § 30 Abs. 2 DSG.
121 § 31 Abs. 7 DSG.

durch den Datenschutzrat, wenn dieser der Ansicht ist, dass die Entwicklungen aus datenschutzrechtlicher Sicht Anlass zu Bedenken oder zumindest Anlass zur Beobachtung geben.[122] Die Auftraggeber eines Informationsverbundsystems haben die Pflicht, soweit dies nicht bereits durch Gesetz geregelt ist, einen geeigneten Betreiber für das System zu bestellen.[123] Der Auftraggeber ist verpflichtet **Videoüberwachungen** der Datenschutzkommission zu melden und geeignet zu kennzeichnen.[124]

Besondere Pflichten der **Auftraggeber des öffentlichen Bereichs** sind wie folgt: Wenn die Datenschutzkommission eine Verletzung von Bestimmungen dieses Bundesgesetzes durch einen Auftraggeber des öffentlichen Bereichs festgestellt hat, so hat dieser mit den ihm zu Gebote stehenden rechtlichen Mitteln unverzüglich den der Rechtsanschauung der Datenschutzkommission entsprechenden Zustand herzustellen.[125] Der Datenschutzrat berät die Bundesregierung und die Landesregierungen auf deren Ersuchen in rechtspolitischen Fragen des Datenschutzes. Zur Erfüllung dieser Aufgabe haben Auftraggeber des öffentlichen Bereichs ihre Vorhaben dem Datenschutzrat zur Stellungnahme zuzuleiten, soweit diese datenschutzrechtlich von Bedeutung sind. Der Datenschutzrat hat das Recht, von Auftraggebern des öffentlichen Bereichs Auskünfte und Berichte sowie die Einsicht in Unterlagen zu verlangen, soweit dies zur datenschutzrechtlichen Beurteilung von Vorhaben mit wesentlichen Auswirkungen auf den Datenschutz in Österreich notwendig ist.[126]

Auftraggeber, Dienstleister und ihre Mitarbeiter haben Daten aus Datenanwendungen, die ihnen ausschließlich **auf Grund ihrer berufsmäßigen Beschäftigung anvertraut** wurden oder zugänglich geworden sind, unbeschadet sonstiger gesetzlicher Verschwiegenheitspflichten, geheim zu halten, soweit kein rechtlich zulässiger Grund für eine Übermittlung der anvertrauten oder zugänglich gewordenen Daten besteht (Datengeheimnis). Mitarbeiter dürfen Daten nur auf Grund einer ausdrücklichen Anordnung ihres Arbeitgebers (Dienstgebers) übermitteln. Auftraggeber und Dienstleister haben, sofern eine solche Verpflichtung ihrer Mitarbeiter nicht schon kraft Gesetzes besteht, diese vertraglich zu verpflichten, dass sie Daten aus Datenanwendungen nur auf Grund von Anordnungen übermitteln und das Datengeheimnis auch nach **Beendigung des Arbeitsverhältnisses** zum Auftraggeber oder Dienstleister einhalten werden. Auftraggeber und Dienstleister dürfen Anordnungen zur Übermittlung von Daten nur erteilen, wenn dies nach den Bestimmungen dieses Bundesgesetzes zulässig ist. Sie haben die von der Anordnung betroffenen Mitarbeiter über die für sie geltenden Übermittlungsanordnungen und über die Folgen einer Verletzung des Datengeheimnisses zu belehren.[127]

Zum Zweck der Einsicht ist die Datenschutzkommission nach Verständigung des Inhabers der Räumlichkeiten und des Auftraggebers (Dienstleisters) berechtigt, Räume, in welchen Datenanwendungen vorgenommen werden, zu betreten, Datenverarbeitungsanlagen in Betrieb zu setzen, die zu überprüfenden Verarbeitungen durchzuführen sowie Kopien von Datenträgern in dem für die Ausübung der Kontrollbefugnisse unbedingt erforderlichen Ausmaß herzustellen. Der Auftraggeber

---

122 § 41 Abs. 2 Ziff. 5 DSG.
123 § 50 Abs. 1 DSG.
124 § 50c Abs. 1 und § 50d Abs. 1 DSG.
125 § 40 Abs. 4 DSG.
126 § 41 Abs. 2 Ziff. 3 und 4 DSG.
127 § 15 Abs. 1-3 DSG.

(Dienstleister) hat die für die Einsicht notwendige **Unterstützung zu leisten**. Die Kontrolltätigkeit ist unter möglichster Schonung der Rechte des Auftraggebers (Dienstleisters) und Dritter auszuüben.[128]

Der **Dienstleisters** hat, unabhängig von allfälligen vertraglichen Vereinbarungen, gesetzlich geregelte Pflichten, welche in § 11 Abs. 1 DSG geregelt sind. Er hat die Pflicht, die Daten ausschließlich im Rahmen der Aufträge des Auftraggebers zu verwenden. Insbesondere ist die Übermittlung der verwendeten Daten ohne Auftrag des Auftraggebers verboten. Er muss zudem alle (gemäß § 14) erforderlichen **Datensicherheitsmaßnahmen** treffen. Insbesondere dürfen für die Dienstleistung nur solche Mitarbeiter herangezogen werden, die sich dem Dienstleister gegenüber zur Einhaltung des Datengeheimnisses verpflichtet haben oder einer gesetzlichen Verschwiegenheitspflicht unterliegen. Er darf weitere Dienstleister nur mit Billigung des Auftraggebers heranziehen und muss deshalb den Auftraggeber von der beabsichtigten Heranziehung eines weiteren Dienstleisters so rechtzeitig verständigen, dass er dies allenfalls untersagen kann. Sofern dies nach der Art der Dienstleistung in Frage kommt – hat er die Pflicht, im Einvernehmen mit dem Auftraggeber, die notwendigen technischen und organisatorischen Voraussetzungen für die Erfüllung der Auskunfts-, Richtigstellungs- und Löschungspflicht des Auftraggebers zu schaffen. Er muss nach Beendigung der Dienstleistung alle Verarbeitungsergebnisse und Unterlagen, die Daten enthalten, dem Auftraggeber zu übergeben oder in dessen Auftrag für ihn weiter aufzubewahren oder zu vernichten. Zudem ist er verpflichtet dem Auftraggeber jene Informationen zur Verfügung zu stellen, die zur Kontrolle der Einhaltung der genannten Verpflichtungen notwendig sind.

Für alle Organisationseinheiten, die Daten verwenden, muss der Dienstleister **Massnahmen zur Gewährleistung der Datensicherheit** treffen. Er ist verpflichtet sicherzustellen, dass die Daten vor zufälliger oder unrechtmäßiger Zerstörung und vor Verlust geschützt sind, dass ihre Verwendung ordnungsgemäß erfolgt und dass die Daten Unbefugten nicht zugänglich sind.[129] Die einzelnen Massnahmen betreffend Datensicherheit sind dieselben **wie jene des Auftraggebers**.

Wird ein Auskunftsbegehren an einen Dienstleister gerichtet und lässt dieses erkennen, dass der Auskunftswerber ihn **irrtümlich** für den Auftraggeber der von ihm betriebenen Datenanwendung hält, hat der Dienstleister das Auskunftsbegehren unverzüglich an den Auftraggeber weiterzuleiten und dem Auskunftswerber mitzuteilen, dass in seinem Auftrag keine Daten verwendet werden.[130]

Spezielle Bestimmungen bestehen zudem für natürliche Personen, welche Daten zu privaten Zwecken verarbeiten (§ 45), für Datenverarbeitungen mit wissenschaftlichem oder statistischem Zweck (§ 46), für die Übermittlung von Adressdaten zum Zwecke ihrer Benachrichtigung oder Befragung der Zustimmung (§ 47), für Datenverwendungen für publizistische Tätigkeit (§ 48) und für die Datenverwendung im Katastrophenfall (§ 48a).

---

128 § 30 Abs. 4 DSG.

129 § 14 Abs. 1 DSG.

130 § 26 Abs. 10 DSG.

# 3. Italien

## 3.1. Grundsätze des Datenschutzes

Section 4 of the Personal Data Protection Code (PDPC) provides that "**processing** shall mean any operation, or set of operations, carried out with or without the help of electronic or automated means, concerning the collection, recording, organization, keeping, interrogation, elaboration, modification, selection, retrieval, comparison, utilization, interconnection, blocking, communication, dissemination, erasure and destruction of data, whether the latter are contained or not in a data bank". In order to be permitted, the operations must comply with the principle of lawfulness, purpose[131], proportionality and necessity[132].

### 3.1.1. Core Principles of data processing

The principles governing the data processing are:

a) principle of lawfulness;
b) principle of purpose;
c) principle of proportionality;
d) principle of necessity.

The principle of **lawfulness** implies that the operations of data processing can be accomplished only if they comply with PDPC. The PDPC makes a distinction between public bodies on one side, and private bodies and profit seeking public bodies on the other side.

As concerns the first, articles 18-23 assume that data processing operations are permitted only **for pursuing their institutional tasks**. Therefore, the data processing operations accomplished by a public body are lawful if they are accomplished for pursuing an institutional task.

As regards the second, articles 23-27 assume that data processing operations are permitted only to the extent to which these are:

a) required by the law[133] ;

---

131 See G. Santianiello, La protezione dei dati personali, Padova, 2005, p. 79 and Bollettino n. 93/April 2008, issued by the Garante della Privacy. In Italian language the principle of purpose is known as *principio di finalità*.

132 See V. Zeno Zencovich, Il codice dei dati personali, Milano, 2005, p. 6.

133 Art. 24 PDPC:

1. Consent shall not be required in the cases referred to in Part II as well as if the processing
a) is necessary to comply with an obligation imposed by a law, regulations or Community legislation;
b) is necessary for the performance of obligations resulting from a contract to which the data subject is a party, or else in order to comply with specific requests made by the data subject prior to entering into a contract;
c) concerns data taken from public registers, lists, documents or records that are publicly available, without prejudice to the limitations and modalities laid down by laws, regulations and Community legislation with regard to their disclosure and publicity;
d) concerns data relating to economic activities that are processed in compliance with the legislation in force as applying to business and industrial secrecy;
e) is necessary to safeguard life or bodily integrity of a third party. If this purpose concerns the data subject and the latter cannot give his/her consent because (s)he is physically unable to do so, legally

b) freely and expressly agreed by the *data subject*[134];
c) authorized by the data protection authority (*Garante*) on the basis of the principle of "*bilanciamento di interessi*"[135].

The **principle of purpose** represents a very fundamental cornerstone for the interpretation of the legal discipline envisaged by PDPC[136]. The principle works on a double perspective. The first one ensures that the interferences on the rights of the data subjects are always accomplished for lawful purposes. In

---

incapable or unable to distinguish right and wrong, the consent shall be given by the entity legally representing the data subject, or else by a next of kin, a family member, a person cohabiting with the data subject or, failing these, the manager of the institution where the data subject is hosted. Section 82(2) shall apply;
f) is necessary for carrying out the investigations by defence counsel referred to in Act no. 397 of 07.12.2000, or else to establish or defend a legal claim, provided that the data are processed exclusively for said purposes and for no longer than is necessary therefore by complying with the legislation in force concerning business and industrial secrecy, dissemination of the data being ruled out;
g) is necessary to pursue a legitimate interest of either the data controller or a third party recipient in the cases specified by the Garante on the basis of the principles set out under the law, also with regard to the activities of banking groups and subsidiaries or related companies, unless said interest is overridden by the data subject's rights and fundamental freedoms, dignity or legitimate interests, dissemination of the data being ruled out;
h) except for external communication and dissemination, is carried out by no-profit associations, bodies or organisations, recognised or not, with regard either to entities having regular contacts with them or to members in order to achieve specific, lawful purposes as set out in the relevant memorandums, articles of association or collective agreements, whereby the mechanisms of utilisation are laid down expressly in a resolution that is notified to data subjects with the information notice provided for by Section 13,
i) is necessary exclusively for scientific and statistical purposes in compliance with the respective codes of professional practice referred to in Annex A), or else exclusively for historical purposes in connection either with private archives that have been declared to be of considerable historical interest pursuant to Section 6(2) of legislative decree no. 499 of 29 October 1999, adopting the consolidated statute on cultural and environmental heritage, or with other private archives pursuant to the provisions made in the relevant codes.

134 According to article 4, i), of the Code, *data subject* "shall mean any natural or legal person, body or association that is the subject of the personal data".
Art. 23 of the Code provides:
1. Processing of personal data by private entities or profit-seeking public bodies shall only be allowed if the data subject gives his/her express consent;
2. The data subject's consent may refer either to the processing as a whole or to one or more of the operations thereof;
3. The data subject's consent shall only be deemed to be effective if it is given freely and specifically with regard to a clearly identified processing operation, if it is documented in writing, and if the data subject has been provided with the information referred to in Section 13.
4. Consent shall be given in writing if the processing concerns sensitive data.

135 See art. 24, g), PDPC, *supra* note 115.
The principle of "*bilanciamento di interessi*" has been defined by legal literature for interpreting the PDPC. In particular, according to some scholars, the *Garante* has the duty to combine the public interest in the free movement of information and the private interest of the *data subject* in impeding that such free movement shall jeopardize his/her dignity and privacy. On this regard, see *supra* note 113, G. Santaniello, op. cit., p. 33.

136 M. Messina, in V. Zeno Zencovich et al., op cit. p. 86.

other words, all the data processing operations are required to pursue purposes which are not contrary to the Italian legal system and to its constitution, even in those cases where the data subject has expressed his/her consent[137]. Thus, in order to be legally permitted, not only the operations of data processing must be lawful, but also their purposes. This is confirmed by article 11, b), of the PDPC, which establishes that

a) the purposes of the data record and collection operation must be specific, explicit and legitimate;
b) the operations of data processing must be consistent with the said purposes.

The second perspective allows for specific legal regulation according to specific purposes[138]. In fact, Part II of PDPC introduces a derogatory regulation of the powers of the *data subject* for specific sectors. It is in fact defined as Provisions Applying to Specific Sectors.

The **principle of necessity** is established by article 3 PDPC[139]. It represents the concern of the legislator for the high-technological devices which are more and more able to record and collect a great number of information regarding the individuals. The idea is that these devices can be employed. Yet, they must be set in a way that they record and collect only those data which are necessary for the purpose of their installation. For example, one might consider the installation of cameras on the speedways with the purpose of analyzing the traffic. This data processing may well be accomplished through anonymous information so that it is not necessary that the cameras record the plates of the vehicles on transit.

At a first glance, the principle of necessity would seem established only for **technical purposes**: it would represent an obligation for software and hardware producers to identify specific procedures for the data collecting and recording. Yet, the norm has a greater range of application. It involves the legal obligation for *data controllers*[140] to process information only to the extent to which the operation "is necessary in a democratic society"[141].

The **principle of proportionality** is strongly connected with the principle of necessity. It is established by article 11, d) of the Code[142] and it provides that the *data controller* has to process the data in accordance

---

137 See point b) envisaged within the discussion on the principle of legality.

138 This approach represents a novel introduced by the PDPC. The previous legislation, the L. 675/96, provided indeed a uniform legal treatment of the data processing operations.

139 Art. 3 provides:
"Information systems and software shall be configured by minimizing the use of personal data and identification data, in such a way as to rule out their processing if the purposes sought in the individual cases can be achieved by using either anonymous data or suitable arrangements to allow identifying data subjects only in cases of necessity, respectively".

140 According to article 4, 'data controller' shall mean any natural or legal person, public administration, body, association or other entity that is competent, also jointly with another data controller, to determine purposes and methods of the processing of personal data and the relevant means, including security matters;

141 See Resta, in V. Zeno-Zencovich at al, *op. cit*., p. 48.

142 Art. 11, let. D) provides that data processing must be:
"relevant, complete and not excessive in relation to the purposes for which they are collected or subsequently processed".

with the purposes for which the data themselves were collected. Moreover, the data collected must be complete and appropriate to the purpose of the processing[143].

### 3.1.2. Visibility/transparency and Consent

The principle of transparency is established by article 7 of the Code[144]. In particular, the first paragraph provides that the *data subject* has the **right to obtain information** as to whether or not personal data concerning him exist, regardless of it being already recorded, and the right to obtain communication of such data in intelligible form. To exert the right to access information it is not necessary that the *data subject* suspects that his/her data are being processed. Rather, the interested individual always has the right to know if that public or private body is processing his/her data.

The concept of consent as established by the code distinguishes **personal data from sensitive data**. In order for personal data to be lawfully processed, art. 23, paragraph 3, establishes that the consent must be expressed freely and specifically in relation to specific data processing. For sensitive data, the consent needs to be given in written form. In addition, previous authorization of the *Garante* is necessary (art. 23, paragraph 4).

Different interpretations related to the **revocability of the consent** have been pointed out by Italian legal literature. On one side, there are not particular problems when the revocability concerns a consent

---

143 According to the Garante, "the principle of proportionality allows, evidently, the data controller to evaluate which personal data are to be collected. Yet, it does not mean that he/she has a total and unchallengeable discretion". See Bollettino del n. 49/aprile 2004.

144 Art. 7 provides:
1. A data subject shall have the right to obtain confirmation as to whether or not personal data concerning him exist, regardless of their being already recorded, and communication of such data in intelligible form.
2. A data subject shall have the right to be informed
a) of the source of the personal data;
b) of the purposes and methods of the processing;
c) of the logic applied to the processing, if the latter is carried out with the help of electronic means;
d) of the identification data concerning data controller, data processors and the representative designated as per Section 5(2);
e) of the entities or categories of entity to whom or which the personal data may be communicated and who or which may get to know said data in their capacity as designated representative(s) in the State's territory, data processor(s) or person(s) in charge of the processing.
3. A data subject shall have the right to obtain
a) updating, rectification or, where interested therein, integration of the data;
b) erasure, anonymization or blocking of data that have been processed unlawfully, including data whose retention is unnecessary for the purposes for which they have been collected or subsequently processed;
c) certification to the effect that the operations as per letters a) and b) have been notified, as also related to their contents, to the entities to whom or which the data were communicated or disseminated, unless this requirement proves impossible or involves a manifestly disproportionate effort compared with the right that is to be protected.
4. A data subject shall have the right to object, in whole or in part,
a) on legitimate grounds, to the processing of personal data concerning him/her, even though they are relevant to the purpose of the collection;
b) to the processing of personal data concerning him/her, where it is carried out for the purpose of sending advertising materials or direct selling or else for the performance of market or commercial communication surveys.

expressed out of a contractual relationship. In cases like this, the *data subject* is always acknowledged to obtain the interruption of the data processing and the destruction of the data themselves. On the other side, when the revocability implies a consent expressed for establishing a contractual relationship, the relevant solution shall depend on the particular meaning conferred to the fundamental right of data protection.
On this respect, Italian scholars have proposed four solutions:

a) the contract is void as its object involves inalienable and not possible to be surrendered rights;
b) the contract is valid but only regarding the economic aspects, so that the consent to the data processing can always be revoked;
c) the contract is valid, but the *data subject* can revoke the consent for lawful reasons;
d) the contract is valid and only another agreement could terminate it.

In the opinion of one author, the solution c) is the one to be preferred[145].

### 3.1.3. Liability and Dignity

Others principles envisaged in the Code that deserve to be mentioned are:

a) the principle of loyalty,
b) the principle of dignity.

The **principle of loyalty** is established by article 1 PDPC[146]. The article reproduces exactly the provisions contained in the art. 8 of the Charter of Fundamental Rights of the European Union. Basically the norm aims at avoiding conflict of interests between the *data controller* and the *data subject*.

The **principle of dignity** is established by article 2 PDPC[147] and it is recalled by articles 17,22,24,83,174,178,179. All these references lead to assume that this principle strongly underpins the whole discipline of the data protection. The norms provide that the data processing must be accomplished while respecting the human dignity. Yet, it is very important to underscore that the abuse of such concept to limit private autonomy could empty out its original meaning[148].

---

145 See Resta, Op. Cit. 11, p. 56.

146 Art.1 CPD: "Everyone has the right to protection of the personal data concerning them. The information on performance of the tasks applying to any entity that is in charge of public functions including the respective evaluation data shall not be the subject of privacy safeguards".

147 Article 2 of the Code provides:
1. This consolidated statute, hereinafter referred to as "Code", shall ensure that personal data are processed by respecting data subjects' rights, fundamental freedoms and dignity, particularly with regard to confidentiality, personal identity and the right to personal data protection.
2. The processing of personal data shall be regulated by affording a high level of protection for the rights and freedoms referred to in paragraph 1 in compliance with the principles of simplification, harmonization and effectiveness of the mechanisms by which data subjects can exercise such rights and data controllers can fulfill the relevant obligations.

148 For example, the concept of dignity has recently been employed by the French *Counseil d'Etat* to prohibit the "Dwarf Tossing" game arguing that it is against the human dignity. For a complete list of cases concerning the employment of the concept of dignity see H. Dreier, *Sub Art. 1 I GG* in Id., a cura di, GrundGesetz Kommentar, München, 2003.

Article 2, at paragraph 2 PDPC[149], reproduces also a typical communitarian principle, the **principle of high level of protection**[150]. According to this norm, the high level of protection of the rights envisaged by the data protection discipline is ensured by complying with harmonization, simplification and effectiveness criteria. In particular, such criteria must be adopted either by the *data controller* in the fulfillment of the obligations required by law and by the *data subjects* in the exertion of the rights acknowledged by the said discipline.

### 3.1.4. Particularly sensitive data processing

The sensitive data are defined by article 4, letter d) PDPC. According to the provision, "'sensitive data' shall mean personal data allowing the disclosure of racial or ethnic origin, religious, philosophical or other beliefs, political opinions, membership of parties, trade unions, associations or organizations of a religious, philosophical, political or trade-unionist character, as well as personal data disclosing health and sex life".

Under article 26(1) PDPC private bodies and profit-seeking public bodies may only process sensitive data upon authorization by the Garante and the *data subjects*' written consent. Therefore, to accomplish sensitive data operations **both conditions must be satisfied**. The data processing is subject to compliance with the conditions and limitations set out in the PDPC as well as in laws and regulations.

As concerns the **written consent**, it is useful to make some remarks. Firstly, the fact that the written form is necessary means that the oral consent is invalid. Secondly, as it is envisaged for normal personal data, the consent must be expressed specifically and freely in relation to a determined subject. Thirdly, according to article 26 paragraph 4 PDPC, consent is not necessary in specific situations (non-profit organizations, protection of third party's life or bodily integrity)[151].

---

149 See *supra* note 129.

150 This principle can indeed found also in art. 153 of the Rome Treaty.

151 1. Sensitive data may only be processed with the data subject's written consent and the Garante's prior authorisation, by complying with the prerequisites and limitations set out in this Code as well as in laws and regulations.
2. The Garante shall communicate its decision concerning the request for authorisation within fortyfive days; failing a communication at the expiry of said term, the request shall be regarded as dismissed. Along with the authorisation or thereafter, based also on verification, the Garante may provide for measures and precautions in order to safeguard the data subject, which the data controller shall be bound to apply.
3. Paragraph 1 shall not apply to processing
a) of the data concerning members of religious denominations and entities having regular contact with said denominations for exclusively religious purposes, on condition that the data are processed by the relevant organs or bodies recognised under civil law and are not communicated or disseminated outside said denominations. The latter shall lay down suitable safeguards with regard to the processing operations performed by complying with the relevant principles as set out in an authorisation by the Garante;
b) of the data concerning affiliation of trade unions and/or trade associations or organisations to other trade unions and/or trade associations, organisations or confederations.
4. Sensitive data may also be processed without consent, subject to the Garante's authorisation,
a) if the processing is carried out for specific, lawful purposes as set out in the relevant memorandums, articles of association or collective agreements by not-for-profit associations, bodies or organisations, whether recognised or not, of political, philosophical, religious or trade-unionist nature, including political

As regards the **authorization** to the data processing, the Garante has so far issued acts containing general authorizations of one year validity. This explains also why these acts are issued each year[152].

All the *data controllers* that deal with the sensitive data which are referred by the authorizations, must accomplish the processing operations in accordance with the conditions, purposes, modalities and limitations established in the acts themselves. The *data controllers* wishing to accomplish data processing operations which do not fall within the general authorizations must apply to the Garante for a specific authorization.

### 3.1.5. Data security

The Code ensures the protection of the data by distinguishing general and specific measures.

The **general measures** are regulated by article 31 PDPC. The article establishes that the data shall be administered in such a way that the risk of their destruction, loss and the illegal access to them shall be kept as low as possible.

The **specific measures** depend on the way the data are processed (electronic or non-electronic devices) and to the type of data processed (sensitive, normal, and judicial). At article 32 PDPC, the law explains that these specific measures aim at ensuring a minimum level of protection of the data. For example to ensure a minimum level of protection to data processed by electronic means, it is necessary to provide a computerized authentication. The technical ways through which such computerized authentication is to

---

parties and movements, with regard to personal data concerning members and/or entities having regular contacts with said associations, bodies or organisations in connection with the aforementioned purposes, provided that the data are not communicated or disclosed outside and the bodies, associations or organisations lay down suitable safeguards in respect of the processing operations performed by expressly setting out the arrangements for using the data through a resolution that shall be made known to data subjects at the time of providing the information under Section 13;
b) if the processing is necessary to protect a third party's life or bodily integrity. If this purpose concerns the data subject and the latter cannot give his/her consent because (s)he is physically unable to do so, legally incapable or unable to distinguish right and wrong, the consent shall be given by the entity legally representing the data subject, or else by a next of kin, a family member, a person cohabiting with the data subject or, failing these, the manager of the institution where the data subject is hosted. Section 82(2) shall apply;
c) if the processing is necessary for carrying out the investigations by defense counsel referred to in Act no. 397 of 07.12.2000, or else to establish or defend a legal claim, provided that the data are processed exclusively for said purposes and for no longer than is necessary therefore. Said claim must not be overridden by the data subject's claim, or else must consist in a personal right or another fundamental, inviolable right or freedom, if the data can disclose health and sex life;
d) if the processing is necessary to comply with specific obligations and/or tasks laid down by laws, regulations or Community legislation in the employment context, also with regard to occupational and population hygiene and safety and to social security and assistance purposes, to the extent that it is provided for in the authorisation and subject to the requirements of the code of conduct and professional practice referred to in Section 111.

[152] The authorization of the Garante may be issued also *ex officio* by way of general provisions applying to specific categories of controller and/or processing. On this regard article 40 of the Code provides: "The provisions of this Code referring to an authorization to be granted by the Garante shall also be implemented by issuing authorizations applying to specific categories of data controller or processing, which shall be published in the Official Journal of the Italian Republic".

be accomplished are described by the Annex B of the Code. The Annex is periodically updated by a degree of the Minister of Justice.

It is important to note that the Annex B does not identify the subjects charged with the adoption of the measures. This means that other than the *data controller*, also the *data processor* and the *persons in charge of the processing*[153] are expected to respect the specific measures. Thus, for instance, the *data controller* shall receive from the installer of a technical device a declaration certifying that the intervention was accomplished complying with the provisions of the Annex B[154].

### 3.1.6. Cross-border notification

The spirit of the law is to liberalize the transfer of personal data among EU countries and even towards non-EU countries. Cross-border notification requires the authorization of the Garante for the specific cases enlisted by art. 37 PDPC.

For transfer of personal data to a EU member state, the movement of data is generally free, yet there are some exceptions. According to the second part of art. 42 of the Code, the exceptions refer to those "prohibition Acts" issued by the Garante and the Courts dealing with data transfers which are accomplished in order to elude the norms of the Code.

The transfer of personal data (even temporary one) to a non-EU member state, is permitted (article 43 PDPC) :

a) if the data subject has given his/her consent either expressly or, where the transfer concerns sensitive data, in writing;
b) if the transfer is necessary for the performance of obligations resulting from a contract to which the data subject is a party, or to take steps at the data subject's request prior to entering into a contract, or for the conclusion or performance of a contract made in the interest of the data subject;
c) if the transfer is necessary for safeguarding a substantial public interest that is referred to by laws or regulations, or else that is specified in pursuance of Sections 20 and 21 where the transfer concerns sensitive or judicial data;
d) if the transfer is necessary to safeguard a third party's life or bodily integrity. If this purpose concerns the data subject and the latter cannot give his/her consent because (s)he is physically unable to do so, legally incapable or unable to distinguish right and wrong, the consent shall be given by the entity legally representing the data subject, or else by a next of kin, a family member, a person cohabiting with the data subject or, failing these, the manager of the institution where the data subject is hosted. Section 82(2) shall apply;
e) if the transfer is necessary for carrying out the investigations by defence counsel referred to in Act no. 397 of 07.12.2000, or else to establish or defend a legal claim, provided that the data are transferred

---

153 According to article 4 PDPC:
g) "data processor" shall mean any natural or legal person, public administration, body, association or other agency that processes personal data on the controller's behalf;

h) "persons in charge of the processing" shall mean the natural persons that have been authorised by the data controller or processor to carry out processing operations.

154 See A. Pinori, La protezione dei dati personali, Milano 2004, p. 192.

exclusively for said purposes and for no longer than is necessary therefore in compliance with the legislation in force applying to business and industrial secrecy;
f) if the transfer is carried out in response to a request for access to administrative records or for information contained in a publicly available register, list, record or document, in compliance with the provisions applying to this subject-matter;
g) if the transfer is necessary, pursuant to the relevant codes of conduct referred to in Annex A), exclusively for scientific or statistical purposes, or else exclusively for historical purposes, in connection with private archives that have been declared to be of considerable historical interest under Section 6(2) of legislative decree no. 490 of 29 October 1999, enacted to adopt the consolidated statute on cultural and environmental heritage, or else in connection with other private
archives pursuant to the provisions made in said codes;
h) if the processing concerns data relating to legal persons, bodies or associations.

In any case, the transfer to a non-EU country is also possible if supported by the Authorization of the Garante. Such authorization must be provided on the basis of adequate warranties concerning the rights of the data subject (art. 44)[155].
Finally, article 45 prohibits transferring personal data to non-EU countries which do not ensure a **minimum level of protection** of individuals.

### 3.1.7. Right to information

The *data controller* is obliged to provide accurate information to the *data subject*. PDPC contains a detailed list of the information expected to be communicated to the *data subject*. Legal literature generally distinguishes three categories of information[156].

The first category concerns the information that **necessarily** must be provided:
a) the identity of the data controller or of his agent (art. 13, paragraph 1, letter f);
b) the possibility to exert the rights acknowledged to the data subject by the art. 7 (art. 13, paragraph 1, letter e);
c) the purposes for which data are collected (art. 13, paragraph 1, let. A).

[155] Art. 44 establishes that:

> 1. The transfer of processed personal data to a non-EU Member State shall also be permitted if it is authorised by the Garante on the basis of adequate safeguards for data subjects' rights
>
> a) as determined by the Garante also in connection with contractual safeguards, or else by means of rules of conduct as in force within the framework of companies all belonging to the same group. A data subject may establish his/her rights in the State's territory as set forth by this Code also with regard to non-compliance with the aforementioned safeguards.
>
> b) as determined via the decisions referred to in Articles 25(6) and 26(4) of Directive 95/46/EC of the European Parliament and of the Council, of 24 October 1995, through which the European Commission may find that a non-EU Member State affords an adequate level of protection, or else that certain contractual clauses afford sufficient safeguards.

[156] See A. Pinori, op. cit., p. 149.

The second category regards the information that, are to be communicated to the *data subject* **for conventional reasons**. This duty of fairness and transparency is due when the *data subject* has not received the mentioned information yet.
In particular these information regard:

a) the modalities of data processing (art. 13, paragraph 1, let. a);
b) the compulsory or voluntary nature of the (*data subject's*) act of providing personal data (art. 13, paragraph 1, let. b);
c) the consequences of a possible refuse to answer (art. 13, paragraph 1, let. c);
d) the indication of the name of at least one responsible (whereas designated), the website of the network and the modalities through which it is possible to know the updated list of the responsible persons;
e) the subjects and the categories to which the data can be communicated and the subjects and the categories that may end up to know the data (article 13, paragraph 1, let. d).

The third category implies the information that **may be omitted** by the *data controller*. The knowledge of this information may in fact hinder the accomplishment of investigation and control activities performed by public authorities for security and defense purposes.

Concerning the **modalities of the information**, the form of the communication of the information may be written as well as oral. The moment of information depends on the way the data are collected. When the personal data are collected directly from the data subject, then the communication of the information must precede the data collection. When the data are collected from a third party, then the information may be transmitted at a later stage.
On this respect, the Code provides that the third party has not to transmit the information when:

a) the data are processed in order to comply with statutory requirements;
b) it is impossible or it involves an employment of devices/tools which is not proportional to the right protected;
c) the data processing is accomplished to protect or to defend a right before the Court; or for the accomplishment of investigation activities in criminal areas.

The scope of these provisions is clearly represented by the attenuation of the difficulties that the communication of the information may involve.

### 3.1.8. Relationship between technology development and data protection

The intense dynamicity of the technological applications and the relentless strengthening of the individual and collective rights do not allow any strict regulation[157]. Therefore, the PDPC is made of **principles and general orientations**, especially in the field of new technologies. It provides for an adoption of a code of conduct in the field of video-surveillance and internet and electronic networks (sections 133 and 134). As discussed above (3.1.1.), the principle of necessity is particularly relevant in the field of new technologies.

---

[157] G. Rasi, Progresso tecnologico e sviluppo civile: la tutela dei dati personali, in Innovazioni Tecnologiche e Privacy, available on: http://www.garanteprivacy.it/garante/document?ID=1595454 (13.09.2010).

The Code does, however, contain specific rules on **electronic communication** services. In that regards, there is a prohibition to use an electronic communication network to gain access to information stored in the terminal equipment of a subscriber or to monitor operations performed by a user, except according to a code of conduct to be established (section 122). The law also requires an eradiction of traffic data when it is not necessary and a strict possibility for processing data for billing or marketing purposes, if information is provided (asection 123 and 124). Exceptions are possible (retention for 30 months) for purposes of criminal prosecution and detection by the relevant authorities (section 132). Several rather detailed provisions exist on calling line identifications, nuisance and emergency calls, automatic call forwarding, directories of subscribers and unsolicited communications, aiming in substance to allow those actions only with consent of the subscriber or, at least, providing for a possibility of opting out (sections 125 to 130).[158] Special provisions Finally, providers of electronic communication services also have a **duty to inform** subscribers and users on the possibility of communications to be known to third persons (section 132).

Concrete and specific regulation in the field of new technologies and their applications can be issued by the *Garante* through the ***provvedimenti generali*** (general acts). The independent authority of the *Garante* has therefore its constant task to adjust, update and monitor the discipline of particular sectors. Thus, the PDPC aims at keeping datra protection in line with technological development by providing for a specific, flexible institution.

### 3.1.9. Difference between the processing performed by private individuals and treatments performed by public authorities (administrations)

The first and very important difference between the data processing performed by private bodies and that performed by public ones concerns the **requirement of the consent** of the *data subject*. On this respect, art. 18 paragraph 4 PDPC provides that "public bodies shall not be required to obtain the data subject's consent".

The mentioned "discrimination" is due to the fact that according to the Italian law, the public bodies necessarily pursue public interests and, as such, they are subject to the **principle of legality**. In other words, the statutes (so, the law) that govern these entities ensure that the data processing shall be accomplished only for institutional tasks (that is, for public interests), as it is required by article 18, paragraph 2[159].

This reasoning becomes clearer if one considers a private *data controller* that pursues public interests. The private data controller is not subject to the principle of legality. Its governance is established by the contractual choices of the parties that have established it. For this reason,

a) there is not any warranty that the data processed by such entities shall aim at pursuing public interests;
b) the consent of the *data subject* is necessary.

---

158 See the translated text of the provisions, available at http://www.privacy.it/privacycode-en.html#sect161 (15.11.2010).

159 Art. 18, paragraph 2 provides in fact that "Public bodies shall only be permitted to process personal data in order to discharge their institutional tasks".

Another important difference is established by article 19 paragraph 1 PDPC which allows the data processing from public bodies even in the **absence of a statutory or regulative** rule[160].

Also concerning the **sensitive data**, the PDPC makes a distinction between private and public *data controller*[161].

The PDPC provides three cases that describe how the sensitive data can be processed by public bodies:

a) when it is expressly provided by a statute and when the statute itself specifies which data are to be processed and for which public purposes;
b) when the law specifies the public purpose but not the data. In such a case the data processing is allowed only for the types of data and the operations that can be identified by an act of the *Garante*. The *Garante* shall take into consideration the types of data and the operations made public by the body concerned (art. 154, paragraph 1);
c) when there is not an express statutory norm. In this case, the public *data controller* may ask to the Garante an authorization aimed at identifying the activities for which it is possible to process sensitive data. The identification of the activities shall be accomplished on the basis of the interpretation of the law concerned (that is, the statute which does not provide the express norm). The Garante of course shall also identify the type of data and the operations in the way described above.

The general principles established by art. 1-17 PDPC apply equally to public bodies. Art. 18-23 PDPC are dedicated exclusively by data processing accomplished by public *data controllers*.

## 3.2. Durchsetzungsrechte der Datenschutzanliegen für Betroffene

### 3.2.1. Data processing by private and by public. Blocking, Rectification, Elimination

The key norm concerning the protection of the personal data is **article 7 PDPC**. Paragraphs 1 and 2 establish the principle of transparency (see above, 3.1.3.). Paragraph 3 establishes that the *data subject* has the "right to obtain" the accomplishment of the actions described in point a), b) and c)[162]. Legal literature suggests that the "right to obtain" reflects also a "right to intervene" into the "legal sphere" of the *data controllers* in order to force them to take measures aimed at protecting the data subject[163].

---

160 See answer 2.1.1, in particular the discussion on the principle of lawfulness.

161 As seen in answer 2.1.5, the private controllers cannot process sensitive data unless they have an express authorization of the Garante and the written consent of the *data subject*.

162 Paragraph 3 provides: "A data subject shall have the right to obtain
a) updating, rectification or, where interested therein, integration of the data;
b) erasure, anonymization or blocking of data that have been processed unlawfully, including data whose retention is unnecessary for the purposes for which they have been collected or subsequently processed;
c) certification to the effect that the operations as per letters a) and b) have been notified, as also related to their contents, to the entities to whom or which the data were communicated or disseminated, unless this requirement proves impossible or involves a manifestly disproportionate effort compared with the right that is to be protected".

163 V.Italia, Codice della privacy, Tomo I, 2004, Milano, p. 80.

To begin with, letter a) provides that whereas the *data subject* is sure, or suspects, that his own personal data – the ones contained in the database – do not correspond to the reality, he can ask that the data are **updated, corrected (rectification), or integrated**.

Concerning the latter, the norm specifies that data can be integrated only if the data subject demonstrates an interest in the integration. In particular, the data subject must demonstrate that the ensemble of personal data is not complete and that the relevant absence of elements jeopardizes his protection.

Letter b) of the paragraph, establishes that the *data subject* – after having ascertained that the data procession was not accomplished in compliance with the law – has the right to require:

a) the **eradiation of the data**. This radical solution is thought to be applicable in the cases where the violation of the rules on the data processing has been so gross that the only way to protect the data consists in deleting thedata;

b) the **transformation into anonymous form of the personal data**. This action would avoid any direct reference to the data subject;

c) the **blocking** of the data. This measure is precautionary, as, according to art. 4 letter o) PDPC, 'blocking' shall mean keeping personal data by temporarily suspending any other processing operation. The temporary character of the suspension is a direct consequence of the fact that the personal data shall return to be processed in accordance with the law.

The measures of eradication, transformation and blocking of the data can be obtained by the *data subject* not only in the cases of unlawful data processing, but also in cases where the data processing is **no longer necessary**. This norm reflects the general principle of necessity established by article 3 of the Code[164].

Finally, letter c) of the paragraph provides that the data subject may obtain that the **certification of the accomplishment** of the above mentioned measures (rectification, integration, cancelation, transformation and block of the data) is transmitted to all the data controllers to which the personal data had been widespread. The norm allows also that these *data controllers* shall know not only the accomplishment of the measure, but also its specific content.

Article 7 paragraph 4 PDPC presents the **right to object**. While the "rights to obtain" somehow involv a request concerning the data processing, the right to object is aimed at contrasting the data processing. Letter a) establishes that the *data subject* has the right to object the data processing only under the following reasons:

a) reasons connected to the lawfulness. That is, when the data processing is accomplished by violating the norms of the Code;

b) reasons connected to the lawfulness and to the lawfulness of the scope of the data processing. The norm basically establishes that even if the scope of the data processing is lawful, the non-compliance with the provisions of the Code allows the data subject to object the data processing.

---

[164] See answer 2.1.1

Letter b) of the paragraph 4, moreover, provides that the *data subject* can **object** to the data processing when such activity involves only **marketing purposes**. The right to the data protection prevails, therefore, on the *lex mercatoria* which promote the private economic initiative under art. 41 of the Italian Constitution. The *data subject* can object in whole or in part.

### 3.2.2. Proceeding, Communication and Publication, Elimination of the Consequences of unlawful processing.

According to article 8, paragraph 1 DPDC, the *data subject* has to exert his rights through a **request** addressed to the *data controller* or to the *data processor*. It is not necessary that the request is personally transmitted. The *data subject* can charge somebody to act on his behalf[165].

As provided by article 145 DPDC, if the data subject is not satisfied with the data controller actions, he may **enforce** the rights provided at art. 7 in Court or through complaints addressed to the Garante. The rights provided at article 7 are not always enforceable. In fact, the mentioned art. 8 provides a series of exceptions concerned with public interests and public security[166]-[167].

---

[165] Article 9 describes the forms of the request. In particular, it establishes that the request can be transmitted also by registered letter, fax or by email. It is possible also to advance an oral request, but only for the rights provided by paragraph 1 and 2 of article 7.

[166] Art. 8, paragraph 2, provides: "The rights referred to in Section 7 may not be exercised by making a request to the data controller or processor, or else by lodging a complaint in pursuance of Section 145, if the personal data are processed:
a) pursuant to the provisions of decree-law no. 143 of 3 May 1991, as converted, with amendments, into Act no. 197 of 5 July 1991 and subsequently amended, concerning money laundering;
b) pursuant to the provisions of decree-law no. 419 of 31 December 1991, as converted, with amendments, into Act no. 172 of 18 February 1992 and subsequently amended, concerning support for victims of extortion;
c) by parliamentary Inquiry Committees set up as per Article 82 of the Constitution;
d) by a public body other than a profit-seeking public body, where this is expressly requiredby a law for purposes exclusively related to currency and financial policy, the system of payments, control of brokers and credit and financial markets and protection of their stability;
e) in pursuance of Section 24(1), letter f), as regards the period during which performance of the investigations by defence counsel or establishment of the legal claim might be actually and concretely prejudiced;
f) by providers of publicly available electronic communications services in respect of incoming phone calls, unless this may be actually and concretely prejudicial to performance of the investigations by defence counsel as per Act no. 397 of 7 December 2000;
g) for reasons of justice by judicial authorities at all levels and of all instances as well as by the Higher Council of the Judiciary or other self-regulatory bodies, or else by the Ministry of Justice;
h) in pursuance of Section 53, without prejudice to Act no. 121 of 1 April 1981.

[167] According to article 9, the *legitimatio* for the enforcement of the rights rests with the *data subject*. Yet, when this is dead, the rights can be exercised by "any entity that is interested therein or else acts to protect a data subject or for family related reasons deserving protection".
Moreover, it is provided that the identity of the *data subject* must be ascertained on the basis of suitable documents. The person who acts on behalf of the data subject has to exhibit or to annex a copy of the power of attorney which shall have been undersigned by the data subject in the presence of a person in charge of the processing or else shall bear the data subject's signature and be produced jointly with a copy of an ID document from the data subject, which shall not have to be certified true pursuant to law. If the

The proceedings before the administrative authority are regulated by articles 141 seq DPDC. Article 141 provides three kinds of procedures before the Garante. In particular, it is possible to apply to the Garante through:

a) **circumstantial claim** ;
b) **report**;
c) **complaint**.

### *3.2.2.1. Complaint*

The most significant of the three proceeding is the complaint, for it represents a "ricorso amministrativo", a very **formal** proceeding[168]. In fact, it is possible to lodge a complaint only if:

a) the formalities envisaged by article 147 PDPC are respected;
b) it concerns one of the rights established by article 7 PDPC;
c) the *data subject* has previously presented a request to the data controller and the relevant response has not been provided within the term of 15 days or 30 when the request is particularly complex or the request has not been fully accepted (art. 146). The article anyways specifies that it is possible to apply directly to the Garante when "the running of time would cause imminent, irreparable harm to a person".

In many respects, proceedings before the Garante are **similar to proceedings before the ordinary judicial court**[169]. This means that the legislator wanted to confer a strong protection of the right to privacy.

---

data subject is a legal person, a body or association, the relevant request shall be made by the natural person that is legally authorized thereto based on the relevant regulations or articles of association.

168 It is important to remark that from a strict legal point of view the "ricorso amministrativo" is lodged against the acts of the Public Administration and is addressed to the Public Administration. Yet, the law speaks about "ricorsi" also concerning the acts of private, as for example the data processing, addressed to the Independent Authorities, such as the Garante.

169 The Code at art. 15 establishes that the *data subject* is entitled to compensation whereas the data processing has caused to him damages. It is possible also to obtain compensation for non-pecuniary damages. Of course, this kind of protection has to be asked to the judicial Court. The burden of proof belongs to the *data controller*, in fact it has to demonstrate the it adopted all the necessary measures. This rule of "special liability" is the one identified by article 2050 of the Civil Code. The hypothetical fact situations that may cause damages to the *data subject* are not expressly identified by the legislation. Yet, they arise pursuant to the violation of the following norms:

- conducts described by art. 11;
- information (art. 13);
- definition of the profiles and of the personality of the data subject (art. 14);
- termination of data processing (art 16);
- particularly risky data processing operations (art. 17);
- prohibition communication and diffusion (art. 25);
- consent (art. 23);
- specific discipline envisaged for the public bodies (art. 18-22);
- specific discipline envisaged for the private bodies and for the economic public bodies (23, 26, 27);
- security measures (art. 33-35);
- transfer of data abroad (art. 42-45).

The “ricorso amministrativo” is therefore an alternative solution to the judicial protection. Its proceeding presents either very similar aspects to the judicial proceedings, for example it is articulated on the basis of the principle of due process (*contraddittorio tra le parti*), but also different ones, such as the great ex officio powers of the Garante.

To begin with, the Garante may declare that the complaint is “manifestamente infondato” (manifestly groundless) or “inammissibile” (inadmissible) (art. 149, paragraph 1). The first case concerns the merit of the question while the second concerns procedural faults. If the Garante declares one of these two conditions, it will not communicate anything to the *data controller*. Otherwise, within three days it has to transmit notice to the data controller, requiring him to comply spontaneously with the *data subject* request. The *data controller* has ten days to decide whether to comply or not. It is worth to remind that he already had 15 or 30 days running from the moment he received the request from the *data subject*. If the *data controller* decides not to comply or to comply only in part, the Garante shall summon the parties for the hearing. The Garante may order, also ex officio, that one or more expert assessments be carried out (art. 149, paragraph 2).

The Garante has to adopt a **decision within 60 days** running from the day of the presentation of the complaint. Yet, a prorogation of maximum 40 days is possible if the question is particularly complex. If the Garante does not adopt any decision, then the complaint is considered as implicitly “rejected” (art. 152, paragraph 2 DPDC).

In addition to final and definitive decisions, the Garante may adopt **cautionary measures**. It may well happen indeed that the time which is necessary to adopt a final decision shall jeopardize the rights of the *data subject*.
The cautionary measures are well identified by the law:

a) **blocking of the data**;
b) **suspension of the data processing**.

The difference between the two measures is the fact that blocking concerns the entire data of the data subject: all processing of such data shall be blocked; the suspension only has an impact on the data processing operations: the measure can in fact be addresses only to certain operations.

It is important to underscore some aspects that render the cautionary measures **different** from the cautionary measures adopted by the **ordinary Court**:

a) the Garante may adopt such measures ex officio;
b) the Garante may adopt such measures even before the hearing is established (*ante causam*);
c) the cautionary measure adopted by the Garante cannot be challenged separately from the challenge of the final decision;
d) the cautionary measures adopted by the Garante can not be “directly enforced” through the intervention of public officers. Their enforcement is indirectly ensured by the crime law sanction provided by art. 170 which provides that “whoever fails to comply with a provision issued by the Garante pursuant to Sections 26(2), 90, 150(1) and (2) and 143(1), letter c), in breach of the relevant obligations, shall be punished by imprisonment for between three months and two years”.

During the proceeding, the Garante has extensive powers which go beyond those of an ordinary judge. This is understandable even by the reading of the peculiarities concerning the cautionary measures.

The Garante may **gather the necessary information**. That implies two things:

a) the Garante may gather information also *ex officio*, therefore without an express request from the parties;
b) in order to gather information, the Garante may use all the inspective, controlling and monitoring powers.

The power of gathering information is supported by the **administrative sanction** that might be applied to everyone that refuses to give or exhibit the information or the documents required by the Garante (art. 164).

The Garante may access even very personal venues, such private houses. Yet, in order to do that, an authorization from the President of a Court is necessary.

The Garante has to **communicate** its decision, whether cautionary or definitive, to the parties within 10 days. The Garante establishes also the modalities through which its decision has to be executed. The decision is definitive in the sense that it cannot be modified unless one of the parties exerts its right to appeal.

The **right of appeal** has to be exerted before the ordinary Court within thirty days from the communication of the decision. The initiation of the proceeding of appeal does not suspend the decision previously adopted by the Garante, unless the judge decides otherwise upon request of one party[170].

Article 152, paragraph 12 PDPC provides that "with its judgment, the court shall grant or dismiss the petition, in whole or in part, order the necessary measures, provide for damages, if claimed, and award legal costs to the losing party, also by derogating from the prohibition referred to in Section 4 of Act no. 2248 of 20 March 1865, Annex E), whenever this is necessary in connection with, inter alia, acts performed by a public body in its capacity as data controller or processor". The decision of the ordinary Court can be challenged only before the Supreme Court.

#### *3.2.2.2. Circumstancial Claim*

Following the order of importance of the proceedings, one finds the **circumstantial claim**. This represents a new instate for the Italian law. The circumstantial claim can be presented for the following reasons/purposes:

a) the *data subject* is not satisfied with the protection of the rights enlisted by art. 7;
b) the *data subject* is meant to promote a decision of the Garante on a question of its competence.

The circumstantial claim is followed by a **preliminary hearing investigation** and the adoption of one of the following measures:

a) urging the *data controller* to spontaneously block the processing of the data indicated in the claim;
b) mandating to the *data controller* to adopt the most opportune and necessary measures in order to the render the data processing lawful;
c) ordering the block of the data processing in whole or in part when:

---

170 This is possible only concerning cases expressly envisaged by the law.

1) the data processing is unlawful;
2) there is the danger that one or more data subjects may be jeopardized by the data processing, considered the particular nature of the data processed;

d) prohibiting, in whole or in part, the data processing when this does not comply with the interests of the community.

The last paragraph of article 143 DPDC establishes that the measures adopted by the Garante are to be **published** in the Gazzetta Ufficiale every time the relevant addressees cannot be easily identified on account either of their number or of the complexity of the inquiries.

#### *3.2.2.3. Report*

The least formal proceeding is the **report**. The article 144 provides that the Garante may take the same actions of those envisaged for the circumstantial claims.
The difference between the report and the circumstantial claim is represented by the fact the latter involves a detailed description of the facts and of the legal questions while the former involves only an **invitation** addressed to the Garante in order to this intervene for the compliance of the discipline. Therefore, a *data subject* would rather initiate a report proceeding when for example he does not have sufficient information to initiate a circumstantial claim.

## 3.3. Nationale Aufsichtsbehörde

### 3.3.1 Form of authority

The National Data protection authority is called "Garante". It is a **panel** made of four members. It carries on its functions in an independent and autonomous way. The Garante is an "Autorità Amministrativa Indipendente" (Independent Administrative Authority).

### 3.3.2. Measures to guarantee independence

#### *3.3.2.1. Election*

The following three factors aim at assuring independence of the "Garante" from the political bodies:

a) its mechanism of members' appointment;
b) the personal requirements for the appointment of the members;
c) the conditions related to the duration of the mandate.

As concerns point a), the law envisages that the **Parliament shall choose the members**. In particular, two of the members shall be elected by the Senate and the other two by the Chamber of Deputies. The election shall be accomplished through a "limited vote" mechanism, i.e. a mechanism according to which each voter can express a number of preferences which is not higher than the seats to be covered. Therefore, every voter can express a maximum of three preferences.

For the formalization of the appointment, a decree by the President of the Republic is not necessary. The Parliamentary legitimization and the limited voted mechanism allow the minorities to be involved into the exertion of such constitutional functions.

As concerns point b), the independence of the panel is ensured by the requirement that the panel shall include members who are expert in law and in computer science (art. 153).

Finally, with regars to point c), the duration of the mandate is shorter than the one of the Parliament: four and five years respectively. There is the possibility that the mandate is confirmed one more time. The rationale of the norm is represented by the intention of avoiding undue interferences and of ensuring a certain degree of action to the Authority.

#### *3.3.2.2. Relation with Other Authorities*

Paragraphs 3, 4, and 6 of article 154 – as well as part of paragraph 5 – PDPC regulate certain obligations and tasks concerning third bodies. According to art. 154 paragraph 3 PDPC the *Garante* has to **cooperate with other national Independent Authorities** such authorities during the accomplishment of its tasks.

Paragraph 4 provides that the Prime Minister and every Minister must **consult** the *Garante* when they have to decide regulatory norms and administrative acts which somehow affect the discipline of the Code. Paragraph 6, finally, mandates that a copy of any measure taken by judicial authorities in connection with either this Act or computer crime matters shall be **transmitted to the *Garante*** by the court clerk's office. This norm is clearly aimed at facilitating the accomplishment of the protection of the privacy from the Garante.

#### *3.3.2.3. Allocation of Financial Ressources*

According to art. 156 paragraph 10 PDPC, the expenses for the functioning of the Authority of Garante are charged to a fund allocated in the financial year of the State. The fund belongs to the **Ministry of Finance**. The Garante also generates its own income, obtained from the administrative fees paid by the parties in occasion of the proceedings.

#### *3.3.2.4. Other aspects of Independence*

An important aspect regarding the independence of the members of the Garante is represented by provisions on incompatibility. Art. 153 paragraph 4 PDPC establishes in fact that President and members shall not be allowed – under penalty of losing office - to carry out professional or advisory activities, manage or be employed by public or private entities or hold elective offices.

#### *3.3.2.5. Jurisdiction in Other Areas*

The Garante has jurisdiction only in relation to personal data protection.

### 3.3.3. Tasks and competences

#### *3.3.3.1. Functions*

The functions of the Garante are listed by art. 154 PDPC.

The first function (letter a)) is that of **monitoring** the sector. The Garante has to verify that the data processing is accomplished in compliance with the law.

The second, which is not less important than the first, (letter b)) is the function of **receiving complaints and reports** as well as taking measures on the complaints lodged by other *data subjects* or the associations representing them. This function ensures transparency to the sector.

Following the list, one finds the attribution (letter c)) of powers that allow the Garante to **issue mandatory orders** in relation to data processing operators which do not comply with the law in force. These measures aim at restoring the lawfulness of the operations.

The Garante (letter d)) may also adopt **prohibitory** measures: it can forbid the data processing, in part or as a whole; it can stop the data processing; it can adopt other measures as provided for by the legislation applying to processing of personal data, whereas the data processing, considered the relevant modalities and the nature of the data processed, potentially jeopardizes the data subjects so that an urgent measure proves necessary.

Another function is the one related to the **promotion of the deontological codes** (letter e)). This is an extension of the field traditionally reserved to self-regulation. The adoption of Codes of Conduct is now envisaged by the law, whereas previously their adoption was entirely voluntary, left to the initiative of the actors.

Moreover, the Garante has **advisory and consulting functions** (letter f) and g)) for the Government and the Parliament, on matters concerning legislative interventions on the sector. In exerting such function the Garante shall take into consideration the protection of the fundamental rights before the evolution of the data processing sector and shall take into consideration also the functions exerted by other Authorities.

Another function relates to **public awareness** (letter h). In fact, the Garante has to spread the knowledge of norms that govern the privacy, their rationale and the norms concerning data security. The promotion of the norms is accomplished through the publication of the measures in the *Gazzetta Ufficiale*, but also through other communication devices as for example newsletter, tv spots, etc.

A further function, which is actually also a legal obligation, is the one provided at letter i). The Garante is obliged to **report** the facts that involve criminal aspects.

The function described by letter l) is more specifically concerned with the safety of the sector, and it provides that the Garante keeps a **registry of the data processing** on the basis of the notification received under article 37. This register contains all the data processing and it must be accessible to everybody, it must be administered electronically. The register is even necessary for the proceedings to be initiated *ex officio* by the Garante.

Finally, the Garante (letter m)) elaborates annually a **report for the Parliament** and the Government in order to keep them informed and updated.

#### *3.3.3.2. Competencies*

In order to exercise the functions, the law establishes several specific measures that the authority can take.

The first of these devices is the **request for information** and for exhibition of documents (art. 157). Even if it is classified as authoritative device, it assumes the collaboration of the counterpart. This activity represents the preliminary stage of a successive proceeding.

The second of the authoritative devices is the **inquiry** according to art. 158 of the Code. The inquiries render possible the exertion of the function described by art. 154, letter a). They are accomplished by the staff of the office of the Garante.

The investigation takes place by **access to databases**, technical operations, extraction of copies of acts, documents, data as sample or specific one, etc. The investigation aims at defining the context of the data processing where the information provided does not permit such assessment.

Among the **other tasks**, article 106(1) of the Code entrusts the *Garante* with the task of encouraging adoption of one or more codes of conduct and professional practice for public and private entities, including scientific societies and professional associations, involved in processing data for statistical or scientific purposes[171].

The *Garante* also has the possibility to **impose fines** (up to 30'000 Euro) in case of failure to provide information or in other cases of non-compliance (section 161 seq of the Code). In addition, the Garante can **publish** an injunctive order in daily newspapers.

## 3.4. Rolle der Organisationen zum Schutz der Betroffenen

Associations representing individuals whose data are processed have a right to lodge a complaint according to article 154, letter b.

Moreover, as discussed at answer 3.5.2, associations play an important role in the drafting of codes of conduct.

## 3.5. Mögliche und vorgeschriebene Aktivitäten der Datenbearbeiter (private und öffentliche)

### 3.5.1 Reporting Duties

The title VI of the Code is defined as Performance of Specific Tasks and is composed of articles 37-41.
The data controller basically has to carry out three tasks:

a) Notification;
b) Communication;
c) Request of authorization.

The **notification** aims at informing the Garante of the fact that a certain data processing will take place. In particular the Garante shall know the peculiarities of this operation. The notification, therefore, must be transmitted before the data processing starts. Yet, it does not mean that the data processing can not begin (art. 38). Notification is compulsory in the cases identified by art. 37, letter a) – letter f). In particular:

---

171 *See* answer 3.5.2

a) genetic data, biometric data, or other data disclosing geographic location of individuals or objects by means of an electronic communications network,
b) data disclosing health and sex life where processed for the purposes of assisted reproduction, provision of health care services via electronic networks in connection with data banks and/or the supply of goods, epidemiological surveys, diagnosis of mental, infectious and epidemic diseases, seropositivity, organ and tissue transplantation and monitoring of health care expenditure,
c) data disclosing sex life and the psychological sphere where processed by not-for-profit associations, bodies or organisations, whether recognised or not, of a political, philosophical, religious or trade-union character,
d) data processed with the help of electronic means aimed at profiling the data subject and/or his/her personality, analysing consumption patterns and/or choices, or monitoring use of electronic communications services except for such processing operations as are technically indispensable to deliver said services to users,
e) sensitive data stored in data banks for personnel selection purposes on behalf of third parties, as well as sensitive data used for opinion polls, market surveys and other sample-based surveys,
f) data stored in ad-hoc data banks managed by electronic means in connection with creditworthiness, assets and liabilities, appropriate performance of obligations, and unlawful and/or fraudulent conduct.

As concerns the **communication** (art. 39), it should inform the Garante of certain circumstances related to the data processing. The communication is due in case:

a) personal data are to be **communicated by a public body** to another public body in the absence of specific laws or regulations, irrespective of the form taken by such communication and also in case the latter is based on an agreement,
b) **data disclosing health** are to be processed in pursuance of the biomedical or health care research programme referred to in Section 110(1), first sentence.

Differently from what happens in the hypothesis of notification, the data processing **cannot be initiated** after the communication has been transmitted. It is in fact necessary to suspend the operation for a term of 45 days within which the Garante could take measures according to the law. These measures can also be taken after the 45 days term.

The norm actually implements art. 7, paragraph 1, letter e) of the 95/46Ce Directive. The EC Act, in fact, provided that the data processing can be accomplished for two categories of cases:

a) when the *data subject* has expressed his consent;
b) when the operation is necessary for peculiar reasons such as: contractual obligations, protection of the data subject interest, accomplishment of public interests or interest related with the exertion of public powers , accomplishment of the interest of the data subject.

The provisions of article 39 do not apply to the cases described by point a), rather only to the category described by point b) and specifically to the cases where the operations are accomplished for following a public interest or for following an interest related with the exertion of public powers.

**Authorization** is required in most cases in which particularly sensitive data are processed. We refer to the circumstances described above under 3.1.3 and 3.1.5.

### 3.5.2. Self-regulation

Art. 102 provides that the Garante shall **encourage** the adoption of a code of conduct and professional practices by private and public entities, including scientific societies and professional associations, which are involved in the processing of data for historical purposes, in pursuance of Section 12.

The encouragement consists in an **invitation** published on the *Gazzetta Ufficiale*, addressed to the associations or professional groups which are, therefore, expected to draft the rules of the Code.
The Garante shall coordinate the study of the rules and, once ascertained that these comply with the discipline of PDPC, it adopts the Code of Conduct. This will make the codes of conduct binding, whereas without this, the norms would be considered as *soft-law.*

To be binding, the code must correspond to the requirements enlisted by paragraph 2 of art. 102:

a) rules based on fairness and non-discrimination in respect of users, to be abided by also in communication and dissemination of data, pursuant to the provisions of this Code that are applicable to the processing of data for journalistic purposes or else for publication of papers, essays and other intellectual works also in terms of artistic expression;

b) the specific safeguards applying to collection, interrogation and dissemination of documents concerning data disclosing health, sex life or private family relations; the cases shall be also specified in which either the data subject or an interested party must be informed by the user of the planned dissemination;

c) arrangements to apply the provisions on processing of data for historical purposes to private archives, as also related to harmonisation of interrogation criteria and the precautions to be taken in respect of communication and dissemination.

# 4. Frankreich

## 4.1. Grundsätze des Datenschutzes

### 4.1.1. Rôle du but indiqué lors de la collecte des informations

L'article 6, 2° de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, et modifiée par la loi du 6 août 2004[172], énonce à propos des données : «elles sont collectées pour des **finalités déterminées, explicites et légitimes** et ne sont pas traitées ultérieurement de manière incompatible avec ces finalités ». La loi réserve cependant le cas de l'utilisation ultérieure des données dans un but statistique ou historique. Depuis la reconnaissance par la loi du 6 août 2004 d'un **principe de finalité**, le but indiqué lors de la collecte vient limiter la liberté de l'auteur du traitement[173]. Le détournement de finalité est incriminé par le Code pénal et fait encourir à son auteur cinq ans d'emprisonnement et 300 000 euros d'amende[174].

### 4.1.2. Principes du traitement des données (licéité, bonne foi, proportionnalité, économie)

Les principes du droit français de la protection des données sont énoncés à l'article 6 de la loi du 6 janvier 1978[175].

Le principe de **licéité** est énoncé d'emblée par l'article 6 de la loi : « les données sont collectées et traitées de manière loyale et licite ». La validité de la collecte puis du traitement est assujettie à des conditions légales telles que celle de recueillir le consentement de la personne ou de lui fournir certaines informations[176]. Le principe de licéité est pénalement sanctionné : tout manquement fait encourir à son auteur cinq ans d'emprisonnement et 300 000 euros d'amende[177].

---

172 Lois n°78-17 et n°2004-801.

173 C.-A. Colliard et R. Letteron, Libertés publiques, 8e éd., Dalloz 2005, p.393.

174 Article L226-21 du Code pénal, introduit par la loi n°95-116 du 4 février 1995.

175 « Un traitement ne peut porter que sur des données à caractère personnel qui satisfont aux conditions suivantes : 1° Les données sont collectées et traitées de manière loyale et licite ; 2° Elles sont collectées pour des finalités déterminées, explicites et légitimes et ne sont pas traitées ultérieurement de manière incompatible avec ces finalités. Toutefois, un traitement ultérieur de données à des fins statistiques ou à des fins de recherche scientifique ou historique est considéré comme compatible avec les finalités initiales de la collecte des données, s'il est réalisé dans le respect des principes et des procédures prévus au présent chapitre, au chapitre IV et à la section 1 du chapitre V ainsi qu'aux chapitres IX et X et s'il n'est pas utilisé pour prendre des décisions à l'égard des personnes concernées ; 3° Elles sont adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs ; 4° Elles sont exactes, complètes et, si nécessaire, mises à jour ; les mesures appropriées doivent être prises pour que les données inexactes ou incomplètes au regard des finalités pour lesquelles elles sont collectées ou traitées soient effacées ou rectifiées ; 5° Elles sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées. »

176 Articles 7 et 32.

177 Article 226-18 du Code pénal.

L'exigence de **bonne foi** n'apparaît pas expressément en matière de traitement de données. La conjugaison des principes de licéité et de loyauté semble de nature à y remédier[178].

La **proportionnalité** est un principe apparu avec la loi du 6 août 2004, conformément à la directive du 24 octobre 1995. Les données « sont adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs »[179]. L'existence du traitement, ainsi que son contenu, doivent être proportionnels aux finalités du fichier. Ce principe conduit à se poser les questions suivantes : à propos de l'existence du traitement « n'y avait-il pas d'autres moyens moins attentatoires à la liberté de réaliser le même objectif que celui poursuivi par le traitement » ? A propos du contenu des traitements, « toutes ces données sont-elles nécessaires, adéquates et pertinentes ? »[180]. Le principe de proportionnalité recouvre l'exigence formulée à l'article 6,5° de la loi du 6 janvier 1978 en vertu de laquelle les données personnelles ne doivent pas être conservées au-delà de la « durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées »[181].

Tout manquement à l'un des principes légaux protégeant les données à caractère personnel peut justifier une **plainte auprès de la Commission Nationale de l'Informatique et des Libertés** (CNIL), qui rendra une décision susceptible de recours devant les juridictions administratives.

Le principe d'**économie** n'apparaît pas dans la loi du 6 janvier 1978.

### 4.1.3. Caractère reconnaissable des finalités du traitement, transparence, consentement

La collecte de données personnelles, ainsi que les finalités du traitement, ont un caractère reconnaissable : les **finalités** de la collecte doivent en effet être **explicites** et sont **contraignantes** dans la mesure où elles restreignent la liberté de l'auteur de leur traitement[182]. En outre, la personne concernée par la collecte d'informations en est avertie puisque son consentement est en principe nécessaire[183]: « un traitement de données à caractère personnel doit avoir reçu le consentement de la personne concernée » – la directive du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données a généralisé l'obligation de l'auteur de la collecte puis du traitement, de recueillir le consentement de la personne concernée[184]. Contrairement à la directive européenne, la loi du 6 janvier 1978 ne définit pas le consentement : elle se réduit finalement à interdire le traitement de

---

178 Cf. infra pour le principe de loyauté.

179 Article 6,3°.

180 Y. Poullet, La loi des données à caractère personnel : un enjeu fondamental pour nos sociétés et nos démocraties ?, Légicom 2009, n°42, p.47, spéc. p.66 ; O. Coutor & M. Griguer, Mise au point sur le champ d'application de la Loi Informatique et Libertés, Cahiers du droit de l'entreprise 2010, n°2, p.22.

181 Sur les difficultés d'apprécier une telle durée : C.A.A. Douai, 29 déc. 2006, n°06DA00107 : « en l'espèce, il ne ressort pas des pièces du dossier que la période ayant couru entre décembre 2000, date de la radiation de M.X. et le 21 octobre 2001, date de la naissance de la décision implicite attaquée, constitue une durée excessive ». Les délibérations de la CNIL constituent ainsi un guide utile pour apprécier la durée nécessaire de conservation.

182 Article 6,2°.

183 Article 7.

184 Un auteur remet en cause le consentement comme fondement de la légitimité des traitements: Poullet, op. cit., spéc. p.66.

données personnelles sur le fondement du silence gardé par la personne concernée[185]. Cette obligation de recueillir le **consentement** disparaît seulement si le responsable du traitement peut invoquer le respect d'une obligation légale lui incombant[186], la sauvegarde de la vie de la personne concernée, l'exécution d'une mission de service public dont le responsable du traitement ou son destinataire serait investi, l'exécution d'un contrat auquel est partie la personne concernée, ou de mesures précontractuelles, ou la réalisation de l'intérêt légitime du responsable du traitement ou de son destinataire si cela ne porte pas atteinte à celui de la personne concernée ou à ses droits et libertés fondamentaux[187].

Le principe de **transparence** n'est pas exprimé expressément dans la loi, mais il se rapproche de celui de **loyauté**, énoncé par l'article 6,1° de la loi du 6 janvier 1978. En vertu de ce dernier principe, « les données nominatives doivent être collectées auprès de l'individu lui- même, qui doit être informé des raisons de cette collecte, et de l'utilisation qui en sera faite »[188]. Le fait de recueillir directement sur Internet des adresses électroniques personnelles de personnes physiques à leur insu a été jugé déloyal[189]. Ce principe supporte cependant quelques exceptions, notamment au profit des fichages organisés par les services de maintien de l'ordre. La collecte de données à caractère personnel par un moyen frauduleux, déloyal ou illicite est pénalement sanctionnée[190]. Les sanctions encourues sont augmentées si l'auteur de l'infraction est une personne morale.

### 4.1.4. Autres

Le principe d'**exactitude** des données conservées est énoncé à l'article 6,4° de la loi du 6 janvier 1978. Il implique une **actualisation** régulière. Ce principe est sanctionné pénalement : est incriminé le fait pour un responsable de traitement de ne pas procéder à la rectification, à la mise à jour, au verrouillage ou à l'effacement de données appartenant à une personne qui lui a demandé d'effectuer ces opérations[191]. La sanction de cette obligation est l'amende applicable aux contraventions de la cinquième classe, d'un montant de 1 500 euros au plus[192].

### 4.1.5. Traitement des données particulièrement sensibles

Les données sensibles sont les « données à caractère personnel qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci»[193]. Le principe est celui de l'**interdiction** de leur **collecte et** de leur **traitement**. Mais certaines **dérogations** à ce principe sont admises dans la mesure où la finalité du traitement l'exige. Ainsi, le

---

185 J.-Cl. Administratif, fasc. 274, V° « *Informatique- traitement de données à caractère personnel* », n°82 et 83.

186 Tel est le cas lorsque les employeurs doivent remplir des obligations déclaratives en matières fiscale et sociale.

187 Article 7.

188 Colliard et Letteron, op.cit., p.393.

189 Cass. crim., 14 mars 2006, n°05-83.423 ; P. Belloir, Le délit de collecte déloyale de données à caractère personnel à l'épreuve d'Internet, Rev. Lamy droit immatériel juin 2006, n°17, p.28 ; A. Lepage, Communication commerce électronique 2006, comm. 131.

190 Article L226-18 du Code pénal.

191 Article R625-12 du Code pénal.

192 Article 131-13 du Code pénal.

193 Article 8 I.

**consentement exprès de la personne** concernée permet une telle collecte, sauf interdiction légale[194]. A défaut, l'auteur de la collecte ou du traitement encourt une sanction pénale[195]. Le Conseil d'Etat a considéré que l'information de l'incorporation dans un fichier nominatif des données ne saurait tenir lieu d'accord exprès[196]. De même, les traitements de données sensibles sont autorisés s'ils sont nécessaires à la **sauvegarde de la vie humaine** quand la personne concernée n'est pas en mesure de donner son consentement par suite d'une incapacité juridique ou d'une impossibilité matérielle[197]. Sont encore possibles les traitements de données sensibles s'ils sont nécessaires, à la constatation, à l'exercice ou à la défense d'**un droit en justice**[198].

La mise en œuvre à bref délai d'un procédé d'anonymisation reconnu conforme permet à la CNIL d'autoriser certains traitements de données sensibles, compte tenu de leur finalité[199].

Enfin, **l'intérêt public** est susceptible de justifier certains traitements de données sensibles[200]. Une autorisation doit alors être délivrée par la CNIL, sous peine de 5 ans d'emprisonnement et/ou 300 000 euros d'amende[201]. La CNIL, dans une délibération du 10 juin 2010 autorise ainsi la mise en œuvre par la Caisse nationale d'assurance maladie des travailleurs salariés (CNAMTS) d'une modification du traitement dénommé Hippocrate tendant à la création d'un entrepôt national de données médicales anonymisées. L'intérêt public justifie ce traitement dont l'objet est « d'améliorer la gestion et le pilotage de l'activité du service médical par la direction générale et les directions déléguées de la CNAMTS, d'analyser les pratiques médicales sur l'ensemble du pays, de détecter les pratiques contraires aux directives données et définir des orientations en matière de prévention »[202].

### 4.1.6. Sécurité des données

La sécurité des données doit « empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès »[203]. L'obligation de sécurité des données pèse sur le **responsable du traitement**[204], tenu de prendre toutes précautions utiles pour assurer la sécurité logicielle et physique du système informatique[205]. A défaut, il engage ses responsabilités civiles et pénales. Quant au **sous-traitant**, il doit présenter des garanties suffisantes et le responsable du traitement reste tenu de veiller à la sécurité du traitement[206].

Les déclarations, demandes d'autorisation et demandes d'avis adressées à la CNIL contraignent le responsable du traitement à rendre compte des dispositions prises pour assurer la sécurité des

---

194 Article 8 II 1°.

195 Article 226-19 du Code pénal.

196 CE, Sect., 5 juin 1987, M.K., n°59674.

197 Article 8 II 2°

198 Article 8 II 5°.

199 Article 8 III.

200 Article 8 IV.

201 Crim., 4 mars 1997, n° de pourvoi : 96-84773.

202 Délibération de la CNIL n°2010-230 du 10 juin 2010, http://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000022502112&fastReqId=705898712&fastPos=2 (17.08.2010)

203 Article 34 alinéa 1.

204 Article 34 alinéa 1.

205 H. Bitan, Une vision expertale de la protection des données dans l'entreprise, Cahiers de droit de l'entreprise 2010, n°2, p.29.

206 Article 35.

traitements et des données et la garantie des secrets protégés par la loi[207]. La **CNIL** contribue à la sécurité du traitement de données en édictant, le cas échéant, des règlements types[208]. En outre, des décrets contenant des prescriptions techniques sont susceptibles d'être pris, après avis de la CNIL[209]. Par ailleurs, le **codage** des données[210] et la **durée limitée** pour leur **conservation**[211] permet aussi de garantir un certain niveau de sécurité.

### 4.1.7. Communication transfrontière de données

Les transferts de données à caractère personnel à destination d'un **Etat membre de l'Union européenne** suivent le régime des traitements nationaux : ils ne sont soumis à aucune autorisation, sauf s'ils entrent dans le cadre d'une disposition spécifique[212].

Les transferts de données personnelles vers des **Etats non membres de l'Union européenne** relèvent des articles 68, 69 et 70 de la loi du 6 janvier 1978. Ils sont possibles à condition que l'Etat de destination du transfert assure un **niveau de protection suffisant** de la vie privée et des libertés et droits fondamentaux de la personne[213]. Un ensemble de critères, tels que les dispositions en vigueur dans l'Etat de destination ou les mesures de sécurité qui y sont appliquées, permettent d'évaluer le caractère suffisant ou non de la protection des données personnelles dans cet Etat[214]. La Commission européenne et les autorités nationales de contrôle sont compétentes pour apprécier le niveau de la protection étrangère. Les pays assurant un niveau de protection suffisant sont ceux de l'Espace Economique Européen – l'Islande, le Liechtenstein et la Norvège – ainsi que ceux dont la protection a été jugée adéquate par la Commission européenne : l'Argentine, le Canada, Guernesey, Ile de Man, Jersey, la Suisse et les Etats-Unis quand les entreprises américaines ont adhéré aux principes du *Safe Harbor*[215]. Des transferts de données vers de tels Etats sont soumis aux mêmes formalités que les traitements nationaux, à cela près que les responsables du traitement doivent mentionner l'existence d'un transfert et le pays de destination[216].

Un transfert de données vers un **Etat dont le niveau de protection des données est insuffisant** est en principe interdit[217]. La notion de « transfert » est donc fondamentale. La CNIL en retient une approche assez large : le transfert de données personnelles vers un pays tiers « peut s'effectuer par copie, par déplacement de données, par l'intermédiaire d'un réseau ou d'un support à un autre »[218].

---

207 Article 30,9°.

208 Article 11 b.

209 Article 34 alinéa 2.

210 Article 55

211 Article 6,5°.

212 J.-Cl. Administratif, fasc. 274, op. cit., n°205.

213 Article 68 alinéa 1.

214 Article 68 alinéa 2.

215 CNIL, «Transfert de données à caractère personnel vers des pays non membres de l'Union européenne », Les Guides de la CNIL 2008, p.14. http://www.cnil.fr/fileadmin/documents/approfondir/dossier/international/Guide-tranfertdedonnees.pdf (11.08.2010)

216 J.-Cl. Administratif, fasc. 274, op. cit., n°211.

217 Article 68.

218 CNIL, « Transferts de données à caractère personnel vers des pays tiers à l'Union européenne », Les Guides de la CNIL 2010, http://www.cnil.fr/fileadmin/documents/Vos_responsabilites/Transferts/GUIDE-transferts-integral.pdf (11.08.2010)

Toutefois, des **dérogations** sont possibles en vertu de l'article 69 de la loi du 6 janvier 1978. Le consentement exprès de la personne à qui se rapportent les informations collectées permet ainsi un transfert de données à caractère personnel vers des Etats n'appartenant pas à la Communauté européenne et n'assurant pas un niveau de protection suffisant[219]. En second lieu, l'article 69 énumère limitativement des hypothèses dans lesquelles un tel transfert est justifié : transfert de données nécessaire à la sauvegarde de la vie de la personne concernée, à la sauvegarde de l'intérêt public ou au respect d'obligations permettant d'assurer la constatation, l'exercice ou la défense d'un droit en justice[220]. Enfin, c'est une autorisation de la CNIL – ou un décret pris en Conseil d'Etat après avis motivé et publié de la commission s'il s'agit du transfert d'un traitement de souveraineté – qui permet de déroger au principe d'interdiction du transfert.

### 4.1.8. Droit d'accès (art.8 LFPD)

Toute personne physique justifiant de son identité a le **droit d'interroger le responsable d'un traitement** de données à caractère personnel et d'obtenir toute une série d'informations. Les informations auxquelles la personne concernée peut accéder sont les suivantes : confirmation que des données à caractère personnel la concernant font ou ne font pas l'objet d'un traitement ; informations relatives aux finalités du traitement, aux catégories de données à caractère personnel traitées et aux destinataires ou aux catégories de destinataires auxquels les données sont communiquées ; informations relatives aux transferts de données à destination de pays non membres de l'Union européenne ; communication des données personnelles et de toute information disponible quant à leur origine ; informations permettant de connaître et de contester la logique qui sous-tend le traitement automatisé en cas de décision prise sur le fondement de celui-ci[221].

Une **copie** est adressée à l'intéressé à sa demande, sans que l'on puisse lui facturer un prix supérieur à celui de la reproduction.

Dans le souci de rendre ce droit d'accès encore plus effectif, la CNIL a publié un guide pratique à destination des personnes concernées par le traitement[222].

Seule une demande manifestement abusive peut justifier un refus de la part du responsable du traitement[223]. Le droit d'accès connaît une seule dérogation : il ne peut être exercé lorsque les informations sont conservées sous une forme excluant tout risque d'atteinte à la vie privée et pendant une durée n'excédant pas le minimum nécessaire[224].

---

219 Le consentement fait défaut s'il n'a pas été donné librement : la subordination hiérarchique des salariés les prive de la faculté de consentir valablement à un transfert de données personnelles les concernant. F. Chafiol-Chaumont, Données personnelles et mondialisation : comment transférer ces données à l'étranger ?, Cahiers de droit de l'entreprise 2008, n°5, p.80.

220 A propos de cette dernière hypothèse, de nombreux professionnels ont estimé que le transfert de données personnelles à destination des Etats-Unis dans le cadre d'une procédure de discovery ne requérait pas d'autorisation de la CNIL. Cette dernière, en vertu d'un principe d'interprétation stricte des exceptions, semble avoir un avis divergent. Chafiol-Chaumont, op. cit., p.80.

221 Article 39 I.

222 CNIL, « Droit d'accès », Les Guides de la CNIL 2010, http://www.cnil.fr/fileadmin/documents/Guides_pratiques/CNIL_Droit_d_acces.pdf (11.08.2010)

223 Article 39 II alinéa 1.

224 Article 39 II alinéa 2.

Des **régimes spécifiques** sont prévus concernant les traitements intéressant la sûreté de l'Etat, la défense ou la sécurité publique[225]. Il en va de même s'agissant des traitements mis en œuvre par les administrations publiques et les personnes privées chargées d'une mission de service public qui ont pour mission de prévenir, rechercher ou constater des infractions, ou de contrôler ou recouvrer des impositions[226]. Enfin, un dernier régime spécial s'applique en matière de santé[227].

Une plainte peut être adressée à la CNIL si le responsable du traitement refuse injustement de se plier à la demande de la personne à qui se rapportent les informations collectées. Le responsable d'un traitement encourt la peine applicable aux contraventions de 5ème classe[228].

### 4.1.9. Relation entre protection des données et nouvelles technologies

Avec le développement des nouvelles technologies, il existe un risque d'atteinte au respect de la vie privée, il était donc nécessaire d'adopter des dispositions spécifiques pour la protection des données personnelles. Mais la loi est rédigée de manière générale : son champ d'application est délimité par la notion de « traitement de données à caractère personnel ». **Aucune disposition spécifique** n'est prévue en considération d'une technologie particulière. La relation entre le développement des nouvelles technologies et la protection des données est assurée par la CNIL : celle-ci est en effet en charge de « [proposer] au gouvernement les mesures législatives ou réglementaires d'adaptation de la protection des libertés à l'évolution des procédés et techniques informatiques »[229].

### 4.1.10. Différence de régime

Le régime de la protection des données à caractère personnel est **unitaire depuis la réforme opérée par la loi du 6 août 2004** tant en ce qui concerne les obligations du responsable du traitement que les droits de la personne concernée. L'unité du régime applicable repose sur « la diffusion de puissants instruments de traitement automatisé de l'information dans les entreprises et chez les particuliers [ce] qui a contribué à réduire la spécificité des applications mises en œuvre par les opérateurs publics ». C'est pourquoi « la différenciation des règles applicables aux traitements selon qu'ils sont ou non opérés pour le compte d'une personne morale de droit public […] a perdu une large part de ses justifications »[230].

Ainsi, la loi du 6 janvier 1978 impose des obligations au responsable du traitement, **sans distinguer selon sa nature privée ou publique**[231]. « Le responsable d'un traitement de données à caractère

---

225 Article 41.

226 Article 42.

227 Article 43.

228 Article R625-11 du Code pénal.

229 Article 11 4° b).

230 G. Braibant, Données personnelles et société de l'information, La documentation française 1998, p.27.

231 Avant la réforme du 6 août 2004, le régime de la protection des données à caractère personnel était dual et reposait sur un critère organique. Selon la nature publique ou privée de l'organisme déclarant, les obligations du responsable du traitement n'étaient pas les mêmes. En vertu de l'ancien article 15 de la loi, « les traitements automatisés d'informations nominatives opérés pour le compte de l'Etat, d'un établissement public ou d'une collectivité territoriale, ou d'une personne morale de droit privé gérant un service public, sont décidés par une loi ou par acte réglementaire pris après avis motivé de la commission nationale de l'informatique et des libertés. Si l'avis de la commission est défavorable, il ne peut être passé outre que par un décret pris sur avis conforme du Conseil d'Etat […] ». S'agissant des

personnel est, sauf désignation expresse par les dispositions législatives ou réglementaires relatives à ce traitement, la personne, l'autorité publique, le service ou l'organisme qui détermine ses finalités et ses moyens »[232]. Le responsable du traitement est ainsi une personne physique ou morale, privée ou publique.

Sur le plan des **droits de la personne protégée**, le régime demeure unitaire : la nature publique ou privée de la personne responsable du traitement n'influence en rien les modalités d'exercice du droit d'accès de la personne concernée. Le régime spécifique du droit d'accès découlant de l'article 41 de la loi s'explique non pas par la personne du responsable du traitement mais par la nature des informations traitées : la personne concernée ne peut exercer elle-même son droit d'accès lorsque les données personnelles intéressent la sûreté de l'Etat, la défense ou la sécurité publique ; le droit d'accès est exercé par un membre de la CNIL.

## 4.2. Durchsetzungsrechte der Datenschutzanliegen für Betroffene

La loi du 6 janvier 1978, modifiée par la loi du 6 août 2004, ne distingue pas selon l'auteur du traitement. Les droits de la personne concernée restent les mêmes, sous réserve parfois de quelques modalités spéciales d'exercice.

Les droits légaux de protection des données à caractère personnel appartiennent seulement à la personne concernée par les traitements. Cette personne est une **personne physique tenue de justifier de son identité** – ainsi, la loi protège les données en interdisant leur accès aux tiers non autorisés[233].

### 4.2.1. Abstention de procéder aux traitements illicites

Le principe de licéité, pénalement sanctionné, interdit au responsable du traitement de procéder à une collecte puis à un traitement de données personnelles en violation des différentes conditions énoncées par la loi du 6 janvier 1978[234].

### 4.2.2. Constatation du caractère illicite du traitement.

La **CNIL** est l'autorité de surveillance en matière de protection des données : si elle est saisie, elle peut constater le caractère illicite du traitement. Depuis la loi du 6 août 2004, **le correspondant** à la protection des données à caractère personnel, veillant à la licéité des traitements de données mis en œuvre par leur responsable, a un rôle dans la constatation du caractère illicite du traitement : il doit en aviser le responsable puis, le cas échéant, saisir la CNIL.

---

« traitements automatisés d'informations nominatives effectués pour le compte de personnes autres que celles qui sont soumises aux dispositions de l'article 15, [l'ancien article 16 de la loi prévoit qu'ils] doivent, préalablement à leur mise en œuvre, faire l'objet d'une déclaration auprès de la commission nationale de l'informatique et des libertés ».

232 Article 3 I.

233 Articles 38 et suivants.

234 Cf Supra.

### 4.2.3. Suppression des effets du traitement illicite.

La suppression des effets d'un traitement illicite repose sur la **vigilance de la personne concernée**. Le droit d'accès de la personne concernée par le traitement est le moyen pour elle de relever toute illicéité et d'obtenir ainsi la suppression des effets du traitement illicite. Le droit d'accès lui permet en effet de dénoncer l'illicéité au responsable du traitement et, éventuellement, de porter plainte auprès de la CNIL puis de poursuivre la procédure devant les juridictions administratives.

### 4.2.4. Opposition à la communication de données personnelles

« Toute personne a le **droit de s'opposer, pour des motifs légitimes**, à ce que des données à caractère personnel la concernant fassent l'objet d'un traitement »[235]. La notion de « motifs légitimes » n'est pas définie : elle sera donc appréciée au cas par cas par les tribunaux[236]. Le droit d'opposition peut s'exercer à l'encontre de tous traitements, y compris ceux effectués dans un cadre philosophique, politique ou religieux[237].

En outre, la personne a le droit de s'opposer sans frais à une utilisation des données la concernant à des fins de **prospection,** notamment **commerciale**.

Toutefois, le droit d'opposition disparaît si le traitement répond à une **obligation légale** ou si l'acte autorisant le traitement a écarté l'application du droit d'opposition. L'opposition n'est pas admise non plus pour les traitements publics de sécurité[238].

Le droit d'opposition de la personne concernée bénéficie d'une protection pénale : le responsable d'un traitement encourt en effet une peine de cinq ans d'emprisonnement et de 300 000 euros d'amende s'il procède à un traitement malgré l'opposition – qui doit être légitime si le traitement n'est pas réalisé à des fins de prospection commerciale – de la personne concernée[239].

### 4.2.5. Rectification (art 15 LFPD).

« Toute personne physique justifiant de son identité peut exiger du responsable d'un traitement que soient […] rectifiées […] les données à caractère personnel la concernant »[240]. Ce droit de rectification permet à la personne concernée d'obtenir la **correction des données erronées**, et plus largement de **compléter** ce qui ne l'avait pas été ou ce qui était équivoque**.**
Le responsable du traitement doit ensuite justifier, sans frais, qu'il a procédé à la rectification demandée. Ce dernier doit notifier aux tiers intéressés la rectification. La charge de la preuve de la rectification pèse sur lui. Ce droit d'obtenir une rectification appartient également aux héritiers de la personne concernée.

---

235 Article 38.

236 J.-Cl. Administratif, fasc.274, op. cit., n°262.

237 Crim., 28 sept. 2004, Juris-Data n° 2004-025. « La légitimité de l'opposition est remplie par le seul exercice de la faculté, pour la personne concernée, de s'opposer au traitement de données nominatives ».

238 Articles 26 et 27.

239 Article 226-18-1 du Code pénal.

240 Article 40 alinéa 1.

Si le responsable du traitement ne respecte pas le droit de rectification de la personne concernée, il encourt la peine prévue pour les contraventions de 5ème classe[241].

### 4.2.6. Destruction (art 15 LFPD).

La personne concernée par le traitement de données a le **droit d'obtenir l'effacement** de celles qui sont périmées ou dont la collecte, l'utilisation, la communication ou la conservation est interdite**.** Le responsable du traitement est tenu des obligations précitées. Les héritiers ont le même droit que précédemment[242] et la même sanction pénale est applicable[243].

### 4.2.7. Ajout de la mention du caractère litigieux d'une donnée (art.15 al.2 LFPD).

L'ajout d'une telle mention n'est **pas prévu** par la loi du 6 janvier 1978 qui s'en tient à une approche binaire : si l'information traitée est exacte, elle demeure inchangée ; si elle est inexacte, elle est actualisée ou effacée[244]. La preuve de l'inexactitude ou de la péremption d'une donnée à caractère personnel repose, en toute logique, sur le demandeur ; par conséquent, si une donnée est litigieuse, elle demeure inscrite telle quelle dans le fichier jusqu'à ce que le demandeur indique son caractère inexact ou périmé.

### 4.2.8. Communication et publication des changements.

Le responsable du traitement doit **notifier** les opérations effectuées **aux tiers** à qui les données avaient été précédemment transmises[245].

### 4.2.9. Procédure (forme, droits procéduraux tels que possibilité d'une *class action*, etc.)

Les **formes** à suivre par la personne qui souhaite exercer son droit d'accès, son droit de rectification ou son droit d'opposition ne sont **pas très contraignantes**. La personne physique doit justifier de son identité[246]. Les demandes adressées par écrit doivent être accompagnées de la photocopie d'un titre d'identité portant la signature du titulaire. Le silence du responsable du traitement gardé pendant plus de deux mois vaut décision de refus. Le demandeur est en droit de se faire assister du conseil de son choix. Les codes, sigles et abréviations figurant dans les documents délivrés par le responsable du traitement doivent être clarifiés, si nécessaire sous la forme d'un lexique[247].

En droit français, la possibilité d'intenter une *class action* n'est pas reconnue.

---

241 Article R625-12 du Code pénal.

242 Article 40.

243 Article R625-12 du Code pénal.

244 Article 40.

245 Article 40 alinéa 5.

246 Articles 39 et 40.

247 « Décret n°2007-451 du 25 mars 2007 modifiant le régime de protection des personnes à l'égard des traitements de données à caractère personnel », JCP E 2007, n°17, act. 198.

### 4.2.10. Demande de tiers

La CNIL est compétente pour recevoir les plaintes relatives à la mise en œuvre des traitements de données à caractère personnel ; elle informe leurs auteurs des suites qui leur sont données[248]. En 2009, la CNIL a reçu 4 265 plaintes[249]. La plainte peut être classée purement et simplement ou donner lieu à des investigations. Ainsi, la CNIL n'a pas le devoir d'établir les faits sur demande d'un tiers ; en revanche, elle le peut.

En outre, la CNIL peut initier un contrôle à la demande d'une autorité exerçant des compétences analogues aux siennes dans un autre Etat de l'Union européenne[250].

## 4.3. Nationale Aufsichtsbehörde

### 4.3.1. Zusammensetzung, Ernennung und Eingliederung der Behörde

La CNIL est **composée de dix-sept membres, dont les modes de nomination varient**. Elle comprend ainsi deux députés et deux sénateurs, désignés respectivement par leurs assemblées ; deux membres du Conseil économique, social et environnemental, élus par cette assemblée ; deux membres ou anciens membres du Conseil d'Etat, d'un grade au moins égal à celui de conseiller, élus par l'assemblée générale du Conseil d'Etat ; deux membres ou anciens membres de la Cour de cassation, d'un grade au moins égal à celui de conseiller, élus par l'assemblée générale de la Cour de cassation ; deux membres ou anciens membres de la Cour des comptes, d'un grade au moins égal à celui de conseiller maître, élus par l'assemblée générale de la Cour des comptes ; trois personnalités qualifiées pour leur connaissance de l'informatique ou des questions touchant aux libertés individuelles, nommées par décret ; deux personnalités qualifiées pour leur connaissance de l'informatique, désignées respectivement par le Président de l'Assemblée nationale et par le Président du Sénat[251].

La CNIL est placée sous l'autorité d'un **président**, élu par les membres de la commission[252]. En cas de partage, il a voix prépondérante[253]. Le président, ainsi que deux vice-présidents et un vice-président délégué composent le **bureau** de la Commission[254]. Le Président attribue à chaque commissaire un secteur en fonction de ses compétences[255].

La commission se réunit en général en **séance plénière**[256], une fois par semaine sur un ordre du jour fixé par son Président. La formation plénière est en droit de déléguer l'une ou l'autre de ses attributions au président ou au vice-président délégué ou au bureau, dans les limites légales[257]. La CNIL

---

248 Article 11, 2° c).

249 CNIL, Rapport annuel d'activité 2009, p.98, http://www.cnil.fr/fileadmin/documents/La_CNIL/publications/CNIL-30erapport_2009.pdf (17.08.2010)

250 Article 49.

251 Article 13 I.

252 Depuis 2004 et encore à l'heure actuelle, le président de la CNIL est Alex Türk.

253 Articles 13 I et 15.

254 Article 13 I.

255 La CNIL est ainsi actuellement divisée en secteurs, tels que finances publiques, justice, santé, …

256 Article 15.

257 Articles 15 et 16. La formation plénière de la CNIL peut ainsi déléguer au président ou au vice-président délégué le pouvoir d'informer sans délai le procureur de la République, conformément à l'article 40 du code de procédure pénale, des infractions dont elle a connaissance […]. Article 11 2° e).

y adopte des **délibérations, collégiales** en dépit de la spécialisation des commissaires par secteur d'activité. La CNIL connaît aussi une **formation restreinte** composée du président, des vice-présidents et de trois membres élus par la commission en son sein pour la durée de leur mandat[258]. Elle peut donner des avertissements au responsable du traitement qui ne respecte pas ses obligations. Depuis la réforme opérée par la loi du 6 août 2004 – et l'octroi à la CNIL d'un pouvoir de sanction –, cette dernière a une **formation contentieuse**, composée de six membres. Cette formation spéciale se réunit une fois par mois au moins pour décider des sanctions susceptibles d'être infligées aux responsables de traitements ne respectant pas la loi. Les décisions sont en principe prises à la **majorité des suffrages exprimés**.

La CNIL est une «**autorité administrative indépendante** »[259]. Elle est en France la première institution de ce type à avoir été créée. Les autorités administratives indépendantes sont placées « hors de la hiérarchie traditionnelle »[260], sans être hors de l'administration, d'où l'ambiguïté de leur statut[261]. Son budget, en effet, est rattaché aux services du premier ministre, ainsi elle dispose des crédits nécessaires à son activité mais elle reste autonome dans leur gestion. En outre, sur le plan du fonctionnement de l'institution, la présence d'un commissaire du gouvernement trahit l'appartenance de la CNIL à l'administration française[262]. Les agents de la CNIL sont des agents contractuels de l'Etat. Le droit administratif s'applique à une institution telle que la CNIL : ses décisions sont susceptibles de faire l'objet d'un recours devant le juge administratif ; les dommages qu'elle pourrait causer engagent la responsabilité de l'Etat.

### 4.3.2. Gewährleistung der Unabhängigkeit

#### *4.3.2.1. Election : corps électoral, régulation du mandat électoral*

Douze des dix-sept **membres** composant la Commission sont **élus** par les assemblées ou les juridictions auxquelles ils appartiennent, ce qui est un gage d'indépendance. De même, la provenance diverse des commissaires –assemblées parlementaires, société civile,… – tend à garantir l'indépendance de l'institution.

Le mandat des membres de la CNIL est de **cinq ans** et **renouvelable une fois**, sauf en ce qui concerne les membres des assemblées parlementaires et du Conseil économique et social qui siègent pour la durée du mandat à l'origine de leur désignation[263]. Le Gouvernement ne peut pas révoquer un membre de la CNIL. Et un certain nombre d'**incompatibilités** assure l'indépendance des commissaires de la CNIL. La qualité de membre de la commission est incompatible avec celle de membre du gouvernement. En outre, un membre de la commission ne peut plus exercer ses fonctions dès lors qu'il a détenu un intérêt, direct ou indirect, a exercé des fonctions ou a détenu un mandat dans l'organisme objet du contrôle dans les trente-six mois précédant la délibération ou les vérifications de la CNIL. Enfin, tout membre de la commission doit informer le président des intérêts directs ou indirects qu'il

---

258 Article 13 I.

259 Article 11.

260 Colliard & Letteron, op. cit., p.140.

261 Le concept d' « autorité administrative indépendante » est des plus difficiles à appréhender. J.-Cl. Administratif, fasc. 75, V° « *Autorités administratives indépendantes* », n°1.

262 Article 18.

263 Article 13.

détient ou vient à détenir, des fonctions qu'il exerce ou vient à exercer et de tout mandat qu'il détient ou vient à détenir au sein d'une personne morale[264].

#### *4.3.2.2. Rapports entre l'autorité de protection et les autres autorités nationales*

La CNIL ne reçoit d'**instruction d'aucune autorité, ni de l'Etat**[265]. Mais elle est **consultée par les autorités publiques**, y compris par les juridictions. Elle doit répondre à toute demande d'avis de leur part[266]. Elle est également susceptible d'apporter son concours aux autres autorités administratives indépendantes[267]. La CNIL est consultée par le gouvernement sur tout projet de loi ou de décret relatif à la protection des personnes à l'égard des traitements automatisés[268]. Elle peut aussi proposer au gouvernement des mesures réglementaires ou législatives. Enfin, sur demande du premier ministre, elle peut contribuer à la définition de la position française dans les négociations internationales[269].

#### *4.3.2.3. Reddition de compte*

La CNIL doit présenter **annuellement un rapport** au Président de la République, au Premier ministre et au Parlement rendant compte de l'exécution de sa mission[270].
La CNIL n'est tenue d'aucune autre obligation envers une quelconque autorité, sauf, comme tout organisme public, la reddition des comptes devant la Cour des comptes.
Aucune autorité n'est en droit de délivrer une **instruction** à la CNIL ou à ses commissaires dans l'exercice de leurs attributions[271].

#### *4.3.2.4. Compétence et droit de regard de l'autorité dans l'attribution de ses propres ressources*

La CNIL dispose d'une **autonomie budgétaire** mais n'a **pas d'indépendance financière** puisque les crédits qui lui sont nécessaires sont rattachés aux services du Premier ministre.

La CNIL a connu en 2009 une **augmentation de ses ressources** (permettant la création de quinze nouveaux emplois[272]), mais continue de dénoncer leur faiblesse. Son président, Alex Türk, milite en faveur d'un financement par la création d'une taxe qui serait supportée par les entreprises, ce qui offrirait à la commission un budget annuel bien plus important et l'indépendance.

#### *4.3.2.5. Référence à des règles relatives au montant des ressources*

---

264 Article 14.
265 Article 21.
266 Article 11 2° d).
267 Article 11 4° c).
268 Article 11 4° a).
269 Article 11 4° d).
270 Article 11 *in fine*.
271 Article 21.
272 Budget 2008 du Ministère de la Justice, disponible sous : http://www.justice.gouv.fr/art_pix/1_budget2008.pdf (26.07.2010)

L'article 12 de la loi du 6 janvier 1978 énonce seulement que « la Commission nationale de l'informatique et des libertés **dispose des crédits nécessaires** à l'accomplissement de ses missions ».
Les comptes de la commission sont présentés au contrôle de la Cour des comptes, même si la loi du 10 août 1922 relative au contrôle financier n'est pas applicable à leur gestion[273].

#### *4.3.2.6. Autres aspects de l'indépendance*

La CNIL élabore elle-même **son propre règlement intérieur** : elle se dote de ses propres règles d'organisation et de fonctionnement, ce qui protège encore son indépendance[274].

### 4.3.3. Zuständigkeitsbereich

La CNIL est compétente, **quel que soit le responsable du traitement** de données à caractère personnel : cette dernière peut donc être une personne privée, une autre autorité ou une administration, conformément à l'article 3 de la loi[275].

Outre son rôle central dans le mécanisme légal de protection des données la CNIL assure aussi une mission plus large: elle **informe** toutes les personnes concernées et tous les responsables de traitements de leurs droits et obligations. Sollicitée par des organisations professionnelles ou des institutions regroupant des responsables de traitements, elle **peut donner un avis** sur la conformité des projets aux dispositions de la présente loi et porter une appréciation sur les garanties offertes. Enfin, la CNIL a un **devoir général de se tenir informée** et de rendre publique le cas échéant son appréciation des conséquences en résultant pour l'exercice des droits et libertés[276].

En France, **la CNIL** est la **seule autorité de surveillance** compétente en matière de protection des données.

### 4.3.4. Aufgaben und Kompetenzen

#### *4.3.4.1. Conseil*

La CNIL « **conseille** les personnes et organismes qui mettent en œuvre ou envisagent de mettre en œuvre des traitements automatisés de données à caractère personnel »[277]. Le fait qu'elle soit **consultée** sur tout projet de loi ou de décret relatif à la protection des personnes à l'égard des traitements automatisés et qu'elle puisse proposer au Gouvernement des mesures législatives ou réglementaires d'adaptation à l'évolution des technologies offrent à la CNIL une véritable mission de conseil en la matière[278].

---

273 Article 12.
274 Article 13 *in fine*.
275 Cf. supra.
276 Article 11.
277 Article 11 2° d).
278 Article 11 4° a) et b). J. Huet & P. Leclercq, La CNIL a-t-elle accompli les missions dévolues par le législateur ?, Légicom 2009, n°42, p.15.

#### *4.3.4.2. Pouvoirs de contrôle et acquisition d'informations*

En vertu de la directive du 24 octobre 1995, l'autorité de surveillance doit être pourvue de **pouvoirs de contrôle** significatifs : « chaque autorité de contrôle dispose notamment de pouvoirs d'investigation, tels que le pouvoir d'accéder aux données faisant l'objet d'un traitement et de recueillir toutes les informations nécessaires à l'accomplissement de sa mission de contrôle »[279]. Conformément à la directive, la loi du 6 janvier 1978 énonce que la CNIL « peut, par décision particulière, charger un ou plusieurs de ses membres ou des agents de ses services, dans les conditions prévues à l'article 44, de procéder à des vérifications portant sur tous traitements et, le cas échéant, d'obtenir des copies de tous documents ou supports d'information utiles à ses missions »[280]. Sur ce fondement, la CNIL a pu réaliser en 2009, 270 contrôles qui ont débouché sur 91 mises en demeure, 5 sanctions financières et 4 avertissements[281]. Cette augmentation des contrôles *a posteriori*, allant de pair avec un allègement des contrôles *a priori*, est conforme à ce qu'annonçait la CNIL dans son 24ème rapport d'activité[282].
La procédure mise en place par l'article 44 de la loi du 6 janvier 1978 issu de la réforme du 6 août 1944, **se rapproche d'une procédure de perquisition**[283]. L'exercice par la CNIL de son pouvoir de contrôle suppose une information préalable du procureur de la République territorialement compétent. Cette information doit être faite par écrit et 24h avant le début du contrôle projeté et préciser les date, heure, lieu et objet du contrôle sur place[284]. Le responsable des lieux doit être avisé de l'opération au plus tard au début du contrôle[285]. Si le responsable des lieux s'oppose au contrôle, l'autorisation du président du tribunal de grande instance, saisi par le président de la CNIL, devient nécessaire[286]. Les membres de la CNIL ainsi que les agents de ses services qui y sont habilités ont accès, de 6 heures à 21 heures aux locaux professionnels[287]. Les agents de la CNIL peuvent aussi procéder à des convocations[288]. Dans le cadre d'un contrôle sur place ou dans celui d'une convocation[289], ils sont en droit de demander communication de tous documents quel que soit leur support et d'en obtenir la copie. A la demande du président de la CNIL, les personnes chargées du contrôle peuvent être assistées d'un expert. Un procès-verbal contradictoire doit être dressé en fin de contrôle[290].

L'article 21 de la loi garantit la liberté d'action des contrôleurs de la CNIL, et l'article 51 sanctionne par une peine d'un an d'emprisonnement et de 15 000 euros d'amende le fait d'entraver leur action.

#### *4.3.4.3. Contrôle préalable*

La mise en place d'un traitement de données à caractère personnel est subordonnée à l'accomplissement de **formalités préalables** aussi bien pour le secteur public que pour le secteur privé.

---

279 Article 28,3°.
280 Article 11, 2° f).
281 CNIL, rapport d'activité 2009, p.98, http://www.cnil.fr/fileadmin/documents/La_CNIL/publications/CNIL-30erapport_2009.pdf (16.08.2010)
282 CNIL, 24ème rapport d'activité, 2003, http://lesrapports.ladocumentationfrancaise.fr/BRP/044000252/0000.pdf (16.08.2010)
283 M.-L. Laffaire, Protection des données à caractère personnel, Editions d'organisation 2005, p.366.
284 Article 61 du décret n°2005-1309 du 20 octobre 2005 pris pour l'application de la loi n°78-17 du 6 janvier 1978.
285 Article 62 du décret.
286 Article 44 II.
287 Article 44 I.
288 Article 44 III.
289 Article 66 du décret.
290 Article 44 III.

Ces formalités varient selon la nature du traitement. Les différentes formes de ce **« contrôle *a priori* »** sont les suivantes : déclaration ordinaire[291], déclaration simplifiée[292], autorisation de la CNIL[293], autorisation par arrêté ou par décision de l'organe délibérant chargé de l'organisation de l'établissement public ou de la personne privée gérant un service public pris après avis motivé et publié de la CNIL[294], autorisation par arrêté du ou des ministres compétents après avis motivé et publié de la CNIL[295], autorisation par décret en Conseil d'Etat après avis publié et motivé de la CNIL[296].
Les déclarations, demandes d'autorisation et demandes d'avis adressées à la CNIL présentent un contenu commun de nature à permettre à l'autorité de surveillance d'exercer son contrôle : doivent être ainsi précisées notamment l'identité et l'adresse du responsable du traitement, les finalités du traitement, les interconnexions avec d'autres traitements, les données personnelles traitées, leur origine et les catégories de personnes concernées, la durée de conservation des informations traitées, etc[297].

La procédure de la **déclaration ordinaire** est la procédure de droit commun : « à l'exception de ceux qui relèvent des dispositions prévues aux articles […], les traitements automatisés de données à caractère personnel font l'objet d'une déclaration auprès de la CNIL ». Le responsable du traitement envoie préalablement à toute opération de traitement un formulaire de déclaration à la CNIL ; cette formalité peut désormais être accomplie en ligne. Le responsable est alors en droit de procéder au traitement dès le récépissé retourné par la CNIL[298]. Pour les catégories les plus courantes de traitements de données à caractère personnel, dont la mise en œuvre n'est pas susceptible de porter atteinte à la vie privée ou aux libertés, le responsable du traitement peut n'avoir à remplir qu'une **déclaration simplifiée**, dans la mesure où la CNIL a édicté une norme simplifiée[299]. A titre d'illustration, la CNIL a ainsi édicté une norme simplifiée relative aux traitements automatisés de données à caractère personnel mis en œuvre par les notaires aux fins de conservation des actes authentiques sur support électronique au sein du Minutier central électronique des notaires de France[300].

La CNIL dispose également d'un pouvoir d'**autorisation**[301]. Cette procédure est applicable quand le traitement projeté par son responsable est d'une nature jugée plus attentatoire aux libertés. L'idée est de renforcer la protection des individus à l'égard de ces traitements, la CNIL procède donc à un examen plus approfondi du traitement avant d'accorder son autorisation. Cela concerne notamment, les traitements de données sensibles faisant l'objet d'un processus d'anonymisation, certains traitements automatisés portant sur des données génétiques, certains traitements portant sur des données relatives aux infractions, condamnations ou mesures de sûreté, ainsi que les traitements automatisés ayant pour objet certains interconnexions, relèvent de cette procédure d'autorisation préalable. La CNIL se prononce alors dans un délai de deux mois à partir de la réception de la demande. Son silence équivaut à un rejet.

---

291 Article 22 I.
292 Article 24.
293 Article 25.
294 Article 27 II.
295 Article 26 I.
296 Articles 26 II et 27 I.
297 Article 30.
298 Article 23.
299 Article 24.
300 Délibération n°2010-032 du 11 février 2010- norme simplifiée n°55.
301 Article 25.

Enfin, la CNIL peut être sollicitée pour rendre un **avis motivé** et publié dans une procédure où l'autorisation est donnée par une autre autorité. Ainsi en va-t-il lorsque sont en jeu des traitements de données personnelles mis en œuvre pour le compte de l'Etat et intéressant la sûreté de l'Etat, la défense ou la sécurité publique[302]. La CNIL doit se prononcer dans un délai de deux mois à compter de la réception de la demande. Le silence de la CNIL vaut autorisation.

Le responsable du traitement a aussi une obligation d'informer sans délai la CNIL dans l'hypothèse où des modifications affectent les informations qu'il lui avait transmises[303].

Tout manquement à l'une ou l'autre de ces formalités fait encourir à son auteur cinq ans d'emprisonnement et 300 000 euros d'amende.

#### *4.3.4.4. Pouvoirs d'intervention*

En cas de comportement fautif du responsable du traitement, la CNIL peut user de différents pouvoirs. En premier lieu, et conformément au droit de la procédure pénale, elle dispose du pouvoir de **saisir les autorités judiciaires** dès lors qu'elle a connaissance d'un crime ou d'un délit[304].

En second lieu, la CNIL est compétente pour **délivrer un avertissement**, **mettre en demeure**, **prononcer des sanctions pécuniaires**, **enjoindre de cesser un traitement** ou **retirer une autorisation**[305]. S'agissant de la sanction pécuniaire, son montant ne peut excéder 150 000 euros ; ce plafond est porté à 300 000 euros lorsque le manquement est réitéré dans les cinq ans, sans que la sanction pécuniaire puisse excéder 5% du chiffre d'affaires hors taxes du dernier exercice[306]. Quelle que soit la sanction prononcée, la CNIL doit respecter le principe du contradictoire[307].

En cas d'**urgence**, lorsque la mise en œuvre d'un traitement viole l'identité humaine, les droits de l'homme, la vie privée, les libertés individuelles ou publiques, la CNIL peut décider de l'interruption du traitement ou du verrouillage de certaines données personnelles pour une durée maximale de trois mois. Si les traitements en cause sont des traitements de souveraineté, la CNIL a seulement un pouvoir d'information du Premier ministre[308].
En cas d'**atteinte grave et immédiate aux droits et libertés précités**, la CNIL peut demander au juge, par la voie du référé, d'ordonner toute mesure de sécurité nécessaire à leur sauvegarde[309].

#### *4.3.4.5. Information au public*

La CNIL peut rendre publique son appréciation des conséquences de l'évolution des nouvelles technologies sur l'exercice des droits et libertés[310]. Elle élabore annuellement un **rapport public** qu'elle présente au Président de la République, au Premier ministre et au Parlement[311].

---

302 Article 26 I.
303 Article 30.
304 Article 11,2° e).
305 Article 45 I.
306 Article 47.
307 Article 46.
308 Article 45 II.
309 Article 45 III.
310 Article 11, 4°.
311 Article 11 dernier alinéa.

La CNIL est en droit de publier les différentes **sanctions** qu'elle peut prononcer, ce qui est dissuasif pour le responsable d'un traitement[312].
Enfin, elle met à disposition du public la **liste des traitements** automatisés ayant été déclarés ou autorisés ; cette liste contient des informations telles que la dénomination ou la finalité du traitement, l'identité et l'adresse de son responsable. Cette information est primordiale dans la mesure où elle permet l'effectivité des droits d'accès et de communication. La CNIL tient à disposition du public ses **avis, décisions ou recommandations**[313].

#### *4.3.4.6. Autres missions et compétences*

(droit de disposition, droit d'intenter une action, qualité pour déposer une plainte préalable susceptible de mettre en mouvement l'action publique, droit de recours contre une décision gracieuse)?

La CNIL ne dispose pas du pouvoir d'engager l'action publique : elle dispose seulement de celui d'**informer le procureur** de la République. En revanche, elle peut émettre des observations au cours de la procédure pénale[314].

La CNIL dispose d'un pouvoir de **recommandation** : « elle détermine en effet sinon les règles, au moins, les conditions de mise en œuvre des traitements »[315], ce qui est d'un grand intérêt pratique. La CNIL a ainsi émis une recommandation relative à la mise en œuvre, par les compagnies d'assurance et les constructeurs automobiles, de dispositifs de géolocalisation embarqués dans les véhicules ainsi qu'une recommandation en matière de transfert de données à caractère personnel dans le cadre de procédures judiciaires américaines dites de « discovery »[316].

### 4.3.5. Weitere Hinweise

La CNIL se dote de son propre **règlement intérieur**, ce qui participe de son pouvoir réglementaire[317].

## 4.4. Rolle der Organisationen zum Schutz der Betroffenen

### 4.4.1. Les compétences ou les droits de ces organisations

(par exemple action collective ou autre, susceptibles d'être subventionnés, autres droits ou compétences)

En matière de **consommation**, contrairement au système retenu pour protéger les données à caractère personnel, les organismes de régulation sont multiples. La Direction Générale de la concurrence, de la consommation et de la répression des fraudes (**DGCCRF**) joue le rôle d'interlocuteur unique pour le consommateur. Une ordonnance du 1er septembre 2005 a consolidé les pouvoirs de

---

312 Article 46 alinéa 2.
313 Article 31.
314 Article 11,2° e).
315 J.-Cl. Administratif, fasc.274, op. cit., n°301.
316 Délibérations 2010-096 du avril 2010 et 2009-474 du 23 juillet 2009.
317 Article 13 in fine.

cette direction dans la constatation et la poursuite des infractions au Code de la consommation[318]. La DGCCRF a aussi une mission d'information du public, qu'elle accomplit par diverses publications telles que le Bulletin officiel de la concurrence, de la consommation et de la répression des fraudes[319]. Le **Conseil national de la consommation** a, quant à lui, une mission de conseil des autorités législatives et réglementaires. Les **associations de consommateurs** sont toutefois les acteurs les plus connus de la défense des intérêts des consommateurs. Les organismes publics tirent leurs ressources directement de l'Etat ; les associations de consommateurs peuvent bénéficier de subventions de la part de l'Etat[320].
Les associations de consommateurs assument une **mission d'information** du consommateur, cherchent à améliorer la situation juridique de ce dernier en étant actives au sein d'instances normatives nationales ou européennes ; enfin, elles peuvent **agir en justice**, si elles sont obtenu un agrément[321]. Les associations de consommateurs peuvent exercer une action civile devant la juridiction pénale quand l'intérêt collectif des consommateurs a été lésé directement ou indirectement[322]. En outre, elles peuvent agir devant les juridictions civiles en cessation d'agissements illicites[323]. Enfin, elles sont en droit d'intervenir devant les juridictions civiles dans l'hypothèse où un consommateur a engagé une action devant ces dernières[324].
A défaut d'action de groupe, il existe seulement à l'heure actuelle une action en représentation conjointe : lorsque plusieurs consommateurs subissent un préjudice causé par un fait imputable au même professionnel, ils peuvent mandater une association de consommateurs agréée pour les représenter en justice[325].

La CNIL est aussi responsable de la protection des **patients** à l'égard des traitements de données de santé, qui font l'objet d'un régime spécial[326].

### 4.4.2. Sous quelle forme les personnes concernées doivent-elles s'adresser aux organisations ?

En ce qui concerne l'action en représentation conjointe, l'association de consommateurs ne pourra agir valablement que dans la mesure où chaque consommateur lui aura décerné un mandat écrit, mentionnant son objet et conférant à l'organisation agréée le pouvoir d'accomplir au nom du consommateur tous les actes de procédure.
Quant aux autres hypothèses d'interventions des associations de consommateurs, elles ne requièrent l'accomplissement d'**aucunes formalités particulières** de la part du consommateur.

---

318 Ord. n°2005-1086.

319 G. Raymond, Droit de la consommation, Litec 2008, p.358 et 359.

320 En 2007, 18 d'entre elles ont été subventionnées. UFC-Que choisir a ainsi reçu une subvention s'élevant à plus de 974 000 euros. DGCCRF, http://www.economie.gouv.fr/directions_services/dgccrf/actualites/docs/financement07.htm (17.08.2010)

321 Raymond, op. cit., p.362.

322 Article L421-1 du Code de la consommation.

323 Article L421-6 du Code de la consommation. Cette illicéité s'apprécie seulement par rapport aux dispositions de droit dérivé de l'Union européenne.

324 Article L421-7 du Code de la consommation.

325 Cette action en représentation conjointe a été créée par la loi n°92-60 du 18 janvier 1992, insérée dans le Code de la consommation aux articles L422-1 à L422-3.

326 Articles 53 à 66.

## 4.5. Mögliche und vorgeschriebene Aktivitäten der Datenbearbeiter (private und öffentliche)

### 4.5.1. Label de qualité de protection des données

Depuis la loi du 6 août 2004, la CNIL est compétente pour délivrer un **label à des produits ou procédures protégeant la protection des données à caractère personnel**[327]. Toutefois, elle peut exercer cette compétence seulement depuis la loi du 12 mai 2009 de simplification et de clarification du droit : la CNIL, qui reste seule titulaire du pouvoir de décerner un label, peut en effet désormais recourir à des experts externes. Le responsable d'un traitement peut ainsi souhaiter l'obtention d'un label attestant de la conformité des instruments et procédures utilisés au droit de la protection des données : en vertu du règlement intérieur de la CNIL, une organisation professionnelle peut soumettre à la CNIL un ensemble de règles professionnelles afin d'obtenir un avis favorable de l'autorité[328].

### 4.5.2. Inscription des fichiers

Au sein de l'organisme responsable du traitement, un **correspondant à la protection des données**, s'il en a été désigné un, tient une liste des différents traitements opérés par l'entreprise[329]. L'inscription des fichiers est aussi le fait de la **CNIL** dont on dit qu'elle tient le « fichier des fichiers » : la liste des fichiers qui lui ont été déclarés ou qu'elle a autorisés est disponible sur son site internet[330].

### 4.5.3. Reconnaissance du correspondant à la protection des données dans les entreprises

Depuis la réforme opérée par la loi du 6 août 2004, le responsable d'un traitement peut désigner « **un correspondant à la protection des données à caractère personnel** chargé d'assurer, de manière indépendante, le respect des obligations prévues [par] la présente loi »[331]. Cette désignation dispense alors le responsable des formalités déclaratives, sauf l'hypothèse d'un transfert de données à caractère personnel vers un Etat non membre de l'Union européenne. Le correspondant à la protection des données tiendra une liste des traitements opérés par l'entreprise, précisera leurs caractéristiques fondamentales, leurs finalités, les données traitées, la durée de conservation… Le correspondant informatique et libertés doit permettre une « amplification de la diffusion de la « culture informatique et libertés »[332].

---

327 Article 11,3° c).

328 Articles 52 et 53 du règlement intérieur de la CNIL.

329 Article 22 III.

330 http://www.cnil.fr/en-savoir-plus/fichiers-en-fiche/ (18.08.2010)

331 Article 22 III.

332 A. Türk, Loi du 6 août 2004. Présentation générale de la loi, Communication Commerce électronique 2005, étude 4.

### 4.5.4. « Data letter » (Information périodique et spontanée des traitements de données à l'attention des personnes concernées)

Certains responsables de traitements de données informent spontanément les personnes concernées de l'objet et des finalités du traitement, mais cela ne paraît être aujourd'hui qu'une **pratique minoritaire**[333].

### 4.5.5. Auto-régulation (code de conduite, BCR,…)

La CNIL a validé différents **codes de déontologie** élaborés par la pratique. Un Code de conduite sur l'utilisation de coordonnées électroniques à des fins de prospection directe ainsi qu'un Code de déontologie de la communication directe électronique, élaborés respectivement par l'Union Française du Marketing Direct et par le Syndicat National de la Communication Directe, ont ainsi été approuvés par la CNIL[334].

### 4.5.6. « Privacy by design »

Les responsables de traitements ne sont pas tenus d'intégrer des considérations tenant à la protection des données dès la conception de l'instrument permettant le traitement de données. La création d'un label garantissant la conformité des instruments et procédures utilisées au droit de la protection des données devrait cependant y contribuer.

---

333 Exemple d'une entreprise pratiquant cette information spontanée : http://www.areva.com/FR/accueil-551/mentions-legales.html (18.08.2010)

334 Délibérations de la CNIL n°2005-51 et n°2005-47 du 22 mars 2005.

## 5. Common Law: Grossbritannien

As a common law country, the UK approach to the resolution of legal questions, in general, and, those concerning data protection in particular, is significantly different from that of civil law jurisdictions, although not as radically different as is the case in the United States. The legislation adopted does not contain sufficient detail to provide clear, general and invariable answers to some of the questions to which we have been requested to respond in this study. Common Law legal decisions are quite fact specific and are made on a case-by-case basis. We have therefore followed the general structure of the questions posed and provided as much information as is possible in the absence of a specific fact situation.

The most important piece of legislation concerning data protection is the **Data Protection Act 1998**. Other legislation exists concerning access to information (Freedom of Information Act 2000 (c. 36)[335]) in general, and concerning environmental issues, in particular, (the Environmental Information Regulations 2004[336]), and direct marketing activities by electronic means as well as the use of cookies and spyware (the Privacy and Electronic Communications Regulations 2003[337]). Specific guidelines have also been published concerning the use of closed circuit television surveillance (CCTV Code of Practice[338]).

The Data Protection Act 1998 (hereinafter "DPA") was enacted to bring UK law into compliance with the European Data Protection Directive 95/46/EC.[339] It replaced and consolidated earlier legislation including, in particular, the Data Protection Act 1984 and the Access to Personal Files Act 1987. The DPA came into force on March 1, 2000. The DPA does not seek to guarantee personal privacy at all costs, but rather to strike a **balance** between the **rights of individuals** and the sometimes competing interests of those with **legitimate reasons for using personal information**. It applies to both data on paper and electronic data. Under the DPA, the Data Protection Registrar was re-named the **Information Commissioner**. Both the Data Protection Act and the Freedom of Information Act are regulated by the Information Commissioner's Office.

The DPA regulates the processing of Personal Data - information about a living individual that is **processed automatically** *(e.g.* by a computer) or **held within a relevant filing system** *(e.g.* manual records system) or recorded with the intention of processing or filing it, and which enables the individual to be identified **or identifiable** in conjunction with any information that the data processor might obtain. It should be noted that the term "relevant filing system" is interpreted broadly and includes such things as an individual's commercial diary or address book.

---

335 Available at : http://www.statutelaw.gov.uk/content.aspx?activeTextDocId=1876329 (consulted September 29, 2010).

336 ST 2004 N° 3391 available at : http://faolex.fao.org/docs/html/uk60491.htm (consulted September 29, 2010.

337 SI 2003 N° 2426, available at : http://www.legislation.gov.uk/uksi/2003/2426/contents/made (consulted September 29, 2010).

338 Available at : http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/ico_cctvfinal_2301.pdf.

339 Directive 95/46/EC of the European Parliament and of the Council of October 24, 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L. 281, 23/11/1995 p. 0031 - 0050.

Personal data can include photographs or images, in digital or analogue (non-digital) form. It also includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual. It should be noted that since the subject of the data ("**Data Subject**") must be a **'living individual'**, data concerning an organisation or company does not fall under the Act. In addition, anonymised or aggregated data is not regulated by the DPA, provided that the anonymisation or aggregation cannot be reversed.[340]

The DPA's definition of processing has a very broad scope and includes: obtaining, recording or holding data as well as specific activities such as organising, adapting, altering, retrieving, consulting, using, disclosing, disseminating, aligning, combining, blocking, erasing or destroying information.

The person who determines how the personal data is processed is referred to as a **Data Controller**. Unlike the Data Subject, the Data Controller is a **'legal person'**, which could include organisations and companies, their members or employees, or individuals. Unless they are only dealing with manual data, Data Controllers are required to provide the Information Commissioner with details about themselves and the data they are processing.

## 5.1. Grundsätze des Datenschutzes

### 5.1.1. Rolle der Zweckbindung

According to schedule 1 DPA, „personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with theat purpose or those purposes." Thus, the DPA recognizes the principle of purpose as one of 8 essential data protection principles.

In addition, the purpose of the data collection is essential for the application of other principles mentioned in schedule 1. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed and they should not be kept for longer than necessary for the purpose for which they are collected and processed.

### 5.1.2. Grundsätze Datenbearbeitung

Schedule 1 to the DPA sets forth 8 data protection principles. In addition to the principle of purpose and its concretizations, it mentions the principle of fairness and lawfulness, the principle data safety and restrictions on transfer.[341]

---

340 See DPA Section 1.

341 1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless—.

(a) at least one of the conditions in Schedule 2 is met, and

(b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. Personal data shall be accurate and, where necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

### 5.1.3. Erkennbarkeit / Transparenz, Einwilligung

According to schedule 1 (1) and schedule 2 DPA, data shall only be processed if the data subject has given his consent to the proceeding or if the processing is necessary for the performance or for entering a contract, for compliance with a legal obligation, to protect the vital interests of the data subjects or for the administration of justice. Consent or some othere interest of the data subjects is thus required for data processing.

### 5.1.4. Bearbeitung besonders schützenswerter Personendaten

Personal Data that consists of information on someone's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health condition, sex life, offences (committed or alleged), or proceedings/sentences for those offences are considered sensitive personal data. They are subject to additional regulation, as processing is not only subject to schedule 2 (see 5.1.3.), but it is only possible if one of the conditions mentioned in schedule 3 is met.

The first possibility mentioned in schedule 3 is “explicit consent to the processing of the personal data”. Other possibilities of schedule 3 include several cases of necessity (performance of right or obligation in connection with employment or protection of vital interest in case of reasonable impossibility to obtain consent, in connection to legal proceedings and the administration of justice or another public enactment; medical purposes, if undertaken by health professionals; fraud prevention in connection to members of anti-fraud organizations, identification of the absence of equal opportunities in connection to information on racial or ethnic origin,), processing of member data by non profit organizations for political, philosophical, religious or trade union purposes with appropriate safegauards, not involving disclosure to third parties, processing of information made public as a result of steps deliberately taken by the subject. In addition, the Secretary of State can make an order establishing circumstances under which sensitive data may be processed.

### 5.1.5. Datensicherheit

According to sechdul 1 to the DPA, “appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.” The safety of data is thus one of the basic principles of Data protection legislation. It requires the data processer to take specific steps to insure the safety of the data.

### 5.1.6. Grenzüberschreitende Bekanntgabe

The Information Commissioner has published guidance concerning the transfer of data outside the EEA.[342] That guidance provides for a 4 step process:

---

6. Personal data shall be processed in accordance with the rights of data subjects under this Act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

342 See Information Commissioner’s Office publication entitled « The eighth data protection principle and international data transfers : The Information Commissioner’s recommended approach to assessing adequacy including consideration of the issue of contractual solutions, binding corporate rules and Safe

• Step 1 - consider whether there will be a transfer of personal data to a third country.

• Step 2 – consider whether the third country and the circumstances surrounding the transfer ensure that an adequate level of protection will be given to that data.

• Step 3 – consider whether the parties have or can put into place adequate safeguards to protect that data (for instance, by entering into model clauses or establishing binding corporate rules

• Step 4 – consider if any of the other derogations to the eighth principle specified in the Act apply (such as the consent of the data subject to the transfer).

#### *5.1.6.1. Step 1*

Where it will be necessary to process personal data and that data will be going out of the EEA to a third country, it must be determined this movement of data represents a 'transfer' for the purposes of the eighth principle. The DPA does not define 'transfer' but the Information Commissioner's office makes it clear that transfer does not mean the same as mere transit. Therefore the fact that the electronic transfer of personal data may be routed through a third country on its way from the UK to another EEA country does not bring such transfer within the scope of the eighth principle.

Section 1(3) of the Act requires that the transfer of information which is not initially personal data but is intended to be processed automatically or as part of a 'relevant filing system'4 [343]only after it has been transferred should be afforded the protection of the Act. An example of this would be where information is provided by someone in the UK over the telephone to someone in a third country who then enters the information on a computer. In the case of Bodil Lindqvist v Kammaraklagaren[344], the European Court of Justice held that there was no transfer of personal data to a third country where an individual loaded personal data onto an internet page in a Member State using a internet hosting provider in that Member State, even though the page was accessible via the internet by people based in a third country. Instead, a transfer was only deemed to have taken place where the internet page was actually accessed by a person located in a third country. In practice, data are often loaded onto the internet with the intention that the data be accessed in a third country, and, as this will usually lead to a transfer, the principle in the Lindqvist case will not apply in such circumstances. However, in situations where there is no intention to transfer the data to a third country and no transfer is deemed to have taken place as the information has not been accessed in a third country (*i.e*. the eighth principle does not apply), data controllers will still need to ensure that the processing complies with all of the other principles. In particular, data controllers must consider the requirement in the first data protection principle that the processing must be fair which may be contravened by making the data so widely accessible.[345]

---

Harbor.Available » at : http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/international_transfers_legal_guidance_v2.0_300606.pdf (consulted October 5, 2010).

343 Section 1(1) of the Act – see Chapter 2 of 'The Data Protection Act 1998 – Legal Guidance' (available at : http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/data_protection_act_legal_guidance.pdf (consulted October 5)), and specifically the clarification of the definition of 'relevant filing system' following the case of Durant v The Financial Services Authority [2003 EWCA Civ 1746].

344 (2003) (Case C-101/01).

345 See Information Commissioner's Office publication entitled « The eighth data protection principle and international data transfers : The Information Commissioner's recommended approach to assessing adequacy including consideration of the issue of contractual solutions, binding corporate rules and Safe Harbor Available », *op. cit.*

### *5.1.6.2. Step 2*

Having established that there is a transfer of personal data to a third country, the data controller must then ask whether that third country ensures an adequate level of protection to the personal data taking into account all the circumstances of the transfer ('adequacy'). A decision of whether or not there is adequacy may be based on a Community finding of adequacy or after an assessment of adequacy made by the data controller itself.

In addition to findings relating to the above countries, the Commission has also made a finding regarding specific transfers to the United States of America by the use of Safe Harbor. The Safe Harbor scheme consists of a set of principles which are similar to the principles found in the DPA[346] and relates to transfers to US entities. It has been operational since 1 November 2000 when the US Department of Commerce opened the on-line self certification process for US organisations wishing to notify their adherence to the principles. The scheme creates a voluntary mechanism enabling US organisations to qualify as offering adequate protection for personal data transferred to them from the EU and is recognised by the Commission as providing adequate protection for the transfer of personal data under the terms of the Directive. The Federal Trade Commission is primarily responsible for enforcing Safe Harbor but the scheme is not available to companies in all sectors, *e.g.* telecommunications companies and financial institutions are not covered by the regime.

Where the data protection regime in the third country has not been subject to a Commission finding of adequacy, it is for exporting controllers to assess adequacy in a way which is consistent with the Directive and the DPA. In carrying out this assessment of adequacy, the Commissioner expects exporting controllers to be able to demonstrate how they have addressed the various criteria set out in the ICO guidance.[347]

Schedule 1, Part II paragraph 13 of the DPA (implementing Article 25(2) of the Directive) states that the level of protection must be "adequate in all the circumstances of the case" and provides that, in assessing adequacy, particular consideration should be given to:

- the nature of the personal data;
- the country or territory of origin of the information contained in the data;
- the country or territory of final destination of that information;
- the purposes for which and period during which the data are intended to be processed;
- the law in force in the country or territory in question;
- the international obligations of that country or territory;
- any relevant codes of conduct or other rules which are enforceable in that country or territory (whether generally or by arrangement in particular cases); and
- any security measures taken in respect of the data in that country or territory.

---

346 See http://www.export.gov/safeharbor/index.asp (consulted October 5, 2010).

347 See Information Commissioner's Office publication entitled « The eighth data protection principle and international data transfers : The Information Commissioner's recommended approach to assessing adequacy including consideration of the issue of contractual solutions, binding corporate rules and Safe Harbor Available », *op. cit.*

#### *5.1.6.3. Step 3*

If it is not possible for an exporting data controller to satisfy itself that there is adequacy, the use of Commission-authorised standard contracts (model clauses) or specific, approved binding corporate rules (BCR) enable the transfer to be made exempt from the restrictions of the eighth principle on the basis that the model clauses or set of BCR provide adequate safeguards for the rights and freedoms of data subjects. This derives from Article 26(2)[348] of the Directive which states that:

> a Member State may authorise a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection […] where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; such safeguards may in particular result from appropriate contractual clauses…

Transfers which are exempt by virtue of Article 26(2) ensure conditions whereby the individuals in question continue to be protected as regards processing of their data even after the data have been transferred. For this reason the ICO believes that it is good practice to attempt to satisfy one of these Article 26(2) derogations before considering the derogations which derive from Article 26(1)[349] (which do not ensure such a high level of protection).[15]

The Information Commissioner has issued authorisations under s54(6) of the DPA in relation to each of the model clauses[350] (on 21 December 2001, 8 March 2003 and 27 May 2005, respectively) providing that, for the purpose of paragraph 9 of Schedule 4 to the DPA, the eighth principle does not apply where the transfer has been made using any of the model clauses. This means that an exporting controller who uses these model clauses does not need to make a separate assessment of adequacy in relation to the transfer.

**Binding corporate rules (BCR)**

BCR are internal codes of conduct operating within a multinational organisation for the purposes of enabling transfer of data outside the EEA (but within the group) to be made on a basis which ensures adequate safeguards for the rights and freedoms of data subjects for the purposes of paragraph 9 of Schedule 4 to the DPA. They are designed to be a global solution for multinational companies by ensuring their intra-group transfers comply with the eighth principle and providing a simple mechanism for obtaining the necessary authorisations across the EU. BCR must be submitted for approval by the Commissioner in order to obtain an authorisation which provides that transfers from the UK may be made within the group on the basis of the BCR.

---

348 Implemented by paragraphs 8 and 9 of Schedule 4 to the DPA.

349 Implemented by paragraphs 1 to 7 of Schedule 4 to the DPA.

350 The clauses appear as an annex to the Decision which approves them. See http://eur-lex.europa.eu/pri/en/oj/dat/2001/l_181/l_18120010704en00190031.pdf; http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002D0016:EN:NOT ; http://eur-lex.europa.eu/LexUriServ/site/en/oj/2004/l_385/l_38520041229en00740084.pdf (consulted October 4, 2010).

### *5.1.6.4. Step 4*

As set out under Step 3 above, the use of BCR and model clauses are two derogations from the eighth principle derived from Schedule 4 of the Act. There are also a number of other derogations in Schedule 4 which may be considered. They are as follows.

- The data subject has consented to the transfer.
- The transfer is necessary for the performance of, or for the taking of steps at the request of the data subject with a view to entering into, a contract between the data subject and the data controller.
- The transfer is necessary for the performance of, or entering into, a contract between the data controller and a third party entering into the contract at the request, or in the interests, of the data subject.
- The transfer is necessary for reasons of substantial public interest.
- The transfer is necessary in connection with legal proceedings, advice or rights.
- The transfer is necessary to protect the vital interests of the data subject.
- The transfer is of part of the personal data on a public register.30

Unlike BCR or model clauses, where these derogations are used there is not necessarily any protection in place in relation to the data being transferred. Instead, these provisions reflect the fact that there are instances where it will be justifiable to transfer data even though there will be a lower level of protection given to those data. As such, in interpreting these provisions, the derogations should be narrowly construed.

Article 2(h) of the Directive defines **consent** as "any freely given specific and informed indication of [the data subject's] wishes by which the data subject signifies his agreement to personal data relating to him being processed". Consequently, exporting controllers should be able to produce clear evidence of the data subject's consent in any particular case and may be required to demonstrate that the data subject was informed as required. Similarly, valid consent means that the data subject must have a real opportunity to withhold their consent without suffering any penalty, or to withdraw it subsequently if they change their mind.

In order to fall within the derogations where "**necessary for a contract** between data controller and data subject or data controller and third party" it needs to be shown that the transfer is **necessary** for the performance or entering into of the contract. If it is a third party entering into the contract, rather than the data subject, then it has to be clearly shown that they are entering into it at the request of the data subject or that it is clearly in the data subject's interests

To qualify for the **substantial public interest derogation**, the transfer must be "**necessary for reasons of substantial public interest**"[351] This is subject to the same strict interpretation as that applied to the other derogations discussed in this section and is a high threshold. The Secretary of State may by order specify circumstances in which a transfer is to be taken to be necessary for reasons of substantial public interest. No such orders are in force to date.[352]

---

351 Article 29 Working Party's Working document on a common interpretation of Article 26(1) of Directive 95/46/EC (2093/05/EN – WP114) page 14.

352 See Information Commissioner's Office publication entitled « The eighth data protection principle and international data transfers : The Information Commissioner's recommended approach to assessing adequacy including consideration of the issue of contractual solutions, binding corporate rules and Safe Harbor.Available » page 25, at : http://www.ico.gov.uk/upload/documents/library/data_protection/

A **legal matters** derogation will apply where the transfer is necessary:

• for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings);

• for the purpose of obtaining legal advice; or

• for the purposes of establishing, exercising or defending a legal right.

Once again, the emphasis in using this derogation is on necessity and the need to balance the legal rights at the centre of the advice or action with the data subject's rights in relation to their personal data.

The Commissioner considers that the **vital interests of the data subject** exception to the eighth principle may only be relied upon where the data transfer is necessary for matters of life and death such as a medical emergency. For instance, it would clearly be essential to be able to transfer data if the data subject is in urgent need of medical attention in a third country and only their usual doctor based in a Member State can supply this data. The derogation could not be relied upon, by contrast, if the data are not transferred for the purpose of treating the data subject but instead are to be used for general medical research in the future.

The **public registers** derogation may be relied upon if the transfer is of part of the personal data on a public register in a Member State and any conditions to which the register is subject are complied with by any person to whom the data are or may be disclosed after the transfer.

If the transfer falls under any of the derogations discussed above then it is exempt from the eighth principle and may proceed without any further requirements or prior authorisation. However, if adequacy has not been adduced in line with Step 2 or the derogations described in Steps 3 and 4 do not apply, the transfer may not proceed without being in breach of the eighth principle.

### 5.1.7. Auskunftsrecht

Article 7 of the DPA provides that an individual is entitled to be informed by any data controller whether personal data concerning him or her are being processed by or on behalf of that data controller. If so, the data controller must provide the individual with a description of

(i) the personal data of which that individual is the data subject,
(ii) the purposes for which they are being or are to be processed, and
(iii) the recipients or classes of recipients to whom they are or may be disclosed.

The data controller must also provide, in an intelligible form

(i) the information constituting any personal data concerning that individual,
(ii) any information available to the data controller as to the source of those data.

In addition, where the processing by automatic means of personal data of which that individual is the data subject for the purpose of evaluating matters relating to him such as, for example, his performance at work, his creditworthiness, his reliability or his conduct, has constituted or is likely to constitute the **sole basis for any decision significantly affecting him**, the individual has a right to be informed by the data controller of the **logic involved in that decision-taking.** In order to obtain such

---

detailed_specialist_guides/international_transfers_legal_guidance_v2.0_300606.pdf (consulted November 9, 2010).

information, the **individual must make a request in writing and pay the relevant fee (**limited by statute).

## 5.1.8. Verhältnis Technologieentwicklung

There are no technical applications explicitly mentioned in the DPA, however some of the Regulations adopted in connection with the DPA contain provisions concerning specific technologies and the ICO has published guidelines and codes of conduct concerning others.

### *5.1.8.1 Cookies and personal data*

The use of devices such as cookies has for some time been commonplace and cookies are important to provide many online services. Using such devices is not, therefore, prohibited by the Privacy and Electronic Communications Regulations[353] ("Regulations") but they do require that subscribers and users should, to some extent, be given the choice as to which of their online activities are monitored in this way. Although devices which process personal data give rise to greater privacy and security implications than those which process data from which the individual cannot be identified, the Regulations apply to all uses of such devices, not just those involving the processing of personal data.

Where the use of a cookie type device does involve the processing of personal data, service providers will need to make sure they comply with the additional requirements of the Data Protection Act 1998. This includes the requirements of the third data protection principle which states that data controllers must not process personal data that is excessive. Where personal data is collected, the data controller should consider the extent to which that data can be effectively processed anonymously. This is likely to be particularly relevant where the data is to be processed for a purpose other than the provision of the service directly requested by the user, for example, counting visitors to a website.[354]

Cookies or similar devices must not be used unless the subscriber or user of the relevant terminal equipment:

- is provided with clear and comprehensive information about the purposes of the storage of, or access to, that information; and
- is given the opportunity to refuse the storage of, or access to, that information.

Regulation 6(3) states that once a person has used such a device to store or access data in the terminal equipment of a user or subscriber, that person will not be required to provide the information described in Regulation 6(2) on subsequent occasions, as long as they met these requirements initially. Although the Regulations do not require the relevant information to be provided on each occasion, they do not prevent this.[355]

The Regulations specify that service providers should not have to provide the information specified in Regulation 6(2) where that device is to be used:

---

353 The Privacy and Electronic Communications (EC Directive) Regulations 2003 SI No. 2426, available at : http://www.legislation.gov.uk/uksi/2003/2426/contents/made (consulted October 11, 2010).

354 The ICO's « Guide to the Privacy and Electronic Communications Regulations », Confidentiality of Communications, available at : http://www.ico.gov.uk/for_organisations/privacy_and_electronic_communications/the_guide/cookies.aspx (consulted October 11, 2010).

355 http://www.ico.gov.uk/for_organisations/privacy_and_electronic_communications/the_guide/cookies.aspx (consulted October 4, 2010).

•for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network; or

•where such storage or access is strictly necessary to provide an information society service requested by the subscriber or user.

In defining an 'information society service' the Electronic Commerce (EC Directive) Regulations 2002 refer to 'any service normally provided for remuneration, at a distance, by means of electronic equipment for the processing (including digital compression) and storage of data, and at the individual request of a recipient of a service'.

The term 'strictly necessary' means that such storage of or access to information should be essential, rather than reasonably necessary, for this exemption to apply. However, it will also be restricted to what is essential to provide the service requested by the user, rather than what might be essential for any other uses the service provider might wish to make of that data. It will also include what is required to comply with any other legislation the service provider might be subject to, for example, the security requirements of the seventh data protection principle.[356]

Location data means any data processed in an electronic communications network that indicates the geographical position of the terminal equipment of a user of a public electronic communications service, including information relating to:

•the latitude, longitude or altitude of the terminal equipment;

•the direction of travel of the user; or

•the time the location information was recorded.

Regulation 14 does not apply to the processing of traffic data.

#### *5.1.8.2. Restrictions on processing*

Location data relating to a subscriber or user of a public electronic communications network may only be processed where:

•the subscriber or user cannot be identified from that data: or

•where it is necessary to provide a value added service with the consent of the relevant user or subscriber.

Location data must only be processed by the communications provider in question, the third party provider of the value added service or a person acting on behalf of either of the above. Where the processing is carried out to provide a value added service, the processing of location data should be restricted to what is necessary for those purposes.

The public communications provider must obtain the prior consent of the user or subscriber to process location data to provide a value added service (where the user or subscriber can be identified from that data). Before consent can be obtained the communications provider must provide the user or subscriber with the following information.

•The types of location data that will be processed

•The purposes and duration of the processing of those data

•Whether the data will be transmitted to a third party to provide the value added service.

---

356 *Id.*

In the case of a corporate subscriber, a person making decisions on behalf of the company is likely to be able to give consent, unless the communications provider has reasonable grounds to believe otherwise.

The Regulations do not prescribe how service providers should obtain this consent. However, to obtain valid informed consent, the subscriber or user should be given enough clear information for them to have a broad appreciation of how the data are going to be used and the consequences of consenting to such use (see the first principle in the guide to data protection).

In light of this, the service provider will not be able to rely on a blanket 'catch all' statement on a bill or a website but rather will need to obtain specific informed consent for each value added service requested and to market their own electronic communications services.[357]

Where a valued added service is provided by a public communications provider with a third party, in the interests of transparency the person who will be seen to be responsible for providing the service should get the consent to process location data for such a purpose. Whether this will be the service provider or the third party will depend on the specific circumstances. The point is that the way in which a service is provided should be consistent with the expectations of the subscriber or user.

Where the user consents to one party to provide a particular service, they should not then be surprised when they are contacted by another party relating to the provision of that service.

Where a user or subscriber has given informed consent to the processing of location data, the user or subscriber can withdraw that consent at any time and the communications provider should make the user or subscriber aware of that fact. The user or subscriber should also be provided with an opportunity to withdraw their consent on the occasion of each connection to the network or on each transmission of a communication.

Although the obligation is to provide for a permanent withdrawal of consent, there is nothing in the Regulations that will prevent the service provider from also offering the user the chance to suspend their consent for a limited, specified period of time. If the user chooses to accept such an option, there is similarly nothing to prevent the provider from reactivating their consent after the specified period of time has elapsed, providing the intention to do so was made clear at the time the user opted for a time-bound suspension.[358]

#### *5.1.8.3. Telemarketing*

Regulation 19 requires that companies or organisations making **automated marketing telephone calls have the prior consent** of the subscribers they are calling.

The regulations require that organisations **do not make 'live' marketing calls** (where there is actually a person talking to them, as opposed to a recorded message) to:

- a subscriber who has indicated a general objection to receiving such calls by registering with the **Telephone Preference Service** (TPS), a subscriber who has indicated a general objection

---

357 See the Information Commissioner's Guidance on the Privacy and Electronic Communications (EC Directive) Regulations 2003 available at : http://www.ico.gov.uk/upload/documents/library/privacy_and_electronic/detailed_specialist_guides/pecr_guidance_part2_1206.pdf (consulted October 7, 2010)

358 http://www.ico.gov.uk/for_organisations/privacy_and_electronic_communications/the_guide/location_data.aspx (consulted October 4. 2010)

to receiving such calls by registering with the **Corporate Telephone Preference Service** (CTPS); or

- **a subscriber who has notified the caller that he does not wish to receive such unsolicited calls**.

The regulations require that organisations not make **automated (pre-recorded phone messages) marketing calls** without the **prior consent** of any subscriber.

Regulation 19(4) clarifies the definition of 'automated calling system'. It refers to a system which is 'capable of automatically initiating a sequence of calls to more than one destination in accordance with instructions stored in that system' and which transmits 'sounds which are not live speech for reception by persons at some or all of the destinations so called'. The UK Information Tribunal ruled on a case where automated calls had been used to promote the Scottish National Party ("SNP") in the lead up to the 2005 General Election.[359] It held that the regulations did apply to political parties and not-for-profit organisations and therefore the SNP's use of automated calling without obtaining prior consent was in violation. It is important to note that automated calling systems do not cover marketing by text, picture or video message, by fax or by email, nor do they cover the technology used by some call centres to dial target numbers automatically in order to facilitate live telephone conversations, so called 'power dialling'. Text, picture and video messages, faxes, live voice telephone calls and emails are covered elsewhere in the Regulations.

#### *5.1.8.4. Marketing via Fax*

All marketing messages sent by fax must include the identity of the caller and a contact address or Freephone number.[360] Marketing faxes **may not be sent to private individuals without their prior consent**. Unsolicited marketing faxes **may be sent to a business** but only if the business is not registered with the Fax Preference Service (FPS).[361]

#### *5.1.8.5. Marketing via Electronic Mail*

Organisations must **have prior consent** to send unsolicited marketing material by **electronic mail to individual subscribers, unless** they have obtained the details during the **course of a sale, or negotiations** towards one, and the **individual is given the opportunity to object in every message**. The prior consent rule does not apply to corporate subscribers. Marketing communications should still identify the sender and provide a valid address. Depending on the information the company holds about it, a corporate subscriber may also have rights under the Data Protection Act.[362]

The Regulations define electronic mail as 'any text, voice, sound, or image message sent over a public electronic communications network which can be stored in the network or in the recipient's terminal

---

359 Scottish National Party v. the Information Commissioner, Appeal Number: EA/2005/0021, May 15, 2006. Available at : http://www.informationtribunal.gov.uk/Documents/decisions/scottish_national_party.pdf (consulted Oct. 4, 2010)

360 Regulation 24(1)(a).

361 See : Information Commissioner's website, Fax Marketing available at : http://www.ico.gov.uk/for_organisations/privacy_and_electronic_communications/the_guide/fax_marketing.aspx.

362 See, Information Commissioner's Guidance for marketers on the Privacy and Electronic Communications (EC Directive) Regulations 2003 available at : http://www.ico.gov.uk/upload/documents/library/privacy_and_electronic/detailed_specialist_guides/guidance_part_1_for_marketers_v3.1_081007.pdf (consulted October 7, 2010)

equipment until it is collected by the recipient and includes messages sent using a short message service'.[363]

In other words, **both e-mail and text, picture and video marketing messages are considered to be 'electronic mail'**. Marketing transmitted in WAP messages is considered to be 'electronic mail'. WAP Push allows a sender to send a specially formatted SMS message to a handset which, when received, allows a recipient through a single click to access and view content stored online, through the browser on the handset.

The Information Commissioner considers that **this rule also applies to voicemail and answerphone** messages left by marketers making marketing calls that would otherwise be 'live'. Therefore, there are stricter obligations placed upon marketers who make live calls but who wish to leave messages on a person's voicemail or answerphone.

A marketer cannot transmit, or instigate the transmission of, unsolicited marketing material by electronic mail to an individual subscriber without having previously received the subscriber's consent to receiving such communications. There is an exception to this rule which has been widely referred to as the **soft opt in**.[364]

The transmission, or instigation of the transmission of, any marketing by electronic mail (whether solicited or unsolicited) to any subscriber (whether corporate or individual) is prohibited where the marketer's identity has been disguised or concealed; or the marketer has not provided a valid address to which the recipient can send an opt-out request.[365] Such materials may be sent where the contact details of the recipient have been obtained in the course of a sale or negotiations for the sale of a product or service to that recipient; the direct marketing material in question relates to similar products and services of the sender only; and the recipient has been given a simple means of refusing (free of charge except for the cost of transmission) the use of their contact details for marketing purposes at the time those details were initially collected and, where they did not refuse the use of those details, at the time of each subsequent communication. This is referred to as the '**soft opt-in'**.

The rules on email **do not apply to emails sent to organisations** except that marketers must still identify themselves and provide an address. Individual employees who have personal corporate email addresses are entitled under the DPA to require that marketers stop using that address for marketing.[366]

## 5.2. Durchsetzungsrechte der Datenschutzanliegen für Betroffene

The DPA makes little distinction between the obligations of public and private Data Controllers. Differences do exist under the **Freedom of Information Act**.

The DPA creates **rights for those who have their data stored**, and responsibilities for those who store, process or collect personal data. The person whose personal data is stored or processed has the right to:

---

363 See Regulation 2 'Interpretation'.

364 See Regulation 22(2).

365 See Regulation 23.

366 ICO Data Protection Good Practice Note « Electronic mail marketing » available at : http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/electronic_mail_marketing_12_06.pdf (consulted October 4, 2010.

- **Access** their personal data.[367] This covers a wide variety of information, for example medical records, files held by public bodies, and financial information held by credit reference agencies.
- A Data Subject has a right to **be informed**, upon request, of any personal data being processed by or on behalf of a Data Controller. They can also request, for a small fee, a copy of that data and information about how and why the information is being processed and to whom it is being disclosed (see above, 5.1.7.).
- Prevent processing for direct marketing (see 5.1.9.3. – 5.1.9.5).[368]
- **Prevent decisions being made** about such things as creditworthiness or work performance **solely on the basis of automatically processed data**.[369]
- Data Subjects and others damaged by the actions of a Data Controller are entitled to claim **compensation**.[370]
- As well as awarding compensation, a court can insist on the **'rectification, blocking, erasure or destruction**' of personal data.[371]

The DPA is structured such that all processing of personal data is covered by the act while providing for a number of exceptions in Part IV. Notable **exceptions** include:

- Section 28 – **National security**. Any processing for the purpose of safeguarding national security is exempt from all of the data protection principles, as well as Part II (subject access rights), Part III (notification), Part V (enforcement) and Section 55 (Unlawful obtaining of personal data).
- Section 29 – **Crime and taxation**. Data processed for the prevention or detection of crime, the apprehension or prosecution of offenders, or the assessment or collection of taxes, are exempt from the first data protection principle.
- Section 36 – **Domestic purposes**. Processing by an individual only for the purposes of the individual's personal, family or household affairs is exempt from all the data protection principles, as well as Part II (subject access rights) and Part III (notification).
- Data processing in the public interest for **journalistic, literary, artistic, and historical or research purposes** benefit from certain exemptions as well pursuant to Sections 32 and 33.

### 5.2.1. Prevention of Processing

A Data Subject has the right **to prevent processing which is likely to cause damage or distress** to him/herself or to another person.[372] The individual must give written notice to the Data Controller. If a court is satisfied such an individual has properly given a notice which appears to the court to be justified and that the data controller in question has failed to comply with the notice, the court may order him to take such steps for complying with the notice as the court thinks fit.

---

367 DPA Part II Section 7.
368 DPA Part II Section 11.
369 DPA Part II Section 12.
370 DPA Part II Section 13.
371 DPA Part II Section 14.
372 DPA Art. 10.

### 5.2.2. Prevention of Decisions based on Automatically Processed Data

An individual is also entitled at any time, by notice in writing to any data controller, to **require** the data **controller to ensure** that no decision taken by or on behalf of the data controller which significantly affects that individual is based solely on the processing by automatic means of personal data in respect of which that individual is the data subject for the purpose of evaluating matters relating to him such as, for example, his performance at work, his creditworthiness, his reliability or his conduct.[373]

Where, **in the absence of such notice**, a decision which significantly affects an individual is based solely on such processing

(a) the data controller must as soon as reasonably practicable **notify the individual** that the decision was taken on that basis, and

(b) the **individual is entitled**, within twenty-one days of receiving that notification from the data controller, by notice in writing to **require the data controller to reconsider the decision** or to take a new decision otherwise than on that basis.

The data controller must then, within twenty-one days of receiving such a notice, give the individual a written notice specifying the steps that he intends to take to comply with the data subject notice. Decisions taken in the context of possibly entering into a contract with the individual or performing such a contract are exempt[374].

### 5.2.3. Damages

An individual who suffers damage by reason of any contravention by a data controller of any of the requirements of the DPA is entitled to compensation from the data controller for that damage. If the contravention relates to the processing of personal data for **artistic, literary or journalistic purposes**, an individual who suffers **distress** may also be entitled to compensation.[375]

### 5.2.4. Rectification, Eradication, Destruction

If a court is satisfied on the application of a data subject that personal data of which the applicant is the subject are **inaccurate,** the **court** may order the data controller to rectify, block, erase or destroy those data and any other personal data in respect of which he is the data controller and which contain an expression of opinion which appears to the court to be based on the inaccurate data. Under certain circumstances, the court may, as an alternative, make an order requiring the data to be **supplemented by such statement of the true facts relating to the matters dealt with** by the data as the court may approve. The court may also, where it considers it reasonably practicable, order the data controller to **notify third parties to whom the data have been disclosed of the rectification, blocking, erasure or destruction.**[376]

### 5.2.5. Procedure

The Information Commissioner's Office suggests that individuals who believe that their rights under the DPA have been violated should initially **contact the organisation** in question to attempt to remedy the situation. If the individual does not obtain satisfaction, it **can file a complaint with the ICO** in order that the ICO can determine whether it believes the organisation has violated the DPA. If such is the

---

373 DPA Art. 12.

374 *Id.*

375 DPA Art. 13.

376 DPA Art. 14.

case, the ICO will attempt to work with the organisation to resolve the problem and, if the organisation does not respond, the ICO can order it to do so.

In addition, a data subject (or anyone acting on his or her behalf) can request the Information Commissioner to assess if data processing is being carried out by a data controller in compliance with the Data Protection Act 1998. The time period for responding to an assessment request is determined by the Information Commissioner.[377]

The ICO cannot, however, **award compensation. Only a court** can do so, if the individual brings a lawsuit against the organisation. This is a separate process that neither requires ICO intervention nor takes into account any ICO determination.[378]

## 5.3. Nationale Aufsichtsbehörde

### 5.3.1. Zusammensetzung, Ernennung und Eingliederung der Behörde

The Information Commissioner is a corporation sole set up initially by the Data Protection Act 1984 under the name of Data Protection Registrar. Following implementation of the Data Protection Act 1998 on 1st March 2000 it continued in existence under the name of Data Protection Commissioner. The Freedom of Information Act 2000 received Royal Assent on 30th November 2000 and the title of the Data Protection Commissioner changed to the Information Commissioner with effect from 30th January 2001.

The Information Commissioner's Office is an **independent authority** body established to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The **Ministry of Justice** is its sponsoring department within the government and it reports directly to Parliament. The ICO enforces and oversees the Data Protection Act, the Freedom of Information Act, the Environmental Information Regulations, and the Privacy and Electronic Communications Regulations.

The Information Commissioner is **appointed by the Queen** for a term of no more than **five years** and may be re-appointed for a second term and for a third or subsequent term only if, by reason of special circumstances, the person's re-appointment for such a term is desirable in the public interest. He or she may not, however, serve beyond the age of sixty-five or for more than fifteen years.[379]

The Information Commissioner has an office (ICOO) with various subdivisions (organisational development, Operations, Corporate Affairs, Data Protection, Freedom of Information) and a managing board.[380]

---

377 See website of the City of London, Data Protection Act, available at : http://www.cityoflondon.gov.uk/Corporation/LGNL_Services/Council_and_democracy/Data_protection_and_freedom_of_information/Data_protection_act.htm (Consulted October 11, 2010).

378 See ICO website, Data Protection, when to complain and how, available at : http://www.ico.gov.uk/complaints/data_protection.aspx (consulted October 8, 2010).

379 DPA Schedule 5 Part I Section 2.

380 For the Organizational Structure, see http://www.ico.gov.uk/upload/documents/library/corporate/practical_application/organisational_chart.pdf (29.09.2010).

### 5.3.2. Gewährleistung der Unabhängigkeit

A Framework Document[381] which sets out the broad framework within which the Commissioner will operate has been agreed. It comprises a Management Statement and a Financial Memorandum. In particular the Framework Document covers:

- the rules and guidelines relevant to the exercise of the Commissioner's functions, duties and powers;
- the conditions under which any public funds are paid to the Commissioner;
- the arrangements for the Commissioner reporting to Parliament; and
- the relationship between the Secretary of State and his Department, and the Commissioner.[382]

The Department's Principal Accounting Officer is **answerable to Parliament**, through the Committee of Public Accounts, for the monies voted to the Department, in particular:

a) the payment of the grant-in-aid to the Commissioner;
b) the conditions attached to the grant-in-aid;
c) monitoring the Commissioner's compliance with those conditions;
d) the steps taken to ensure that the financial and other management controls applied by the Department and the Commissioner conform to the requirements of good financial management and are appropriate and sufficient to safeguard public funds and
e) the Department reserves the right to arrange for independent reviews of internal audit arrangements of the Commissioner.

The Commissioner by virtue of his duty of signing the Accounts as Accounting Officer is answerable to Parliament, through the Committee of Public Accounts, for the management of all monies allocated to him. The Commissioner and his staff may be called to give evidence before the relevant Select Committee of Parliament.[383]

Once the Commissioner has received a formal statement of its financial provision, and subject to any restrictions imposed by statute, the Director General Policy, the Management Statement and the Financial Memorandum, the Commissioner will have authority to incur expenditure approved in the budget without further approval, provided that a) the Commissioner complies with the delegations set out in the Financial Memorandum and b) the Commissioner complies with the conditions set out in section 3.3 of the Financial Memorandum regarding novel, contentious or repercussive proposals.

### 5.3.3. Zuständigkeitsbereich

The Information Commissioner regulates the following legislation:

- The Data Protection Act 1998
- The Freedom of Information Act 2000

---

381 Available at : http://www.ico.gov.uk/upload/documents/library/corporate/detailed_specialist_guides/management_statement_april_2005.pdf (consulted September 29, 2010).

382 http://www.ico.gov.uk/about_us/what_we_do/corporate_information.aspx.

383 http://www.ico.gov.uk/upload/documents/library/corporate/detailed_specialist_guides/management_statement_april_2005.pdf.

- The Environmental Information Regulations 2004
- Privacy and Electronic Communications Regulations 2003
- The Public Records Act 1958
- The Re-Use of Public Sector Information Regulations 2005

The ICO oversees and investigates compliance with the provisions of those Acts but also provides services, information and advice to both individual members of the public and organisations. It publishes numerous brochures, guidelines and codes of conduct to assist the various actors in complying with the relevant provisions of the law as well as offering assistance and information to individuals in enforcing their rights under the law. Individuals therefore turn to the ICO, rather than to any consumer protection organisation, for help and advice in these areas.

There are four main focuses to the work of the ICO:

**Educating and influencing**

- Providing an enquiry service for individuals and organisations.
- Publishing guidance and information to encourage organisations to achieve good practice and help individuals to understand their rights.
- The ICO speaks to groups to raise awareness of the law and how it works.
- The ICO influences thinking on privacy and access issues.

**Resolving problems**

- The ICO resolves eligible complaints from people who think the Data Protection Act or Freedom of Information Act has been breached.

**Enforcing**

- The ICO maintains the public register of data controllers.
- The ICO monitors the approved model publication scheme which must be adopted by public authorities under the Freedom of Information Act.
- The ICO prosecutes those who commit offences under the legislation.

**Privacy by design**

Although the ICO has been active in research in and promotion of privacy by design,[384] there are no legislative provisions in this area.

---

384 See : http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/privacy_by_design.aspx (consulted September 29, 2010).

### 5.3.4. Aufgaben und Kompetenzen

The Commissioner has certain, albeit limited, powers in connection with its investigatory and oversight roles. They include non-criminal enforcement and assessments of good practice.

Specifically, where authorities repeatedly or seriously fail to meet the requirements of the legislation, or conform to the associated codes of practice, the ICO can conduct assessments (5.3.4.1.), serve information notices (5.3.4.2.), serve enforcement notices (5.3.4.3.), prosecute those who commit criminal offences under the Act, including assessing monetary penalties (5.3.4.4. and 5.3.4.5.).

In order to **ensure compliance**, the ICO can also issue undertakings committing an authority to a particular course of action to improve its compliance, issue practice recommendations specifying steps the public authority should take to ensure conformity to the codes; issue decision notices detailing the outcome of the ICO's investigation to publically highlight particular issues with an authority's handling of a specific request and report to Parliament on freedom of information issues of concern.

#### *5.3.4.1. Assessment notice*

The Commissioner may serve a data controller with a notice for the purpose of enabling the Commissioner to determine whether the data controller has complied or is complying with the data protection principles. An assessment notice is a notice which requires the data controller to do all or any of the following—.

(a) permit the Commissioner to enter any specified premises;.

(b) direct the Commissioner to any documents on the premises that are of a specified description;.

(c) assist the Commissioner to view any information of a specified description that is capable of being viewed using equipment on the premises;.

(d) comply with any request from the Commissioner for—.

(i) a copy of any of the documents to which the Commissioner is directed;.

(ii) a copy (in such form as may be requested) of any of the information which the Commissioner is assisted to view;.

(e) direct the Commissioner to any equipment or other material on the premises which is of a specified description;.

(f) permit the Commissioner to inspect or examine any of the documents, information, equipment or material to which the Commissioner is directed or which the Commissioner is assisted to view;.

(g) permit the Commissioner to observe the processing of any personal data that takes place on the premises;.

(h) make available for interview by the Commissioner a specified number of persons of a specified description who process personal data on behalf of the data controller (or such number as are willing to be interviewed).

An order by the Secretary of State is required for the Commissioner to serve a data controller with an assessment notice unless the data controller is a government department.[385]

#### *5.3.4.2. Information notice*

If a request under the Data Protection Act 1998 has been made of the Information Commissioner for an assessment of a data controller, or if anyone enquires as to whether a data controller is complying with the principles, the Information Commissioner can ask the data controller for further information, specifying the time within which to respond to the request. This is called an 'information notice'. There are rights of appeal to the Information Tribunal against an information notice. Thereafter, a person who fails to comply is guilty of an offence.[386]

#### *5.3.4.3. Enforcement Notice*

When satisfied that a contravention has taken place under the Act, the Information Commissioner can issue an 'enforcement notice', specifying a time within which compliance must take place.

The Notice must state the data protection principles contravened; state that damage and distress is a key criteria; and, if principle 4 has been contravened, the Information Commissioner may request the data controller to rectify, block, erase or destroy the data. There may also be a request that, if practicable, third parties to whom the information has been made available, are informed of corrections. There are rights of appeal to the Information Tribunal against an enforcement notice. Thereafter, a person who fails to comply is guilty of an offence.[387]

#### *5.3.4.4. Powers of entry and inspection; Search and seizure*

If a judge is satisfied by information supplied by the Information Commissioner that there are reasonable grounds for suspecting that a data controller has contravened any of the data protection principles, or a criminal offence under the Act has been committed then the judge may grant the Commissioner a warrant giving powers to enter and search premises, inspect and seize documents and inspect equipment in which personal data may be stored. However, other than in cases of urgency, such a warrant may not issue unless the occupier of the premises has been given 7 days' notice of the search and has either refused access or refused to cooperate.[388] The person executing the warrant may use such reasonable force as is necessary.[389]

#### *5.3.4.5. Monetary Penalty Notices*

The enforcement powers of the ICO were expanded with the adoption of the Criminal Justice and Immigration Act 2008, which entered into effect in April 2010.[390] The Commissioner may impose a

---

385 DPA Part V Section 41A

386 DPA Part V Section 43.

387 DPA Part V Section 40.

388 DPA Schedule 9 Issue of Warrants.

389 *Id.*

390 Available at : http://www.legislation.gov.uk/ukpga/2008/4/contents (Consulted on October 11, 2010). Article 77 of that Act provides:

monetary penalty notice of up to £500,000 if a data controller has seriously contravened the data protection principles and the contravention was of a kind likely to cause substantial damage or substantial distress. In addition the contravention must either have been deliberate or the data controller must have known or ought to have known that there was a risk that a contravention would occur and failed to take reasonable steps to prevent it.[391] It is clear from the wording of sections 55A and 55B of the Act that a monetary penalty notice will only be appropriate in the most serious situations. Therefore in such cases the monetary penalty must be sufficiently meaningful to act both as a sanction and also as a deterrent to prevent non-compliance of similar seriousness in the future by the contravening data controller and by other data controllers.[392]

There is no provision for the Commissioner assessing monetary penalties against certain parties who process data for the Crown.[393]

#### *5.3.4.6. Caution*

A caution represents an alternative to prosecution where a criminal offence under the Act has been admitted but a caution is a more appropriate response than prosecution.

---

1) The Secretary of State may by order provide for a person who is guilty of an offence under section 55 of the Data Protection Act 1998 (c. 29) (unlawful obtaining etc. of personal data) to be liable—.
(a)on summary conviction, to imprisonment for a term not exceeding the specified period or to a fine not exceeding the statutory maximum or to both,.
(b) on conviction on indictment, to imprisonment for a term not exceeding the specified period or to a fine or to both..
(2) In subsection (1)(a) and (b) "specified period" means a period provided for by the order but the period must not exceed—.
(a) in the case of summary conviction, 12 months (or, in Northern Ireland, 6 months), and.
(b) in the case of conviction on indictment, two years..
(3) The Secretary of State must ensure that any specified period for England and Wales which, in the case of summary conviction, exceeds 6 months is to be read as a reference to 6 months so far as it relates to an offence committed before the commencement of section 282(1) of the Criminal Justice Act 2003 (c. 44) (increase in sentencing powers of magistrates' courts from 6 to 12 months for certain offences triable either way)..
(4) Before making an order under this section, the Secretary of State must consult—.
(a) the Information Commissioner,.
(b) such media organisations as the Secretary of State considers appropriate, and.
(c) such other persons as the Secretary of State considers appropriate..
(5) An order under this section may, in particular, amend the Data Protection Act 1998.

391 See ICO's brochure « Data Protection Act 1998 : Information Commissioner's guidance about the issue of monetary penalties prepared and issued under section 55C (1) of the Data Protection Act 1998 », p. 3, available at : http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/ico_guidance_monetary_penalties.pdf (Consulted October 11, 2010).

392 *Id.* See also Data Protection (Monetary Penalties) (Maximum Penalty and Notices) Regulations 2010 available at : http://www.legislation.gov.uk/uksi/2010/31/contents/made (consulted October 11, 2010) and the Data Protection (Monetary Penalties) Order 2010, available at : http://www.opsi.gov.uk/si/si2010/draft/ukdsi_9780111490723_en_1 (consulted October 11, 2010).

393 DPA Section Part VI 55A and 63(3)

#### *5.3.4.7. Appeal procedures*

There are rights of appeal to the Information Tribunal against an information notice or enforcement notice. Appeals from notices are heard by First–tier Tribunal (Information Rights), part of the General Regulatory Chamber (GRC). The First–tier Tribunal (Information Rights) specifically hears appeals of enforcement notices, decision notices and information notices issued by the Information Commissioner. The GRC brings together a range of previously separate tribunals that hear appeals on regulatory issues.

Appeal from the decision of the Information Tribunal can be made only on a point of law. This appeal would be made to the High Court.

#### *5.3.4.8. Civil proceedings*

The Data Protection Act 1998 permits civil proceedings by data subjects against data controllers. This is in relation to the six rights described in the section on 'Rights of data subjects and others'. The jurisdiction for civil proceedings is the High Court or a County Court. Should damages be awarded, the amount that may be awarded is unlimited.

#### *5.3.4.9. EU Enforcement Action*

The European Commission has requested the UK to strengthen the ICO's powers so that it complies with the EU's Data Protection Directive. The Commission has worked with UK authorities to resolve a number of issues, but claims that several remain, notably limitations of the Information Commissioner's Office's powers:

- it cannot monitor whether third countries' data protection is adequate. These assessments should come before international transfers of personal information;

- It can neither perform random checks on people using or processing personal data, nor enforce penalties following the checks.

Furthermore, courts in the UK can refuse the right to have personal data rectified or erased. The right to compensation for moral damage when personal information is used inappropriately is also restricted.[394]

The Commission request takes the form of a reasoned opinion – the second stage under EU infringement procedures. In the UK, national data rules are curtailed in several ways, leaving the standard of protection lower than required under EU rules. The UK now has two months to inform the Commission of measures taken to ensure full compliance with the EU Data Protection Directive.[395]

---

394 See Press Release, June 24, 2010 : Data Protection : Commission requests UK to strengthen powers of national data protection authority, as required by EU law » available at : http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/811&format=HTML&aged=0&language=EN&guiLanguage=fr (Consulted October 11, 2010).

395 See Press Release, June 24, 2010 : Data Protection : Commission requests UK to strengthen powers of national data protection authority, as required by EU law » available at :

## 5.4. Rolle der Organisationen zum Schutz der Betroffenen

The ICO is a public service organisation with specific expertise and obligations in the data protection sector. For this reason, individuals turn to the ICO rather than to a consumer protection organisation for assistance and information in this specific sector.[396]

## 5.5. Mögliche und vorgeschriebene Aktivitäten der Datenbearbeiter (private und öffentliche)

Generally speaking, the DPA makes no distinction between public and private data processing. The following therefore applies to both publc and private sector data controllers and data processors.

Data Controllers and Data Processors are required to respect the eight principles. More specifically, **Data controllers must be registered** with the Information Commissioner ("Commissioner") prior to processing any data.[397] They must provide information to the Data Subject concerning the information held and processed, which data, why they are held, where they came from, and where they may be sent, upon written request.[398]

### 5.5.1 Notification

Section 17 of the DPA prohibits the processing of personal data unless an entry in respect of the data controller is included in the **register** maintained by the Commissioner under section 19. This is referred to in the DPA as "**notification"**. The Data Protection Act 1998 requires every data controller who is processing personal information in an automated form to notify, unless they are exempt.[399] Failure to notify is a criminal offence. Register entries must be renewed annually.

A notification to the Commissioner must specify:

(a) the registrable particulars, and

(b )a general description of measures to be taken for the purpose of complying with the seventh data protection principle.

The notification must be accompanied by such fee as may be prescribed by fees regulations and must be renewed every year. Any changes to the information provided must be notified as well.[400]

The Commission must make the information contained in the register available for inspection by the public free of charge.

---

http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/811&format=HTML&aged=0&language=EN&guiLanguage=fr (Consulted October 11, 2010).

396 See also discussion under section 5.3.3, *supra.*

397 DPA Part III Sections 17-20.

398 DPA Part II Section 7.

399 DPA Part III Section 18.

400 DPA Part III Section 19

### 5.5.2 Privacy Notice

The DPA provides that personal information shall be processed fairly –processing includes obtaining, using or disclosing it. Personal information is not to be treated as processed fairly unless the organisation in control of the processing ensures, so far as is practicable, that the **individual has, is provided with, or has made readily available**:

- **the identity of the organisation** in control of the processing;
- **the purpose**, or purposes, for which the information will be processed;
- any further information necessary, in the specific circumstances, to enable the processing in respect of the individual to be fair.

This is generally accomplished through a privacy notice.

The specific circumstances, and the individuals concerned must be considered in drafting the privacy notice. The basic legal requirement is to make sure that the data subjects know who the Data Controller is, what he/she/it intends to do with their information and who it will be shared with or disclosed to.[401]

In the event that it is already obvious who is collecting personal data and what they are going to be used for, it is enough for the organisation to have a privacy notice available on request for those people who want further information. In other cases, a privacy notice should be actively provided to Data Subjects. This is the case where:

- it is not clear who is collecting the information; and
- the information will be used in a way the Data Subject wouldn't expect.[402]

---

401 The ICO's Privacy notices code of practice, available at : http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/privacy_notices_cop_final.pdf (consulted October 8, 2010)

402 See http://www.ico.gov.uk/for_the_public/personal_information/collecting_my_info.aspx (consulted October 8, 2010).

# 6. Spanien

## 6.1. Grundsätze des Datenschutzes

La loi espagnole sur la protection de données (LEPD)[403], énumère - au chapitre relatif aux principes sur lesquels se fonde la protection des données – toute une série de principes directeurs dans ce domaine. Ces principes concernent :

1. La qualité des donnés,
2. Les droits d'information relatifs à la collecte des données
3. Le consentement de la personne concernée
4. Les donnés spécialement protégés
5. La sécurité des données
6. L'obligation de confidentialité
7. La communication des données
8. L'accès par des tiers

### 6.1.1. Le rôle du but

L'article 4 LEPD[404] contient une série de normes, assez hétérogènes, régroupés sous la denomination générique de « qualité des données ».[405]

---

403 Ley de Protección de Datos 1999, Ley Orgánica 15/1999, de 13 diciembre, RCL\1999\3058.

404 Art 4 LEPD : « Calidad de los datos.
1. Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.
2. Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos.
3. Los datos de carácter personal serán exactos y puestos al día de forma que respondan como veracidad a la situación actual del afectado.
4. Si los datos de carácter personal registrados resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados, sin perjuicio de las facultades que a los afectados reconoce el Art. 16 .
5. Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados.
No serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados.
Reglamentariamente se determinará el procedimiento por el que, por excepción, atendidos los valores históricos, estadísticos o científicos de acuerdo con la legislación específica, se decida el mantenimiento íntegro de determinados datos.
6. Los datos de carácter personal serán almacenados de forma que permitan el ejercicio del derecho de acceso, salvo que sean legalmente cancelados.
7. Se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos ».

- La permière de ces normes (art. 4.1 LEPD), dispose que les données peuvent être collectées seulemement lorsqu'ils sont **adéquats, pertinents et non excessifs** (principe de la **proportionalité) par rapport au but** poursuivi. Le fait que le but soit indiqué lors de la collecte des informations, permet d'assurer que les données ne seront pas utilisées dans un but incompatible avec ceux pour lesquels elles ont été collectées.[406] Le but poursuivi doit être déterminée, explicite et légitime. L'art. 4.7 LEPD, prévoit l'interdiction de traiter des données par des moyens déloyaux, frauduleux ou illicites. Dès lors, il ne suffit pas d'obtenir le consentement de la personne concernée pour soumettre ses données au traitement, il faut encore que la légitimité de ce traitement soit garantie par son adéquation à atteindre le but poursuivi.[407]

- La séconde norme (art. 4.2. LEPD), prévoit que les données ne peuvent pas être utilisés pour des **buts qui sont incompatibles avec ceux de la collecte** (il existe une exception à cette règle, dans la figure du traitement ultérieur des données historiques, statistiques ou scientifiques). L'article 8.2 du Règlement de la LEPD[408] (« Règlement de la LEPD »), ajoute que les données personnelles peuvent être collectées **seulement pour accomplir les buts déterminés, explicites et légitimes du responsable du traitement**.

- La troisième norme (art. 4.3 LEPD), dispose que les donnés doivent être **exactes** (principe d'exactitude) et seront **actualisés,** afin de correspondre à la situation actuelle de la personne concernée. Ce principe est aussi repris à l'art. 4.4 LEPD selon lequel les données qui s'avèrent inexactes, dans leur totalité ou seulement en partie, voire incomplèts, seront **effacés et substitués d'office par les donnés rectifiés ou complétés**. L'article fixe un délai de 10 jours pour effectuer les corrections, comptés à partir du moment de la prise de connaisance du défaut. En autre, les donnés seront **effacés lorsqu'ils cessent d'être nécessaires ou pertinents** pour atteindre le but pour lequel ils ont été collectés (art. 4.5. LEPD).

Dans la communication des données à des tierces personnes, le but joue également un rôle important. Selon l'art 11 LEPD, la communication de données est seulement permise pour accomplir les **buts qui sont directement liés aux fonctions légitimes** de celui qui les communique et de celui qui les reçoit. En plus, il est nécessaire d'obtenir le consentement préalable de la personne concernée. Le consentement (qui est revocable) ne sera pas valable lorsque la personne concernée n'a pas été sufisamment informée du but du transfert ou du type d'activité qui réalise le destinataire de ces donnés. Toutefois, l'obtention d'un tel consentement n'est pas nécessaire dans certains cas, notamment :

a. lorsque la communication est autorisée par la loi,

b. lorsque les donnés ont été collectés dans des sources accessibles au public,

---

405 Selon un auteur, certaines de ces normes ne devraient pas se trouver dans l'article 4 LEPD, car elles ne concernent pas la qualité des données. : J. Salom, Principios de la protección de datos, in A. Reigada (dir.), Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal, Navarra : Thomson Reuters 2010, p. 324.

406 Art. 4. 2. LEPD « Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos ».

407 Salom, Principios, op. cit., p. 324.

408 Real Decreto 1720/2007, de 21 diciembre RCL\2008\150 - Protección de datos de carácter personal. Aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13-12-1999 (RCL 1999\3058), de protección de datos de carácter personal, disponible sous http://noticias.juridicas.com/base_datos/Admin/rd1720-2007.html (3.8.2010).

c. lorsque le traitement découle de l'existence d'une relation juridique dont le developpement, l'exécution et le control nécessite la conexion avec d'autres fichiers (dans ce cas la communcation est légitime seulement si celle-ci se limite au but qui l'a justifié),

d. lorsque la communication est prévue par la loi, lorsque les données ont été collectées à partir de sources ouvertes au public, lorsque le traitement se fait dans le cadre d'une relation juridique dont l'exécution implique nécessairement la communication à des tiers, lorsque la communication est adressée à certaines instances publiques, telles que l'Ombudsman (*Defensor del Pueblo)*, le Ministère public, des juges ou tribunaux ou la Cour de comptes, lorsque la communication se fait dans le cadre de l'administration et ne concerne que des donnés statistiques, historiques ou scientifiques, etc.),

e. lorsque la communication est faite entre les administrations publiques pour un traitement ultérieur des donnés pour des but historiques, statistiques ou scientifiques,

f. lorsque la communication de donnés relatifs à la santé d'une personne est nécessaire pour resoudre une urgence médicale.

Le destinataire des donnés communiqués s'oblige, du seul fait de la communication, à

respecter les dispositions de la LEPD.

### 6.1.2. Les droits d'information relatifs à la collecte des données

L'obligation d'information est une obligation « de faire » imposée au responsable du fichier ou du traitement.[409]

En vertu de l'article 5 LEPD, les personnes auxquelles on sollicite des données devront être **informées au préalable de façon expresse, précise et sans équivoque** :

a. de l'existence du fichier ou du traitment des données, du but de la collecte de ces données et des destinataires de l'information,

b. du caractère obligatoire ou facultatif de répondre aux questions posées,

c. des conséquences de l'obtention de ces données ou du refus de les donner,

d. de la possibilité d'exercer le droit d'accès, rectification, opposition et effacement,

e. de l'identité et l'adresse du responsable du traitement ou de son représentant.

Lorsque les données ne sont pas collectés directement de la personne concernée, celle-ci doit être informée **de façon expresse, précise et sans équivoque** dans les trois mois qui suivent l'introduction des donnés dans la base. Ceci n'est pas applicable lorsque la collecte des donnés est prescrite par la loi ou lorsque celle-ci se fait avec des propos historiques, statistiques ou scientifiques. Ceci ne s'applique non plus lorque l'information à l'intéressé est impossible ou exige des efforts disproportionnés.

---

409 A. Gil, Derecho de información en la recogida de datos, in A. Reigada (dir.), Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal, Navarra : Thomson Reuters 2010, p. 401.

### 6.1.3. Le consentement de l'intéressé

Sauf si la loi dispose autrement, le traitement de données personnel requiert le **consentement non équivoque (inequívoco) de la personne concernée** (art. 6 LEPD). Le consentement n'est pas nécessaire lorsque :

a. la collecte des données se fait par les administrations publiques dans le cadre de leurs compétences,

b. lorsque le sdonnées concernent les parties à une relation commerciale (*negocial*), de travail ou administrativa et ils sont nécessaires pour son maintient ou exécution,

c. lorsque le but du traitement est le maintient d'un intérêt vital de la personne concernée (il s'agit des données concernant principalement l'état de santé),

d. lorsque les données sont disponibles dans des sources ouvers au public et leur traitment est nécessaire pour satisfaire l'intérêt légitime poursuivi per le responsable du fichier – à condition de ne pas violer les droits fondamentaux de la personne concernée.

Le consentement peut être révoqué lorsqu'il existe des « motifs fondés et légitimes concernant une situation personnelle concrète» et lorsque la loi ne prévoit autrement (art. 6.4 LEPD).

### 6.1.4. Les données spécialement protégés

Selon l'art. 16.2 de la Constitution espagnole, personne ne peut être contrainte à donner des informations sur son **opinion politique, sa religion ou ses croyances**.

Selon l'art. 7 LEPD[410], des données concernant l'opinion politique, l'affiliation syndicale, la religion et les croyances pourront être collectées seulement avec le consentement de la personne concernée

---

410 Art. 7 LEPD : « Datos especialmente protegidos
1. De acuerdo con lo establecido en el apartado 2 del Art. 16 de la Constitución (RCL 1978, 2836) , nadie podrá ser obligado a declarar sobre su ideología, religión o creencias. Cuando en relación con estos datos se proceda a recabar el consentimiento a que se refiere el apartado siguiente, se advertirá al interesado acerca de su derecho a no prestarlo.
2. Sólo con el consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias. Se exceptúan los ficheros mantenidos por los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, en cuanto a los datos relativos consentimiento sus asociados o miembros, sin perjuicio de que la cesión de dichos datos precisará siempre el previo consentimiento del afectado.
3. Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente.
4. Quedan prohibidos los ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico, o vida sexual.
5. Los datos de carácter personal relativos a la comisión de infracciones penales o administrativas sólo podrán ser incluidos en ficheros de las Administraciones públicas competentes en los supuestos previstos en las respectivas normas reguladoras.
6. No obstante lo dispuesto en los apartados anteriores, podrán ser objeto de tratamiento los datos de carácter personal a que se refieren los apartados 2 y 3 de este Art. , cuando dicho tratamiento resulte necesario para la prevención o para el diagnóstico médicos, la prestación de

(exception faite des fichiers tenus par les syndicats, les églises, les fondations et autres entités sans but lucratif et concernant leurs membres et avec leur consentement). D'autre part, sont interdits les fichiers crées exclusivement pour stocker des renseignements personnels sur l'opinion politique, l'affiliation syndicale, les croyances, l'origine raciale ou ethnique ou l'orientation sexuelle. Les donnés concernant la santé et la sexualité peuvent être collectées seulement sur la base d'une loi. L'alinéa 6 de l'art. 7 LEPD, prévoit, toutefois, que ces données pourront faire l'objet d'un traitement lorsque celui-ci est nécessaires pour la prévention ou le diagnostique médical, l'assistance sanitaire, les traitements médicaux ou la gestion des services de santé, à condition que le traitement soit fait par un professionnel de santé soumis au secret médical ou professionnel ou par une personne soumise à des limitations équivalentes. Les fichiers concernant les infractions pénales ou administratives peuvent être tenus seulement par les administrations concernées et seulement sur la base d'une disposition légale.

### 6.1.5. La sécurité des données

La sécurité des donnés vise principalement deux objectifs :

a. **éviter que le système d'information cesse d'être éficace.** Pour ceci il faut réaliser des actions de prévention et de protection empêchant que le système soit endomagé,

b. réduire l'impact des incidents de sécurité lorsqu'il n'a pas été possible de les éviter. Il faut minimiser les effets des incidents, par exemple par la mise en place de mécanismes de récupération des donnés en cas d'incident afin de pouvoir retourner aux conditions de fonctionnement normales.[411]

La **sécurité des données** est réglée à l'art. 9 LEPD et aux articles 81, 101-104, 11-114 du Règlement de la LEPD[412]. Le stockage de donnés dans des fichiers qui ne remplissent pas les exigences de sécurité est interdite. Le responsable du fichier a l'obligation **d'adopter toutes les mesures techniques et organisationnelles nécessaires pour garantir la sécurité des informations personnelles stockées**. Il

---

asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto.
También podrán ser objeto de tratamiento los datos a que se refiere el párrafo anterior cuando el tratamiento sea necesario para salvaguadar el interés vital del afectado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento ».

411 R. López, Seguridad de la información y protección de datos personales, in A. Reigada (dir.), Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal, Navarra : Thomson Reuters 2010, p. 769.

412 Art. 9 LEPD : « Seguridad de los datos 1. El responsable del fichero, y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativas necesarias que garantice la seguridad de los datos de carácter personal y evite su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana del medio físico o natural.
2. No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.
3. Reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el Art. 7 de esta Ley ».

doit notamment veiller à éviter la perte, l'altération et tout accès non-autorisé. Il doit prendre ces mesures sur la base de l'état de la technologie, la nature des données stockées et les risques (soit humains soit de la nature) auxquels les fichiers sont exposés.

### 6.1.6. L'obligation de confidentialité

L'art. 10 LEPD impose au **responsable du fichier** un devoir de confidentialité. La même obligation est imposée à toute autre personne interventant dans le traitement des donnés. Ces personnes continuent à être soumises à l'obligationd e confidencialité, même après la finalisation de leurs tâches ou de leurs relations avec le fichier ou le responsable du traitement. Selon la doctrine, lorsque le responsable du traitemenr engage une personne pour travailler avec les fichiers, il doit songer à inclure dans le contrat des clauses spécifiant le devoir de confidentialité, de garder le sécret et de veiller à la sécurité des données.[413]

Dans la pratique, le devoir de confidentialité ne peut pas être absolu, car l'information doit parfois être partagée avec des tiers. Ceci dit, l'obligation de confidentialité est étroitement lié au problème de la **communication ou du transfert des donnés**, un sujet qui est traité dans le point suivant.

### 6.1.7. La communication transfrontière

Pour ce qui concerne la **communication transfrontière de donnés,** le transfer de données personneles vers une juridiction qui ne prévoit pas une protection suffisante n'est pas permis. En effet, l'art. 33 LEPD[414] interdit de tels les transferts lorsque l'État de destination n'accorde pas un niveau de protection équivalent à la protection accordée par la loi espagnole. Le niveau de protection accordée par un État étranger est évalué par l'AEPD « en prennant compte de toutes les circonstances drelatives au transfert ». Entre autre, l'AEPD tiendra compte de la nature des données, le but et la durée du traitement, le lieu d'origine et le lieu final, les normes juridiques en vigueur dans l'État de destination, les rapports préparés par la Commission de l'UE et les mesures de sécurité en vigueur. Il existe, toutefois, la possibilité de transférer des donnés vers un tel État, lorque le Directeur de l'Agence espagnole de protection des donnés (AEPD), l'autorise sur la base de garanties appropriées.

---

413 A. Pérez, El deber de secreto, in A. Reigada (dir.), Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal, Navarra : Thomson Reuters 2010, p. 937.

414 Art. 33 LEPD : « 1. No podrán realizarse transferencias temporales ni definitivas de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento con destino a países que no proporcionen un nivel de protección equiparable al que presta la presente Ley, salvo que, además de haberse observado lo dispuesto en ésta, se obtenga autorización previa del Director de la Agencia de Protección de Datos, que sólo podrá otorgarla si se obtienen garantías adecuadas.
2. El carácter adecuado del nivel de protección que ofrece el país de destino se evaluará por la Agencia de Protección de Datos atendiendo a todas las circunstancias que concurran en la transferencia o categoría de transferencia de datos. En particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de derecho, generales o sectoriales, vigentes en el país tercero de que se trate, el contenido de los informes de la Comisión de la Unión Europea, así como las normas profesionales y las medidas de seguridad en vigor en dichos países ».

### 6.1.8. L'accès par des tiers

L'art. 12 LEPD règle **l'accès à des donnés par des tiers** qui sont des prestataires de service du responsable du fichier.[415] À cet égard, la LEPD dispose que ce type d'accès n'est pas une « communication » des donnés. Dans ces cas de figure, le responsable du fichier doit conclure un contrat avec le prestateur de services, prévoyant le respect des dispositions de la LEPD. Entre autre, ledit contrat doit prévoir que la personne qui prête le service au responsable du fichier s'engage:

- à se conformer aux instructions du responsable du fichier,
- à ne pas utiliser les données avec un but autre que celui qui est prévu dans le contrat,
- à ne pas communiquer des données à des tiers, même en vu de leur conservation,
- à respecter les mesures de sécurité nécessaires et exigées par la législation,
- à détruire les données ainsi que tout autre support ou document dans lesquels est contenu un donné lorsque sa prestation est exécutée.[416]

Le responsable du fichier sera tenu responsable des infractions qu'il aurait commis en cas de communication interdite par la personne en charge du traitement.

### 6.1.9. Relation entre protection des données et nouvelles technologies

Le develpement des nouvelles technologies, tel qu'Internet, posent des sérieux problèmes liés à la protection des donnés. La LEPD est rédigée de façon générale et ne contient pas des dispositions ponctuelles qui règlent ce problème. Dans certaines normes de rank inférieur on trouve des références aux nouvelles technologies. Par exemple, dans l'Ordre du Ministère de la science et la technologie du 21 février 2000 (qui valide le Règlement d'accréditation de prestataires de services de certification et de certains cas de signature électronique)[417], il est fait mention que dans la préparation de cette norme on a tenu compte des modèles de certification déjà **existants ainsi que de ceux qui sont en voie de développement** en Europe pour évaluer la sécurité des technologies de l'information et des communications.

### 6.1.10. Différences de régime

La LEPD traite des fichiers tenus par des entités publiques aux articles 20 – 24 et des fichiers tenus par des privés aux articles 25 – 32.

Bien que l'art. 2 LEPD dispose que la LEPD s'applique aux données personnelles collectées dans par les **secteurs public et privé**, il existe certaines différences entre ces deux cas.

---

415 Le droit d'accès par la personne concernée est traité au point 6.2.

416 R. Vizcaya, Encargado del tratamiento, in : A. Reigada (dir.), Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal, Navarra : Thomson Reuters 2010, p. 1082 s.

417 Orden del Ministerio de Ciencia y Tecnología de 21 de febrero de 2000 por la que se aprueba el Reglamento de acreditación de prestadores de servicios de certificación y de certificación de determinados productos de firma electrónica, disponible sous http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/normativa_estatal/common/pdfs/E.37-cp--Orden-CTE-DE-21-DE-FEBRERO-DE-2000.pdf (21.10.2010).

L'une de ces différences concerne le **droit d'accès, de cancellation et de rectification de données**. A ce propos, l'art. 23 LEPD[418] dispose que les responsables de fichiers de police et des corps de sécurité peuvent refuser le droit d'accès, de rectification et de destruction de données en fonction des dangers potentiels pour la sécurité. De même, les responsables de fichiers portant sur l'économie et les finances de l'Etat (Hacienda pública) peuvent refuser l'exercise de ces droits lorsque ceci risque de porter atteinte à la perception des impôts (spécialement lorsque la personne qui demande ces mesures est soumise à un contrôle). Les personnes qui s'estiment lésées par ces mesures peuvent informer l'AEPD.

Un autre domaine où l'on trouve des différences est celui de la **cession de données**. En effet, dans les fichiers tenus par des privés le besoin du consentement de la personne concernée est plus présent que dans le cas de fichiers tenus par des entités publiques. Par exemple, la cession de donnés entre les administrations publiques n'exigent pas une autorisation législative expresse. Ce type de cessions peut se faire sur la base de compétences administratives contenant une habilitation générale suffisante.[419]

En autre, la LEPD contient des normes spécifiques qui règlent la **communication de données entre les diverses administrations publiques** (art. 21 LEPD). Selon cette dispisition, en principe les données collectés ou traités par une administration publique pour les buts de ses fonctions ne peuvent pas être communiquées à d'autres administrations publiques ayant des compétences différentes ou des compétences sur des matières différentes. Toutefois, si la communication a été prévue dans les dispositions de création du fichier ou par une norme de rank supérieur, la cession sera possible. De même lorsque le transfert se fait pour le traitement ultérieur des données avec des but historiques, scientifiques ou statistique. En vertu de l'article 21.2 LAPD, une administration publique qui a collecté des donnés en faveur d'une autre pourra les transférer à cette dernière. Dans ces cas, il n'y a pas besoin d'obtenir le consentement de la personne concernée.

---

418 Art 23 LEPD « Excepciones a los derechos de acceso, rectificación y cancelación
1. Los responsables de los ficheros que contengan los datos a que se refieren los apartados 2, 3 y 4 del artículo anterior podrán denegar el acceso, la rectificación o cancelación en función de los peligros que pudieran derivarse para la defensa del Estado o la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que se estén realizando.
2. Los responsables de los ficheros de la Hacienda Pública podrán, igualmente, denegar el ejercicio de los derechos a que se refiere el apartado anterior cuando el mismo obstaculice las actuaciones administrativas tendentes a asegurar el cumplimiento de las obligaciones tributarias y, en todo caso, cuando el afectado esté siendo objeto de actuaciones inspectoras.
3. El afectado al que se deniegue, total o parcialmente, el ejercicio de los derechos mencionados en los apartados anteriores podrá ponerlo en conocimiento del Director de la Agencia de Protección de Datos o del organismo competente de cada Comunidad Autónoma en el caso de ficheros mantenidos por Cuerpos de Policía propios de éstas, o por las Administraciones tributarias autonómicas, quienes deberán asegurarse de la procedencia o improcedencia de la denegación ».

419 A. Reigada, La comunicación de datos personales, in : A. Reigada (dir.), Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal, Navarra : Thomson Reuters 2010, p. 979.

## 6.2. Durchsetzungsrechte der Datenschutzanliegen für Betroffene

### 6.2.1. Droits d'accès des demandes de protections des données pour concernés

Le **droit d'accès** est garanti par l'art. 15 LEPD[420]. Selon cette disposition, la personne concernée a le droit de solliciter et d'obtenir gratuitement des informations concernant le traitement de ses données personnelles. Elle a aussi le d'accès aux communications faites ou qui sont prévues de se faire par rapport à ses données. Sauf cas d'exceptions, ce droit ne peut être exécuté qu'une seule fois chaque 12 mois.

Les **moyens d'action** disponibles pour une personne concernée peuvent consister en la révocation du consentement pour le traitement des données (art. 17 LEPD), la rectification (art 24 LEPD), la destruction (art. 24 LEPD), l'opposition (art. 24 LEPD). Il existe aussi la possibilité d'exiger une indemnisation en cas de dommages (art. 19.1 LEPD)[421]. La procédure pour mettre en œuvre ces moyens d'action se trouve aux articles 24-26 du Règlement de la LEPD.

Finalement, l'art. 13 LEPD[422] dispose que les citoyens ont le droit de ne pas être soumis à des décisions ayant des effets juridiques ou qui les affectent de façon importante, lorsque celles-ci se base sur un traitement de données ayant pour but d'**évaluer des aspects déterminés de leur personnalité**. Dans ce cas, la personne concernée peut attaquer les actes administratifs ou les décisions privées qui

---

420 Art. 15 LEPD : « Derecho de acceso.
1. El interesado tendrá derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos.
2. La información podrá obtenerse mediante la mera consulta de los datos por medio de su visualización, o la indicación de los datos que son objeto de tratamiento mediante escrito, copia, telecopia o fotocopia, certificada o no, en forma legible o inteligible, sin utilizar claves o códigos que requieran el uso de dispositivos mecánicos específicos.
3. El derecho de acceso a que se refiere este Art. sólo podrá ser ejercitado a intervalos no inferiores a doce meses, salvo que el interesado acredite un interés legítimo al efecto, en cuyo caso podrán ejercitarlo antes ».

421 Art. 19. Derecho a indemnización
1. Los interesados que, como consecuencia del incumplimiento de lo dispuesto en la presente Ley por el responsable o el encargado del tratamiento, sufran daño o lesión en sus bienes o derechos tendrán derecho a ser indemnizados.
2. Cuando se trata de ficheros de titularidad pública, la responsabilidad se exigirá de acuerdo con la legislación reguladora del régimen de responsabilidad de las Administraciones pública.
3. En el caso de los ficheros de titularidad privada, la ACCIÓN se ejercitará ante los órganos de la jurisdicción ordinaria ».

422 Art. 13 LEPD : « Impugnación de valoraciones
1. Los ciudadanos tienen derecho a no verse sometidos a una decisión con efectos jurídicos, sobre ellos o que les afecte de manera significativa, que se base únicamente en un tratamiento de datos destinados a evaluar determinados aspectos de su personalidad.
2. El afectado podrá impugnar los actos administrativos o decisiones privadas que impliquen una valoración de su comportamiento, cuyo único fundamento sea un tratamiento de datos de carácter personal que ofrezca una definición de sus características o personalidad.
3. En este caso, el afectado tendrá derecho a obtener información del responsable del fichero sobre los criterios de valoración y el programa utilizados en el tratamiento que sirvió para adoptar la decisión en que consistió el acto.
4. La valoración sobre el comportamiento de los ciudadanos, basada en un tratamiento de datos, únicamente podrá tener valor probatorio a petición del afectado ».

impliquent une évaluation de leur comportement ayant comme fondement unique un traitement de données personnelles qui définit les caractéristiques de sa personnalité.

Pour ce faire, la personne concernée aura le droit d'exiger du responsable du fichier le détail des critères d'évaluation ainsi que du programme utilisé pour le traitement de ces données, qui a donné lieu au résultat contesté.

### 6.2.2. Datenbearbeitungen durch Private

L'art. 55 du Décret royal 1720/2007, du 21 septembre 2007 dispose que l'existence de tout fichier mis en place dans des structures privées, sera notifiée à l'AEPD.[423] Dans le cas de traitement de données mis en place par des structures privées, plusieures actions sont possibles pour les personnes supçonant une violation de leurs droits.

Par exemple, lorsque la loi ne prévoit pas autrement, une personne **peut s'opposer à la communication de données** la concernant. D'autre part, l'art. 16 LEPD[424] prévoit le droit de demander la

---

423 Real Decreto 1720/2007, de 21 diciembre RCL\2008\150, Art 55. « NOTIFICACIÓN de ficheros
1. Todo fichero de datos de carácter personal de titularidad pública será notificado a la Agencia Española de Protección de Datos por el órgano competente de la Administración responsable del fichero para su inscripción en el Registro General de Protección de Datos, en el plazo de treinta días desde la publicación de su norma o acuerdo de creación en el diario oficial correspondiente.
2. Los ficheros de datos de carácter personal de titularidad privada serán notificados a la Agencia Española de Protección de Datos por la persona o entidad privada que pretenda crearlos, con carácter previo a su creación. La notificación deberá indicar la identificación del responsable del fichero, la identificación del fichero, sus finalidades y los usos previstos, el sistema de tratamiento empleado en su organización, el colectivo de personas sobre el que se obtienen los datos, el procedimiento y procedencia de los datos, las categorías de datos, el servicio o unidad de acceso, la indicación del nivel de medidas de seguridad básico, medio o alto exigible, y en su caso, la identificación del encargado del tratamiento en donde se encuentre ubicado el fichero y los destinatarios de cesiones y transferencias internacionales de datos.
3. Cuando la obligación de notificar afecte a ficheros sujetos a la competencia de la autoridad de control de una Comunidad Autónoma que haya creado su propio registro de ficheros, la notificación se realizará a la autoridad autonómica competente, que dará traslado de la inscripción al Registro General de Protección de Datos.
El Registro General de Protección de Datos podrá solicitar de las autoridades de control de las Comunidades Autónomas el traslado al que se refiere el párrafo anterior, procediendo, en su defecto, a la inclusión de oficio del fichero en el Registro.
4. La notificación se realizará conforme al procedimiento establecido en la sección primera del capítulo IV del título IX del presente Reglamento ».

424 Art 16 LEPD : « Derecho de rectificación y cancelación
1. El responsable del tratamiento tendrá la obligación de hacer efectivo el derecho de rectificación o cancelación del interesado en el plazo de diez días.
2. Serán rectificados o cancelados, en su caso, los datos de carácter personal cuyo tratamiento no se ajuste a lo dispuesto en la presente Ley y, en particular, cuando tales datos resulten inexactos o incompletos.
3. La cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse a la supresión.

**rectification** et la **destruction** des données inexactes ou qui ne sont pas conformes aux exigences de la loi.

L'art. 18 LEPD[425] règle la protection des droits du point de vue de la **procédure.** Selon cette disposition, les actes contraires à la LEPD peuvent faire l'objet d'une plainte (réclamación) devant l'AEPD. Ainsi, la personne à qui on a contesté le droit d'accès, d'opposition, de ratification ou de destruction de donnés peut informer l'AEPD. Ensuite, l'AEPD vérifie la pertinence du refus ou son illégalité. Le délai maximal rendre une décision est de 6 mois. Il est possible est possible de faire appel de ces décisions devant les instances du contentieux-administratif.

Le Décret royal 1720/2007 du 21.12.2007 (ci-après : DR 1720/2007), prévoit les procédures prévues pour l'exercice des droits d'accès, de rectification, de destruction et d'opposition. Les articles 24.1 et 24.2[426] du DR 1720/2007 prévoient que **chacun de ces droits est indépendant et peut être exercé de façon autonome et gratuite**. En vertu de l'art. 24.3 *in fine* du DR 1720/2007[427], en aucun cas la requête ne pourra être conditionnée à l'envoi d'un courrier recommandé, ni par d'autres moyens de communication impliquant des coûts supplémentaires. Même si le responsable de la base des données

---

4. Si los datos rectificados o cancelados hubieran sido comunicados previamente, el responsable del tratamiento deberá notificar la rectificación o cancelación efectuada a quien se hayan comunicado, en el caso de que se mantenga el tratamiento por este último, que deberá también proceder a la cancelación.
5. Los datos de carácter personal deberán ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado ».

425 Art. 18 LEPD : « Tutela de los derechos
1. Las actuaciones contrarias a lo dispuesto en la presente Ley pueden ser objeto de reclamación por los interesados ante la Agencia de Protección de Datos, en la forma que reglamentariamente se determine.
2. El interesado al que se deniegue, total o parcialmente, el ejercicio de los derechos de oposición, acceso, rectificación o cancelación, podrá ponerlo en conocimiento de la Agencia de Protección de Datos o, en su caso, del organismo competente de cada Comunidad Autónoma, que deberá asegurarse de la procedencia o improcedencia de la denegación.
3. El plazo máximo en que debe dictarse la resolución expresa de tutela de derechos será de seis meses.
4. Contra las resoluciones de la Agencia de Protección de Datos procederá recurso contencioso-administrativo.

426 Art. 24 DR 1720/2007 « Condiciones generales para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición
1. Los derechos de acceso, rectificación, cancelación y oposición son derechos independientes, de tal forma que no puede entenderse que el ejercicio de ninguno de ellos sea requisito previo para el ejercicio de otro.
2. Deberá concederse al interesado un medio sencillo y gratuito para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición ».

427 Art. 24.3 DR 1720/2007. « El ejercicio por el afectado de sus derechos de acceso, rectificación, cancelación y oposición será gratuito y en ningún caso podrá suponer un ingreso adicional para el responsable del tratamiento ante el que se ejercitan.
No se considerarán conformes a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y en el presente Reglamento los supuestos en que el responsable del tratamiento establezca como medio para que el interesado pueda ejercitar sus derechos el envío de cartas certificadas o semejantes, la utilización de servicios de telecomunicaciones que implique una tarificación adicional al afectado o cualesquiera otros medios que impliquen un coste excesivo para el interesado ».

met en place une procédure d'accueil des requêtes, une requête ne pourra pas être rejetée parce qu'elle n'a pas suivi ses procédures (l'art. 24.5 DR 1720/2007[428]), si le plaignant a utilisé un moyen de communication permettant de vérifier son envoi.

Les articles 25 et 26 DR 1720/2007 établissent des règles sur le **contenu des requêtes**. Selon l'article 25 DR 1720/2007[429], s'agissant de la forme la requête, elle doit inclure, entre autres :

a) le nom de l'intéressé, une copie de sa carte national d'identité, ou de son passeport ou d'un autre document valable

b) les fondements de sa requête

c) l'adresse pour les notifications, la date et sa signature

d) les documents justifiant sa requête

---

428 Art. 24.5 DR 1720/2007. « El responsable del fichero o tratamiento deberá atender la solicitud de acceso , rectificación , cancelación u oposición ejercida por el afectado aún cuando el mismo no hubiese utilizado el procedimiento establecido específicamente al efecto por aquél, siempre que el interesado haya utilizado un medio que permita acreditar el envío y la recepción de la solicitud, y que ésta contenga los elementos referidos en el párrafo 1 del Art. siguiente ».

429 Art. 25 DR 1720/2007. « Procedimiento

1. Salvo en el supuesto referido en el párrafo 4 del Art. anterior, el ejercicio de los derechos deberá llevarse a cabo mediante comunicación dirigida al responsable del fichero, que contendrá:

a) Nombre y apellidos del interesado; fotocopia de su documento nacional de identidad, o de su pasaporte u otro documento válido que lo identifique y, en su caso, de la persona que lo represente, o instrumentos electrónicos equivalentes; así como el documento o instrumento electrónico acreditativo de tal representación. La utilización de firma electrónica identificativa del afectado eximirá de la presentación de las fotocopias del DNI o documento equivalente.

El párrafo anterior se entenderá sin perjuicio de la normativa específica aplicable a la comprobación de datos de identidad por las Administraciones Públicas en los procedimientos administrativos.

b) Petición en que se concreta la solicitud.

c) Dirección a efectos de notificaciones, fecha y firma del solicitante.

d) Documentos acreditativos de la petición que formula, en su caso.

2. El responsable del tratamiento deberá contestar la solicitud que se le dirija en todo caso, con independencia de que figuren o no datos personales del afectado en sus ficheros.

3. En el caso de que la solicitud no reúna los requisitos especificados en el apartado primero, el responsable del fichero deberá solicitar la subsanación de los mismos.

4. La respuesta deberá ser conforme con los requisitos previstos para cada caso en el presente título.

5. Corresponderá al responsable del tratamiento la prueba del cumplimiento del deber de respuesta al que se refiere el apartado 2, debiendo conservar la acreditación del cumplimiento del mencionado deber.

6. El responsable del fichero deberá adoptar las medidas oportunas para garantizar que las personas de su organización que tienen acceso a datos de carácter personal puedan informar del procedimiento a seguir por el afectado para el ejercicio de sus derechos.

7. El ejercicio de los derechos de acceso, rectificación, cancelación y oposición podrá modularse por razones de seguridad pública en los casos y con el alcance previsto en las Leyes.

8. Cuando las leyes aplicables a determinados ficheros concretos establezcan un procedimiento especial para la rectificación o cancelación de los datos contenidos en los mismos, se estará a lo dispuesto en aquéllas ».

Le responsable du traitement devra répondre à la requête dans tous les cas, indépendamment du fait que les données personnelles du plaignant ne figurent pas dans le fichier.

Si la requête ne réunit pas les conditions mentionnées, le responsable du fichier devra solliciter leur inclusion.

L'exercice des droits d'accès, de rectification, d'annulation et d'opposition pourra être aménagé pour des raisons de sécurité publique dans les cas prévus par la loi.

Lorsqu'une loi prévoit une **procédure spéciale** pour certains fichiers, il faut suivre ladite procédure.

Dans le cas de fichiers privés, une **action en responsabilité civile** peut-être exercée à l'encontre du responsable devant les tribunaux de l'ordre judiciaire. La class action n'est pas prévue. En vertu de l'art. 117 du Décret royal 1720/2007 du 21.12.2007, après avoir sollicité des renseignements auprès du préposé au fichier, l'AEPD réalise une enquête dans le cadre de laquelle elle collecte des preuves et établit les faits.[430]

### 6.2.3. Datenbarbeitungen durch Behörde

L'art. 55 du Décret royal 1720/2007, du 21 septembre 2007 dispose que l'existence de tout fichier tenu par l'administration, sera notifiée à l'AEPD.[431] Une personne peut ainsi s'opposer à la communication

---

430 Art 117 LEPD : « Instrucción del procedimiento .
1. El procedimiento se iniciará a instancia del afectado o afectados, expresando con claridad el contenido de su reclamación y de los preceptos de la Ley Orgánica 15/1999, de 13 de diciembre, que se consideran vulnerados.
2. Recibida la reclamación en la Agencia Española de Protección de Datos, se dará traslado de la misma al responsable del fichero, para que, en el plazo de quince días, formule las alegaciones que estime pertinentes.
3. Recibidas las alegaciones o transcurrido el plazo previsto en el apartado anterior, la Agencia Española de Protección de Datos, previos los informes, pruebas y otros actos de instrucción pertinentes, incluida la audiencia del afectado y nuevamente del responsable del fichero, resolverá sobre la reclamación formulada ».

431 Real Decreto 1720/2007, de 21 diciembre RCL\2008\150, Art 55. « NOTIFICACIÓN de ficheros
1. Todo fichero de datos de carácter personal de titularidad pública será notificado a la Agencia Española de Protección de Datos por el órgano competente de la Administración responsable del fichero para su inscripción en el Registro General de Protección de Datos, en el plazo de treinta días desde la publicación de su norma o acuerdo de creación en el diario oficial correspondiente.
2. Los ficheros de datos de carácter personal de titularidad privada serán notificados a la Agencia Española de Protección de Datos por la persona o entidad privada que pretenda crearlos, con carácter previo a su creación. La notificación deberá indicar la identificación del responsable del fichero, la identificación del fichero, sus finalidades y los usos previstos, el sistema de tratamiento empleado en su organización, el colectivo de personas sobre el que se obtienen los datos, el procedimiento y procedencia de los datos, las categorías de datos, el servicio o unidad de acceso, la indicación del nivel de medidas de seguridad básico, medio o alto exigible, y en su caso, la identificación del encargado del tratamiento en donde se encuentre ubicado el fichero y los destinatarios de cesiones y transferencias internacionales de datos.
3. Cuando la obligación de notificar afecte a ficheros sujetos a la competencia de la autoridad de control de una Comunidad Autónoma que haya creado su propio registro de ficheros, la

de données la concernant. Toutefois, l'art. 11 LEPD[432] dispose que le consentement n'est pas nécessaire dans certains cas de figure par exemple, lorsque la communication est prévue par la loi, lorsque les données ont été collectées à partir de sources ouvertes au public, lorsque le traitement se fait dans le cadre d'une relation juridique dont l'exécution implique nécessairement la communication à des tiers, lorsque la communication est adressée à certaines instances publiques (voir chiffre 6.1.7.).

L'art. 20 LEPD[433] dispose que la création, modification ou suppression des fichiers de l'administration seront faites seulement par le biai d'une disposition générale publiée dans le Journal officiel (*Boletín*

---

notificación se realizará a la autoridad autonómica competente, que dará traslado de la inscripción al Registro General de Protección de Datos.
El Registro General de Protección de Datos podrá solicitar de las autoridades de control de las Comunidades Autónomas el traslado al que se refiere el párrafo anterior, procediendo, en su defecto, a la inclusión de oficio del fichero en el Registro.
4. La notificación se realizará conforme al procedimiento establecido en la sección primera del capítulo IV del título IX del presente Reglamento ».

[432] Art. 11 LEPD : « Comunicación de datos
1. Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado.
2. El consentimiento exigido en el apartado anterior no será preciso:
a) Cuando la cesión está autorizada en una ley.
b) Cuando se trate de datos recogidos de fuentes accesibles al público.
c) Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. En este caso la Comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.
d) Cuando la Comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas. Tampoco será preciso el consentimiento cuando la Comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas.
e) Cuando la cesión se produzca entre Administraciones públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos y científicos.
f) Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica ».
3. Será nulo el consentimiento para la comunicación de los datos de carácter personal a un tercero, cuando la información que se facilita al interesado no le permita conocer la finalidad a que destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquel a quien se pretenden comunicar.
4. El consentimiento para la comunicación de los datos de carácter personal tiene también un carácter de revocable.
5. Aquel a quien se comuniquen los datos de carácter personal se obliga, por el solo hecho de la comunicación , a la observancia de las disposiciones de la presente Ley.
6. Si la comunicación se efectúa previo procedimiento de disociación, no será aplicable lo establecido en los apartados anteriores».

[433] Art. 20 LEPD : « Creación, modificación o supresión

*Oficial del Estado*) indiquant l'objet du fichier, les personnes sur lesquelles les données porteront, les personnes qui seront obligées de fournir des données, la procédure de collecte, la structure du fichier, la communication des données, incluant la communication transfrontalière, les organes administratifs responsables du fichier et la sécurité du fichier.

Du point de vue de la procédure, s'il s'agit de fichiers de l'administration, il faut d'abord utiliser les recours administratifs, puis en dernier recours il y a la possibilité de saisir les tribunaux administratifs (tribunal de lo contencioso-administrativo).

Le Décret royal 3/2010[434] régit la sécurité dans le cadre de l'Administration électronique de l'État, notamment les communications entre les citoyens et les administrations. Ce dispositif, qui impose des normes minimales de sécurité appliquées aux données échangées entre l'administration et les citoyens, dispose à l'art. 27.2[435], que lorsqu'un système de l'administration traite des données personnelles, la LEPD lui sera appliquée, sans préjudice des exigences de sécurité imposées par le Décret royal 3/2010.

---

1. La creación, modificación o supresión de los ficheros de las Administraciones públicas sólo podrán hacerse por medio de disposición general publicada en el «Boletín Oficial del Estado» o Diario Oficial correspondiente.
2. Las disposiciones de creación o de modificación de ficheros deberán indicar:
a) La finalidad del fichero y los usos previstos para el mismo.
b) Las personas o colectivos sobre los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos.
c) El procedimiento de recogida de los datos de carácter personal.
d) La estructura básica del fichero y la descripción de los tipos de datos de carácter personal incluidos en el mismo.
e) Las cesiones de datos de carácter personal y, en su caso, las transferencias de datos que se prevean a países terceros.
f) Los órganos de las Administraciones responsables del fichero.
g) Los servicios o unidades ante los que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición.
h) Las medidas de seguridad con indicación del nivel básico, medio o alto exigible.
3. En las disposiciones que se dicten para la supresión de los ficheros, se establecerá el destino de los mismos o, en su caso, las previsiones que se adopten para su destrucción ». Les arts. 22-23 LEPD traite des fichiers crées par les corps de sécurité.

434 Real Decreto 3/2010, de 8 enero RCL\2010\158, ADMINISTRACIÓN ELECTRÓNICA. Regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

435 Ibid., Art. 27 LEPD : « Cumplimiento de requisitos mínimos
1. Para dar cumplimiento a los requisitos mínimos establecidos en el presente Real Decreto, las Administraciones públicas aplicarán las medidas de seguridad indicadas en el Anexo II, teniendo en cuenta:
a) Los activos que constituyen el sistema.
b) La categoría del sistema, según lo previsto en el Art. 43.
c) Las decisiones que se adopten para gestionar los riesgos identificados.
2. Cuando un sistema al que afecte el presente Real Decreto maneje datos de carácter personal le será de aplicación lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y normativa de desarrollo, sin perjuicio de los requisitos establecidos en el Esquema Nacional de Seguridad ».

## 6.3. Nationale Aufsichtsbehörde

En Espagne, l'autorité chargée de la protection des données est l'AEPD.

Le service d'inspection de l'AEPD vérifie la légalité des fichiers publics. En cas d'infractions constatées, il instruit le dossier et impose des mesures de correction et peut aussi imposer des mesures disciplinaires à l'encontre du responsable des agissements illicites. Le service informe l'Ombudsman (*Defensor del Pueblo*) de ses décisions.

### 6.3.1. Zusammensetzung, Ernennung und Eingliederung der Behörde

Sur la base de l'art. 11 du Décret-royal 428/1993[436] (DR 428/1993), sur la protection des données, les autorités de l'AEPD sont le **Directeur** et le **Conseil de consultation** (*Consejo consultivo*).[437]

Le **Directeur** de l'AEPD est nommé par le Gouvernement, par la voie d'un décret, sur proposition du Ministre de la justice. Il est choisi parmi les membres du Conseil de consultation et il siège à ce poste pendant quatre ans (art. 14 DR 428/1993[438]).

Les **membres** du Conseil de consultation de l'AEPD sont nommés par le Gouvernement sur proposition des entités et organes suivants :

a. le Congrès des députés propose un membre (un député)

b. le Sénat propose un membre (un sénateur)

c. le Ministre de la justice propose un membre (de l'administration de l'État)

d. les Communautés autonomes choisissent un membre par décision prise à la majorité

---

436 Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia Española de Protección de Datos, disponible sous http://noticias.juridicas.com/base_datos/Admin/rd428-1993.html#c3s2 (09.8.10), Art. 10. « Sistema de Información Schengen.
1. La Agencia Española de Protección de Datos ejercerá el control de los datos de carácter personal introducidos en la parte nacional española de la base de datos del Sistema de Información Schengen (SIS).
2. El Director de la Agencia designará dos representantes para la autoridad de control común de protección de datos del Sistema de Información Schengen ».

437 Art. 11 DR 428/1993. « Estructura orgánica.
La Agencia Española de Protección de Datos se estructura en los siguientes órganos:
1. El Director de la Agencia Española de Protección de Datos.
2. El Consejo Consultivo.
3. El Registro General de Protección de Datos, la Inspección de Datos y la Secretaría General, como órganos jerárquicamente dependientes del Director de la Agencia ».

438 Art. 14 DR 428/1993 : « Nombramiento y mandato.
1. El Director de la Agencia Española de Protección de Datos será nombrado por el Gobierno, mediante Real Decreto, a propuesta del Ministro de Justicia, de entre los miembros del Consejo Consultivo.
2. El Director de la Agencia Española de Protección de Datos gozará de los mismos honores y tratamiento que los Subsecretarios.
3. El mandato del Director de la Agencia Española de Protección de Datos tendrá una duración de cuatro años contados desde su nombramiento y sólo cesará por las causas previstas en el Art. 15 del presente Estatuto ».

e. la Fédération espagnole de municipalités et provinces choisit un membre (de l'administration locale)

f. l'Académie royale d'histoire choisit un membre (de son corps)

g. le Conseil des universités choisit un membre (un expert dans le traitement de données automatisées)

h. le Conseil de consommateurs et usagers choisit un membre

i. le Conseil supérieur des Chambres de commerce, d'industrie et de navigation choisit un membre.

Ces propositions sont présentées au Gouvernement par la voie du Ministère de la justice[439].

Les membres du Conseil de consultation siègent pendant quatre ans.

L'AEPD possède quatre divisions :

1. L'I**nspection générale** (chargée, entre autres, de l'instruction de l'illicéité des traitements des données)

2. Le **Registre général** (chargé de veiller à la publicité du traitement des données, comme l'inscription des bases de traitement de données)

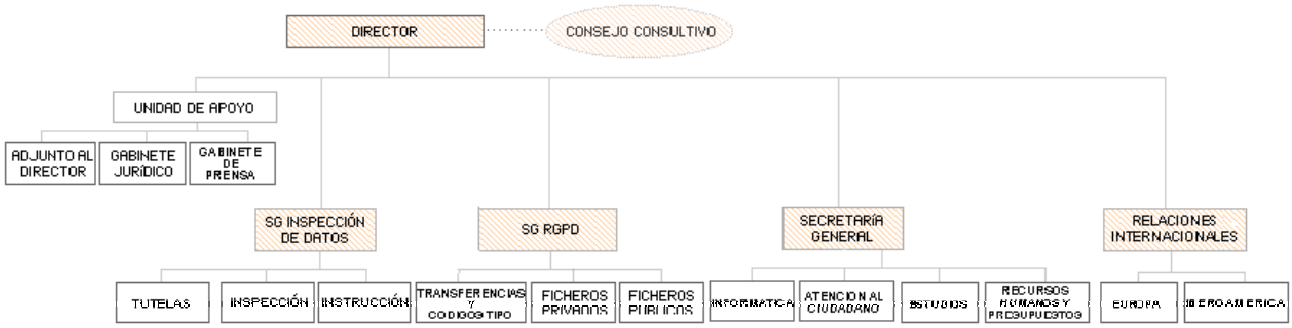
3. Le **Secrétariat général** (chargé du fonctionnement de l'AEPD)

4. Les **Relations internationales** (chargées des relations transfrontalières).

---

439 Art. 19 DR 428/1993. « Propuesta y nombramiento.
1. Los miembros del Consejo Consultivo serán propuestos en la forma siguiente:
a. El Congreso de los Diputados propondrá, como Vocal, a un Diputado.
b. El Senado propondrá, como Vocal, a un Senador.
c. El Ministro de Justicia propondrá al Vocal de la Administración General del Estado.
d. Las Comunidades Autónomas decidirán, mediante acuerdo adoptado por mayoría simple, el Vocal a proponer.
e. La Federación Española de Municipios y Provincias propondrá al Vocal de la Administración Local.
f. La Real Academia de la Historia propondrá, como Vocal, a un miembro de la Corporación.
g. El Consejo de Universidades propondrá a un Vocal experto en la materia de entre los cuerpos docentes de enseñanza superior e investigadores con acreditado conocimiento en el tratamiento automatizado de datos.
h. El Consejo de Consumidores y Usuarios propondrá, mediante terna, al Vocal de los usuarios y consumidores.
i. El Consejo Superior de Cámaras de Comercio, Industria y Navegación propondrá, mediante terna, al Vocal del sector de ficheros privados.
2. Las propuestas serán elevadas al Gobierno por conducto del Ministro de Justicia.
3. Los miembros del Consejo Consultivo serán nombrados y, en su caso, cesados por el Gobierno ».

Organigrame de l'AEPD




### 6.3.2. Gewährleistung der Unabhängigkeit

La principale garantie d'independence est le fait que l'AEPD est une **entité de droit public avec personnalité juridique propre**.

L'AEPD possède la capacité juridique pour agir tant dans le domaine du droit public que du droit privé (art. 35.1 LEPD[440]).

En vertu de l'article 35.1 LEPD, dans le cadre de ses compétences, l'AEPD – qui possède son propre statut - agit « **en totale indépendence »** par rapport à l'administration publique de l'État espagnol.

Les **ressources financières** sont pourvues par l'État. L'AEPD propose annuellement son budget et le remet au gouvernement pour intégration dans le budget général[441].

### 6.3.3. Zuständigkeitsbereich

L'art. 37 LEPD dispose que les compétences de l'AEPD sont les suivantes:

a) Veiller au respect de la législation sur la protection des données et contrôler son application,

b) délivrer les autorisations prévues par la loi,

c) traiter les réclamations soumises par les personnes concernées

d) fournir des informations sur le droit des personnes en matière de traitement de données

f) exiger des personnes chargées du traitement de données d'adopter les mesures nécessaires afin de respecter la LEPD, incluant la destruction de fichiers

---

440 Art. 35.1. LEPD : « La Agencia deProtección deDatos es un ente de derecho público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena INDEPENdencia de las Administraciones públicas en el ejercicio de sus funciones. Se regirá por lo dispuesto en la presente Ley y en un Estatuto propio, que será aprobado por el Gobierno »

441 Art. 37 Statut de l'AEPD, Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia Española de Protección de Datos ; Art. 35 Ley Organica 15/1999.

g) Imposer des sanctions en cas de violation de la LEPD

h) Informer sur les projets de reforme de la LEPD

i) obtenir des responsables de fichiers les informations nécessaires pour l'application de la LEPD

j) veiller à la publication périodique d'informations sur l'existence de fichiers

K) rédiger un rapport annuel pour le Ministère de la justice

l) exercer le contrôle et adopter les mesures pertinentes par rapport au transfert international de données et exercer les fonctions de coopération internationale en cette matière.

m) veiller à l'application de la loi par les services de statistique de l'État pour tout ce qui concerne la collecte de données statistiques et le secret des statistiques, et édicter des instructions précises sur les conditions de sécurité des fichiers de statistiques

n) toute autre compétence attribuée par la loi

### 6.3.4. Aufgaben und Kompetenzen

L'unité d'inspections fonctionne dans le cadre de l'AEPD. Elle est composée d'une section « d'inspection » proprement dite et d'une section « d'instruction » des affaires.

Le service est dirigé par un sous-directeur général qui répond directement au Directeur de l'AEPD.

Le service d'inspection est constitué de 65 membres[442], qui sont des fonctionnaires de carrière de l'État només à vie.

Les membres de l'Inspection sont només par la voie d'un concours. Les mérits des candidats sont évalués par une commission de l'AEPD. Cette commission est composée du Sécretaire général de l'AEPD, du subdirecteur de l'unité d'Inspection, du subdirecteur du Registre, du chef de l'Administration générale, d'un membre du Séretariat de l'État pour la fonction publique et d'un représentant des associations sindicales les plus représentatives (ayant plus de 10% de représentants dans l'Administration publique). Le sécretariat est assuré par le Chef de ressources humaines de l'AEPD.[443]

La section d'inspections prépare un rapport annuel d'activités et notifie l'Ombudsman (Defensor del pueblo) des décisions prises.

En vertu de l'art. 40 LEPD[444], l'autorité d'inspection est compétente pour enquêter sur les fichiers et pour collecter toutes les informations nécessaires pour l'exercice de ses tâches.[445] Pour ce faire, les

---

442 http://html.rincondelvago.com/agencia-de-proteccion-de-datos.html

443 Art. 46, Real Decreto 364/1995, du 10.3.1995, disponible sous http://noticias.juridicas.com/base_datos/Admin/rd364-1995.html (5.12.2010).

444 Art 40 LEPD : « Potestad de inspección.
1. Las autoridades de control podrán inspeccionar los ficheros a que hace referencia la presente Ley, recabando cuantas informaciones precisen para el cumplimiento de sus cometidos.

inspecteurs peuvent solliciter l'envoi de documents, les examiner sur place, inspecter les éléments et supports dans lesquels les données se trouvent ou sont traitées. Les inspecteurs ont aussi le droit d'entrer dans les locaux où le traitement a lieu. A cet égard, ils sont considérés comme une autorité publique agissant dans le cadre de ses pouvoirs.

Les inspecteurs ont l'obligation de garder le secrete des informations dont ils prennent connaissance dans le cadre de leurs fonctions, même après avoir cesser de s'en s'occuper.

## 6.4. Rolle der Organisationen zum Schutz der Betroffenen

Mis à part le fait qu'un représentant des consommateurs fasse partie du Conseil de consultation de l'AEPD (art. 38 LEPD), la LEPD ne prévoit pas de rôle spécifique pour ces organisations. En théorie, les organisations de protection des consommateurs pourront agir en justice si le dommage causé par un traitement de données illicite peut être prévu par la loi de protection des consommateurs[446], qui ne règle pas spécialement les questions relatives au traitement des données.

La LEPD n'attribue pas de droit d'action collective à ces organisations[447].

---

A tal efecto, podrán solicitar la exhibición o el envío de documentos y datos y examinarlos en el lugar en que se encuentren depositados, así como inspeccionar los equipos físicos y lógicos utilizados para el tratamiento de los datos, accediendo a los locales donde se hallen instalados.
2. Los funcionarios que ejerzan la inspección a que se refiere el apartado anterior tendrán la consideración de autoridad pública en el desempeño de sus cometidos.
Estarán obligados a guardar secreto sobre las informaciones que conozcan en el ejercicio de las mencionadas funciones, incluso después de haber cesado en las mismas ».

445 Le 21 décembre 2007 a été publié dans le Journal officiel le Règlement de la LEPD, qui contient des dispositioon sur les activités de la section d'inspections : 21 décembre 2001, disponible sous : http://www.derecho.com/l/boe/real-decreto-1720-2007-aprueba-reglamento-desarrollo-ley-organica-15-1999-proteccion-datos-caracter-personal/#A283 (10.09.2010).

446 Ley de Consumidores y Usuarios de 2007, Real Decreto Legislativo 1/2007, de 16 noviembre RCL\2007\2164.

447 J. Lago, La Responsabilidad Civil de los responsables de ficheros de datos personales y los encargados de su tratamiento, loc. cit. : « La LEPD no ampara a las personas jurídicas , sin perjuicio de que éstas puedan obtener la tutela de su derecho al honor o a la intimidad en virtud de la aplicación de la Ley Orgánica 1/1982 y **tampoco se contempla la posibilidad del ejercicio de acciones colectivas** , salvo en el caso de que se trate de consumidores y usuarios afectados, en cuyo caso sería de aplicación la legitimación que atribuye a las asociaciones de éstos y a las entidades legalmente constituidas que tengan por objeto su protección o defensa, de conformidad con las previsiones del art. 11 de la LECiv ( RCL 2000, 34, 962 y RCL 2001, 1892). No parece tampoco que pueda atribuirse legitimación activa a terceros distintos de los propios interesados cuyos datos son objeto de tratamiento, aunque sí a las personas fallecidas, aplicando supletoriamente las previsiones del art. 4 de la Ley Orgánica 1/1982 (y obviamente las normas que rigen la sucesión procesal por causa de muerte, ex art. 16 de la LECiv) ».

## 6.5. Mögliche und vorgeschriebene Aktivitäten der Datenbearbeiter (private und öffentliche)

L'art. 55 du Décret royal 1720/2007, du 21 septembre 2007 dispose que l'existence de tout fichier (soit tenu par l'administration, soit par des structures privées), sera notifiée à l'AEPD.[448]

Mises à part les obligations découlant des principes sur la protection de données (chiffre 6.1.), l'art. 10 LEPD[449] impose au responsable du fichier, ainsi qu'à toute personne intervenant dans le traitement des données, le devoir de respecter le secret professionnel. Une telle obligation subsiste même après la fin de sa mission.

Dans le chapitre sur les sanctions, la LEPD **reprime administrativement** certains comportements du respnsable de fichier, entre autres :

a) de ne pas s'occuper, pour des motifs formels, de la demande d'une personne sollicitant la rectification ou l'annulation des données personnelles objet de traitement

b) de ne pas fournir l'information que sollicite l'AEPD

c) de ne pas solliciter l'enregistrement d'un fichier

d) de procéder à la collecte de données à caractère personnel sans obtenir le consentement requis

---

448 Real Decreto 1720/2007, de 21 diciembre RCL\2008\150, Art 55. « Notificación de ficheros
1. Todo fichero de datos de carácter personal de titularidad pública será notificado a la Agencia Española de Protección de Datos por el órgano competente de la Administración responsable del fichero para su inscripción en el Registro General de Protección de Datos, en el plazo de treinta días desde la publicación de su norma o acuerdo de creación en el diario oficial correspondiente.
2. Los ficheros de datos de carácter personal de titularidad privada serán notificados a la Agencia Española de Protección de Datos por la persona o entidad privada que pretenda crearlos, con carácter previo a su creación. La notificación deberá indicar la identificación del responsable del fichero, la identificación del fichero, sus finalidades y los usos previstos, el sistema de tratamiento empleado en su organización, el colectivo de personas sobre el que se obtienen los datos, el procedimiento y procedencia de los datos, las categorías de datos, el servicio o unidad de acceso, la indicación del nivel de medidas de seguridad básico, medio o alto exigible, y en su caso, la identificación del encargado del tratamiento en donde se encuentre ubicado el fichero y los destinatarios de cesiones y transferencias internacionales de datos.
3. Cuando la obligación de notificar afecte a ficheros sujetos a la competencia de la autoridad de control de una Comunidad Autónoma que haya creado su propio registro de ficheros, la notificación se realizará a la autoridad autonómica competente, que dará traslado de la inscripción al Registro General de Protección de Datos.
El Registro General de Protección de Datos podrá solicitar de las autoridades de control de las Comunidades Autónomas el traslado al que se refiere el párrafo anterior, procediendo, en su defecto, a la inclusión de oficio del fichero en el Registro.
4. La notificación se realizará conforme al procedimiento establecido en la sección primera del capítulo IV del título IX del presente Reglamento ».

449 Art. 10 LEPD : « Deber de secreto. El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo ».

e) de ne pas respecter le devoir de secret

f) de tenir un fichier sans veiller aux mesures de sécurité nécessaires,

g) de maintenir des données inexactes ou de s'abstenir d'effectuer les modifications ou destruction nécessaires

h) d'empêcher ou de limiter les inspections

i) de ne pas cesser la collecte de données lorsque l'AEPD le requiert,

En vertu de l'art. 31 LEPD[450], par le biais d'accords sectoriels, de conventions administratives ou de décisions d'entreprise, les responsables de traitements de données (publiques ou privées), pourront élaborer des **codes de conduite** établissant les conditions d'organisation, de fonctionnement, de sécurité, les procédures applicables et les garanties pour l'exercice des droits des personnes concernées.

[450] Art. 32 LEPD : « Códigos tipo. 1. Mediante acuerdos sectoriales, convenios administrativos o decisiones de empresa, los responsables de tratamientos de titularidad pública y privada, así como las organizaciones en que se agrupan, podrán formular códigos tipo que establezcan las condiciones de organización, régimen de funcionamiento, procedimientos aplicables, normas de seguridad del entorno, programas o equipos, obligaciones de los implicados en el tratamiento y uso de la información personal, así como las garantías, en su ámbito, para el ejercicio de los derechos de las personas con pleno respeto a los principios y disposiciones de la presente Ley y sus normas de desarrollo.

2. Los citados códigos podrán contener o no reglas operacionales detalladas de cada sistema particular y estándares técnicos de aplicación.

En el supuesto de que tales reglas o estándares no se incorporen directamente al código, las instrucciones u órdenes que los establecieran deberán respetar los principios fijados en aquél.

3. Los códigos tipo tendrán el carácter de códigos deontológicos o de buena práctica profesional, debiendo ser depositados o inscritos en el Registro general de Protección de Datos y, cuando corresponda, en los creados a estos efectos por las Comunidades Autónomas, de acuerdo con el Art. 41. El Registro general de Protección de Datos podrá denegar la inscripción cuando considere que no se ajusta a las disposiciones legales y reglamentarias sobre la materia, debiendo, en este caso, el Director de la Agencia de Protección de Datos requerir a los solicitantes para que efectúen las correcciones oportunas ».

# 7. Osteuropa: Slowenien

## 7.1. Grundsätze des Datenschutzes

Slovenia has been a member of the European Union since 2004, which means that all EU directives are effective in the country. Slovenia enacted in 2004 (in force from 1 January 2005) **the Personal Data Protection Act** (PDPA)[451] fully based on the EU Data Protection Directive and the Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention No. 108). In this law, private entities may process personal data only if they have obtained individuals' written consent[452], or if law regulates the data processing. Article 38 of **the Slovenian Constitution** states, "[T]he protection of personal data relating to an individual shall be guaranteed. Any use of personal data shall be forbidden where that use conflicts with the original purpose for which it was collected. The collection, processing and the end-use of such data, as well as the supervision and protection of the confidentiality of such data, shall be regulated by statute. Each person has the right to be informed of the personal data relating to him which has been collected and has the right to legal remedy in the event of any misuse of that data".[453]

**PDPA covers processing of personal data**[454], **use of video surveillance cameras, biometrics, collecting of data about entrances and leavings from premises.** PDPA meets all requirements of the 1995 EU Data Protection Directive.[455]

### 7.1.1. Rolle der Zweckbindung der Datenbearbeitung

The PDPA provides that everything that is not explicitly allowed in connection with personal data collection and processing is prohibited. **Public entities** may only process personal data for which they have been granted legal authorization, while private entities must receive written consent from

---

451 Personal Data Protection Act is in Slovene language: Zakon o varstvu osebnih podatkov. ZVOP-1 is its official acronym in Slovene language. This Act was published in: Official Gazette of the Republic of Slovenia, No. 86/2004, as of 5 August 2004 and was partly annulled and corrected by the Information Commissioner Act which was published in: Official Gazette of the Republic of Slovenia, No. 113/2005, as of 16 December 2005.

452 Written consent of the individual is the signed consent of the individual having the form of a document, the provision of a contract, the provision of an order, an appendix to an application or other form in accordance with statute; a signature shall also mean on the basis of a statute a form equivalent to a signature given by means of telecommunication and a form equivalent by statute to a signature given by an individual who does not know how to write or is unable to write.

453 Constitution of the Republic of Slovenia, Ustava Republike Slovenije, UL RS 33/91, p. 1373, 28.12. 1991.

454 According to PDPA i. e. any operation or set of operations performed in connection with personal data that are subject to automated processing or which in manual processing are part of a filing system or which are intended for inclusion in a filing system, such as in particular collection, acquisition, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, communication, dissemination or otherwise making available, alignment or linking, blocking, anonymising, erasure or destruction; processing may be performed manually or by using automated technology (means of processing).

455 Directive 95/46/EC of the European Parliament and of the Council of October 24, 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L. 281, 23/11/1995 p. 0031 - 0050.

individuals. Persons whose personal data are gathered must be informed in advance of the purpose of the collection of data (by giving their written consent or where the purpose of collection is authorized by law). In principle, personal data can be gathered and stored for **only as long as needed** to meet that objective, and deleted or blocked once the objective is met. **All exemptions must be defined in the law**. Use of video surveillance in the workplace is allowed only under special circumstances (if it is necessary for security of the people or wealth, protecting secret data or business secrets and this purpose cannot be achieved by less intrusive means). Employees must be presented with a written notice about this measure, the same applies to the use of biometrics in the private sector.[456]

**The purpose** of processing personal data must be **provided by statute**, and in cases of processing on the basis of personal consent of the individual, the individual must be informed in advance in writing or in another appropriate manner of the purpose of processing of personal data (Article 8 PDPA).

### 7.1.2. Grundsätze Datenbearbeitung

PDPA determines the rights, responsibilities, principles and measures to prevent unconstitutional, unlawful and unjustified encroachments on the privacy and dignity of an individual in the processing of personal data (Article 1 PDPA). In addition, it establishes the following principles:

**Principle of lawfulness and fairness**: Personal data shall be processed lawfully[457] and fairly (Article 2 PDPA).

**Principle of proportionality**: Personal data that are being processed must be adequate and in their extent appropriate in relation to the purposes for which they are collected and further processed (Article 3 PDPA).

**Prohibition of discrimination**: Protection of personal data shall be guaranteed to every individual irrespective of nationality (citizenship), race, colour, religious belief, ethnicity, sex, language, political or other belief, sexual orientation, material standing, birth, education, social position, citizenship, place or type of residence or any other personal circumstance (Article 4 PDPA).

#### *7.1.2.1. Datenbearbeitungen durch Private*

**Private sector** is defined in PDPA as legal or natural persons performing an activity in accordance with the statute regulating commercial companies or a commercial public service or craft, and persons of private law; public commercial institutes, public companies and commercial companies, irrespective of the share or influence held by the state, self-governing local communities or self-governing communities of nationalities, are a part of the private sector. According to Article 10 PDPA **personal data in the private sector may be processed** if the processing of personal data and the personal data being processed are **provided by statute**, or **if the personal consent of the individual** has been given for the processing of certain personal data.

---

456 If processing of personal data is necessarily required to protect the life or body of an individual, his personal data may be processed irrespective of the fact that there are no other statutory legal grounds for the processing of such data (Article 12 PDPA).

457 A verbatim translation would be: "statutorily" - meaning by the statute/following a statute (a general act of Parliament).

Irrespective of that, in the private sector personal data may be furthermore processed in respect of individuals that have contractual relations with the private sector or on the basis of the individual's initiative are negotiating on the conclusion of a contract, provided that the processing of personal data is necessary and appropriate for conducting negotiations for the conclusion of a contract or for the fulfillment of a contract.

Irrespective of the rules set above, personal data may be processed in the private sector if this is essential for the **fulfillment of the lawful interests of the private sector** and these interests clearly outweigh the interests of the individual to whom the personal data relate.

#### *7.2.1.2. Contractual Processing*

According to Article 11 PDPA data controller may **by contract entrust individual tasks related to processing of personal data to data processor**[458] that is registered to perform such activities and ensures the appropriate procedures and measures pursuant to Article 24 of the PDPA.[459]

---

458 Data processor is a natural person or legal person that processes personal data on behalf and for the account of the data controller.

459 Article 24 (Security of Personal Data):
"(1) Security of personal data comprises organisational, technical and logical-technical procedures and measures to protect personal data, and to prevent accidental or deliberate unauthorised destruction, modification or loss of data, and unauthorised processing of suchdata:
1. by protecting premises, equipment and systems software, including input-output units;
2. by protecting software applications used to process personal data;
3. by preventing unauthorised access to personal data during transmission thereof, including transmission via telecommunications means and networks;
4. by ensuring effective methods of blocking, destruction, deletion or anonymisation of personal data;
5. by enabling subsequent determination of when individual personal data were entered into a filing system, used or otherwise processed, and who did so, for the period covered by statutory protection of the rights of an individual due to unauthorised supply or processing of personal data.
(2) In cases of processing of personal data accessible over telecommunications means or network, the hardware, systems software and software applications must ensure that the processing of personal data in filing systems is within the limits of authorisations of the data recipient.
(3) The procedures and measures to protect personal data must be adequate in view of the risk posed by processing and the nature of the specific personal data being processed.
(4) Functionaries, employees and other individuals performing work or tasks at persons that process personal data shall be bound to protect the secrecy of personal data with which they become familiar in performing their functions, work and tasks. The duty to protect the secrecy of personal data shall also be binding on them after termination of their function, work or tasks, or the performance of contractual processing services."
Article 25 (Duty to secure):
"(1) Data controllers and data processors shall be bound to ensure the protection of personal data in the manner set out in Article 24 of PDPA.
(2) Data controllers shall prescribe in their internal acts the procedures and measures for security of personal data and shall define the persons responsible for individual filing systems and the persons who, due to the nature of their work, shall process individual personal data."

**Data processor** may perform individual tasks associated with processing of personal data **within the scope of the client's authorisations**, and may not process personal data for any other purpose. Mutual rights and obligations shall be arranged by contract, which must be concluded in writing and must also contain an agreement on the procedures and measures pursuant to Article 24 of PDPA. Data controller oversees the implementation of these procedures and measures.

In the event of a **dispute between the data controller and the data processor**, the data processor is bound on the basis of a request from the data controller to return to the controller without delay the personal data processed under contract. He is obliged to destroy immediately or to supply any copies of such data to the state body competent by statute for detection or prosecution of criminal offences, to a court or to another state body, if so provided by statute. In the event of cessation of a data processor, personal data must be returned to the data controller without unnecessary delay.

#### *7.2.1.3. Datenbarbeitungen durch Behörde*

**Personal data in the public sector**[460] may be processed if the processing of personal data and the personal data being processed are **provided by statute. Statute may provide that** certain personal data may **only be processed on the basis of personal consent** of the individual (Article 9 PDPA).

**Holders of public powers** may also process personal data on the basis of personal consent of the individual **without statutory grounds** where this does not involve the performance of their duties as holders of public powers. Filing systems created on such basis must be held separate from filing systems created on the basis of the performance of duties of the holder of public powers.

Irrespective of this, **in the public sector personal data** may be processed in respect of individuals that have contractual relations with the public sector or on the basis of the individual's initiative are negotiating on the conclusion of a contract, provided that the processing of personal data is **necessary and appropriate** for conducting negotiations for **the conclusion of a contract or for the fulfilment of a contract**.

Personal data may in exceptions also be processed in the public sector where they are essential for the **exercise of lawful competences, duties or obligations by the public sector**, provided that such processing does not encroach on the justified interests of the individual to whom the personal data relate.

### 7.1.3. Erkenbarkeit/Transparenz, Einwiligung

Personal data may only be processed if the processing of personal data and the personal data being processed are provided by **statute,** or if the personal **consent** of the individual has been given for the processing of certain personal data. Personal consent of an individual is defined as a voluntary statement of the will of an individual that his personal data may be processed for a specific purpose, and this is given on the basis of **information that must be provided** to such individual by the data; personal consent of an individual may be written, oral or some other appropriate consent of the individual.

---

460 Public sector are state bodies, bodies of self-governing local communities, holders of public powers, public agencies, public funds, public institutes, universities, independent institutions of higher education and self-governing communities of nationalities.

### 7.1.4. Sensitive Daten

Special protections are set out for **"sensitive data"** defined as data on racial or other origins, political, religious or other beliefs, trade union membership, sexual behavior, criminal convictions and medical data. This data must be specially labeled and may only be transferred across telecommunications networks if it is protected by "encryption methods" and an "electronic signature" that can guarantee illegibility (Article 14 PDPA). The law also imposes cross-border restrictions providing that data may only be transferred to countries that have a data protection legal framework as adequate as the Slovenian one. Article 62 PDPA explicitly states that there are no cross-border restrictions for the EU member states.

According to Article 13 PDPA sensitive **personal data may only be processed** in the following cases:

1. if the individual has given explicit personal consent for this, such consent as a rule being in writing, and in the public sector provided by statute;

2. if the processing is necessary in order to fulfil the obligations and special rights of a data controller in the area of employment in accordance with statute, which also provides appropriate guarantees for the rights of the individual;

3. if the processing is necessarily required to protect the life or body of an individual to whom the personal data relate, or of another person, where the individual to whom the personal data relate is physically or contractually incapable of giving his consent pursuant to subparagraph 1 of this Article;

4. if they are processed for the purposes of lawful activities by institutions, societies, associations, religious communities, trade unions or other non-profit organisations with political, philosophical, religious or trade-union aim, but only if the processing concerns their members or individuals in regular contact with them in connection with such aims, and if they do not supply such data to other individuals or persons of public or private sector without the written consent of the individual to whom they relate;

5. if the individual to whom the sensitive personal data relate publicly announces them without any evident or explicit purpose of restricting their use;

6. if they are processed by health-care workers and health-care staff in compliance with statute for the purposes of protecting the health of the public and individuals and the management or operation of health services;

7. if this is necessary in order to assert or oppose a legal claim;

8. if so provided by another statute in order to implement the public interest.

**Automated data processing** according Article 15 PDPA, in which a decision may be taken regarding an individual that could have legal effect in relation to him, or substantive influence on him, and which is based solely on automated data processing intended for the evaluation of certain personal aspects relating to him, such as in particular his success at work, credit rating, reliability, handling or compliance with conditions required, is only permitted if the decision:

1. is taken during the conclusion or implementation of a contract, provided that the request to conclude or implement a contract submitted by the individual to whom the personal data relate has been fulfilled or that there exist appropriate measures to protect his lawful interests, such as in particular agreements enabling him to object to such decision or to express his position;

2. is provided by statute which also provides measures to protect the lawful interests of the individual to whom the personal data relate, particularly the possibility of legal remedy against such decision.

Personal data **may only be collected for specific and lawful purposes**, and may not be further processed in such a manner that their processing would be counter to these purposes, unless otherwise provided by statute (Article 16 PDPA).

### 7.1.5. Bearbeitung besonders schützenswerten Daten

**Protection of individuals (Article 18-23 PDPA)**

Personal data being processed must be **accurate and kept up to date**. Data controller may prior to input into a filing system verify the accuracy of personal data by examining an identity document or other suitable public document of the individual to whom the data relate.

If personal data are collected directly from the individual to whom they relate, the **data controller or his representative must communicate to the individual the following information**, if the individual is not yet acquainted with them:

- data on the data controller and his possible representative (personal name, title or official name respectively and address or seat respectively),

- the purpose of the processing of personal data.

If in view of the special circumstances of collecting personal data there is a need to ensure lawful and fair processing of personal data of the individual, the data controller must also communicate to the individual the additional information, if the individual is not yet acquainted with them, and in particular:

- a declaration as to the data recipient or the type of data recipients of his personal data,

- a declaration of whether the collection of personal data is compulsory or voluntary, and the possible consequences if the individual will not provide data voluntarily,

- information on the right to consult, transcribe, copy, supplement, correct, block and erase personal data that relate to him.

If personal data were not collected directly from the individual to whom they relate, the data controller or his representative must communicate to the individual the following information no later than on the recording or supply of personal data to the data recipient:

- data on the data controller and his possible representative (personal name, title or official name respectively and address or seat respectively),

- the purpose of the processing of personal data.

If in view of the special circumstances of collecting personal data there is a need to ensure lawful and fair processing of personal data of the individual, the data controller must also communicate to the individual additional information, and in particular:

- information on the type of personal data collected,

- a declaration as to the data recipient or the type of data recipients of his personal data,

- information on the right to consult, transcribe, copy, supplement, correct, block and erase personal data that relate to him.

### 7.1.6. Datensicherheit

Security of personal data comprises organizational, technical and logical-technical procedures and measures to protect personal data, and to prevent accidental or deliberate unauthorized destruction, modification or loss of data, and unauthorized processing of such data:
1. by protecting premises, equipment and systems software, including input-output units;
2. by protecting software applications used to process personal data;
3. by preventing unauthorized access to personal data during transmission thereof, including transmission via telecommunications means and networks;
4. by ensuring effective methods of blocking, destruction, deletion or anonymisation of personal data;
5. by enabling subsequent determination of when individual personal data were entered into a filing system, used or otherwise processed, and who did so, for the period covered by statutory protection of the rights of an individual due to unauthorized supply or processing of personal data.

In cases of processing of personal data accessible over telecommunications means or network, the hardware, systems software and software applications must ensure that the processing of personal data in filing systems is within the limits of authorizations of the data recipient.
The procedures and measures to protect personal data must be adequate in view of the risk posed by processing and the nature of the specific personal data being processed. Functionaries, employees and other individuals performing work or tasks at persons that process personal data are bound to protect the secrecy of personal data with which they become familiar in performing their functions, work and tasks. The duty to protect the secrecy of personal data is also binding on them after termination of their function, work or tasks, or the performance of contractual processing services.
Data controllers and data processors are bound to ensure the protection of personal data. Data controllers prescribe in their internal acts the procedures and measures for security of personal data and define the persons responsible for individual filing systems and the persons who, due to the nature of their work, shall process individual personal data (Article 24+25 PDPA).
In the acquisition of personal data from filing systems in the areas of health, police, national intelligence-security activities, national defence, judiciary and the state prosecution and criminal record and minor offence records, **the same connecting code may not be used in such manner that only such code would be used to obtain personal data**. Irrespective of this, the same connecting code may exceptionally be used to obtain personal data if this is the only item of data in a specific case that can enable the detection or prosecution of a criminal offence *ex officio*, to protect the life or body of an individual, or to ensure the implementation of the tasks of the intelligence and security bodies provided by statute. An official annotation or other written record must be made thereof without delay.

Personal data may only be stored for **as long as necessary** to achieve the purpose for which they were collected or further processed. On completion of the purpose of processing, personal data shall be erased, destroyed, blocked or anonymised, unless pursuant to the statute governing archive materials and archives they are defined as archive material, or unless a statute otherwise provides for an individual type of personal data.

### 7.1.7. Grenzüberschreitende Bekanngabe

Whenever personal data are supplied to data controller, data processor or data recipient established, has its seat or is registered in a Member State of the European Union or the European Economic Area

or otherwise subject to the legal order thereof, the provisions of PDPA on the transfer of personal data to third countries shall not apply (Article 62 PDPA).

The supply of personal data that are processed or will be processed only after being supplied to a third country, will be permitted in accordance with the provisions of PDPA and provided that the National Supervisory Body issues a decision that the country to which the data are transferred ensures an adequate level of protection of personal data. This decision is not required if the third country is on the list of those countries that have been found to fully ensure an adequate level of protection of personal data[461]. This decision is also not required if the third country is on the list of those countries that have been found in part to ensure an adequate level of protection of personal data, if those personal data are transferred and for those purposes for which an adequate level of protection has been found (Article 63 PDPA).

The National Supervisory Body initiates a procedure to determine an adequate level of protection of personal data in a third country on the basis of a conclusion of inspection supervision or at the suggestion of a natural person or legal person who can show a legal interest in the issuing of a decision.
At the request of the National Supervisory Body, the Ministry responsible for foreign affairs obtains from the competent body of a third country the necessary information as to whether such country ensures an adequate level of protection of personal data.
The National Supervisory Body may obtain additional information on the adequate level of protection of personal data in a third country directly from other supervisory bodies and the competent body of the European Union.
The National Supervisory Body issues a decision within two months of receipt of full information. It may also issue a decision only for a certain type of personal data or for their processing for an individual purpose. The National Supervisory Body is obliged no later than within 15 days of the issuing of a decision that a third country fails to ensure an adequate level of protection of personal data to inform the competent body of the European Union in writing. (Article 64 PDPA). There is no appeal against this decision, but an administrative dispute shall be permitted (Article 65 PDPA).

In decision-making on the adequate level of protection of personal data in a third country, the National Supervisory Body is bound to determine all circumstances relating to the transfer of personal data. In particular, it shall be obliged to take account of the type of personal data, the purpose and duration of proposed processing, the legal arrangements in the country of origin and the recipient country, including arrangements for protection of personal data of foreign citizens, and measures to secure personal data used in such countries (Article 68 PDPA). In this decision-making, the National Supervisory Body in particular takes account of:

---

461 The National Supervisory Body maintains a list of third countries for which it finds that have fully or partly ensured an adequate level of protection of personal data, or have not ensured such protection. If it has been determined that a third country only partly ensures an adequate level of protection of personal data, the list also sets out in which part an adequate level has been ensured. The Chief National Supervisor publishes the list from the previous paragraph in the Official Gazette of the Republic of Slovenia (Article 66 PDPA). The National Supervisory Body is in its decision-making be bound by the decisions of the competent body of the European Union with regard to assessment as to whether third countries ensure an adequate level of protection of personal data (Article 67 PDPA).

1. whether the transferred personal data are used solely for the purpose for which they were transferred, or whether the purpose may change only on the basis of permission of the data controller supplying the data or on the basis of personal consent of the individual to whom the personal data relate;
2. whether the individual to whom personal data relate has the possibility of determining the purpose for which his personal data have been used, to whom they were supplied and the possibility of correcting or erasing inaccurate or outdated personal data unless this is prevented due to the secrecy of the procedure by binding international treaties;
3. whether the foreign data controller performs adequate organizational and technical procedures and measures to protect personal data;
4. whether there is an assigned contact person authorised to provide information to the individual to whom the personal data relate, or to the National Supervisory Body on the processing of personal data transferred;
5. whether the foreign data recipient may transfer personal data only on the condition that another foreign data recipient to whom personal data will be supplied ensures adequate protection of personal data also for foreign citizens;
6. whether effective legal protection is ensured for individuals whose personal data were transferred.

Following a proposal of the Chief National Supervisor, the Minister responsible for justice, with the consent of the Minister responsible for foreign affairs, issues rules that define in greater detail the information considered necessary in the decision-making of the National Supervisory Body on the transfer of personal data to third countries (Article 69 PDPA).

Irrespective of PDPA, personal data may be transferred and supplied to a third country, if:
1. so provided by another statute or binding international treaty;
2. the individual to whom the personal data relate gives personal consent and is aware of the consequences of such supply;
3. the transfer is necessary for the fulfillment of a contract between the individual to whom the personal data relate and the data controller, or for the implementation of pre-contractual measures adopted in response to the request of the individual to whom the personal data relate;
4. the transfer is necessary for the conclusion or implementation of a contract to the benefit of the individual to whom the personal data relate, concluded between the data controller and a third party;
5. the transfer is necessary in order to protect from serious danger the life or body of an individual to whom the personal data relate;
6. the transfer is performed from registers, public books or official records which are intended by statute to provide information to the public and which are available for consultation by the general public or to any person who demonstrates a legal interest that in the individual case the conditions provided by statute for consultation have been met;
7. the data controller ensures adequate measures of protection of personal data and of the fundamental rights and freedoms of individuals, and declares the possibility of their fulfillment or protection, especially in the provisions of contracts or in the general terms of business.
In the last mentioned case of transfer of personal data, the person intending to transfer personal data must obtain a special decision from the National Supervisory Body permitting the transfer of personal data. There is no appeal against a such decision, but an administrative dispute is permitted. The administrative dispute procedure shall be urgent and a priority (Article 70 PDPA).

## 7.1.8. Auskunftsrecht

### *7.1.8.1. Right of the individual to information*

According Article 30 PDPA is **data controller obliged on request of the individual**:

1. to enable consultation of the filing system catalogue;

2. to certify whether data relating to him are being processed or not, and to enable him to consult personal data contained in filing system that relate to him, and to transcribe or copy them;

3. to supply him an extract of personal data contained in filing system that relate to him;

4. to provide a list of data recipients to whom personal data were supplied, when, on what basis and for what purpose;

5. to provide information on the sources on which records contained about the individual in a filing system are based, and on the method of processing.

6. to provide information on the purpose of processing and the type of personal data being processed, and all necessary explanations in this connection;

7. to explain technical and logical-technical procedures of decision-making, if the controller is performing automated decision-making through the processing of personal data of an individual.

The **request for information** according Article 30 PDPA is to be lodged in writing or orally in a record with the data controller. Such request may be lodged once every three months, and in respect of sensitive personal data and personal data once a month. When required to ensure fair, lawful or proportionate processing of personal data, particularly when an individual's personal data in a filing system are frequently updated or sent or could be frequently updated or sent to data recipients, the data controller must permit the individual to lodge the request within an appropriately shorter period, which is not less than five days from the day of acquainting with personal data that relate to him or from the refusal of this acquaintance. The Minister responsible for justice, at the proposal of the Information Commissioner, issues rules[462] prescribing a tariff for the material costs and shall publishes them in the Official Gazette of the Republic of Slovenia.

### *7.1.8.2. Right of information against third parties*

Data controllers are obliged against payment of the cost of supply, unless otherwise provided by statute, to supply personal data to data recipients. The data controller of the Central Population Register or of Records of Permanently and Temporarily Registered Residents is obliged in the manner defined for the issuing of certificates to supply to authorised party demonstrating a lawful interest in exercising rights before public sector persons the personal name and address of permanent or temporary residence of an individual against whom they are exercising their rights.

Data controller is obliged for each supply of personal data to ensure that it is subsequently possible **to determine which personal data were supplied, to whom, when and on what basis**, for the period covered by statutory protection of the rights of an individual due to non-allowed supply of personal data. Irrespective of this, data controllers in the public sector shall be bound to supply to data recipient

---

462 See: Rules on the charging of expenses concerning the execution of the individual's right to acquaint himself with his own personal data, published in: Official Gazette of the RS, No. 85/2007 (in Slovene language: "Pravilnik o zaračunavanju stroškov pri izvrševanju pravice posameznika do seznanitve z lastnimi osebnimi podatki").

in the public sector personal data without payment of the cost of supply, unless otherwise provided by statute or unless it involves use for historical, statistical or scientific-research purposes.

Data controller may supply data on a deceased individual only to those data recipients authorised to process personal data by statute. Irrespective of this, data controller supplies data on a deceased individual to the person who under the statute governing inheritance is the deceased person's legal heir of the first or second order, if they demonstrate a lawful interest in the use of personal data and the deceased individual did not prohibit in writing the supply of such personal data.

## 7.1.9. Verhältnis von Technologieentwicklung und Datenschutz

Fast development of information communication technologies is increasing the potential of personal data abuse. One of the main strategies of PDPA for combating abuse in this field is to regulate new technological phenomena. The Personal Data Protection Act is in this direction the Slovenian system act, which regulates in its Part VI new sectoral arrangements.

### *7.1.9.1. Direct marketing*

Data controller may use the personal data of individuals that he obtained from publicly accessible sources or within the framework of the lawful performance of activities, also for the purposes of offering goods, services, employment or temporary performance of work through the use of postal services, telephone calls, electronic mail or other telecommunications means (hereinafter: direct marketing in accordance with the provisions of PDPA.
For the purposes of direct marketing, data controller may use only the following personal data collected in accordance with PDPA: personal name, address of permanent or temporary residence, telephone number, e-mail address and fax number. On the basis of personal consent of the individual, data controller may also process other personal data, but may only process sensitive personal data if he possesses the personal consent of an individual, that is explicit and as a rule in writing.
Data controller must perform direct marketing in such a way that upon the performance of direct marketing the individual is informed of his rights[463]. If a data controller intends to supply personal data to other data recipients for the purposes of direct marketing or to data processors, he is bound to inform the individual of this and prior to the supply of personal data obtain the individual's written consent. The notification to the individual regarding the intended supply must contain information as to the data intended to be supplied, to whom, and for what purpose. The costs of notification shall be borne by the data controller (Article 72 PDPA).

Individual may at any time in writing or in another agreed manner request that the data controller permanently or temporarily cease to use his personal data for the purpose of direct marketing. The data controller shall be obliged within 15 days to prevent as appropriate the use of personal data for the purpose of direct marketing, and within the subsequent 5 days to inform in writing or another

---

[463] Rights of individual according to Article 73 PDPA:
(1) Individual may at any time in writing or in another agreed manner request that the data controller permanently or temporarily cease to use his personal data for the purpose of direct marketing. The data controller shall be obliged within 15 days to prevent as appropriate the use of personal data for the purpose of direct marketing, and within the subsequent 5 days to inform in writing or another agreed manner the individual who so requested.
(2) The costs of all actions of the data controller in relation to request from the previous paragraph shall be borne by the controller.

agreed manner the individual who so requested. The costs of all actions of the data controller in relation to request from the previous paragraph shall be borne by the controller (Article 73 PDPA).

#### *7.1.9.2. Video surveillance*

The provisions of this Chapter shall apply to the implementation of video surveillance, unless otherwise provided by another statute. A public or private sector person that conducts video surveillance must publish a notice to that effect. Such notice must be visible and plainly made public in a manner that enables individuals to acquaint themselves about its implementation at the latest when the video surveillance of them begins.
The notice must contain the following information:
1. that video surveillance is taking place;
2. the title of the person in the public or private sector implementing it;
3. a telephone number to obtain information as to where and for which period recordings from the video surveillance system are stored.
The video surveillance system used to conduct video surveillance must be protected against access by unauthorized persons(Article 74 PDPA) .

##### **7.1.9.2.1. Access to official office premises and business premises**

(1) The public and private sector may according to Article 75 PDPA implement video surveillance of access to their official office premises or business premises if necessary for the security of people or property, for ensuring supervision of entering to or exiting from their official or business premises, or where due to the nature of the work there exists a potential threat to employees. The decision is taken by the competent functionary, head, director or other competent or authorized individual of the person in the public sector or person in the private sector. The written decision must explain the reasons for the introduction of video surveillance. The introduction of video surveillance may also be laid down by statute or a regulation issued pursuant thereto.
Video surveillance may only be implemented in a manner that does not show recordings of the interior of residential buildings that do not affect entrance to their premises, or recordings of entrances to apartments.
All employees of the person in the public or private sector working in the premises under surveillance must be informed in writing of the implementation of video surveillance.
The filing system under this regulation contains a recording of the individual (an image or sound), and the date and time of entry to and exit from the premises, it may also contain the personal name of the recorded individual, the address of his permanent or temporary residence, employment, the number and data on the type of his personal document, and the reason for entry, if the personal data listed are collected in addition to or through the recording of the video surveillance system. Personal data may be stored for a maximum of one year from their creation, and must then be erased, unless otherwise provided for by statute.

##### **7.1.9.2.2. Apartment buildings**

The written consent of joint owners with a share of more than 70% of the ownership is required for the introduction of video surveillance in an apartment building (Article 76 PDPA).
Video surveillance may only be introduced in an apartment building when necessary for the security of people and property.
Video surveillance in apartment buildings may only monitor access to entrances and exits and common areas of apartment buildings. Video surveillance of the housekeeper’s apartment and the workshop for the housekeeper is prohibited.

It is prohibited to enable or implement current or subsequent examination of recordings of video surveillance systems through internal cable television, public cable television, the Internet or the use of other telecommunications means able to transmit such recordings. Entrances to individual apartments may not be recorded by video surveillance systems.

**7.1.9.2.3. Work areas**

Video surveillance within work areas may only be implemented in exceptional cases when necessarily required for the safety of people or property or to protect secret data and business secrets, and where such purpose cannot be achieved by milder means.

Video surveillance may only be implemented for those parts of areas where the above mentioned interests from the previous paragraph must be protected. Video surveillance is prohibited in work areas outside of the workplace, particularly in changing rooms, lifts and sanitary areas. Employees must be informed in advance in writing prior to the commencement of implementation of video surveillance.

Prior to the introduction of video surveillance in a person of the public or private sector, the employer is obliged to consult the representative trade union at the employer.

(6) In the area of national defense, national intelligence-security activities and the protection of secret data, obligation to inform employees and to consult trade unions does not apply (Article 77 PDPA).

***7.1.9.3. Biometrics***

The properties of an individual can be determined or compared through the processing of biometric characteristics so as to identify him or confirm his identity (hereinafter: biometric measures) under the conditions provided by PDPA.

**7.1.9.3.1. Biometric measures in the public sector**

Biometric measures in the public sector may only be provided for by statute if it is necessarily required for the security of people or property or to protect secret data and business secrets, and this purpose cannot be achieved by milder means.

Irrespective of PDPA, biometric measures may be provided by statute where they involve compliance with obligations arising from binding international treaties or for identification of individuals crossing state borders.

**7.1.9.3.2. Biometric measures in the private sector**

The private sector may implement biometric measures only if they are necessarily required for the performance of activities, for the security of people or property, or to protect secret data or business secrets. Biometric measures may only be used on employees if they were informed in writing thereof in advance. If the implementation of specific biometric measures in the private sector is not regulated by statute, a data controller intending to implement biometric measures will prior to introducing the measures be obliged to supply the National Supervisory Body with a description of the intended measures and the reasons for the introduction thereof.

The National Supervisory Body will on receipt of this information be obliged within two months to decide whether the intended introduction of biometric measures complies with PDPA. The deadline may be extended by a maximum of one month if the introduction of such measures would affect more than 20 employees in a person in the private sector, or if the representative trade union at the employer requests to participate in the administrative procedure.

The data controller may implement biometric measures upon receipt of a decision whereby the implementation of biometric measures is permitted. There is no appeal against this decision of the National Supervisory Body, but an administrative dispute is permitted (Article 80 PDPA).

**7.1.9.3.3. Biometric measures in connection with public sector employees**

Irrespective of the provision mentioned above, biometric measures may be implemented in the public sector in connection with entry into a building or parts of a building and recording the presence of employees at work, and they can be implemented with the mutatis mutandis application of the biometric measures in the private sector (Article 81 PDPA).

***7.1.9.4. Records of entry to and exit from premises***

Persons in the public or private sector may, for the purposes of protecting property or the life and bodies of individuals, and order in their premises, require individuals intending to enter or leave such premises to state all or some of the personal data (as defined further) and the reason for entry or exit. If required, the personal data may be verified by examining a personal document of the individual. The records of entry and exit may only contain the following personal data for individuals:
personal name, number and type of personal document, address of permanent or temporary residence, employment, and the date of, time of and reason for entry or exit to or from the premises.
Records are regarded as official records in accordance with the statute regulating the general administrative procedure, if the acquisition of data is required in terms of benefiting a minor or for the implementation of the competences of the police, and intelligence-security activities. Personal data from these records may be stored for a maximum of three years from their recording, and then shall be erased, unless otherwise provided by statute (Article 82 PDPA).

***7.1.9.5. Public books and protection of personal data***

Personal data from public books regulated by statute may only be used in accordance with the purpose for which they were collected or are processed, if the statutory purpose of their collection or processing is defined or definable (Article 83 PDPA).

Filing systems from official records and public books may be linked if so provided by statute. Data controllers or a data controller linking two or more filing systems kept for different purposes shall be obliged to inform the National Supervisory Body in writing thereof in advance. If at least one filing system to be linked contains sensitive data, or if the linking would result in disclosure of sensitive data, or if implementation of the linking requires the use of the same connecting code, linking shall not be permitted without the prior permission of the National Supervisory Body. The National Supervisory Body permits linking on the basis of a written application of the data controller if it determines that the data controller ensures adequate protection of personal data. There is no appeal against decisions from the previous paragraph, but an administrative dispute shall be permitted (Article 84 PDPA).

According to Article 85 of PDPA linking filing systems from criminal record and minor offence records to other filing systems, and linking filing systems from criminal records and minor offence records, is prohibited. Data on linked filing systems from official records and public books shall be kept separately in the Register of Filing Systems.

## 7.2. Durchsetzungsrechte der Datenschutzanliegen für Betroffene

### 7.2.1. General

In addition to the right to information (7.1.8.), the data controller must, on the request of an individual to whom personal data relate, **supplement, correct, block or erase personal data which the individual proves as being incomplete**, inaccurate or not up to date, or that they were collected or processed contrary to statute. On the request of the individual the data controller must inform all data recipients and data processors to whom the controller has supplied the personal data of the individual, before these measures have been carried out, of their supplementation, correction, blocking or erasure. Exceptionally the data controller is not obliged to do this if it would incur large costs, disproportionate efforts or would require a large amount of time.

The data controller is obliged to perform the supplementing, correction, blocking or deletion of personal data **within 15 days of the date of receipt of the request**, and to inform the person who lodged the request thereof, or within the same interval to inform him of the reasons why he will not do so. The controller must decide on an objection within the same deadline.

The data controller of such databases **must enable access to the individual free of charge** within fifteen days of receiving his or her request, as well as provide a copy of an individual's personal data within thirty days of receiving the request. If a data controller fails to fulfill this obligation, he or she must provide a motivation for doing so in writing. In case an individual's personal data are transferred to recipients, the data controller must supply, at that individual's request, the list of recipients within a thirty-day deadline.

If the data controller concludes on his own that the personal data are incomplete, inaccurate or not up to date, he has to supplement or correct them and **inform the individual thereof, unless otherwise provided by statute**. Costs relating to the supplementing, correction and erasure of personal data, and of the notification and decision on the objection, shall be borne by the data controller.

### 7.2.2. Judicial protection of the rights of the individual

An individual who finds that his rights provided by PDPA have been violated may request judicial protection for as long as such violation lasts. If the violation ceases, the individual may file a suit to rule that the violation existed if he is not provided with other judicial protection in relation to the violation.

The **competent court decides** in the procedure under the provisions of the statute regulating administrative disputes unless otherwise provided by PDPA. The procedure is not public unless the court decides otherwise at the suggestion of the individual for well-founded reasons. The procedure is urgent and a priority.

In a suit filed due to violations of rights from PDPA, an **individual may request the court to bind the data controller**, until a final decision is issued in the administrative dispute, to prevent any kind of processing of the disputed personal data, if their processing could cause with difficulty reparable damage to the individual, to whom the personal data relate, while the postponement of processing should not be contrary to the public interests and neither is there any danger of greater irredeemable damage being done to the opposing party.

**The rights of an individual from PDPA may exceptionally be restricted by statute** for reasons of protection of national sovereignty and national defence, protection of national security and the constitutional order of the state, security, political and economic interests of the state, the exercise of

the responsibilities of the police, the prevention, discovery, detection, proving and prosecution of criminal offences and minor offences, the discovery and punishment of violations of ethical norms for certain professions, for monetary, budgetary or tax reasons, supervision of the police, and protection of the individual to whom the personal data relate, or the rights and freedoms of others. Restrictions may only be provided in the extent necessary to achieve the purpose for which the restriction was provided.

## 7.3. Nationale Aufsichtsbehörde

With the merger of two offices, the Inspectorate for Personal Data Protection and the Commissioner for Access to Public Information, **the Information Commissioner** (IC), an autonomous and independent body, was established on the basis of the Information Commissioner Act (ICA) on December 31, 2005.[464] The body supervises both the protection of personal data and access to public information. The competencies of the Information Commissioner[465], as laid down in ICA, Personal Data Protection Act (PDPA) and Inspection Act[466] (IA), are relatively wide.

According to Article 2 ICA **the Information Commissioner is an autonomous and independent state body, competent for**:
- **deciding on the appeal against the decision** with which a body refused or dismissed the applicant's request for access or violated the right to access or re-use of public information in some other way, and within the frame of appellate proceedings also for supervision over implementation of the Act regulativ the access to public information and regulations adopted there under,
**- inspection supervision over implementation of the Act and other regulations**, governing protection or processing of personal data or the transfer of personal data from Slovenia, as well as carrying out other duties, defined by these regulations,
- **deciding on the appeal of an individual** when the data controller refuses his request for data, extract, list, examination, confirmation, information, explanation, transcript or copy in accordance with provisions of the Act governing personal data protection.
**The Information Commissioner is an independent body, competent for supervision over ICA and PDPA.**

The Information Commissioner has further the following competencies:
- organizes and manages the work of all employees, including the national supervisors for personal data protection;
- carries out other competencies of the head of the state body;
- conducts supervision in accordance with the Act governing personal data protection.

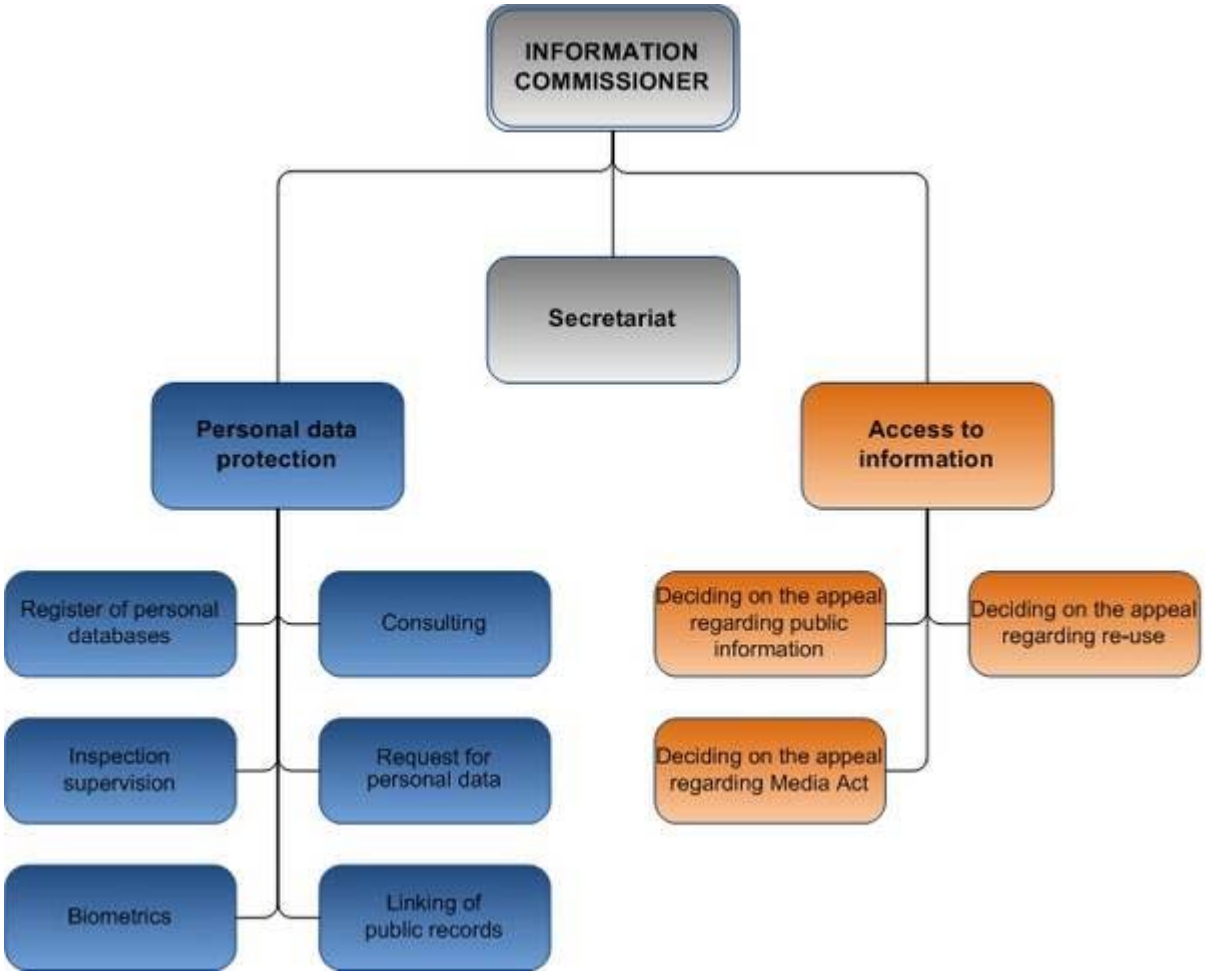
The structure of the Information Commissioner's office is as follows:

---

464 Information Commissioner Act, published in Official Gazette of the Republic of Slovenia, no.113/2005 as of 16 December 2005

465 When another Slovenian Act or regulation use terms "Chief National Supervisor", "National supervisory body for personal data protection" or "Commissioner for access to public information" these terms now mean "Information Commissioner".

466 The Inspection Act (Official Gazette of the Republic of Slovenia, no.43/07).




### 7.3.1. Zusammensetzung, Ernennung und Eingliederung der Behörde

The Information Commissioner is **appointed by the National Assembly** of the Republic of Slovenia on proposal of the president of the Republic of Slovenia. Information Commissioner is appointed for **a five year's term** and can be reappointed once.
The seat of Information Commissioner is in Ljubljana and he/she has the status of officer of state. Information Commissioner establishes his organizational structure with standing orders and other general acts.

The Information Commissioner employs **National Supervisors** for personal data protection (hereinafter: Supervisors). Supervisors are appointed by Information Commissioner in accordance with the Civil Servants Act. Information Commissioner has also an expert and administrative-technical staff.

The Information Commissioner can file to the **Constitutional Court of the Republic of Slovenia** a request for constitutional review of a statute, of other regulations and general acts, adopted to perform public powers, in case of questions of constitutionality and legality in connection with a procedure being dealt with.

The Information Commissioner sends **an annual report** on his work to the National Assembly at the latest until 31. May for the previous year and publishes the report on his web site[467]. The annual report consists of data on previous year's activities as well as estimates and recommendations in the area of personal data protection and access to public information (Articles 4- 14 PDPA).

### 7.3.2. Gewährleistung der Unabhängigkeit

Information Commissioner is **appointed by the National Assembly of the Republic of Slovenia** on proposal of the president of the Republic of Slovenia. For the appointment as Information Commissioner, a person must fulfil the following conditions:

- be **a citizen** of the Republic of Slovenia;

- hold a **university degree**;

- have at least **five years of working experience**;

- **must not have been convicted** by a final decision of a criminal offence punishable by an unconditional punishment of deprivation of liberty.

Information Commissioner is appointed for a five year's term and can be **reappointed once.**

Funds for Information Commissioner's operation are provided from the **Budget of the Republic of Slovenia** and shall be **determined by the National Assembly** of the Republic of Slovenia **on proposal** of the Information Commissioner.

Information Commissioner has the status **of officer of state and he may be subject to early dismissal** by the National Assembly of the Republic of Slovenia only if:

- he himself so **demands**,

- if he **no longer fulfils the conditions** for execution of the function determined in the Article 6(2)[468] of ICA.

- if he becomes **permanently incapable** of performing his function,

- if he **neglects to execute his powers** in accordance with the Law and Constitution.

The procedure for the **dismissal of the Information Commissioner shall be started on proposal of the president of the Republic of Slovenia**.

### 7.3.3. Zuständigkeitsbereich

Information Commissioner is an autonomous and independent body, established on 31 December 2005, with the Information Commissioner Act. The body **supervises both the protection of personal**

---

467 Annual Reports are available here: www.ip-rs.si/index.php (13.09.2010).

468 Article 6 (2): "For the appointment as Information Commissioner, a person must fulfil the following conditions: - be a citizen of the Republic of Slovenia; - hold a university degree; - have at least five years of working experience; - must not have been convicted by a final decision of a criminal offence punishable by an unconditional punishment of deprivation of liberty.

**data, as well as access to public information.** Competencies of the Information Commissioner based on the Information Commissioner Act are:

1. **deciding on the appeals** against the decisions by which another body has refused or dismissed the applicant's request for access, or violated the right to access or re-use public information; in the context of appellate proceeding the Information Commissioner is also responsible for **supervising the implementation of the Act governing access to public information** and regulations adopted within the framework of appellate proceedings;
2. **exercising inspection supervision** of the implementation of act and other regulations which regulate **processing and protection of personal data** and transfer of personal data from Republic of Slovenia;
3. exercises other tasks defined by these provisions;
4. **deciding as appellate body on individuals' complaints** when controller of personal data refuses his request for access to data relating to him or request for extract, list, examination, confirmation, information, explanation, transcript or copy in accordance with provisions of the act governing personal data protection;
5. as offence body the Information Commissioner **supervises implementation of Information Commissioner Act, Access to Public Information Act** in the context of Appellate proceeding and **Personal data protection Act** (Art. 2 of Information Commissioner Act and Art. 32 of Access to Public Information Act).

### 7.3.4. Aufgaben und Kompetenzen

Competencies of the Information Commissioner under the Personal data protection Act, are:

1. **performing supervision over the implementation** of the provisions of Personal data protection Act (PDPA), (handle cases of complaints, appeals, notifications and other applications, explaining possible breach of law);

2. **issuing supervision measures based on Art. 54 of PDPA** (prohibition to process personal data, anonymization, blocking, erasing or destroying personal data, when established that the data is not processed according to the law).

3. issuing **other supervision measures** in accordance with the Act governing inspection supervisions and the Act governing general administrative procedure (Point 5, Para. 1 Art. 54 of PDPA);

4. performing **preventive supervision** with personal data **controllers in public and private sectors;**

5. managing and maintain a **register of personal databases**, ensure its updating and public internet access (Art. 28 of PDPA);

6. **ensure viewing and transcription of data from the database register** (as a rule on the same day or in eight days at the latest – Art. 29 of PDPA);

7. performing procedures with regard to **violations in the field of personal data protection** (expedient procedure);

8. **filing a criminal information** or perform procedures in accordance with the Act governing violations, if during an inspection, **a suspicion of criminal offence** or violation arises;

9. deciding on **an individual's complaint with regard to processing of personal data** based on Art. 9(4)[469] and Art. 10(3)[470] of PDPA;

10. **issuing decisions on ensuring an adequate level** of personal data protection in third countries (Art. 63[471] of PDPA);

11. **performing procedures of assessing an adequate level of personal data protection in third countries** based on findings of supervisions and other information (Art. 64[472] of PDPA);

---

469 Article 9 (4) states that "personal data may in exceptions be processed in the public sector where they are essential for the exercise of lawful competences, duties or obligations by the public sector, provided that such processing does not encroach on the justified interests of the individual to whom the personal data relate".

470 Article 10 (3) states that "personal data may be processed in the private sector if this is essential for the fulfilment of the lawful interests of the private sector and these interests clearly outweigh the interests of the individual to whom the personal data relate.

471 Article 63 states following: "(1) The supply of personal data that are processed or will be processed only after being supplied to a third country, shall be permitted in accordance with the provisions of this Act and provided that the National Supervisory Body issues a decision that the country to which the data are transferred ensures an adequate level of protection of personal data. (2) The decision from the previous paragraph shall not be required if the third country is on the list of those countries from Article 66 of this Act that have been found to fully ensure an adequate level of protection of personal data. (3) The decision from the first paragraph of this Article shall not be required if the third country is on the list of those countries from Article 66 of this Act that have been found in part to ensure an adequate level of protection of personal data, if those personal data are transferred and for those purposes for which an adequate level of protection has been found."

472 Article 64 states procedure for determining an adequate level of protection of personal data:

"(1) The National Supervisory Body shall initiate a procedure to determine an adequate level of protection of personal data in a third country on the basis of a conclusion of inspection supervision or at the suggestion of a natural person or legal person who can show a legal interest in the issuing of a decision.(2) At the request of the National Supervisory Body, the Ministry responsible for foreign affairs shall obtain from the competent body of a third country the necessary information as to whether such country ensures an adequate level of protection of personal data. (3) The National Supervisory Body may obtain additional information on the adequate level of protection of personal data in a third country directly from other supervisory bodies and the competent body of the European Union. (4) The National Supervisory Body shall issue a decision within two months of receipt of full information from the second and third paragraphs of this Article. It may also issue a decision only for a certain type of personal data or for their processing for an individual purpose. (5) The National Supervisory Body shall be obliged no later than within 15 days of the issuing of a decision that a third country fails to ensure an adequate level of protection of personal data to inform the competent body of the European Union in writing."

12. **managing a list of third countries** ascertained to have partially or entirely adequate or inadequate personal data protection levels; in case only a partial adequacy of personal data protection is ascertained, the list will also state the scope of adequate protection (Art. 66[473] of PDPA).

13. managing administrative procedures to issue **permissions to transfer personal data to a third country** (Art. 70[474] of PDPA);

---

473 Article 66 PDPA: "(1) The National Supervisory Body shall maintain a list of third countries for which it finds that have fully or partly ensured an adequate level of protection of personal data, or have not ensured such protection. If it has been determined that a third country only partly ensures an adequate level of protection of personal data, the list shall also set out in which part an adequate level has been ensured.

(2) The Chief National Supervisor shall publish the list from the previous paragraph in the Official Gazette of the Republic of Slovenia."

474 Article 70 PDPA: "(1) Irrespective of the first paragraph of Article 63 of this Act, personal data may be transferred and supplied to a third country, if: 1. so provided by another statute or binding international treaty; 2. the individual to whom the personal data relate gives personal consent and is aware of the consequences of such supply; 3. the transfer is necessary for the fulfilment of a contract between the individual to whom the personal data relate and the data controller, or for the implementation of pre-contractual measures adopted in response to the request of the individual to whom the personal data relate; 4. the transfer is necessary for the conclusion or implementation of a contract to the benefit of the individual to whom the personal data relate, concluded between the data controller and a third party; 5. the transfer is necessary in order to protect from serious danger the life or body of an individual to whom the personal data relate; 6. the transfer is performed from registers, public books or official records which are intended by statute to provide information to the public and which are available for consultation by the general public or to any person who demonstrates a legal interest that in the individual case the conditions provided by statute for consultation have been met; 7. the data controller ensures adequate measures of protection of personal data and of the fundamental rights and freedoms of individuals, and declares the possibility of their fulfilment or protection, especially in the provisions of contracts or in the general terms of business.

(2) In the case of transfer of personal data under subparagraph 7 of the previous paragraph, the person intending to transfer personal data must obtain a special decision from the National Supervisory Body permitting the transfer of personal data.

(3) The person may transfer personal data only upon receipt of the decision from the previous paragraph permitting transfer.

(4) There shall be no appeal against a decision from the second paragraph of this Article, but an administrative dispute shall be permitted. The administrative dispute procedure shall be urgent and a priority.

(5) The National Supervisory Body shall be obliged no later than within 15 days of the issuing of a decision from the second paragraph of this Article to communicate it to the competent body of the European Union and to the Member States of the European Union.

(6) If the competent body of the European Union decides upon receipt of a decision that the transfer on the basis of a decision from the second paragraph of this Article is not permissible, the National Supervisory Body shall be bound by that body's decision, and shall be obliged within five days of receipt of such decision to issue to the person from the second paragraph of this Article a new decision prohibiting him from making further transfer of personal data."

14. managing administrative procedures to issue **permissions to link public records and registers**, in cases when one of the personal databases to be linked, contains sensitive personal data or if implementation of the linking requires the use of the same connecting code (such as the EMŠO – the standardized personal registration number or tax number);

15. managing administrative procedures to issue **declaring decisions on whether a planned implementation of biometric measures in private sector is accordant with the provisions of PDPA**;

16. **working with government bodies, competent EU bodies for protection of individuals** with regard to processing personal data, international organizations, foreign personal data protection bodies, institutions, associations, and other bodies and organizations with regard to questions of personal data protection;

17. issuing and **publishing preliminary opinions** to state bodies and public powers holders on harmonizing the provisions of proposals of legislation with Acts and other legislation governing personal data;

18. issuing and **publishing non-obligatory opinions** on conformity of professional ethics codes, general conditions of business or the proposals thereof, with regulations in the field of personal data protection;

19. preparing, issuing and **publishing non-obligatory recommendations** and instructions with regard to personal data protection in a particular field;

20. the **publication on the internet page** or in another appropriate manner of preliminary opinions on compliance with positive Acts and other legislation of proposals of Acts and other regulations in the field of personal data protection as well as publication of requests for constitutional review of statutes, issue internal bulletin and expert publications, publish decisions and court resolutions dealing with personal data protection, as well as non-obligatory opinions, explanations, positions and recommendations with regard to personal data protection (Art. 49[475] of PDPA);

---

[475] Publicity concerning work according Article 49 PDPA:

"(1) The National Supervisory Body may:

1. issue an internal journal and professional literature;

2. on the website or in another appropriate manner publish the prior opinion from the first paragraph of Article 48 of this Act, after the statute or other regulation has been adopted and published in the Official Gazette of the Republic of Slovenia, in the journal of a self-governing local community or publish it in another lawful manner;

3. on the website or in another appropriate manner publish requests from the second paragraph of Article 48 of this Act, after the Constitutional Court has received them;

4. on the website or in another appropriate manner publish decisions and rulings of the Constitutional Court on requests from the second paragraph of Article 48 of this Act;

5. on its website or in another appropriate manner publish decisions and rulings of courts of general jurisdiction and the Administrative Court relating to the protection of personal data, such that it is not possible to read from them the personal data of parties, injured parties, witnesses or experts;

21. **issuing press releases** on performed supervisions and prepare annual reports on its work in the current year;

22. **Information Commissioner is an appellate body**, competent for supervision over implementation of Information Commissioner Act, Act on access to public information within the frame of its appellate proceedings and the Act on personal data protection;

23. **deciding on the appeal of an individual** when the data controller refuses his request for access to data relating to him or request for extract, list, examination, confirmation, information, explanation, transcript or copy in accordance with provisions of the Act governing personal data protection (competency established in the Information Commissioner Act);

24. Information Commissioner also **participates in working groups for personal data protection, formed within the EU framework** and bringing together independent bodies for protection of personal data in member states (Working party 29 based on Directive 95/46/EC; supervisory bodies dealing with processing of personal data in Schengen information system, Customs information system and Europol; and Eurodac Supervision Coordination Group);

**Access to Public Information Act**[476] defines additionally also the competency of the Information Commissioner to **keep records of all granted exclusive rights to re-use information** (Art. 36a(5) of Access to Public Information Act).

**The IC may file a request to the Constitutional Court of the Republic of Slovenia** to assess the constitutionality of statutes, other regulations and general acts issued to exercise public powers if the question of constitutionality and lawfulness arises in connection with a procedure it conducts (in cases rearding access to public information and personala data protection).

The Information Commissioner also **manages and maintains the Register of data filing systems of data controllers** (Article 28 of the PDPA), which is available at the Commissioner's website.[477]

Under **the Access to Public Information Act**[478], Information Comissioner is:

---

6. issue non-binding opinions on the compliance of codes of professional ethics, general terms of business or drafts thereof with regulations in the area of the protection of personal data;

7. issue non-binding opinions, clarifications and positions on issues in the area of protection of personal data, and publish them on the website or in another appropriate manner;

8. prepare and issue non-binding instructions and recommendations regarding protection of personal data in individual fields;

9. issue public statements on inspection supervision undertaken in individual cases;

10. hold media conferences relating to the work of the National Supervisory Body and publish transcripts of statements or recordings of statements from media conferences on the website;

11. publish other important announcements on its website.

476 The Access to Public Information Act, Official gazette of RS, UL RS, p. 24-900/2003 (p. 2786), 7.3.2003 (consolidated text Uradni list RS, no. 51/2006,).

477 The Information Commissioner's website: http://www.ip-rs.si/

478 The Access to Public Information Act, op. cit.,

- **deciding on the appeals against the decisions** by which another body has refused or dismissed the applicant's request for access, or violated the right to access or re-use public information,
- **supervising the implementation of** the Act governing access to public information and regulations adopted within the framework of appellate proceedings.

Competencies of the Information Commissioner under **the Electronic Communications Act**[479], are:

1. performing supervision over the **storage of traffic and location data**, which are acquired or processed in relation to provision of public communications networks or services in accordance with the Art. 107a -107e of the Act (in accordance with Art. 112(2) of the Electronic Communications Act);

2. deciding, within the sphere supervised, on offences of this Act and regulations thereof, acting as offence body , in compliance with Act, governing the offences. For the offences of this Act Information Commissioner may impose a fine in the amount, higher than the minimum prescribed fine for each offense, acting as offence body (in accordance with Art. 147 of the Electronic Communications Act);

3. Information Commissioner also acts to prevent the misuse of and the lawful implementation of Directive on privacy and electronic communications 2002/58/EC and the new proposal of Directive on retention on traffic telecommunications data, adopted on 15.12.2005 in Brussels.

Competencies of the Information Commissioner under **the Act on Patient's Rights**[480] are:

1. deciding in **appellate proceeding on appeals filed by patients and other eligible persons against infringement of the provisions regulating the procedure of access to medical files**. The provider of medical services is considered in this procedure as first instance body (in accordance with Art. 41(10) of Act on patient's rights);

2. **deciding in appellate proceeding on appeals** against partial or **complete refusal of request for access to medical files** after patients death which have been filed by eligible persons (in accordance with Art. 42(5) of Act on patient's rights);

3. deciding on appeals filed by eligible persons against partial or complete refusal of request for access relating to the duty of **protection of information on patient's health status** when these information originate from medical files (in accordance with Art. 45(7) of Act on patient's rights).

Competencies of the Information Commissioner under the **Passports Act** are:

1. performing supervision over the implementation of the provision of Art. 4 a, which governs when and how **data controllers may photocopy passports** and regulates ways of retention of such photocopies;

2. **performing procedures** with regard to violations of Art. 4 a (in accordance with Art. 34 a).

---

479 The Electronic Communications Act (Uradni list RS, no. 43/04).

480 The Act on Patient's Rights Zakon o pacientovih pravicah, Uradni list RS, no. 15/2008, 11. 2. 2008.

Competencies of the Information Commissioner based on the **Identity Card Act** are:

1. performing supervision over the implementation of the provision of Art. 3 a, which governs when and how **data controllers may photocopy identity cards** and regulates ways of retention of such photocopies;

2. **performing procedures** with regard to violations of Art. 3 a (in accordance with Art. 19 a).

Competencies of the Information Commissioner under **the Banking Act**[481] are:

1. giving consent to administrators to manage the SISBON system prior to the application of the internal policies guiding the **technical conditions for accessing the system** by the members and other **measures for protection of personal data**;

2. performing supervision over Article 309.a of the Banking Act, which regulates **the collection, processing and system for exchanging the information on the credit standing of the customers** (the SISBON system), and performing procedures with regard to violations of Art. 309.a.

Convention of 19 June 1990 implementing the **Schengen agreement** of 14 June 1985[482]):

The Information Commissioner has with the entry of Republic of Slovenia in the Schengen area as of 21. 12. 2007 in accordance with Art. 114 of the Schengen convention also become designated supervisory authority **responsible for carrying out independent supervision of the national section of Schengen information system** and for checking that the processing and **use of data** entered in the SIS does not violate the rights of the data subjects. Any person has the right to ask the supervisory authorities to check data entered in the SIS which relate to them and the use of these data. This right is governed by the national law of the contracting party to which the request is made. In Slovenia Personal data protection act and Information commissioner act regulate this.

### 7.3.5. Weitere Hinweise

In an **annual report for the past year 2009**, the Information Commissioner noted that the number of complaints and handled matters in both working areas - the right of access to public information and the right to the protection of personal data - **increased**. The Commissioner estimates that this is a result of increasing awareness of individuals of the existence and respect of the data protection as constitutional right.

Commissioner notes that the complaints she receives are becoming more demanding and complex. Last year, the Commissioner resolved more than 600 inspection matters, around two-thirds of which were in private sector, and about one hundred inspection procedures were initiated ex officio, meaning that **the Commissioner reviews randomly selected data controllers who process a great amount of personal data**. Due to breaches of the provisions of the Personal Data Protection Act, the Commissioner initiated more than 160 violation procedures and issued almost 60 warnings, slightly less than 70 cautions and 26 fines. One of the latter was the **highest ever issued fine in the amount** of

---

481 The Banking Act, Zakon o bančništvu, Ur.l. RS, no. 131/2006.

482 Schengen agreement, OJ L 239/2000 with amendments.

112,000 Euros. The most common violations are illegal processing of personal data, inappropriate protection of personal data, misuse of personal data for direct marketing purposes, and illegal video surveillance. Growing awareness of the right to protection of personal data is also reflected in a number of published opinions and responses, which - in comparison with the previous year - increased by nearly a half. The most frequently asked questions covered areas of official proceedings (judicial, administrative, police) and employment relationships.

The Commissioner has pointed out that practically since the beginning of its operation there is a **lack of legislation on protection of privacy in the workplace**, which would lay down the foundations for questions like control and use of e-mail and mobile phones etc. Due to the lack of such initiative, last year the Commissioner decided to prepare the framework of Privacy in the Workplace Act.

### 7.4. Rolle der Organisationen zum Schutz der Betroffenen

Proceedings in accordance with the Personal Data Protection Act:

Every individual is entitled to **file an application to the Information Commissioner** if he believes that a person (either public or private) is infringing on the Personal Data Protection Act. The Information Commissioner can according to his official duties on the basis of the Inspection Act start all appropriate inspection proceedings.

The individual must file an application, pertaining to any acts relating to notification of the individual with regard to processing of personal data, in writing or by verbal dictation with the personal data controller. The controller must **enable the individual to view and transcribe personal data** according to the points 1 and 2 of the Article 19 of the PDPA at the latest in 15 days from the day of the received application or within the same time-limit notify the individual in writing on the reasons for the refusal of viewing and transcription[483].

The similar is also valid for the extract from point 3 and a list from point 4 of Article 19 of the PDPA which the filing system controller must provide to the individual in 30 days from the day of the receipt of the application or notify him in the same time on reasons for the refusal to provide the extract or the list. In case when the personal data controller fails to notify the individual in the prescribed time on its decision it is deemed that the application has been refused.

The state supervisory body for personal data protection (Information Commissioner) must allow everyone to examine the Register of personal databases and to copy its contents. The examination and copying must, as a rule, be allowed **on the same day** and **at the latest in 8 days**, or it shall be deemed that the request was denied.

The **personal data controller must on an individual's request**:

1. **enable the examination** of the personal database's catalogue;
2. **confirm whether the data** in connection with an individual **is or is not being processed**, and enable the individual examination thereof, as well as its transcription or copying;
3. **transmit a copy of personal data**, contained in the personal database, referring to the individual;
4. **transmit a list of users**, the data was transmitted to, when, on which legal grounds and for what purpose;

---

[483] For the provisions about informing the individual of the processing of personal data see above.

5. **give information on sources**, on which the database entries referring to an individual are based, and on the method of processing;
6. **give information on purpose** of processing and type of personal data being processed, as well as all necessary pertaining explanations;
7. **explain technical or logically-technical** decision procedures in case automated decision-making of an individual's data is being performed.

### 7.5. Mögliche und vorgeschriebene Aktivitäten der Datenbearbeiter (private und öffentliche)

The PDPA defines in detail the **duties of the data controller**. Data controller is a natural person or legal person or other public or private sector person which alone or jointly with others determines the purposes and means of the processing of personal data or a person provided by statute that also determines the purposes and means of processing. It is prohibited to use the same identifier in databases maintained in the areas of public safety, state security, defense, judiciary and health. The connection between these databases is allowed only if there is a legal basis or the individual has given his or her written consent.

The data controller must keep a separate catalogue for each database, which contains, among other things, a detailed description of the kind of data gathered and the manner in which they are gathered, the purpose of their use and the **duration of storage**, the list of their users and a description of how they are secured. Furthermore, the Ministry of Justice, which is responsible for the protection of personal data, must keep a register of all databases containing personal data. Information in this register is provided by data controllers and is publicly available on the Internet.

According to Personal Data Protection Act (Articles 26-28 PDPA), **the obligations of data controllers are:**

1. To **report personal data filing systems to the register** managed by the Information Commissioner,
2. To assure effective protection of personal filing systems,
3. To adopt **detailed internal regulations** governing the protection of personal data,
4. Prior to starting **video surveillance**, to post a **visible notice and** acquire **opinion from the syndicate representatives**,
5. Prior to starting **biometric measures**, the employees must be **notified** in writing and the Commissioner must issue a decision to this end,
6. In case when two or more filing systems are being linked, the Information Commissioner must be notified,
7. In case when **sensitive personal data is being linked** the information Commissioner must issue a decision to this end,
8. In case the **data is being transferred to third countries** the information Commissioner must issue a decision to this end.

# 8. Benelux: Holland

## 8.1. Grundsätze des Datenschutzes

### 8.1.1. Introduction

The most important rules for recording and using personal data have been set forth in the Dutch Data Protection Act[484] (in Dutch: *Wet bescherming persoonsgegevens* or *Wbp*)[485]. The Data Protection Act came into force on 1 September 2001 and replaces the Personal Data Files Act (in Dutch: *Wet Persoonsregistraties* or *Wpr*). Other acts that govern the use of personal data in the Netherlands are the Data Protection Police Files Act (in Dutch: *Wet politieregisters*[486]) and the Municipal Database Personal Records Act (in Dutch: *Wet gemeentelijke basisadministratie*[487]). Besides the abovementioned acts, there are also a number of codes of conduct and self-regulations that guarantee compliance with the data protection legislation.

The Data Protection Act (hereinafter also referred to as the Act) regulates how companies, authorities and institutions are to deal with processing personal data. The Act does not apply to processing of data carried out as a purely personal or household activity.

The Dutch Data Protection Act relates to every use - 'processing' - of personal data, from the collection of these data up to and including the destruction of personal data.

Pursuant to the Dutch Data Protection Act, the processing of personal data is every action or every aggregate of actions relating to these personal data. Thus, it is a very broad term. The Dutch Data Protection Act specifies in article 1 of the Act, a number of actions that are indicated as processing: collecting, recording, grouping, keeping, updating, changing, retrieving, consulting, using, transferring, distributing, making available, putting together, linking, screening, deleting, and destroying data. Processing can consist of one or more of these actions. Processing actions that are considered as a unit are seen as a single data processing operation on the basis of common opinion. For example, client records or complaint registration is considered as a single data processing operation.

The Act uses two important definitions (article 1 under d and e). First, the ‘responsible party‘ which means the natural person, legal person, administrative body or any other entity which, alone or in conjunctions with others, determines the purpose of and means for processing personal data. Second, the ‘processor’ which means the person or body that processes personal data for the responsible party, without coming under the direct authority of that party.

In article 4 of the Dutch Data Protection Act it is stated that the Act applies to the processing of personal data carried out in the contact of the activities of an establishment of a responsible party in the Netherlands or to the processing of personal data by or for responsible parties who are not

---

484 Act of 6 July 2000, Bulletin of Acts, orders and decrees 302, containing rules regarding the protection of personal data (Dutch Data Protection Act), as amended by Acts dated 5 April 2001, Bulletin of Acts, Orders and Decrees 180, 6 December 2001.

485 An unofficial English translation of the Dutch Data Protection Act is available at: http://www.dutchdpa.nl/Pages/en_ind_wetten_wbp_wbp.aspx (17.08.2010).

486 Available in Dutch at: www.overheid.nl.

487 Available in Dutch at: www.overheid.nl.

established in the European Union, whereby use is made of automated or non-automated means situated in the Netherlands, unless those means are used only for forwarding personal data. Responsible parties who are not established in the European Union are prohibited from processing personal data unless they designate a person or body in the Netherlands to act on their behalf in accordance with the provisions of the Act.

The Dutch Data Protection Act also governs the tasks and powers of the supervisor of the act, the Dutch Data Protection Authority. As a national supervisory authority, the Dutch Data Protection Authority is the successor of the former *Registratiekamer*. The Dutch Data Protection Authority is authorized to impose sanctions.[488]

The supervisory authority, the Dutch Data Protection Authority (in Dutch: *College Bescherming Persoonsgegevens* or *CBP*)[489] must be **notified** of all processing of personal data. The Dutch Data Protection Authority keeps a public register of these notifications. However, a large number of socially well known and accepted processing operations have been exempted from the notification obligation. On their web site, the Dutch Data Protection Authority offers a checklist for the use of the exemption decree.[490]

Organizations can also appoint their own internal supervisor, the **Data Protection Officer**.[491]

### 8.1.2. Principles

The principles governing the processing of personal data are laid down in Chapter two Section 1 'Conditions for the lawful processing of personal data, Processing of personal data in general' of the Dutch Data Protection Act. According to articles 6-15 Dutch Data Protection Act, data shall be processed fairly, in a proper and careful manner and lawfully. Personal data shall be collected for specified, explicit defined and legitimate purposes and personal data shall not be processed in a way that is inconsistent with the purposes for which they have been collected.

Personal data shall not be kept in a form which allows the data subject to be identified for any longer than is necessary for achieving the purposes for which they were collected or subsequently processed. The controller shall take measures to ensure that personal data, taking into account the purposes for which they are processed, are adequate, correct, accurate, sufficient, relevant and not excessive.

#### *8.1.2.1 Role of the appropriation of data processing*

Personal data shall be collected for specified, explicit defined and legitimate purposes. Personal data may only be processed if and insofar as such is consistent with at least one of the following legal grounds:[492]
a. the data subject has unambiguously given his consent for the processing of personal data;
b. processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

---

488 See also and in more detail question 1.3.
489 See www.cbpweb.nl, partly available in English (17.08.2010).
490 See also and in more detail question 1.5.
491 See also and in more detail question 1.5.
492 See article 8 Dutch Data Protection Act.

c. processing of personal data is necessary in order to comply with a legal obligation to which the responsible party is subject;
d. the processing of personal data is necessary in order to protect a vital interest of the data subject;
e. processing of personal data is necessary for the proper performance of a public law duty by the administrative body concerned or by the administrative body to which the data are provided , or
f. the processing is necessary for upholding the legitimate interests pursued by the controller or by of a third party to whom the personal data are disclosed, except where such interests are overridden by the fundamental rights and freedoms of the data subject, particularly the right to protection of individual privacy.
Personal data shall not be processed in a way that is inconsistent with the purposes for which they have been collected.

#### *8.1.2.2. Principles of data processing (legality, loyal and believe, proportionality, thrift)*

The controller shall, according to article 11 of the Dutch Data Protection Act, take measures to ensure that personal data, taking into account the purposes for which they are processed, are adequate, relevant and not excessive. Besides this, the responsible party shall take the necessary steps to make sure that the personal data, given the purposes for which they are collected or subsequently processed, are correct and accurate.

### 8.1.3. Visibility/transparency, consent

If personal data are obtained from the data subject, the responsible party shall inform the data subject about his identity and the purposes of the processing of the personal data of the data subject, unless the responsible party may assume on reasonable grounds that the data subject is already cognizant of this (see article 33 *et seq.* of the Dutch Data Protection Act). This obligation to provide information shall be fulfilled before the data are obtained. If the personal data are obtained in any other way, the responsible party shall inform the data subject of this at the time of undertaking the recording of the data, or, if the personal data are destined to be provided to a third party, at the time when the data are first disclosed. The obligation does not apply if the data subject is already aware of this or if the provision of such information to the data subject proves impossible or could involve a disproportionate effort. In that case the origin of the personal data shall be recorded. Nor does the obligation apply if the recording or provision of the data is prescribed by or under the law.
If, in view of the nature of the data, the circumstances in which they are obtained or the use that is made of them, such is vital to the safeguarding of the fair and careful processing of personal data, additional information shall be provided to the data subject besides the information referred to before.

### 8.1.4. Particularly sensitive data processing

Chapter two, Section 2 'Conditions for the lawful processing of personal data, processing of special personal data' deals with sensitive data processing (articles 16-24 Dutch Data Protection Act). It is forbidden to process personal data concerning a person's religion or philosophy or life, race, political persuasion, health and sexual life, or personal data concerning trade union membership, except as otherwise provided in Chapter two, Section 1 of the Dutch Data Protection Act.[493] This prohibition also

[493] Article 16 Dutch Data Protection Act.

applies to personal data concerning a person's criminal behavior, or unlawful or objectionable conduct connected with a ban imposed with regard to such conduct.

The prohibition on processing sensitive data does not apply where this is carried out with the express consent of the data subject, the data have manifestly been made public by the data subject and this the processing is necessary for the establishment, exercise or defense of a right in law or to comply with an obligation of international public law. It might also be necessary with a view to an important public interest, all where appropriate guarantees have been put in place to protect individual privacy and this is provided for by law or else the Data Protection Authority has granted an exemption.[494]

Processing sensitive personal data for the purpose of scientific research or statistics has also several exceptions. There is no prohibition on the processing of personal sensitive data when the research serves a public interest and the processing is necessary for the research or statistics concerned. Besides this, it has to be impossible or would involve a disproportionate effort to ask for express consent and sufficient guarantees are provided to ensure that the processing does not adversely affect the individual privacy of the data subject to a disproportionate extent.[495]

Processing **health-related personal data** – so called 'special personal data' – is dealt with in the articles 16 through 24 of the Dutch Data Protection Act. These provisions implement article 8 of The European Data Protection Directive 95/46/EC.[496] Article 16 Dutch Data Protection Act contains a general prohibition of the processing of personal data concerning a person's religion or philosophy of life, race, political persuasion, health and sex life, or personal data concerning trade union membership. Nonetheless, articles 17 through 23 list several exceptions to this prohibition and indicate that the processing of such sensitive data may be considered lawful under several hypothesises and the exceptions must satisfy strict conditions. On the whole, the Dutch Act seems rather restrictive in permitting processing (or disclosure) of health related personal data.

Article 21 states that the prohibition on processing personal data concerning a person's health does not apply where the processing is carried out by:
a) medical professionals, healthcare institutions or facilities or social services, provided that this is necessary for the proper treatment and care of the data subject, or for the administration of the institution or professional practice concerned;
b) insurance companies referred to in Article 1(1)(h) of the Insurance Supervision Act 1993 (in Dutch: *Wet toezicht verzekeringsbedrijf 1993*), insurance companies referred to in Article 1(c) of the Funeral Insurance Supervision Act (in Dutch: *Wet toezicht natura-uitvaartverzekeringsbedrijf*), and intermediaries and sub-agents referred to in Article 1(b) and 1(c) of the Insurance Mediation Act (in Dutch: *Wet assurantiebemiddelingsbedrijf*), provided that this is necessary in order to assess the risk of being insured by the insurance company and the data subject has not indicated any objection thereto, or the performance of the insurance agreement;

---

494 When granting an exemption, the Commission can impose rules and restrictions according to article 23 (1) under e. Dutch Data Protection Act.

495 article 23 (2) Dutch Data Protection Act

496 Richtlijn nr. 95/46/EG van het Europees Parlement en de Raad van de Europese Unie van 23 november 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (PbEG L 281), available in several languages at: http://eur-lex.europa.eu/ (17.08.2010).

c) schools, provided that this is necessary with a view to providing special support for pupils or making special arrangements in connection with their state of health;
d) institutions for probation, child protection or guardianship, provided that this is necessary for the performance of their legal duties;
e) the Dutch Minister of Justice, provided that this is necessary in connection with the implementation of prison sentences or detention measures, or; administrative bodies, pension funds, employers or institutions working for them, provided that this is necessary for the proper implementation of the provisions of laws, pension regulations or collective agreements which create rights dependent on the state of health of the data subject, or the reintegration of or support for workers or persons entitled to benefit in connection with sickness or disability.
Moreover, personal data concerning a person's health may only be processed by persons subject to an obligation of confidentiality by virtue of office, profession or legal provision, or under an agreement. Where responsible parties personally process data and are not already subject to an obligation of confidentiality by virtue of their office, their profession or a specific legal provision, they are required to treat the data as confidential, except where they are required by law or in connection with their duties to communicate such data to other parties who are authorized to process such data in accordance with article 21 Dutch Data Protection Act.

### 8.1.5. Data security

Article 10 of the Dutch Data Protection Act states that personal data shall not be kept in a form which allows the data subject to be identified for any longer than is necessary for achieving the purposes for which they were collected or subsequently processed. Personal data may, however, be kept for longer than provided where this is for historical, statistical or scientific purposes, and where the responsible party has made the necessary arrangements to ensure that the data concerned are used solely for these specific purposes.

The Dutch Data Collection Act has a separate article on the use of technology in the protection of personal data. According to article 13 Dutch Data Protection Act, the responsible party shall implement appropriate technical and organizational measures to secure personal data against loss or against any form of unlawful processing. This will guarantee an appropriate level of security, taking into account the state of the art and the costs of implementation, and having regard to the risks associated with the processing and the nature of the data to be protected. These measures shall also aim at preventing unnecessary collection and further processing of personal data.

Article 14 of the Act stipulates the difference in responsibility between the processor and the responsible party. This article mentions that where responsible parties have personal data processed for their purposes by a processor, these responsible parties shall make sure that the processor provides adequate guarantees concerning the technical and organizational security measures for the processing to be carried out. The responsible parties shall make sure that these measures are complied with. The carrying out of processing by a processor shall be governed by an agreement or another legal act whereby an obligation is created between the processor and the responsible party. Furthermore, the responsible party shall make sure that the processor processes the personal data in accordance with article 12 of the Dutch Data Protection Act (which states that anyone acting under the authority of the responsible party or the processor, as well as the processor himself - where they have access to personal data - shall only process such data on the orders of the responsible party, except where

otherwise required by law.) and complies with the obligations that derive from the use of technology in the protection of personal data (see article 13 Dutch Data Protection Act as explained above).

## 8.1.6. Cross-border notification

### 8.1.6.1. Transfer of data within the European Union

The Dutch Data Protection Act does not have any individual provisions governing data movements within the European Union, as the Dutch Data Protection Act implemented the European Directive 95/46/EC for the Dutch jurisdiction.

The Directive 95/46/EC has two objectives:

- an equivalent protection of personal data, and
- free movement of personal data within the European Union.

The European Union will thus be one single jurisdiction with regard to the protection of personal data once all Member States have adapted their legislation to the directive.

Therefore, data movement from the Netherlands to another European Union Member State only has to conform to the general requirements of the Dutch Data Protection Act.

### 8.1.6.2. Transfer to countries outside the European Union

In view of the increasing technical scope of large-scale data exchange and the internationalization of business and commerce, the legislator felt it necessary to devote a separate chapter (Chapter 11, articles 76 - 78) to data traffic between the European Union and third countries. Third countries are all countries outside the European Union, with the exception of the countries of the European Economic Area (EEA). These three countries (Norway, Liechtenstein and Iceland) have committed themselves to implementing the Directive in their respective national legislations.

A transfer of personal data to a third country is any act by which personal data is made available to a party located outside the legal jurisdiction of an European Union country. To fall within the legal definition, such an act must be performed knowingly, with the purpose of conveying the data in question beyond European Union territory to a third country.

The primary rule is that personal data may only be transferred to a third country if the general requirements of the Dutch Data Protection Act have been conformed to and the third country ensures an adequate level of protection.

If a third country does not provide an adequate level of protection, there are two possibilities for still being entitled to transfer data to these third countries.

- transfer based on the exceptions mentioned in the Act (Article 77(1) Dutch Data Protection Act):

  a. the data subject has given his explicit consent for this, or

b. transfer is necessary for the performance of the contract between the data subject and the controller, or for taking steps at the request of the data subject prior to entering into a contract, and that are necessary of the conclusion of a contract, or
c. transfer is necessary for the conclusion or performance of a contract to be concluded between the controller and a third party in the data subject's interest, or
d. transfer is necessary for an important general interest, or the establishment, implementation or defense at law of any right, or
e. transfer is necessary for the protection of vital interests of the data subject.

- transfer based on a permit of the Minister of Justice. Such a permit will be made subject to additional conditions that serve as a guarantee for the protection of personal data.

### 8.1.7. Right to information (Art. 8 DSG)

In Chapter five of the Dutch Data Protection Act, there is foreseen in the subject 'Information provided to the data subject' (articles 33-34 Dutch Data Protection Act). The legislator considered it important that the data subject can check what happens with his personal data.[497] That is the reason why the data subject needs to be informed about the purposes of the processing and the name and address of the responsible party. The Data Protection Authority has created a website: www.mijnprivacy.nl (in Dutch) where data subjects can find all the relevant information on their rights and standard forms and letters to fill in if they want to claim their rights against a responsible party.

Articles 33 and 34 Dutch Data Protection Act state that where personal data are to be obtained from a data subject, the responsible party shall provide the data subject with the following **information prior to obtaining** the said personal data (unless the data subject is already acquainted with this information). First, the responsible party shall inform the data subject of its identity and the purposes of the processing for which the data are intended. Further, the responsible party shall provide more detailed information, where given the type of data and the circumstances in which they are to be obtained or the use to be made thereof. This is necessary in order to guarantee with respect to the data subject that the processing is carried out in a proper and careful manner.

Where the personal data are obtained in a different matter than is referred to in article 33 of the Data Protection Act, the responsible party shall provide the data subject with the same information as mentioned above, unless the data subject is already acquainted with this information at the time that the data relating to him is recorded or when it is intended to supply the data to a third party, at the latest on the first occasion that the said data are so supplied. The foregoing does however not apply if it appears to be impossible or would involve a disproportionate effort to provide the said information to the data subject. In that case, the responsible party shall record the origin of the data. It likewise not applies if the recording or provision of the data is required by or under the law. In that case, the responsible party must inform the data subject, upon his request, about the legal provision which led to the recording or supply of data relating to the data subject.

In Chapter six ('Rights of the data subject', articles 35-42 Dutch Data Protection Act), it is laid down in article 35 that a data subject has the **right, freely and at reasonable intervals**, to request the responsible party to inform him as to whether or not personal data relating to him are being processed. The responsible party shall inform the data subject in writing within four weeks as to

---

497 Governmental explanation. Tweede Kamer, vergaderjaar 1997–1998, 25 892, nr. 3 174, available at (in Dutch): http://www.cbpweb.nl/downloads_wetten/wbp_mvt.pdf (17.08.2010).

whether personal data relating to him are being processed. The responsible party may require a payment (maximum 5 Euros unless this amount is modified in special cases by general administrative regulation[498]) for expenses incurred in providing this information (see article 39 Dutch Data Protection Act).

In case that such data are being processed, the information provided shall contain a full and clear summary thereof, a definition of the purpose or purposes of the processing, the data categories to which the processing relates and the recipients or categories of recipients, as well as the available information about the origin of the data. Prior to the providing of the requested information to which a third party may be expected to object, the responsible party shall give the third party an opportunity to express its views where such information contains data concerning that third party unless this appears to be impossible or would be disproportional. Please note that upon request, the responsible party needs to provide information concerning the underlying logic of the automated processing of data relating to the data subject.

### 8.1.8. Relationship Between New Technologies and Data Protection

There are no technical applications explicitly mentioned in the Dutch Data Collection Act. There is, however, a general provision on the use of technology in the protection of personal data as regards to data security (see 8.1.5.). According to article 13 Dutch Data Protection Act, the responsible party shall implement appropriate technical and organizational measures to secure personal data against loss or against any form of unlawful processing.

### 8.1.9. Difference of Treatment for Public and Private Data Processing

There is no different scheme for the processing performed by private individuals and treatments performed by public authorities. As explained in the Introduction, in article 1 of the Dutch Data Protection Act, the definition of a responsible party includes a natural person, a legal person, an administrative body or any other entity which, alone or in conjunction with others. Also with the definition of processor there is no distinction made between private individuals and public authorities since processor shall mean the person or body which processes personal data for the responsible party without coming under the direct authority of that party. The Dutch Data Protection Act thus makes no difference between processing by private individuals and public authorities. However, as indicated below (8.2.), the rights of the concerned persons are different depending on the public or private nature of the data processing agency.

## 8.2. Durchsetzungsrechte der Datenschutzanliegen für Betroffene

### 8.2.1. Datenbearbeitungen durch Private

In the Dutch Data Protection Act there is in principle no difference in the claim if a concerned person wants to enforce their rights towards the processing of their personal data by a private party or by the authorities and/or the administration.[499] If there is an exception, it will be explicitly mentioned in this

---

498 In Dutch: *algemene maatregel van bestuur.*

499 Governmental explanation. Tweede Kamer, vergaderjaar 1997–1998, 25 892, nr. 3 174, available at (in Dutch): http://www.cbpweb.nl/downloads_wetten/wbp_mvt.pdf.

advice. The main difference between enforcing the right against private and public authorities is the **way of the proceedings** to claim the rights. Chapter six 'Rights of the data subjects' treats this subject.

#### *8.2.1.1. Blocking, Rectification, Elimination, Note (according to Art. 15 Abs. 2 DSG)*

When the data subject has received the personal data relating to him (based on the right of information, see under 1.1), he may request the responsible party to correct, supplement, delete or block the said data in the event that it is factually inaccurate, incomplete or irrelevant to the purpose or purposes of the processing, or in case it is being processed in any other way which infringes a legal provision. The request itself shall contain the modifications to be made (article 36 Dutch Data Protection Act). If the responsible party, who has to respond to such a request within four weeks, refuses to comply with the request, the refusal must be accompanied by the reasons for the refusal. However, there is no special provision in place for putting a note with the personal data (like there is foreseen in e.g. article 15 Abs. 2 DSG).

If there is a **special procedure** in place for correcting, supplementing, deleting or blocking data of public registers, the provisions of the Dutch Data Protection Act will not be followed (article 36 (4) Dutch Data Protection Act).

#### *8.2.1.2. Communication and publication*

If a request is complied with, the responsible party must make sure that the decision to correct, supplement, delete or block data is implemented as quickly as possible. In case the personal data is recorded on a data carrier to which no modifications can be made, the responsible party must take the necessary steps to inform the data user that it is impossible to amend the data even when there are grounds for doing so.

If the is an important interest of the requester, the responsible party shall reply to the request for modification in a form, other than in writing.

The responsible party who has modified the personal data in response to a request of a data subject has an obligation to inform, as soon as possible, third parties to whom the data has previously been supplied. This does not have to be done if this is impossible or would involve a disproportionate effort. Upon request, the responsible party would inform the requester of those parties to whom it has provided such information (see article 38 Dutch Data Protection Act).

#### *8.2.1.3. Others*

Where personal data are undergoing the processing referred to in article 8 under e and f Dutch Data Protection Act (article 8 e: the processing is necessary for the proper performance of a public law duty by the administrative body concerned or by the administrative body to which the data are provided; article 8 f: it is necessary upholding the legitimate interest of the responsible or third party to whom the data are supplied except where the interest or fundamental rights and freedoms of the data subject, in particular privacy prevail) the data subject may at all times **register an objection** with the responsible party in connection with his particular personal circumstances (see article 40 (1) Dutch Data Protection Act). In case the objection is justified, which has to be decided within four weeks, the responsible party shall **stop the processing** with immediate effect. This provision does, however, not apply to public registers set up by law.

#### *8.2.1.4. Proceeding (Form, procedural rights, such as opportunity for the class action, etc.)*

Following the content of article 45 Dutch Data Protection Act, a decision taken by an administrative body in response to a request to modify the personal data and a decision taken in response to the registering of an objection following article 40 Dutch Data Protection Act, shall be equivalent to a decision within the meaning of the General Administrative Regulations Act (in Dutch: *Algemene wet bestuursrecht*). The procedural rules and the timeframes as laid down in the General Administrative Act thus have to be followed.

If the decision is not taken by an administrative body, the party involved can file a petition to the District Court with at written request to order the responsible party to grant or reject a request for modification or to request a recognition or rejection of an objection referred to in article 40 Dutch Data Protection Act (see article 46 Dutch Data Protection Act).

The application for the District Court must be submitted within six weeks after receiving the reply from the responsible party or six weeks after the time limit for the reaction of the responsible party had been expired. The Court shall, if necessary, give the parties concerned an opportunity to put forward their views.

Besides these two proceedings, article 47 Dutch Data Protection Act foresees in a procedure in front of the Data Protection Authority. The party involved can ask, within the given timeframes for the other proceedings, the Data Protection Authority to mediate or give its opinion in the dispute with the responsible party or make use of the provisions concerning the arrangement of disputes in a code of conduct which has been approved by the Data Protection Authority (see article 25 Dutch Data Protection Act). Please note that if there is a code of conduct in place in which it is laid down that there are certain bodies responsible for dealing with the dispute, these bodies can also obtain the opinion of the Data Protection Authority.

Please note also that there are no special provisions in place in the Dutch Data Protection Act for an opportunity for a class action based on a claim deriving from the Dutch Data Protection Act. There is, however, discussion going on during the process of amending the Telecommunications Act (In Dutch: *Telecommunicatiewet*) in order to comply with article 13 (6) of Special Privacy Directive (2002/58/EG) to insert such a possibility of a class action in the Telecommunications Act. The Data Protection Authority, who are granted a right of advice in article 51 under 2 Dutch Data Protection Act (article 51 (2): '*The Authority shall be asked to issue an opinion on bills and draft texts of general administrative regulations relating entirely or substantial to the processing of personal data*'), advised to insert a class action possibility in the draft bill of the Telecommunications Act.[500]

#### *8.2.1.5. If third persons report, clarification by the assignee concerning data protection (can he clarify? Has he to clarify?)*

See above.

### 8.2.2. Datenbarbeitungen durch Behörde

See 8.2.1.

---

[500] Letter of advice of the College Bescherming Persoonsgegevens to Ministry of Economic affairs, dated 4 June 2010, available (in Dutch) at: www.cbpweb.nl.

## 8.3. Nationale Aufsichtsbehörde

### 8.3.1. Zusammensetzung, Ernennung und Eingliederung

In articles 53 – 57 of the Dutch Data Protection Act, the rules concerning the conditions and the appointment of the Data Protection Authority have been laid down.

In short, the Dutch DPA comprises **a chairperson and two other members**. They receive remuneration for their work. The term of office and payment of expenses are laid down in general administrative regulation.

In addition, **special members** (who receive a session fee) may be appointed to the Commission. In the appointment of special members, all efforts shall be made to reflect the various sectors of society. The chairperson must fulfill the requirements governing the appointment of District Court judges.[501] The chairperson shall be appointed by royal decree, on the proposal of the Ministry of Justice, for six years and the other members for four years. The chairperson and the two other members may not carry out any other remunerated work where the nature of scale of this work is incompatible with the work for the Dutch Data Protection Authority unless they have approval of the Minister. All members can be reappointed immediately after this. At their own request, the members are discharged by the Minister. Members shall in any case be discharged by royal decree on the proposal of the Minister with effect from the first month following the month in which they reach the age of 65.

There is also an **advisory board** installed with the task to advise the Dutch DPA on general aspects of the protection of personal data. The members of this board shall be drawn from the various sectors of society and shall be appointed by the Minster on the proposal of the Dutch DPA.

The Dutch DPA also has a **secretariat** of which the officials are appointed (an organization consisting of about 70 members of staff), suspended and discharged by the Minister on proposal of the chairperson. The chairperson shall direct the work of the Dutch DPA and the secretariat.

### 8.3.2. Gewährleistung der Unabhängigkeit

The framework for performing the task has been set forth in the Dutch Data Protection Act and other related legislation. In this context, the legislator has implemented Article 28 of the European Data Protection Directive 95/46/EC, which explicitly provides for the existence of such a supervisory authority and which also provides that this authority should fulfill its task completely independently. This independency is laid down in article 52 (2) Dutch Data Protection Act.

The tasks of the authority sometimes relate to obligations, but as a rule they relate to powers. Subject to the law and the opinion of the court, the Dutch Data Protection Authority is entitled to **take decisions itself** regarding the execution of these powers. Other tasks, such as providing information and conducting studies of new developments, result from the general supervisory task. Also in view of its independence, the Dutch DPA is considerable free to work out the details of its tasks within the frameworks of the act and to set the necessary priorities and decide where to lay particular emphasis.

The Dutch DPA shall **adopt rules of procedure**. These rules shall in any case include provisions relating to the financial management and administrative organization of the Authority as well as to working methods and procedures with a view to a proper and careful discharge of their various tasks. The rules

---

501 As laid down in article 48 (l) of the Judicature Act (in Dutch : *Wet op de rechterlijke organisatie*)

shall provide guarantees against the mixing of the supervisory, advisory and enforcement tasks of the Dutch DPA. They may also give more detailed provisions for the advisory board. The rules itself and any modification need to be approved by the Minister (article 56 Dutch Data Protection Act).

### 8.3.3. Zuständigkeitsbereich

In the execution of its powers, the Dutch Data Protection Authority is bound by the standards laid down in the **General Administrative Law Act**. In view of the enforcement powers, the guarantees regarding the proper fulfillment of the tasks have been specified more stringently in the General Administrative Act:

- The possibility of objection to and appeal against Dutch Data Protection Authority decisions to the administrative law court.
- The possibility of submitting a complaint to the National Ombudsman.
- The Freedom of Information Act (In Dutch: *Wet openbaarheid van bestuur* or *WOB*) applies.
- Pursuant to Article 56(3) Data Protection Act, the Dutch Data Protection Authority is obliged to adopt administrative regulations, among other things providing for rules regarding the work methods and procedures in view of the proper and careful performance of the various tasks.
- As an administrative body, the Dutch Data Protection Authority is of course also bound by the general principles of proper administration.

Each year, the Dutch DPA publishes a public report explaining its work and findings. The website of the Dutch Data Protection Authority contains summaries of the annual reports for recent years (article 58 Dutch Data Protection Act).

### 8.3.4. Aufgaben und Kompetenzen

#### *8.3.4.1. Supervision of Compliance*

The Dutch Data Protection Authority (hereinafter also referred to as the Dutch DPA) **supervises compliance** with acts that govern the use of personal data. In particular, the Dutch Data Protection Authority supervises compliance with and application of the Dutch Data Protection Act, the Police Data Act and the Municipal Database (Personal Records) Act.

Pursuant to the Dutch Data Protection Act, the Dutch DPA (or the Data Protection Officer (see under 1.5)) must be **notified of the processing of personal data**, unless specific processing has been exempted from the notification obligation. If someone fails to notify the Dutch DPA of their data processing, the Dutch DPA may impose a fine of maximum EUR 4,500. A fine can also be imposed if someone has incorrectly or incompletely reported their data processing and/or if they fail to report changes (in time).[502] Periodically, the Dutch DPA will subject notifications from specific sectors or of specific processing to a further investigation. The Dutch DPA will also act upon complaints from data subjects.

---

[502] Based on article 72 Dutch Data Protection Act, the authority to impose a fine lapses five years after the infringement has been committed.

The notifications have to been inserted in the **public registry of notifications** (it is a statutory task of the Dutch Data Protection Authority to keep such a register). The public registry provides for openness around the processing of personal data in organizations. This enables a person to check how his or her personal data are being handled, so that he or she can exercise his or her rights, if necessary. In addition, the notifications enable an efficient supervision by the Dutch Data Protection Authority.

#### *8.3.4.2. Additional Tasks*

In addition to the tasks mentioned above, the Data Protection Act establishes the following tasks:

- Making recommendations regarding legislation (article 51 (2))
- Testing codes of conduct (article 25)
- Testing regulations (article 51 (2))
- Notification and preliminary examination (article 60)
- Information (e.g. article 30)
- Exemption from the prohibition to process sensitive data (article 23)
- Making recommendations regarding permits for transfers to third countries (article 77 (2))
- International affairs (e.g article 23 (3))
- Mediation and handling of complaints (article 47)
- Official investigation (articles 31 and 32)
- Enforcement (articles 65 through 75)
- International tasks (e.g. article 31 (4))[503]

#### *8.3.4.3. Competencies*

According to article 60 of the Dutch Data Protection Act, the Commission may initiate an investigation (on its own or upon request of an interested party) into the manner in which the Act is applied. Provisional findings will be presented to the responsible party as well as to the minister concerned.

In order to carry out an investigation, members of the Commission are authorized to entere a residence without the consent of the resident. The Commission also has the authorization to apply administrative measure of constraint (article 61 Dutch Data Protection Act).

---

503 '*The Dutch Data Protection Authority's chief tasks include participation in the Working Party of supervisory authorities as referred to in Article 29 of Directive 95/46/EC and the membership of the Joint Supervisory Authorities for Europol, the Schengen information system and the Customs information system.*
*Within the scope of its international activities, the Dutch DPA takes part in the following working parties and conferences abroad: Article 29 Working Party, Safe Harbour Panel, Consultative committee Council of Europe, Spring conference European Supervisory Authorities, International Conference of Supervisory Authorities, Berlin Telecom Group.*
*Within the scope of the supervision of European information systems that are used by police and the Justice Department, the Dutch DPA is a member of the following supervisory bodies on behalf of the Netherlands:*
*Joint Supervisory Authority for Europol, Joint Supervisory Authority for the Schengen Information System and*
*Joint Supervisory Authority for the Customs Information System*'. Information available at: http://www.dutchdpa.nl/Pages/en_ind_cbpint.aspx (17.08.2010).

#### *8.3.4.4. Sanctions*

According to article 66 of the Dutch Data Protection Act, the Commission may require responsible parties how do not comply with the notification requirement to pay a fine. The **control** of the Data Protection Authority (which started in 2003) for complying with the notification obligation deriving from the Dutch Data Protection Act resulted in 29 fines (fines between € 3.000 and € 15.000 for multiply failures).[504] The fines have been imposed to 14 Municipalities, 3 Direct marketing companies, 3 Health insurance companies and 9 Safety, health and welfare services (in Dutch: *Arbodiensten*). The 13 Municipalities and 1 of the Safety, health and welfare services have filed an objection towards the fine at the Dutch DPA and in 2 cases the fine has been decreased by the Dutch DPA. In all the other cases, the Dutch Data Protection Authority has not changed their decision. Nine Municipalities and the Safety, health and welfare service brought their case in front of the (Administrative) court. In 1 of these cases (which is published), the court ruled on 19 January 2005, that the Dutch DPA was allowed to control the complying with the Dutch Data Protection Act and therefore the fine was legitimate.[505]

## 8.4. Rolle der Organisationen zum Schutz der Betroffenen

As explained above, the Dutch DPA is a governmental, independent organization that deals – amongst other things – with the compliance of the Dutch Data Protection Act as well as the protection of the data subject. By installing a website (in Dutch) called *www.mijnprivacy.nl* the Dutch DPA wanted to inform the citizens about all practical questions they might have about this subject. On this website data subjects can also file a complaint about an organization that does not process the personal data in a proper way and citizens can request the Dutch DPA to mediate in a dispute a data subject might have with an organization. If there is a complaint about the Dutch DPA, there is an internal complaint procedure in place and if the data subject is not satisfied with the result of this complaint procedure, the data subject can go to the so called *Ombudsman* or go to Court (see 1.3.3).

## 8.5. Mögliche und vorgeschriebene Aktivitäten der Datenbearbeiter (private und öffentliche)

### 8.5.1. Certification of the data protection

See 'Reporting of data collections'

### 8.5.2. Reporting of data collections

According to the Dutch Data Protection Act, the automatic processing of personal data (fully or partly) intended to serve a single purpose or different related purposes must be notified to the Data Protection Commission or the Data Protection Officer **before the processing** is started (see article 27

---

504 See www.cbpweb.nl (17.08.2010).

505 The Dutch decision is available at: http://www.cbpweb.nl/downloads_melden/20050201_denbosch.pdf (17.08.2010).

*et seq*. Data Protection Act). This is not necessary if the data processing is exempted for notification.[506] Non-automated processing of personal data intended to serve a single purpose or different related purposes, must be notified where this is subject to a prior investigation. The notification shall contain the name and address of the responsible party, the purpose(s) of the processing and collecting, a description of the categories of recipients to whom the data may be supplied, the planned transfers of data to countries outside the European Union and a general description allowing a preliminary assessment by the Dutch DPA of the suitability of the planned measures to guarantee the security of the processing. It is important that every individual processing must also be reported separately. It is not permitted, for example, to combine personnel records and a client file in one notification. A number of data processing operations are subjected to Preliminary Examination by the Dutch DPA. This involves processing that in the opinion of the legislator involves a special risk for the personal privacy of the persons involved.

The Dutch Data Protection Authority can be **notified in three ways**[507]: a person can download the Dutch Data Protection Act Notification Program (in Dutch) on the website or via the website request a copy of the diskette with the Dutch Data Protection Act Notification Program or request the special Data Protection Act Notification Form.

The Dutch Data Protection Authority can only accept notifications that have been made in the prescribed way. The Data Protection Authority will not accept notifications that have been sent on diskette or by e-mail without a completed and signed authentication form and notifications that are not in Dutch. All information must have been included on the diskette or on the form itself. For this reason, a person cannot enclose any appendices with the notification or refer to appendices. Nor is it permitted to send in your 'own' versions of the notification form.

Whether or not the notification is valid, is only established at the time the indicated contact has received a **confirmation of receipt** with the notification number from the Dutch DPA. If the notification has been made on behalf of a data controller, the contact must inform the data controller of this.

Please note that no rights can be derived from a notification, because a notification does not result in approval of a data processing operation. Usually, the Dutch Data Protection Authority uses a formal test to establish whether the notification is complete and initially acceptable. The party making the notification continues to be responsible for a correct and complete notification and for complying with the other provisions of the Dutch Data Protection Act.

---

506 Categories exempted from processing (list in English can be found on the website of the Dutch Data Protection Authority: www.cbpweb.nl) are for example data regarding child care facilities, individual health care, personnel administration, travel documents, grave rights, compulsory military service, registration of visitors, retirement and early retirement, Subscriptions, *et cetera.*

507 Information available at: http://www.cbpweb.nl/Pages/ind_melden.aspx (17.08.2010)

### 8.5.3. Recognition of operational data protection officer

Businesses, branch organizations, governments and institutions can appoint their **own internal supervisor** of the processing of personal data: the Data Protection Officer (articles 62-64 Dutch Data Protection Act). Within the organization, the Data Protection Officer supervises the application of and compliance with the Dutch Data Protection Act. The statutory tasks and powers of the Data Protection Officer give this officer an independent position in the organization.

Citizens, customers, clients, employees, in short all persons in question whose personal data are being processed, can **contact** a Data Protection Officer for information, inspection of their own processed data or for complaints.

The Dutch Data Protection Authority must be **notified** of all Data Protection Officers (appointed pursuant to articles 62-64 of the Act). The Dutch Data Protection Authority has the statutory task of keeping a public register of Data Protection Officers.

Appointing a Data Protection Officer will mean that the Dutch Data Protection Authority will **exercise restraint** with regard to organizations in which this Data Protection Officer functions properly. The Dutch Data Protection Authority will, wherever possible, refer persons with questions or complaints to the Data Protection Officer. However, as the national supervisory authority, the Dutch Data Protection Authority retains all powers with regard to organizations that have appointed a Data Protection Officer.

### 8.5.4. Data letter (periodic unsolicited notification of data processing to concerned persons)

Dutch Law does not provide for a data letter.

### 8.5.5. Self-regulation (Code of Conduct, BCR, …)

Apart from the legal framework concerning the processing of personal data, the Dutch authorities are convinced that self-regulation will contribute effectively to the achievement of the individual's fundamental right to the protection of his privacy. As such, the Dutch Data Protection Authority promotes the appointment of a data protection officer (see above under **Recognition of operational data protection officer)** and is encouraging companies to formulate a code of conduct for their branch of industry or sector.

Chapter three of the Dutch Data Protection Act (articles 25 and 26) provides societies with a framework within which to draft a code of conduct implementing the Dutch Data Protection Act with regard to the particular features of the sector or sectors of society in which these organizations operate. In accordance with article 25 (1), the Dutch Data Protection Authority may issue a declaration stating that such a code of conduct properly implements the Dutch Data Protection Act. The Dutch DPA shall only consider requests where, in its opinion, the requester or requesters are sufficiently representative and the sector or sectors concerned are defined with sufficient precision in the code (article 25 (3)). The Dutch DPA is responsible for publishing the declaration, together with the associated code, in the Official Gazette (in Dutch: *Staatscourant*), (see article 25 (6)).

Moreover, the Data Protection Authority developed a number of audit products in a joint venture with umbrella organisations of auditors and market parties (audit and consultancy organisations). These audit products allow a self-assessment by organizations which handle personal data concerning their compliance with the Dutch Data Protection Act. Compliance tools include Quickscan, a Data Protection Act Self-evaluation (in Dutch: *Zelfevaluatie*) and the Privacy Audit Framework (in Dutch: *Raamwerk Privacy Audit*).[508]

### 8.5.6. Privacy by design

Other than article 13 of the Dutch Data Protection Act regarding the implementing of appropriate technical and organizational measures to secure personal data (see under 1.1), there is not foreseen in privacy by design in the Dutch legislation.

---

[508] See the website of the Dutch Data Protection Authority: www.cbpweb.nl for additional information on these compliance tools.

## 9. Norwegen

Der Datenschutz ist in Norwegen im Gesetz über die Behandlung von persönlichen Informationen geregelt (*personopplysningsloven*) aus dem Jahr 2000 geregelt.[509] Es wird in der Folge mit der in Norwegen gängigen Bezeichnung „pol" abgekürzt.

Norwegen hat sich im EWR-Vertrag (so wie die anderen EWR-Staaten) verpflichtet, die Datenschutzrichtlinie der EU umzusetzen.[510] Der pol aus dem Jahr 2000 basiert in ganz überwiegendem Masse auf der **Datenschutzrichtlinie der EU**.[511] Die Richtlinie ist ausserst detailliert und führte im Ergebnis eine umfassende Rechtsharmonisierung herbei. In einigen wenigen Punkten geht die norwegische Umsetzung über die Mindeststandards der Richtlinie hinaus.[512] Der pol setzt zudem in grossem Umfang die Datensschutz-Konvention des Europarates um.

Der gesetzlich definierte **Zweck** des pol ist es, den Einzelnen davor zu schützen, dass sein Persönlichkeitsrecht durch die Behandlung seiner persönlichen Informationen nicht verletzt wird. Das Gesetz soll einen Beitrag dazu leisten, dass Personeninformationen in Übereinstimmung mit Grundsätzen des Persönlichkeitsschutzes behandelt werden, dazu zählen unter anderem der Bedarf an persönlicher Integrität, die Freiheit des Privatlebens und ausreichende Qualität der Personeninformationen.[513]

Personeninformationen sind solche, die direkt oder indirekt einer Einzelperson zugordnet werden können. Der popplyl gilt nur für den Schutz natürlicher aber **nicht für den Schutz juristischer Personen**.[514]

---

509 Gesetz Nr. 31 vom 14.4.2000. Version : zuletzt geändert am 1.6.2009 (Stand September 2010).

510 Siehe Den Beschluss des EWR-Komites Nr. 83/1999 vom 25.6.1999 über die Änderung des EWR-Vertrages, Protokoll 37 und Anhang XI.

511 RL Nr. 46/1995.

512 Schartum/Bygrave, Personvern i informasjonssamfunnet, Fagbokforlaget, Oslo 2004, S. 104 mit drei eher unwesentlichen Beispielen (§ 21 pol über Personenprofile; § 22 pol über Informationspflichten bei automatisierten Entscheidungen; Erweiterter Anwendungsbereich des Konzessionssystems).

513 § 1 popplyl.

514 § 2 Nr. 1 popplyl.

## 10. Aussereuropäisch: Kanada

La protection des renseignements personnels –soient les renseignements non publics qui permettent l'identification d'individus donnés– fait partie, selon les conceptions canadiennes, de la préservation du **droit à la vie privée**.

Le régime canadien de la protection des renseignements personnels s'est implanté en deux temps[515]. On a d'abord assisté à l'émergence, correspondant avec le virage informatique de l'appareil gouvernemental[516], de lois portant sur la protection des renseignements personnels et l'accès à l'information dans le **secteur public**[517] –de telles lois existent désormais dans toutes les juridictions canadiennes–, puis, plus récemment, de lois visant le **secteur privé**. À cet égard, le législateur fédéral a pris sur lui, insprié par la directive européenne 95/46/CE sur la protection des données à caractère personnel[518], d'adopter la **Loi sur la protection des renseignements personnels et les documents électroniques** (« LPRDE »)[519]. Cette loi s'applique aux affaires de toute entreprise canadienne, sauf s'il

---

515 Toutes les lois en vigueur sont recensées à l'Annexe A, à laquelle on se reportera pour leur titre exact. Par souci de commodité, nous renverrons aux lois provinciales et territoriales comme suit: les lois notées *L.pub.* visent le secteur public, les lois notées *L.priv.,* le secteur privé et les lois notées *L.s.*, le secteur de la santé. Suivra l'indication de la province ou du territoire. Par exemple, la *Loi* québécoise *sur la protection des renseignements personnels dans le secteur privé*, L.R.Q. c. P-39.1 sera noté *L.priv.Qué*. Les lois fédérales, soit la *Loi sur la protection des renseignements personnels,* L.R.C., 1985, c. P-21 et la *Loi sur la protection des renseignements personnels et les documents électroniques* L.C. 2000, c. 5 seront respectivement notées *LPRP* et *LPRPDÉ*. Finalement, par «CPVPC», on renvoie, selon le contexte, au commissaire ou au commissariat à la protection de la vie privée du Canada.

516 Groupe d'étude sur l'ordinateur et la vie privée*, L'ordinateur et la vie privée*, Rapport du groupe d'étude établi conjointement par le ministère des Communications et le ministère de la Justice (Ottawa, Éd. Off., 1972) [*Ordinateur et vie privée*]; Paul-André Comeau, «Protection des personnels – Projet et réalité» (2009), en-ligne: www.priv.gc.ca/information/pub/gd_com_2009_f.cfm [Comeau, «Protection»], à la p. 17.

517 Le terme «droit d'accès» se trouve à couvrir à la fois la notion d'accès aux documents des institutions publiques, dans l'optique du droit des contribuables de connaître l'utilisation qui est faite des fonds publics et de s'enquérir de la marche des affaires de l'administration, et le droit d'accès des particuliers aux renseignements personnels détenus par autrui sur leur compte, que cette détention soit le fait d'une institution publique ou d'une entité privé. Le présent document s'attarde la protection des renseignements personnels et n'aborde le droit d'accès aux documents des organismes publics que par la bande, c'est-à-dire, dans la mesure de la similarité de la procédure. Sur la connexité des notions et leur confusion voir LaForest, *infra* note 697.

518 *Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données*, J.O. n° L 281 du 23/11/1995 p. 0031-0050 [*Directive européenne*]. Cette directive a très certainement fortement poussé le Canada à l'adoption d'un schème législatif visant le secteur privé, voir: Jennifer McClennan et Vadim Schick, "'O, Privacy' Canada's Importance in the Development of the International Data Privacy Regime", (2007) 38 Georgetown J. of Int'l L. 669 [McClennan-Schick], aux pp. 670-671; Leah E. Frazier, «Extraterritorial Enforcement of PIPEDA, a Multi-Tiered Analysis» (2004) 36 Geo. Wash. Int'l L. Rev 203 [Frazier], à la p. 203.

519 *Loi sur la protection des renseignements personnels et les documents électroniques* L.C. 2000, c. 5 [*LPRPDÉ*]. Cette loi est réputée offrir une protection adéquate par le Conseil de l'Europe, *Décision de la Commission du 20 décembre 2001 constatant, conformément à la directive 95/46/CE du Parlement européen et du Conseil, le niveau de protection adéquat des données à*

s'agit d'affaires strictement intraprovinciales dans une province où il existe une loi «essentiellement similaire».

Si la LPRPDÉ se trouve à supplanter la plupart des **interventions législatives sectorielles** qui existaient auparavant[520], certains domaines continuent de faire l'objet, parfois, d'un régime particulier. Il en est ainsi notamment du secteur de santé[521], et, dans une certaine mesure, des services correctionnels, notamment en ce qui a trait à a justice pénale pour les adolescents[522].

Pour toute fragmentée qu'elle soit dans ses sources, la protection des renseignements personnels au Canada est traversée des **mêmes principes**[523]. Les principes seront à la base des explications dans 10.1 à 10.3, alors que quelques particularités des différents régimes canadiens seront inclues sous 10.4.

## 10.1. Principes et fondements de la protection des données au Canada

### 10.1.1. Rôle du but indiqué lors de la collecte des informations

#### *10.1.1.1. Le fondement : la protection de la vie privée*

Etant donné que la protection des renseignements personnels au Canada fait partie de la **protection de la vie privée**, il convient de commencer par quelques mots sur le statut privilégié dont jouit cette dernière.

La vie privée jouit d'un statut privilégié au Canada où elle a été élevée au rang de **valeur quasi constitutionnelle** par les tribunaux. Elle se trouve protégée, en certains aspects par la *Charte canadienne*[524] ainsi, en ce qui concerne notamment l'interception des communications, par le *Code criminel*[525]. Le droit à la vie privée est également consacré en divers endroit du droit commun canadien, de façon assez large au Québec par l'article 5 de la *Charte* québécoise[526] et dans le *Code civil du Québec*[527] et, de façon plus restreinte, par le *tort of privacy* de la common law voire les dispositions d'une *Privacy Act* le codifiant[528]. Le Canada est également signataire de la *Déclaration universelle des*

---

*caractère personnel assuré par la loi canadienne sur la protection des renseignements personnels et les documents électroniques* [notifiée sous le numéro C(2001) 4539], J.O. L. 2 du 4.1.2002, aux pp. 13-16.

520 Elle a ainsi largement supplanté certaines dispositions de la *Loi sur les banques*, L.C. 1991, c. 46, de la *Loi sur les sociétés d'assurances*, L.C. 1991, c. 47 ou de la *Loi sur les télécommunications*, L.C. 1993, c. 38 qui assujettissaient institutions financières, compagnies d'assurances et fournisseurs de services de télécommunications à certaines obligations en la matière.

521 Ce qui fera l'objet de commentaires détaillés en fin de seconde partie, *infra* p. 38.

522 *Loi sur le système de justice pénale pour les adolescents,* L.C. 2002, c. 1; *Loi sur le système correctionnel et la mise en liberté sous condition,* L.C. 1992, c. 20.

523 Comeau, «Protection», *supra* note 516, aux pp. 19, 27.

524 *Charte canadienne des droits et libertés* formant la partie I de la *Loi constitutionnelle de 1982* (R.-U.), constituant l'annexe B de la *Loi de 1982 sur le Canada* (R.-U.), 1982, c. 11 [*Charte canadienne*].

525 *Code criminel,* L.R.C. 1985, c. C-46, partie VI «Atteintes à la vie privée».

526 *Charte des droits et libertés de la personne*, L.R.Q. c. C-12 [*Charte* québécoise].

527 *Code civil du Québec,* L.R.Q. 1991, c. 64, art. 35-41.

528 *Privacy Act*, R.S.B.C. 1996, c. 373; *Privacy Act*, R.S.S. 1978, c. P-24; *Privacy Act,* R.S.N.L. 1990, c. P-22; *The Privacy Act*, C.C.S.M. c. P125. Ces lois n'ont pas fait l'objet d'une jurisprudence abondante.

*droits de l'homme*[529] et du *Pacte international relatif aux droits civils et politiques*[530], deux instruments qui consacrent le caractère fondamental du droit à la vie privée.

La protection du droit à la vie privée ne fait cependant **pas l'objet d'une disposition propre** dans la *Charte canadienne*[531]. Elle s'y trouve toutefois consacrée dans deux de ses aspects: d'une part, l'article 8 protège les «attentes raisonnables»[532] face aux «fouilles, perquisitions et saisies abusives»[533]. D'autre part, le droit à la vie privée a parfois été invoqué avec succès dans le cadre du droit à la vie, à la liberté et à la sécurité de la personne, garanti par l'article 7[534]. En outre, certains auteurs ont suggéré que le droit à l'égalité de l'article 15 puisse lui aussi servir d'assise constitutionnelle à sa protection[535].

En tout état de cause, la **jurisprudence** canadienne a assurément pris soin de souligner le caractère «privilégié et fondamental du droit à la vie privée dans notre culture sociale et juridique[536]», l'élevant au rang de valeur quasi constitutionnelle[537]. C'est un droit dont jouissent tous ceux qui se trouvent en sol canadien[538].

> « [La protection de la vie privée] aide à garantir, en premier lieu, que les citoyens possèdent l'information nécessaire pour participer utilement au processus démocratique, et, en second lieu, que les politiciens et bureaucrates demeurent comptables envers l'ensemble de la population. […]

---

529 *Déclaration universelle des droits de l'homme*, A.G. Rés. 217 A (III), Doc. A/810 N.U., p. 71 (1948), art. 12.

530 *Pacte international relatif aux droits civils et politiques*, 19 décembre 1966, [1976] R.T. Can. n° 47, art. 17.

531 *Charte canadienne, supra* note 524.

532 Éternelle question! Comme le faisait remarquer la Cour suprême dans *R. c. Tessling*, 2004 CSC 67, [2004] 3 R.C.S. 432, aux para. 23 et 25:

> Au-delà de notre intégrité corporelle et des lieux où nous vivons et travaillons, toutefois, se pose l'épineuse question des renseignements qui nous concernent et des activités que nous pouvons soustraire à la curiosité […] La vie privée étant une notion protéiforme, il est difficile de fixer la limite du «caractère raisonnable».

533 *Hunter c. Southam Inc.,* [1984] 2 R.C.S. 145. L'article 8 a fait l'objet d'une abondante jurisprudence. On voudra bien voir *R. c. Edwards,* [1996] 1 R.C.S. 126; *R. c. Plant,* [1993] 3 R.C.S. 281; *Collins c. R.,* [1987] 1 R.C.S. 265; *British Columbia Securities Commission c. Branch*, [1995] 2 R.C.S. 3; *Charkaoui c. Canada (Citoyenneté et Immigration),* [2007] 1 R.C.S. 350 [*Charkaoui*].

534 *R. c. Hébert*, [1990] 2 R.C.S. 151; *R. c. Broyles*, [1991] 3 R.C.S. 595; *Ruby c. Canada (Solliciteur général)*, [2002] 4 R.C.S. 3. V.a. Ian Kerr et Jena McGill, «Emanations, Snoop Dogs and Reasonable Expectations of Privacy» (2007) 52 Crim. L. Q. 392.

535 Voir dans Daphne Gilbert, «Privacy's second home - Building a New Home for Privacy Under Section 15 of the Charter», Ian Kerr, Valerie Steeves et Carole Lucock (dir.), Lessons *from the Identity Trail – Anonymity, Privacy and Identity in a Networked Society* (Oxford, OUP, 2009) [Kerr *et al.*], 144.

536 *Dagg c. Canada (Ministre des Finances),* [1997] 2 R.C.S. 403 [*Dagg*]*,* au para. 69; v.a. *Lavigne c. Canada (Commissariat aux langues officielles),* [2002] 2 R.C.S. 773 [*Lavigne*]*,* au para. 25

537 *Dagg*, *ibid.*, aux paras. 65-66; *Lavigne*, aux paras. 24; *Canada (Commissaire à l'information) c. Canada (Commissaire de la Gendarmerie royale du Canada)*, [2003] 1 R.C.S. 66 [*Canada (Commissaires)*]; *Cie H.J. Heinz du Canada ltée c. Canada (Procureur général)*, [2006] 1 R.C.S. 441 [*Heinz*], au para. 28; *Pro Swing Inc. c. Elta Golf Inc.,* 2006 CSC 52, [2006] 2 R.C.S. 612, au para. 60.

538 *États-Unis c. Burns*, [2001] 1 R.C.S. 283.

> Étant l'expression de la personnalité ou de l'identité unique d'une personne, la notion de vie privée repose sur l'autonomie physique et morale __la liberté de chacun de penser, d'agir et de décider pour lui-même. »[539]

### *10.1.1.2. La restriction d'utilisation à certaines fins*

Les renseignements personnels sont les informations qui, seules ou en combinaison avec d'autres, permettent **d'identifier**, de manière directe ou indirecte, une personne physique. La plupart des lois illustrent la notion de nombreux exemples[540], mais le terme a une portée encore plus large[541]. La protection de ces données participe évidemment de celle de la vie privée. Cette filiation, reconnue de manière liminaire dans plusieurs lois[542], est consacrée de longue date par la Cour suprême:

> Enfin il y a le droit à la vie privée en matière d'information. Cet aspect aussi est fondé sur la notion de dignité et d'intégrité de la personne. Comme l'affirme le groupe d'étude[[543]] (à la p. 13): «Cette conception de la vie privée découle du postulat selon lequel l'information de caractère personnel est propre à l'intéressé, qui est libre de la communiquer ou de la taire comme il l'entend»[544].

Si la position de principe est ainsi celle de la **confidentialité des renseignements personnels**, force est de reconnaître que la vie dans un État moderne s'accommode mal de velléités d'isolation[545]. Alors que croît le nombre des opérations requérant l'utilisation ou le transfert d'informations personnelles – autant dans les transactions de nature commerciale que dans les rapports des citoyens avec les instances publiques–, comment assurer les avantages et les promesses de l'ère de l'information tout en évitant les entorses à la vie privée susceptibles d'en découler?

En permettant la collecte, l'utilisation et la transmission d'informations mais en **restreignant cette permission à certaines fins** seulement, la législation canadienne se trouve à la fois à reconnaître et à légitimer le besoin informationnel de certaines organisations[546] et à poser les balises nécessaires à la préservation du droit des individus au respect de leur vie privée. L'atteinte d'un tel équilibre entre le

---

539 *Dagg*, *ibid.*, aux para. 61 et 65.

540 La *LPRP,* par exemple parle de renseignements relatifs à la race, à l'origine nationale, à la couleur, la religion, l'âge, la situation familiale, l'éducation, le dossier médical, le casier judiciaire, les antécédents professionnels, les opérations financières auxquelles il a participé, les numéros, symboles, adresses, empreintes digitales, groupe sanguin, opinions personnelles (sauf celles portant sur autrui), les opinion d'autrui sur l'individu, la correspondance, etc.

541 *Dagg, supra* note 536, aux para. 68-69; *Canada (Commissaires), supra* note 536 aux para. 23-24; *Canada (Commissaire à l'information) c. Canada (Solliciteur général)*, [1988] 3 C.F. 551, à la p. 557.

542 P.ex., l'article 3 de la *LPRPDÉ* prévoit avoir pour objet de «fixer […] des règles régissant la collecte, l'utilisation et la communication de renseignements personnels d'une manière qui tient compte du droit des individus à la vie privée à l'égard des renseignements personnels qui les concernent». De même, l'article 1 de la *Loi sur l'accès à l'information et la protection de la vie privée*, L.R.O. 1990, fait état de deux préoccupations, d'une part, «procurer un droit d'accès à l'information» régie par le gouvernement (al. 1a)) et, d'autre part, «protéger la vie privée des particuliers que concernent les renseignements personnels».

543 *Ordinateur et vie privée, supra* note 516.

544 *R. c. Dyment,* [1988] 2 R.C.S. 417 [*Dyment*], au para. 22.

545 Jennifer Chandler, «Privacy versus National Security – Clarifying the Trade-off», dans Kerr *et al., supra* note 535, 122 [Chandler], p. 128.

546 On emploiera le terme «organisations» lorsqu'il s'agira de désigner à la fois les institutions visées par les lois portant sur le secteur public et les entreprises ou organismes couverts par celles visant le privé.

respect des droits de la personne et les exigences pratiques de l'administration ou du commerce est d'ailleurs le dessein admis de plusieurs lois[547] ou déclarations de principes[548]. À cet égard, il importe toutefois de souligner que ce ne sont pas deux concepts d'égale valeur que l'on met ici en balance: l'orientation de base demeure la **protection des renseignements**[549], seulement, la législation participe également d'un souci d'accommoder d'autres intérêts, établissant le cadre d'opération des exceptions à ce principe de confidentialité (cf. également 10.1.2.).

## 10.1.2. Principes du traitement des données et principes de transparence

### *10.1.2.1. Principes fondamentaux*

Évidemment, étant donné la nature variable des renseignements personnels et la diversité des utilisations qui peuvent en être faites, ce cadre doit à la fois être souple, c'est-à-dire convenir à des besoins multiples, et suffisamment clair pour fermer la porte aux abus. Les principes qui traversent la législation canadienne peuvent en ce sens être concentrés en deux objectifs[550], l'un plus matériel, l'autre, plus procédural.

D'abord, il doit exister un critère qui gouverne la divulgation de l'information, afin d'assurer qu'elle n'empiète pas indûment sur la vie privée. Au Canada, un consensus s'est généralement formé autour des **principes de nécessité** –sans l'information, la transaction ne peut avoir lieu–, **de rationalité** –la

---

547 La *LPRPDÉ* le reconnaît d'ailleurs expressément, dans son titre complet –*Loi visant à faciliter et à promouvoir le commerce électronique en protégeant les renseignements personnels recueillis, utilisés ou communiqués dans certaines circonstances* […]– ainsi que dans l'article 3, portant sur son objet:

> 3. La présente partie a pour objet de fixer, dans une ère où la technologie facilite de plus en plus la circulation et l'échange de renseignements, des règles régissant la collecte, l'utilisation et la communication de renseignements personnels d'une manière qui tient compte du droit des individus à la vie privée à l'égard des renseignements personnels qui les concernent et du besoin des organisations de recueillir, d'utiliser ou de communiquer des renseignements personnels à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances.

On trouve des formulations similaires dans les lois britanno-colombienne et albertaine. Cet objectif est implicite dans la loi québécoise.

548 *Déclaration sur la libre circulation de l'information et du commerce en Amérique du Nord* (février 2008), en-ligne: www.spp-psp.gc.ca/eic/site/spp-psp.nsf/fra/00097.html; [548] Organisation de coopération et de développement économiques, *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel* (23 septembre 1980), en-ligne: www.oecd.org/document/18/0,3343,fr_2649_34255_1815225_1_1_1_1,00.html [*Lignes directrices de l'OCDÉ*].

549 *Heinz*, au para. 31.

550 *Lavigne*, au para. 24:

> La *Loi sur la protection des renseignements personnels* est également une loi fondamentale du système juridique canadien. Elle a deux objectifs importants. Elle vise, premièrement, à protéger les renseignements personnels relevant des institutions fédérales et, deuxièmement, à assurer le droit d'accès des individus aux renseignements personnels qui les concernent.

personne raisonnable y verrait-elle une objection? – et du **respect des finalités** –qui doivent donc être déterminées au plus tard au moment de la collecte, et expliquées au besoin[551].

> Dans la société contemporaine tout spécialement, la conservation de renseignements à notre sujet revêt une importance accrue. Il peut arriver, pour une raison ou pour une autre, que nous voulions divulguer ces renseignements ou que nous soyons forcés de le faire, mais les cas abondent où on se doit de **protéger les attentes raisonnables** de l'individu que ces renseignements seront gardés confidentiellement par ceux à qui ils sont divulgués, et qu'ils ne seront utilisés que pour les fins pour lesquelles ils ont été divulgués[552].

De plus, il doit exister des formes de contrôle qui permettent d'assurer le respect de l'interdit matériel et de ses exceptions. Ce contrôle se présente à la fois *a priori*, sous la forme de saines pratiques de gestion, voire de **privacy by design**[553], et *a posteriori,* sous la forme d'un **droit d'accès** large aux dossiers contenant des renseignements sur le compte d'un particulier et, le cas échéant, d'un droit de demander la rectification de données erronées ou la suppression d'informations non pertinentes, que ce droit soit exercé directement par l'individu concerné ou par le biais d'une autorité désignée à cette fin. On aura l'occasion d'y revenir plus en détail lorsque l'on étudiera les recours des particuliers et les pouvoirs des autorités de protection[554].

#### *10.1.2.2. Les dix principes*

Les objectifs cadres peuvent bien sûr être mise en œuvre de diverses manières. Il convient d'entrée de jeu de glisser un mot des **dix principes de traitement des données** recensés au *Code type sur la protection des renseignements personnels* de l'Association canadienne de normalisation[555], un code qui repose en bonne partie sur les *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données à caractère personnel*[556] proposées par l'Organisation de coopération et de développement économiques et auxquelles le Canada a adhéré en 1984. Ces principes sont la responsabilité, la détermination des fins de la collecte des renseignements, le consentement, la limitation de la collecte, la limitation de l'utilisation, de la communication et de la conservation, l'exactitude, les mesures de sécurité, la transparence, le droit d'accès et le droit de contestation.

S'il s'agissait à la base d'un code d'autorégulation des entreprises, autrement dit, de pratiques auxquelles elles étaient libres de souscrire, le *Code type* a depuis acquis un **caractère obligatoire**, de par son intégration à la LPRPDÉ, dont il constitue l'annexe 1. Non seulement les entreprises assujetties

---

551 Voir Philippa Lawson et Mary O'Donoghue, «Approaches to Consent in Canadian Data Protection Law», dans Kerr *et al., supra* note 535, 23 [Lawson-O'Donoghue].

552 *Dyment*, *supra* note 544, au para. 22.

553 La commissaire à l'information et à la vie privée de l'Ontario se présentant d'ailleurs comme la chef de file en la matière, sinon comme l'inventrice de l'expression, voir: Ann Cavoukian, *Privacy by Design* (2009), en-ligne: www.ipc.on.ca/images/Resources/privacybydesign.pdf.

554 Respectivement *infra* aux pp. 35 et 26.

555 Association de normalisation du Canada, *Code type sur la protection des renseignements personnels,* CAN/CSA-Q830-96 (mars 1996), en-ligne: www.csa.ca/cm/ca/fr/protection-des-renseignements-personnels/publications-fr/code-canadien-de-protection-renseignements-personnels [*Code type*].

556 *Lignes directrices de l'OCDÉ*, *supra* note 7.

à la LPRPDÉ sont-elles obligées de se conformer à ses prescriptions[557], leur respect est également l'un des critères de reconnaissance du caractère équivalent d'une loi provinciale visant le privé[558]. Cette norme devient ainsi, en quelque sorte, la trame de toutes les politiques en matière de protection des renseignements dans le secteur privé.

### 10.1.3. Traitement des données particulièrement sensibles et sécurité de donnés

Pas de disposition spécifique.

### 10.1.4. Communication transfrontière des données

En matière de communications transfrontières, seule la *LPRPDÉ* gouverne, même les entreprises dont l'utilisation des renseignements est généralement soumise à une loi provinciale. Le transfert intracanadien de renseignements personnels ne pose pas réellement problème, eu égard à l'uniformité des régimes (et à l'uniformité du droit criminel). La question de l'application extraterritoriale de la LPRPDÉ, par contre, a fait l'objet de certains débats.

En effet, rien dans son libellé ne restreint son application aux entreprises opérant physiquement au Canada, ni, au contraire, n'indique qu'elle entend s'appliquer à toute transaction se déroulant canadien[559]. Qu'en est-il alors d'un fournisseur basé à l'étranger mais dont les services sont disponibles par Internet à des Canadiens? Selon les règles générales de compétence, il est hors de portée de la LPRPDÉ et, si ses pratiques peuvent faire l'objet d'une plainte, les **pouvoirs d'enquête** du Commissariat à la protection de la vie privée du Canada (CPVPC) se trouvent toutefois considérablement **réduits** «parce qu'elle ne peut ni assigner les membres d'une organisation à comparaître ni entrer dans ses locaux au Wyoming»[560].

La LPRPDÉ ne s'étend donc pas aux entreprises étrangères faisant affaire au Canada sans s'y trouver. Par contre, elle s'applique aux entreprises canadiennes impartissant de l'information à l'étranger, qu'il

---

557 On a reproché au *Code type* de contenir à la fois des obligations et des recommandations: Comeau «Protection», *supra* note 516, à la p. 21. Quoi qu'il en soit, ce double niveau d'obligation se reflète dans l'article 5 *LPRDPÉ*:

> **5.** (1) Sous réserve des articles 6 à 9, toute organisation doit se conformer aux obligations énoncées dans l'annexe 1. (2) L'emploi du conditionnel dans l'annexe 1 indique qu'il s'agit d'une recommandation et non d'une obligation.

558 *LPRPDÉ,* art. 26(2)b):

> **26.** (2) [Le gouverneur en conseil] peut par décret: […] *b*) s'il est convaincu qu'une loi provinciale essentiellement similaire à la présente partie s'applique à une organisation — ou catégorie d'organisations — ou à une activité — ou catégorie d'activités —, exclure l'organisation, l'activité ou la catégorie de l'application de la présente partie à l'égard de la collecte, de l'utilisation ou de la communication de renseignements personnels qui s'effectue à l'intérieur de la province en cause.

559 Ce qui est probablement sage quand on sait comment il peut être difficile d'établir le lieu véritable d'une cybertransaction: Frazier, *supra* note 518, aux pp. 210-211

560 *Lawson c. Accusearch Inc.,* 2007 CF 125, [2007] 4 R.C.F. 314, au para. 28; v.a. *Société canadienne des auteurs, compositeurs et éditeurs de musique c. Association canadienne des fournisseurs Internet,* 2004 CSC 45, [2004] 2 R.C.S. 427.

s'agisse de partenariats, de contrats de sous-traitance ou de maintenance de bases de données[561]. Leurs obligations ne se trouvent pas modifiées par le caractère transfrontalier de la communication. Si elles sont **libres de transférer** des données dans quelque endroit que ce soit, en revanche, elles exposent alors leur propre responsabilité si un «**degré comparable de protection**» n'est pas assuré par leur partenaire ou si l'information transférée est utilisée à des fins autres que celles pour lesquelles elle a été consentie[562].

Autrement dit, contrairement à l'approche de direction étatique qui a prévalu en Europe[563] et au Québec[564], c'est aux entreprises qui désirent faire traiter à l'étranger de l'information sur des Canadiens qu'il revient, «personnellement», de **s'assurer de la fiabilité** de leurs partenaires internationaux. En pratique, cela revient à tenir compte des politiques de gestion du partenaire étranger lui-même, mais aussi, inévitablement, du cadre juridique général de son État, voire du climat sociopolitique –car même les plus strictes stipulations d'un contrat d'impartition ne sauraient avoir préséance sur une loi, peut-être intrusive mais dûment adoptée[565].

---

561 *Commissaire à la protection de la vie privée du Canada c. SWIFT [Society for Worldwide Interbank Financial Telecommunication],* rapport de conclusions (2 avril 2007), en-ligne: www.priv.gc.ca/cf-dc/2007/swift_rep_070402_f.cfm.

562 CPVPC, *Lignes directrices sur le traitement transfrontalier des données personnelles* (janvier 2009), en-ligne: www.priv.gc.ca/information/guide/2009/gl_dab_090127_f.cfm

563 *Supra* note 518.

564 Le Québec a retenu l'approche européenne, avec l'adoption en 2006 de l'article 70.1 *L.pub. Qué.*, qui se lit:

**70.1.** Avant de communiquer à l'extérieur du Québec des renseignements personnels ou de confier à une personne ou à un organisme à l'extérieur du Québec la tâche de détenir, d'utiliser ou de communiquer pour son compte de tels renseignements, l'organisme public doit s'assurer qu'ils bénéficieront d'une protection équivalant à celle prévue à la présente loi.

Si l'organisme public estime que les renseignements visés au premier alinéa ne bénéficieront pas d'une protection équivalant à celle prévue à la présente loi, il doit refuser de les communiquer ou refuser de confier à une personne ou à un organisme à l'extérieur du Québec la tâche de les détenir, de les utiliser ou de les communiquer pour son compte. 2006, c. 22, a. 47.

La disposition équivalente existe dans la *L.priv.Qué.*:

**17.** La personne qui exploite une entreprise au Québec et qui communique à l'extérieur du Québec des renseignements personnels ou qui confie à une personne à l'extérieur du Québec la tâche de détenir, d'utiliser ou de communiquer pour son compte de tels renseignements doit au préalable prendre tous les moyens raisonnables pour s'assurer:

1° que les renseignements ne seront pas utilisés à des fins non pertinentes à l'objet du dossier ni communiqués à des tiers sans le consentement des personnes concernées sauf dans des cas similaires à ceux prévus par les articles 18 et 23;

2° dans le cas de listes nominatives, que les personnes concernées aient une occasion valable de refuser l'utilisation des renseignements personnels les concernant à des fins de prospection commerciale ou philanthropique et de faire retrancher, le cas échéant, ces renseignements de la liste.

Si la personne qui exploite une entreprise estime que les renseignements visés au premier alinéa ne bénéficieront pas des conditions prévues aux paragraphes 1° et 2°, elle doit refuser de communiquer ces renseignements ou refuser de confier à une personne ou à un organisme à l'extérieur du Québec la tâche de les détenir, de les utiliser ou de les communiquer pour son compte.

565 À cet égard, le Bureau du surintendant des institutions financières, *Ligne directrice - Impartition d'activités, de fonctions et de méthodes commerciales* (mai 2001, rév. mars 2009), en-ligne: www.osfi-bsif.gc.ca/app/DocRepository/1/fra/directrices/saines/directrices/b10_f.pdf, à la p. 11, recommande aux établissements financiers envisageant une impartition à l'extérieur du Canada [d']accorder une attention particulière aux exigences juridiques du territoire en question, de même qu'à la situation

À cet égard, l'examen des lois visant la **répression du crime et la sécurité nationale** est particulièrement pertinent. L'adoption par les États-Unis de la USA PATRIOT Act[566] qui permet aux autorités policières américaines d'obtenir de leurs tribunaux, dans le cadre d'une enquête antiterroriste, le droit d'accéder à tout renseignement personnel sur le territoire américain, et ce, à l'insu de la personne concernée, a ainsi suscité de nombreuses inquiétudes[567]. Le CPVPC ne semble toutefois pas s'en être alarmé outre mesure[568]. Malgré le cadre controversé d'adoption de cette loi et même si les États-Unis sont le principal partenaire commercial du Canada[569] et, partant, son plus grand partenaire de transferts informationnels, l'exception qu'elle consacre n'est pas nouvelle: le Canada lui-même possède de semblables règles[570]. La *USA PATRIOT Act* ne change donc pas, comme telle, les obligations des entreprises canadiennes, y compris les institutions financières[571], à qui il demeure loisible de transmettre de l'information à un partenaire américain, pour autant que les règles habituelles de responsabilité, de transparence, de respect des fins, etc., soient honorées[572].

Les préoccupations du Commissariat (CPVPC) sont d'un autre ordre, s'inscrivant dans la tension, souvent soulignée[573], entre les impératifs de la **coopération internationale en matière de sécurité** –et les divulgations transfrontalières qu'ils supposent– et la nature vraisemblablement délicate des renseignements susceptibles de faire l'objet d'une demande de transfert au motif de sécurité nationale. La commissaire s'est ainsi dite soucieuse du flou et de la culture du secret entourant les

---

politique, économique et sociale étrangère et aux événements susceptibles de réduire la capacité du fournisseur de services étranger d'assurer le service, sans oublier tout autre facteur de risque pouvant nécessiter l'ajustement du programme de gestion des risques.

566 *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act*, 115 Stat. 272 (2001).

567 Voir pour les politiques fédérales, Secrétariat du Conseil du Trésor, *Politique sur la protection de la vie privée* (1er avril 2008), en-ligne: www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=12510&section=text.

568 CPVP, *Communication transfrontalière de renseignements sur les Canadiens et les Canadiennes – Répercussions de la* USA PATRIOT Act*,* Mémoire du Commissariat à la protection de la vie privée du Canada présenté au Commissariat à l'information et à la protection de la vie privée de la Colombie Britannique (18 août 2004), en-ligne: www.priv.gc.ca/media/nr-c/2004/sub_usapa_040818_f.cfm; v.a. Secrétariat du Conseil du Trésor, «Protéger les renseignements personnels – Un impératif: La stratégie fédérale visant à répondre aux préoccupations suscitées par la USA PATRIOT Act et le flux de données transfrontière» (mars 2006), en-ligne: www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_128/pm-prp/pm-prp-fra.asp.

569 McClennan-Schick, *supra* note 518, à la p. 682.

570 On pensera ainsi à certaines dispositions de la *Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes*, L.C. 2000, c. 17, de la *Loi sur le ministère de la Citoyenneté et de l'Immigration,* L.C. 1994, c. 31 ou de la *Loi sur le Service canadien du renseignement de sécurité*, L.R.C. 1985, c. C-23.

571 *Affaire Visa-CIBC, supra* note 647

572 Voir, pour un fin mot sur la question, Kris Klein, «Clarification de l'application du droit canadien de la protection des renseignements personnels au transfert transfrontalier de ces renseignements du Canada vers les États-Unis» (septembre 2008), en-ligne: www.ic.gc.ca/eic/site/ecic-ceac.nsf/fra/gv00508.html.

573 P.ex., dans le sillage de l'affaire *Charkaoui, supra* note 533; v.a. Chandler, *supra* note 545, aux pp. 122-125; Stephen Townley, «Use and Misuse of Secret Evidence in Immigration Cases: A Comparative Study of the United States, Canada, and the United Kingdom» (2007) 32 Yale J. Int'l L. 219; Thomas Poole, «Recent Developments in the "War on Terrorism" in Canada» (2007) 7 HR. L. Rev. 633.

échanges d'informations entre États, autrement dit de l'information *librement consentie* par le gouvernement canadien à des gouvernements étrangers.

> « Le droit des personnes de savoir quels renseignements le gouvernement détient à leur égard, tout comme le droit d'insister pour que ces renseignements soient pertinents et exacts, est un élément fondamental du droit au respect de la vie privée. [Dans le régime des certificats de sécurité[574], le gouvernement canadien] a caché indûment et inutilement des renseignements importants aux personnes concernées. Le caractère obscur de nombreuses initiatives visant la sécurité nationale va carrément à l'encontre du droit à la protection des renseignements personnels, à savoir le droit des personnes de vérifier la nature et l'exactitude des renseignements recueillis à leur égard par des organismes publics et privés. »[575]

La **Cour suprême** a d'ailleurs reconnu que la légitimité de ses préoccupations en concluant que le secret entourant les informations recueillies dans le régime des certificats de sécurité contrevenait aux principes de justice naturelle garantis par l'article 7 de la *Charte canadienne* e empêchant la personne visée de répondre effectivement aux accusations du gouvernement[576]. Appelant à la vigilance, elle a **recommandé de renforcer les dispositions de la LPRP** sur la sécurité nationale ou à tout le moins de définir un cadre de protection pour la transmission de telles données[577]. Cette proposition a fait l'objet de vifs débats en commission parlementaire. Si personne n'a proposé l'approche radicale qui prévaut en Colombie-Britannique ou en Nouvelle-Écosse où il est simplement interdit à l'administration de transférer des renseignements à l'extérieur du Canada[578], certains ont suggéré la négociation d'ententes bilatérales, d'autres, l'adoption d'un standard de «protection équivalente», à l'européenne (ou à la québécoise). Dans la tendance inverse, d'autres estiment que toute modification législative rigidifierait inutilement des échanges par nature confidentiels et protégés et, de ce fait, traités avec circonspection[579]. La question est désormais à l'étude par Justice Canada[580].

## 10.1.5. Droit d'accès

### *10.1.5.1. Principe et exceptions*

En principe, une organisation est tenue de communiquer à celui qui en fait la demande écrite[581] **tout renseignement qu'elle détient** sur son compte (ou sur le compte de son mandant[582]). Ce principe

---

574 *LPRP,* art. 70.1; *LPRPDÉ,* art. 4.1; *LAI,* art. 69.1; *Loi sur la preuve au Canada,* L.R.C. 1985, c. C-5, art. 38.13 *et s.*

575 CPVPC, Addendum au document Responsabilité du gouvernement en matière de renseignements personnels: Réforme de la Loi sur la protection des renseignements personnels (avril 2008), en-ligne: www.priv.gc.ca/information/pub/pa_ref_add_080417_f.cfm, à la p. 4

576 *Charkaoui*, *supra* note 533.

577 CPVPC, *Recommandations 2009*, *op. cit.*, à la recommandation n$^{o}$ 10; Jennifer Stoddart, «Droits et réalité: augmenter la surveillance des programmes en matière de sécurité nationale du Canada», Mémoire présenté au Comité permanent de la sécurité publique et nationale (Ottawa, le 7 mai 2009), en-ligne: www.priv.gc.ca/parl/2009/parl_sub_090507_f.cfm.

578 *L.pub. C.-B.*, art. 30.1-30.2, 33.1-33.2; *Personal Information International Disclosure Protection Act,* S.N.S. 2006, c. 3 encore que cette dernière n'interdise pas, contrairement à la première, aux gouvernements étrangers d'avoir accès aux renseignements.

579 Rapport Szabo, *supra* note 639, aux pp. 22-24.

580 *Ibid.*

581 Au Québec, la demande d'accès faite à une institution publique peut être orale, mais le refus ne pourra alors faire l'objet d'un contrôle (art. 43 *et s. L.pub.Qué*).

582 Exception inusitée, l'article 8(2)g) *LPRP* permet au député d'obtenir certaines informations sur un commettant qui aurait sollicité son intervention.

souffre néanmoins certaines exceptions, dont la preuve est toutefois à la charge de celui qui désire empêcher la divulgation[583]. Ainsi, un particulier ne pourra obtenir l'accès à une information concernant également un **tiers**, sauf consentement de ce dernier, non plus qu'à de l'information susceptible de causer **préjudice**, à lui-même ou à autrui[584].

Ces deux exceptions valent tant pour le secteur public que pour le secteur privé. Le **secteur public** en connaît cependant d'autres, eut égard aux **fonctions particulières de l'État**. Selon le cas, le responsable de l'institution public devra ou pourra –l'absoluité et l'existence des interdits variant selon les lois, il faut se reporter aux termes de chacune– refuser de divulguer certains documents de nature **politique** (p.ex., les documents portant sur les relations intergouvernementales, sur la défense ou la sécurité du Canada, l'agenda du Premier ministre[585], les documents du Conseil privé ou du conseil exécutif), **législative** (p.ex. les projets de loi en cours d'élaboration, les avis juridiques), susceptibles d'entraver l'exécution de la loi (p.ex., entrave à un agent de la paix ou à un enquêteur, représailles à la suite de dénonciation[586]) ou de porter atteinte à l'administration de la justice, à la sécurité publique, à l'environnement, ou au bien-être économique d'une province. Il dispose également d'une marge d'appréciation en ce qui a trait aux documents couverts par le secret professionnel ou de fabrique. Le responsable institutionnel est enfin dispensé de communiquer des renseignements qui seront rendus publics sous peu. La nature vraisemblablement préjudicielle de la communication est implicite dans ces exceptions[587].

En outre, dans certaines juridictions, peuvent être constitués, par décret, des **fichiers spéciaux**[588] où seront versés des renseignements personnels visant à prévenir, détecter ou réprimer le **crime** ou les infractions aux lois ou, dans le cas du fédéral, touchant à la défense et aux affaires internationales. Ces fichiers seront inaccessibles aux particuliers et seul le commissaire à la vie privée pourra en évaluer le contenu.

---

583 *Reyes c. Canada (Secrétariat d'État)*, [1984] A.C.F. n$^{o}$ 1135 (QL) (C.A.F.), au para. 3.

584 Barbara McIsaac *et al*, *The Law of Privacy in Canada* (Toronto, Carswell, feuilles mobiles), à la p. 3-15, trad. et cité avec approbation dans *Lavigne,* au para. 29: «Le critère de la prévisibilité raisonnable du dommage exige une attente raisonnable de préjudice "probable"».

585 La question, débattue depuis une dizaine d'année devant les tribunaux, fait désormais l'objet d'un pourvoi devant la Cour suprême du Canada. Les audiences ont eu lieu le 7 octobre 2010 et le jugement a été pris en délibéré (voir: *Commissaire à l'information du Canada c. Commissaire de la Gendarmerie royale du Canada*, dossier n$^{o}$ 33297, permission d'en appeler accordée le 17 décembre 2009 dans *Information Commissioner of Canada v. Commissioner of the Royal Canadian Mounted Police*, 2009 CanLII 71480).

586 *Loi sur la protection des fonctionnaires divulgateurs d'actes répréhensibles*, L.C. 2005, c. 46.

587 Exceptions dont on fera remarquer à juste titre que plusieurs relèveront vraisemblablement davantage du droit de savoir ce qu'il advient des fonds publics que de la protection des renseignements personnels d'un particulier. Sur cette question voir *supra*, p. 3, n. 517. Sur la nature antipréjudicielle de ces exceptions, voir Commission d'accès à l'information du Québec, *Une réforme de l'accès de l'information: le choix de la transparence* (Québec, Éd. off., 2002), en-ligne: qww.cai.gouv.qc.ca/06_documentation/01_pdf/quin.pdf [CAI, *Quatrième rapport quinquennal*], aux pp. 30 à 43.

588 La terminologie varie Québec parle de «fichiers confidentiels» (*L.pub.Qué.* art. 80), le fédéral de «fichiers inconsultables» (*LPRP,* art. 18).

#### *10.1.5.2. Recours pour accès en cas de refus*

Le particulier à qui l'on a refusé l'accès aux renseignements personnels le concernant (ou dont on a ignoré la demande, ce qui est assimilé à un refus) peut, pourvu qu'il ait épuisé les recours disponibles au sein de l'organisation avec laquelle il a maille à partir, se tourner vers le **commissaire à la vie privée**. Le dépôt d'une plainte recevable auprès du commissaire enclenchera le processus d'enquête prévu par la loi. Lorsque l'accès a été refusé au motif que la demande portait sur un fichier confidentiel ou inconsultable, le commissaire pourra, lui, consulter le fichier en question et, le cas échéant, amorcer une enquête de conformité. C'est également le commissaire qui pourra consulter les dossiers des curateurs publics ou des protecteurs des incapables ou les dossiers d'adoption, c'est-à-dire des dossiers qui concernent des personnes qui ne sont pas en mesure de faire leur propre demande d'accès –certaines lois le prévoient d'ailleurs expressément[589].

Au terme de l'enquête, qui doit se faire dans la plus grande confidentialité, le commissaire sera tenu de faire **rapport à la fois au plaignant et à l'organisation visée**. Comme on l'a vu, dans certaines provinces, s'il conclut au bien-fondé de la plainte, le commissaire pourra ordonner la communication des documents. Le responsable organisationnel devra alors obtempérer, sauf à se pourvoir en contrôle judiciaire. Dans les autres cas, le commissaire s'en remettra à la seule force de persuasion de ses recommandations.

Lorsqu'il conclut au bien-fondé du refus de communication, le commissaire doit aviser le plaignant de ses recours, notamment de l'instance à laquelle s'adresser pour obtenir une **ordonnance de communication**. Le commissaire peut parfois instituer cette procédure au nom du plaignant. Les délais pour se porter en révision sont assez courts, mais n'emportent pas la déchéance absolue et le demandeur peut être relevé de son défaut. Le recours en révision sera généralement instruit selon une procédure sommaire ou allégée. Puisque le refus d'accès est l'exception, le fardeau de la preuve repose sur l'organisation. Après audition des parties, le tribunal saisi de la requête pourra rendre, le cas échéant, l'ordonnance de communication appropriée. Souvent, il disposera en sus d'un pouvoir d'octroyer des dommages-intérêts[590].

### 10.1.6. Impact des nouvelles technologique

#### *10.1.6.1. Rédaction législative*

Le support électronique a gagné sa place dans la législation canadienne. Le contraire serait étonnant lorsque 90% des dossiers de l'administration fédérale –le plus important dépositaire d'informations personnelles au pays– sont désormais dématérialisés[591]. Signatures électroniques, paiements en ligne,

---

589 P.ex., *L.pub.Qué.*, art. 127.

590 Ce n'est notablement pas le cas en vertu de la *LPRP*, la CPVPC ayant d'ailleurs recommandé une modification en ce sens: CPVPC, *Recommandations 2009*, *supra* note 628, à la recommandation n° 2.

591 Chantal Bernier, «Questions pressantes en matière de protection de la vie privée dans le secteur fédéral», notes pour une allocution devant le Congrès de l'Association sur l'accès et la protection de l'information (Québec, 6 mai 2009), en-ligne:www.priv.gc.ca/speech/2009/sp-d_20090506_cb_f.cfm [Bernier, «Questions»]

e-enregistrement des actes, la valeur et le mode de ces transactions sont explicités de manière assez précise dans la **seconde partie de la LPRPDÉ** et dans les lois provinciales analogues[592].

Ceci étant, bien qu'elle reconnaisse à l'occasion les incidences des percées technologiques[593], dans son ensemble, la législation canadienne sur la protection des renseignements personnels est **technologiquement neutre dans sa formulation**, c'est-à-dire que les obligations des détenteurs de renseignements ne se trouvent pas modifiées par le support sur lequel ils se trouvent[594]. La règle est celle d'une protection adéquate et ce n'est qu'une modalité d'application que de tenir compte de l'impact de telle ou telle technologie pour détermination le niveau de protection requis. Reflet d'une tendance globale, cette approche minimaliste s'évite l'obsolescence par des références trop précises[595]. Certains estiment en outre qu'elle permet de mettre la protection des renseignements personnels en amont de la conception de toute politique liée aux technologies[596].

#### *10.1.6.2. Préoccupations*

Assurément, les nouvelles technologies peuvent être mobilisées pour la défense de la vie privée. On parle alors de **technologies d'amélioration de la confidentialité**[597]. Si certaines initiatives ont été

---

592 Comeau, «Protection», *supra* note 516, à la p. 21; p.ex., *Loi portant Réforme de l'enregistrement immobilier,* L.R.O. 1990, c. L.4, *Electronic Information and Documents Act*, 2000, S.S. 2000, c. E-7.22; *Loi sur l'enregistrement sur support électronique (lois du ministère de la Justice),* L.R.Y. 2002, c. 68; *Loi sur le commerce et l'information électroniques*, C.P.L.M. c. E55.

593 *Supra* note 547.

594 Encore que certaines législations semblent exclure l'information orale (voir *Renseignements personnels sur la santé au Nouveau-Brunswick: Mettre en équilibre les droits à la protection des renseignements personnels et les exigences en matière d'accès,* Rapport du Groupe de travail du Nouveau-Brunswick sur les renseignements personnels sur la santé présidé par by Jean-Guy Finn and Kevin Malone (22 septembre 2007), en-ligne: www.gnb.ca/0051/personal_health_information/pdf/4853f-web%20version.pdf [Finn-Malone], à la p. 14) ou l'information qui n'est pas enregistrée, p.ex. une caméra de surveillance vidéo dont la bande s'effacerait à mesure (voir CPVPC, *Recommandations 2009*, *supra* note 628, à la recommandation n$^{o}$ 4).

595 John D. Gregory, «Canadian and American Legislation on Electronic Signatures with reflections on the European Union Directive», dans Georges Chatillon (dir.), *Internet international law – International and European studies and comments* (Bruxelles, Bruylant, 2005), 399, aux pp. 401 et s.

596 Voir www.privacybydesign.ca et plus particulièrement le document de la commissaire à l'information et à la vie privée de l'Ontario qui s'est fait le chantre du concept, Ann Cavoukian, *Privacy By Design – The Seven Foundational Principles* (2009, rév. août 2010), en-ligne: www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf. Idéalement, le respect des renseignements personnels devrait être le principe directeur de toute gestion –il ne s'agirait plus de respecter des cadres juridiques, il s'agit plutôt d'en faire la position par défaut.

597 Souvent appelées *PETs,* pour *privacy-enhancing technologies.* Par exemple, la dématérialisation des données permet leur centralisation, ce qui évite les doublons et les consignations inutiles. Elle permet également à l'usager de tenir à jour lui-même les renseignements qui le concerne (autodétermination) ou de juger du niveau d'anonymat qu'il désire (voire, de fragmenter son identité pour être plus difficilement identifiable). Elle permet aussi une diffusion accrue des politiques de vie privée de divers organismes. S'il est vrai que l'utilisation d'Internet laisse beaucoup de traces, il est également vrai que ces traces permettent de retracer, justement, certaines utilisations ou communication de renseignements. Un article instructif, quoique daté, Éloïse Gratton, «The legality of online Privacy-Enhancing Technologies» (2002) 7 *Lex electronica* 2.

prises pour mettre de l'avant leur capacité de protection[598], à vrai dire, les nouvelles technologies ont surtout été abordées dans l'optique où elles ont le potentiel de constituer autant de nouvelles sources d'érosion de la vie privée.

Les commissaires à la vie privée ont ainsi largement fait état de leurs préoccupations quant aux **nouveaux modes de communication**[599]: cyberinsécurité, marketing intrusif, sollicitation indésirable, vol d'identité, cartes à puce (trop) intelligentes, fraude, diffusion de masse erronée, etc. À l'image de l'Internet, ces inquiétudes sont multiformes et leur examen détaillé dépasse le cadre du présent document, mais quelques-unes des plus pressantes peuvent être évoquées en vrac. Il y a d'abord la question du volume: si ces nouvelles technologies rendent les transactions plus efficaces, elles en permettent davantage et augmentent d'autant, en nombre absolu évidemment, les risques de communication illégale. Vient ensuite la crainte que le développement des systèmes de sécurité ne suive pas le rythme du développement des nouvelles technologies: le CPVPC s'est ainsi souvent prononcé sur les risques d'interception des données associés à l'utilisation d'Internet, des réseaux à distance ou des terminaux sans fil. Il y aussi la crainte inverse, soit celle de l'introduction de défaillances techniques dans les systèmes pour en permettre la surveillance par l'État –mais également, en théorie, la captation illicite[600]. Il y a encore le problème de la délocalisation des données et de leur éparpillement, qui fait souvent obstacle à l'application efficace de la loi[601]. Et que dire encore de la protection des données sur les sites personnels et de réseautage, dont le but est, justement, le partage de renseignements personnels[602]?

---

598 V. p.ex., CPVPC, *Vie privée, confiance et innovation – Étayer l'avantage numérique du Canada,* Observations du Commissariat à la protection de la vie privée du Canada présentées dans le cadre de la consultation sur la Stratégie sur l'économie numérique du Canada (9 juillet 2010), en-ligne: www.priv.gc.ca/information/pub/sub_de_201007_f.pdf [CPVPC, *Avantage numérique*]; Information and Privacy; Commissioner for Ontario, «Moving Forward from PETs to PETs Plus: The Time for Change is Now» (janvier 2009), en-ligne: www.ipc.on.ca/images/Resources/petsplus_3.pdf.

599 CPVPC, *Avantage numérique, ibid.*; Bernier, «Questions», *supra* note 591.

600 Chandler, *supra* note 545, aux pp. 134-135 [Chandler]

601 On aura l'occasion d'y revenir, *infra* 10.1.4. Communication transfrontière des données, p. 21.

602 Pour une approche plus théorique, voir Robert Carey et Jacquelyn Burkell, «Heuristics approach to understanding privacy-protecting behaviors in digital social environments», dans Kerr *et al., supra* note 535, 65, pour une analyse empirique voir Jennifer Barrigar, «La vie privée sur les sites de réseau social – Analyse comparative de six sites, Analyse préparée pour le Commissariat à la protection de la vie privée du Canada» (février 2009), en-ligne: www.priv.gc.ca/information/pub/sub_comp_200901_f.cfm. La dénonciation du CPVPC à l'endroit de Facebook éclaire quelques aspects des deux dernières interrogations. En 2009, la commissaire ajointe à la protection de la vie privée du Canada, Élizabeth Denham, déposait son *Rapport de conclusions de l'enquête menée à la suite de la plainte déposée par la Clinique d'intérêt public et de politique d'Internet du Canada contre Facebook Inc. aux termes de la* LPRPDÉ (16 juillet 2009), en-ligne: www.priv.gc.ca/cf-dc/2009/2009_008_0716_f.pdf, lequel dénonçait largement certaines pratiques du site de réseautage social dont on apprenait récemment qu'il avait, à la suite du rapport, modifié certaines de ses politiques: CPVPC, «Le suivi de l'enquête sur Facebook est terminé», Fiche documentaire (22 septembre 2010), en-ligne: www.priv.gc.ca/media/nr-c/2010/bg_100922_f.cfm. On pourra du reste trouver dans cette affaire un certain réconfort quant au poids des recommandations (et réprimandes) du CPVPC dans la mesure où Facebook, une entreprise étrangère, n'est pas assujetti à la *LPRPDÉ*.

Les communications ne sont pas le seul domaine où l'émergence de nouvelles technologies suscite certains questionnements: la biologie et les sciences de la vie soulèvent également leur part d'interrogations. Qu'en est-il des prélèvements génétiques[603]? de la pharmacogénomique? des biobanques? des portraits biométriques[604]? des prélèvements d'ADN? de la filiation[605]? des utilisations secondaires à des fins cliniques ou de recherche[606]? On oppose ici les besoins de la science et l'intérêt public à la conduite de recherche, notamment en génétique et en génomique, et les intrusions à la vie privée que constituent l'utilisation sans consentement de matériel génétique, donnée au caractère hautement identificatoire[607]. Pour le CPVPC, il n'y a pas lieu de relaxer le principe général de consentement éclairé qui préside aux soins de la personne:

> « Les coûts et les inconvénients ne semblent pas valables comme motifs pour contourner le droit fondamental à la vie privée, en particulier pour des renseignements aussi précieux que des renseignements génétiques [...] ceux qui veulent vraiment prendre part à une biobanque donneront le consentement nécessaire. »[608]

Plusieurs **groupes d'études**, estimant qu'une telle approche est inadéquate car elle ne reflète pas le caractère évolutif des projets de recherche ou la nature de pool des biobanques, ont réclamé l'adoption d'un **encadrement juridique propre à la recherche scientifique**[609] et diverses études sont depuis en cours[610].

---

603 Voir Marsha Hanen, «Genetic technologies and medicine – Privacy, Identity, and Informed Consent», dans Kerr *et al*., *supra* note 535, 174.

604 Voir Shoshana Magnet, «Using biometrics to revisualize the Canada–U.S. border», dans Kerr *et al*., *supra* note 535, 359

605 Voir Michelle Giroux, «Le droit fondamental de connaître ses origines biologiques: impact des droits fondamentaux sur le droit de la filiation» dans Barreau du Québec, La Charte québécoise: origines, enjeux et perspectives (Cowansville, Qc, Yvon-Blais, 2006), 255

606 Voir Donald J. Willison, «Utilisation des données du dossier de santé électronique pour la recherche en santé – Défis en matière de gouvernance et approches possibles» (mars 2009), en-ligne: www.priv.gc.ca/information/pub/ehr_200903_f.cfm [Willison, «Utilisation»], à la p. 8.

607 Voir Bartha M. Knoppers, «Introduction: Of Genomics and Public Health: Building Public "Goods"?», 143 et Mark A. Rothstein et Herbert F. Boehl, «Privacy Issues in Public Health Genomics», 149, tous deux dans Bartha M. Knoppers, *Genomics and public health: legal and socio-ethical perspectives* (Boston, Martin Nijhoff, 2006).

608 Chantal Bernier «Sous les auspices de Génome Canada et du Commissariat à la protection de la vie privée», notes pour une allocution présentée lors d'un atelier sur la protection des renseignements génétiques» (Otttawa, 27 novembre 2009), en-ligne: www.priv.gc.ca/speech/2009/sp-d_20091127_cb_f.cfm

609 M. Anne Harris, Adrian R. Levy, Kay E. Teschke, «Personal privacy and public health: Potential impacts of privacy legislation on health research in Canada», (2008) 99 Can. J. of Pub. Health 293; Donald J. Willison et al., «Alternatives to project-specific consent for access to personal information for health research: Insights from a public dialogue» (2007) 14 J. of the Am. Med. Informatics Ass. 706 [Willison, «Alternative»]

610 Le Fonds de la recherche en santé du Québec a ainsi proposé dans son rapport *Banques de données et banques de matériel biologique – Pour un nouveau cadre éthique et légal* (Québec, Éd. off, 2007), en-ligne: www.frsq.gouv.qc.ca/fr/ethique/pdfs_ethique/Rapport_groupe_conseil_francais.pdf, à la p. 4

> [un] cadre normatif qui aborde les douze objets suivants: • Rôle de fiduciaire de la banque • Responsabilité • Formation continue des membres du personnel • Approbation obligatoire d'un [comité d'éthique de la recherche] compétent [dans les cas d'utilisation secondaire d'information anonymisée] • Détermination des objectifs de l'initiative •Détermination de la nécessité d'obtenir le consentement libre et éclairé • Obtention du consentement libre et éclairé si

La **dématérialisation des dossiers du secteur de la santé** a également attiré l'attention des législateurs canadiens. Les initiatives en la matière sont pour la plupart au stade de l'étude préparlementaire ou du projet de loi[611], mais il convient de signaler l'adoption, en 2008, de la *E-Health Act*[612] et en 2009, de l'ajout de la partie 5.1 «Alberta Electronic Health Record» à la *Health Information Act* albertaine[613]. Ces dispositions prévoient les paramètres d'opération d'un système informatisé de gestion des dossiers médicaux, concrétisant ainsi des obligations générales dans un cadre précis, celui de la santé. L'interdiction formelle d'utiliser des banques de données médicales pour la conduite d'études de marché n'est ainsi qu'une forme du principe général de non-divulgation comme le droit des individus de «masquer» certaines données de leur dossier l'est du principe de retrait du consentement. Si quelques projets-pilotes ont déjà été entrepris ou si certains centres hospitaliers ont numérisé leurs propres dossiers, ces projets de lois sont d'abord préventifs car le système unique qu'ils cherchent à baliser n'existe pas encore au Canada[614].

## 10.1.7. Secteur privé et secteur public

### *10.1.7.1. Structure de la protection*

Si, dans l'ensemble, les **attentes législatives sont les mêmes pour les secteurs privé et public**[615], la structure de la protection dans le secteur privé appelle quelques commentaires, notamment eu égard à la structure fédérale de l'État canadien.

En effet, la **LPRPDÉ** s'applique en principe à l'entièreté du **secteur privé** au pays, c'est-à-dire qu'elle s'intéresse tant aux entreprises fédérales qu'aux entreprises provinciales. Le gouverneur en conseil peut toutefois soustraire à son application les entreprises par ailleurs assujetties à une loi provinciale, s'il juge que la protection conférée par cette loi est«essentiellement similaire»[616]. Sera reconnue comme tel la loi provinciale qui «incorpor[e] les dix principes de l'annexe I de la LPRPDÉ; fourni[t] un mécanisme indépendant et efficace de surveillance et de recours et des pouvoirs d'enquête et restrein[t] la collecte, l'utilisation et la communication des renseignements personnels à des fins

---

nécessaire • Conservation et protection de la confidentialité des données et du matériel biologique • Transparence dans la gestion des données et du matériel biologique • Accès aux renseignements personnels • Possibilité de porter plainte• Partage et protection de la confidentialité.
Cette liste n'est pas sans rappeler les dix principes du *Code type*, *supra* note 555. V.a. Willison, «Utilisation», *supra* note 606.

611 Sur la question, Inforoute Santé du Canada, *Livre blanc sur la gouvernance de l'information dans le dossier de santé électronique (DSE) interopérable* (mars 2007), en-ligne: www2.infoway-inforoute.ca/Documents/Information%20Governance%20Paper%20Final_20070328_FR.pdf [*Livre blanc*]; Collectif, *Les dossiers de santé électroniques – Survol des rapports de vérifications fédéral et provinciaux* (avril 2010), rapport des bureaux de vérification de l'Alberta, de la Colombie-Britannique, de l'Île-du-Prince-Édouard, de la Nouvelle-Écosse, de l'Ontario, de la Saskatchewan et du Canada (Ottawa, Éd. off, 2010).

612 *E-Health (Personal Health Information Access and Protection of Privacy) Act,* S.B.C. 2008, c. 38.

613 *Health Information Amendment Act,* 2009, S.A. 2009, c. 25.

614 Willison, «Utilisation» *supra* note 606.

615 Comeau, «Protection», *supra* note 516, à la p. 27.

616 *LPRPDÉ,* art. 26(2)b).

appropriées et légitimes.»[617]. L'exemption ne vaut cependant que pour les affaires intraprovinciales de ces entreprises, qui demeurent soumises à la LPRPDÉ pour toute impartition transfrontalière.

À ce jour, les trois provinces ayant adopté leur **propre loi sur le secteur privé**, soit le Québec, la Colombie-Britannique, l'Alberta, bénéficient de l'exemption[618]. Un décret d'équivalence vise également la loi ontarienne portant sur le secteur de la santé[619].

Ces décrets sont à la source de deux conflits, l'un constitutionnel, l'autre institutionnel. D'abord, des doutes ont été soulevés quant à la **validité constitutionnelle de la LPRPDÉ** au regard du partage des compétences. Certains ont avancé qu'il y avait empiétement dans la sphère de compétence provinciale, dans la mesure où une loi provinciale, adoptée en toute légalité en vertu de l'habilitation constitutionnelle des provinces à légiférer sur «la propriété et les droits civils»[620], catégorie qui comprend les renseignements personnels, pourrait néanmoins, en pratique, se trouver «neutralisée» du fait de son double emploi avec la loi fédérale[621]. Pour d'autres cependant, la compétence générale du gouvernement fédéral en matière de commerce suffit à justifier un tel schème législatif[622]. Les tribunaux ne se sont pas encore prononcés sur la question[623].

Le second conflit engendré par ces décrets oppose Industrie Canada au **Commissaire à la protection de la vie privée** du Canada. Le ministère joue un rôle prééminent en matière de protection des renseignements personnels dans le secteur privé. En effet, non seulement est-ce lui qui est à l'origine

---

617 Industrie Canada, «Processus de détermination du caractère "essentiellement similaire" d'une loi provinciale par le gouverneur en conseil» (3 août 2002), G.O. vol. 136, n° 31, en-ligne: http://gazette.gc.ca/archives/p1/2002/2002-08-03/html/notice-avis-eng.html.

618 *Décret d'exclusion visant des organisations de la province de Québec,* DORS/2003-374, C.P. 2003-1842 (19 novembre 2003); *Décret d' exclusion visant des organisations de la province d'Alberta,* DORS/2004-219, C.P. 2004-1163 (12 octobre 2004); *Décret d' exclusion visant des organisations de la province de la Colombie-Britannique,* DORS/2004-220, C.P. 2004-1164 (12 octobre 2004*).*

619 *Décret d'exclusion visant des dépositaires de renseignements sur la santé de la province d'Ontario,* DORS/2005-399, C.P. 2005-2224 (28 novembre 2005).

620 *Loi constitutionnelle de 1867* (R.-U.), 30 & 31 Vict., c. 3, art. 92(13).

621 «Rapport dissident du Bloc Québécois» (23 avril 2007), dans Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique, *Examen, prévu par la loi, de la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDÉ) – Quatrième rapport* (mai 2007, 39e législature, 1re session), (Ottawa, Éd. off., 2007), en-ligne: www2.parl.gc.ca/content/hoc/Committee/391/ETHI/Reports/RP2891060/ethirp04/ethirp04-f.pdf, 85; Jacques Frémont (professeur de droit constitutionnel, Université de Montréal), «Témoignage devant le Comité permanent de l'Industrie» (36e législature, 1re session, le 16 mars 1999), en-ligne: www2.parl.gc.ca/HousePublications/Publication.aspx?DocId=1039366&Language=F&Mode=1&Parl=36&Ses=1, à la p. 1115.

622 Mahmud Jamal, «Is PIPEDA Constitutional?» (2004) 43 Rev. can. du droit de commerce 434; John Nisker, «PIPEDA: A Constitutional Analysis» (2005) 85 Rev. du B. can 317.

623 Le 17 décembre 2003, le gouvernement québécois avait autorisé le procureur général à saisir la Cour d'appel du Québec d'un renvoi portant sur la validité constitutionnelle de la *LPRPDÉ* (décret n°1368-2003-12-30). L'appel a été suspendu à la demande des parties en septembre 2006 et aucun acte de procédure n'a été produit au dossier depuis (n° de dossier 500-09-014067-037).

Plus récemment, le demandeur ayant eu gain de cause sur une question suffisant à disposer du litige, le juge Mainville n'a pas estimé opportun de se prononcer sur le bien-fondé de ses arguments sur l'invalidité constitutionnelle de la *LPRPDÉ*: *State Farm Mutual Automobile Insurance Company v. Privacy Commissioner of Canada*, 2010 FC 736 [*State Farm*].

de la LPRPDÉ, mais c'est encore sur sa recommandation que le gouverneur en conseil adopte, le cas échéant, un décret d'équivalence[624]. Or, il est désormais notoire que le commissariat estime que les critères employés par le ministère ne garantissent pas nécessairement une protection véritablement équivalente, tel que le requiert la loi. Les tensions ouvertes par cette divergence ont été mises au jour par la décision d'accorder l'équivalence aux lois albertaine et britanno-colombienne, lesquelles avaient été ouvertement critiquée par le commissaire de l'époque[625].

***10.1.7.2. Niveau de protection***

La lecture du *Code type,* annexe 1 à la LPRPDE (cf. supra, 10.1.2.2.), donc intégré dans la législation destiné aux acteurs privés, qui tout à la fois oblige et suggère, a fait dire à certains que la protection des renseignements personnels était mieux balisée pour les entreprises que pour l'État[626]. Sans doute en effet la Loi sur la protection des renseignements personnels (LPRP) souffre-t-elle un peu de la comparaison, mais trois nuances s'imposent. Pour commencer, la LPRP, qui ne fait pas l'objet d'une révision systématique, est sans conteste la moins moderne des lois visant le secteur public. Le modèle présenté par les autres lois visant l'administration, qu'il ait été affiné par modification législative ou que leur adoption soit plus tardive, fait davantage écho à celui de la LPRPDÉ. Il suffit pour se convaincre de la tendance à l'homogénéisation, *mutatis mutandis*, de prendre plutôt en regard la loi néo-brunswickoise entrée en vigueur à l'automne.

Ensuite, le libellé de la loi ne reflète pas toujours avec exactitude la rigueur des exigences auxquelles sont soumises les organisations puisque la loi n'est pas la seule source normative en jeu. On ne saurait ici passer sous silence l'impact des **lignes directrices** déployées par les ministères délégués à la protection des renseignements personnels dans l'ensemble de leur appareil gouvernemental. Ces guides peuvent expliciter la portée des obligations de l'administration, à l'instar des illustrations comprises au *Code type*, auquel, d'ailleurs, elles renvoient parfois[627]. Elles peuvent aussi suppléer à des lacunes perçues[628] en haussant les standards auxquels les institutions seront tenues. Le

---

624 Paul-André Comeau, «Les autorités de contrôle – Données personnelles et francophonie» (septembre 2007), en-ligne: www.cai.gouv.qc.ca/06_documentation/01_pdf/autcont.pdf [Comeau, «Autorités»], à la p. 16.

625 Commissaire à la vie privée, *Rapport au Parlement relativement aux lois provinciales essentiellement similaires* (Ottawa, Éd. off, 2003), en-ligne: www.priv.gc.ca/legislation/leg-rp_030611_f.pdf, aux pp. 7-9.

626 Lawson-O'Donogue, *supra* note 551, à la p. 28.

627 Ainsi le Secrétariat du Conseil du Trésor du Canada suggère-t-il dans sa *Politiques de l'information et de la protection des renseignements personnels* (2005, rév. 2008, en-ligne: www.tbs-sct.gc.ca/atip-aiprp/tools/priv-prp-fra.asp [SCTC, *Politique de l'information*] la consultation des *Lignes directrices de l'OCDÉ* et du *Code type*. La *Loi sur la protection des renseignements personnels,* L.N.-B. 1998, c. P-19.1, remplacée et abrogée par la *L.pub. N.-B.*, contenait un «Code de pratiques statutaires» et une annexe interprétative qui reprenaient pour l'essentiel le *Code type*.

628 Commissariat à la protection de la vie privée du Canada [CPVPC], *Rapport annuel au Parlement 2007-2008 – Rapport concernant la Loi sur la protection des renseignements personnels* par Jennifer Stoddart (Ottawa, Éd. off, 2008) [CPVPC, *Rapport 2008*], à la p. 47; v.a. CPVPC, *Responsabilité du gouvernement en matière de renseignements personnels: Réforme de la Loi sur la protection des renseignements personnels* par Jennifer Stoddart (juin 2006), en-ligne: www.priv.gc.ca/information/pub/pa_reform_060605_f.cfm; *Recommandations pour la réforme de la* Loi sur la protection des renseignements personnels (2009), en-ligne: www.priv.gc.ca/parl/2009/parl_090511_02_f.cfm [CPVPC, *Recommandations 2009*], à la recommandation n$^{o}$ 1.

fonctionnement des institutions fédérales offre un exemple frappant d'un tel renforcement: alors que la LPRP ne pose qu'un critère de connexité dans la collecte de renseignements[629], les lignes directrices du secrétariat du Conseil du Trésor, elles, fixent un critère de nécessité, avec le résultat qu'*en pratique*, l'administration canadienne se trouve tenue à une norme aussi sévère que les administrations provinciales[630]. Sans doute serait-il préférable que la législation reflète la pratique[631] mais, à défaut d'une refonte, la démarche du Conseil du trésor s'inscrit tout à fait dans l'esprit qui anime la protection des renseignements personnels[632].

Enfin, la **nature particulière de l'État** coupe court à toute tentative de correspondance parfaite. D'emblée, on voudra illustrer par certaines limites du droit d'accès propre à la raison d'État: une entreprise pourra difficilement invoquer le secret-défense, l'administration de la justice ou la préservation du patrimoine pour justifier un refus de communication alors que ces exceptions sont tout à fait envisageables dans le contexte public.

C'est cependant certainement **la notion de consentement** qui offre l'exemple le plus saillant du décalage qui peut exister entre la logique du secteur privé et celle du secteur public –mais qui montre également comment une protection comparable peut être atteinte de diverses manières[633]. Étroitement lié au principe de détermination des finalités, le consentement est un précepte capital dans la protection des données personnelles dans le secteur privé: l'individu est libre de partager ou non des renseignements à son sujet, et libre aussi de changer d'avis[634]. Ce principe ne saurait animer de la même manière les relations des particuliers avec l'appareil public, puisqu'elles ne sont généralement pas volontaires. Le consentement n'est que l'une des justifications à la collecte des renseignements par l'État[635], qui peut également avoir lieu là où «elle est expressément autorisée ou

---

629 *LPRP,* art. 4, «Les seuls renseignements personnels que peut recueillir une institution fédérale sont ceux qui ont un lien direct avec ses programmes ou ses activités.» [Nous soulignons.]

630 SCTC, *Politique de l'information, supra* note 627.

631 *Supra* note 628.

632 CPVPC, *Rapport 2008*, *ibid.*

633 Voir généralement Lawson-O'Donoghue, *supra* note 551.

634 Les exigences du principe 4.3 de l'annexe 1 de la *LPRPDÉ* peuvent être résumés ainsi. Le consentement doit être obtenu de manière honnête, licite et sans subterfuge, mais peut l'être sous plusieurs formes: il peut faire l'objet d'une déclaration écrite, être obtenu de vive voix, il peut être fourni électroniquement ou encore être donné par un représentant. Le niveau de consentement requis varie selon la nature de l'information recherchée –on fournit davantage volontiers son prénom que ses empreintes digitales. S'il doit parfois être éclairé, il est souvent implicite. Ainsi, celui qui paie avec une carte de crédit consent nécessairement au transfert de certaines informations sur son compte, de même, celui qui s'abonne à une revue peut s'attendre à ce que son adresse soit utilisée pour l'envoi d'un formulaire de réabonnement. La législation dans le domaine de la santé offre une illustration intéressante des niveaux de consentement: s'il doit d'abord être éclairé, le consentement à la transmission des renseignements ainsi acquis entre les mains de certains professionnels du domaine est ensuite acquis, ou implicite: comparez les articles 18(1) et 18(3) de la *L.s. Ont.* (qui parlent respectivement de consentement éclairé et de consentement explicite) et 17 et 18 de la *L.s. N.B.* (qui parlent plutôt de consentement éclairé puis de consentement présumé être éclairé).

635 Lawson-O'Donoghue, *supra* note 551, à la p. 28, pour qui, en outre, alors que le consentement est une *condition* à la collecte dans le secteur privé, ce n'est qu'une *justification* dans le secteur public (aux pp. 23-24).

requise en vertu d'une loi de la province ou d'une loi fédérale» ou lorsque «les renseignements sont recueillis aux fins de l'exécution de la loi»[636]. En ces cas, elle se passe de consentement.

Certes, certains services dispensés par le gouvernement, comme la santé ou l'éducation, répondent à une logique plus marchande ou supposent davantage d'élection de la part des citoyens, mais on saurait difficilement en dire autant du rapport des contribuables avec l'agence du revenu du Canada ou des voyageurs avec le service des douanes[637]. Il faut alors trouver un précepte homologue pour faire mêmement jalonner la collecte –on a parfois vu dans les exigences de notifications et de collecte auprès de l'individu directement un équivalent fonctionnel[638]– ou une autre forme de garde-fou: le respect des critères de nécessité, de raisonnabilité et de fiabilité y gagnerait d'autant en importance[639]. Mais encore là, la logique est celle d'un rapport, sinon d'identité, au moins d'analogie entre les secteurs privé et public.

La **concordance** est ainsi plus manifeste dans la plupart des principes. Ainsi, rien dans la nature de l'État ne justifie une dérogation, par exemple, à l'exigence d'exactitude des renseignements. L'administration doit elle aussi assurer la confidentialité des informations qu'elle recueille, utilise ou transmet, ce qui suppose qu'elle prend des mesures de sécurité adéquates[640]. Ici encore ces mesures seront à la fois matérielles (acoustique des bureaux, pièces en retrait, classeurs verrouillés), technologiques (mots de passe, encryptions) et administratives (formation, information et politiques de gestion), refléteront l'utilisation et le degré de sensibilité envisagé et inclure toutes les étapes du «cycle de vie» du renseignement personnel, y compris sa destruction. Les fonctionnaires traitants sont autant que les intermédiaires privés autorisés à communiquer les renseignements qu'ils détiennent sur autrui à leur procureur (qui est lui-même tenu à la confidentialité), à toute personne disposant d'un pouvoir de contrainte (commissaire à la vie privée, commission d'enquête, tribunal), à une autorité pour la prévention ou la répression d'actes de violence ou de crimes ainsi qu'à certaines fins artistiques, journalistiques, archivistiques ou statistiques, pourvu que les renseignements aient été anonymisés.

L'administration est elle aussi susceptible d'être visée par une demande de renseignement quant à ses politiques ou par une demande de consultation, à laquelle elle doit acquiescer. À cet égard, l'accès se trouve facilité par l'obligation souvent faite aux institutions publiques de centraliser les

---

636 La formulation est celle de la *L.pub. N.-B.,* art. 37, mais on trouve des équivalents

637 Sur la différence de «philosophie», voir David Fraser (représentant de l'Association du Barreau canadien, témoignage devant la Chambre des communes), témoignage devant le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique (39e législature, 2e session, le 3 juin 2008), en-ligne: www2.parl.gc.ca/HousePublications/Publication.aspx?DocId=3544656&Language=F&Mode=1&Parl=39&Ses=2.

638 Lawson-O'Donoghue, *supra* note 551, à la p. 27.

639 *La Loi sur la protection des renseignements personnels: premiers pas vers un renouvellement*, Rapport du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique (40e législature, 2e session) présidé par Paul Szabo (juin 2009), en-ligne: www2.parl.gc.ca/content/hoc/Committee/402/ETHI/Reports/RP3973469/402_ETHI_Rpt10/402_ETHI_Rpt10-f.pdf [Rapport Szabo], à la p. 5.

640 Sur ce point, bien qu'une telle obligation soit sous-entendue, la CPVPC a recommandé l'incorporation dans la *LPRP* d'une disposition exigeant en toutes lettres l'adoption de mesures de sécurité adéquates visant la protection des renseignements personnels: CPVPC, *Recommandations 2009*, *supra* note 628, à la recommandation no 11.

renseignements détenus sur le compte de chaque particulier[641] et, parfois, de publier des registres portant sur ces renseignements[642].

De la même manière que dans le privé, chaque institution est tenue désigner un responsable qui veillera au respect de ses obligations en matière d'accès à l'information et de protection de la vie privée. En sus, la loi désigne généralement un ministre pour voir à de la mise en place, à l'évaluation et à l'amélioration de l'uniformité des pratiques de son ordre gouvernemental[643].

Au final, la parenté est loin d'être surprenante[644] puisque les deux régimes dérivent des mêmes impératifs quasi constitutionnels de respect de la vie privée[645].

***10.1.7.3. Rapports des entreprises avec les tiers***

La jurisprudence est venue clarifier les droits et obligations ressortant à l'impartition de renseignements aux tiers. D'abord, les entreprises peuvent faire affaire avec des tiers. Rien ne leur interdit la transmission de données, tant qu'elle se fait dans le respect de leurs obligations, notamment l'exigence de **consentement** et le principe de respect des **finalités**. L'interprétation du Commissariat de protection à la vie privée du Canada (CPVPC) est assez libérale[646]. Ainsi, une entreprise n'est pas obligée d'offrir à ses clients une option de refus, lorsque ses services sont fournis par un tiers, même si cela n'avait pas fait l'objet d'un consentement explicite, pourvu que les services fournis par le tiers soient «liés directement aux buts premiers pour lesquels les renseignements personnels ont été recueillis»[647].

Par ailleurs, les entreprises doivent en quelque sorte être prêtes à se porter garantes des ceux avec qui elles font affaire car leurs engagements s'étendent des renseignements qu'elles recueillent à ceux qu'elles leur confient. Elles doivent ainsi s'assurer que leurs tiers contractants observent un **niveau de protection équivalent**[648], faute de quoi, elles exposeront leur propre responsabilité. Cela est particulièrement vrai en contexte international, puisqu'il ne peut être présumé que la loi étrangère tient les tiers impartis aux mêmes garanties de protection que la loi canadienne[649].

Attention cependant, cette règle d'imputation vaut pour les renseignements qu'une entreprise transmet à un tiers et non pour les renseignements recueillis par le tiers, même s'il est lié l'entreprise par une relation commerciale. Une récente décision[650] a jugé que les renseignements ainsi recueillis ne sont pas des «renseignements personnels de l'entreprise» au sens de la LPRPDÉ et donc, ne peuvent faire l'objet d'une demande d'accès à l'information. En l'absence de relation commerciale entre le tiers et l'individu, ce dernier devra s'en remettre aux règles générales sur la protection de la vie privée.

---

641 *L.pub. Qué.*, art. 71 *et s.*; *LPRP*, art. 9.

642 *LPRP*, art. 10; v.a. *L.pub. Man.*, art. 75; *L.pub. Yuk.*, art. 63.

643 Au fédéral, cette tâche est assurée par le Secrétariat du Conseil du Trésor, auprès duquel le ministère de la Justice joue par ailleurs le rôle de conseiller juridique.

644 Comeau, «Protection», *supra* note 516, à la p. 19.

645 *Dyment, supra* note 544, au para. 22.

646 Jennifer Barrigar, Jacquelyn Burkell et Ian Kerr, «Let's Not Get Psyched Out of Privacy: Reflections on Withdrawing Consent to the Collection, Use and Disclosure of Personal Information», dans Kerr *et al., supra* note 535, 1.

647 *Un avis expédié aux clients d'une banque suscite des inquiétudes à propos de la* USA PATRIOT Act, Résumé de conclusions d'enquête du CPVPC en vertu de la *LPRPDÉ* n$^{o}$ 313 (19 octobre 2005) 2005 CanLII 37353 [*Affaire Visa-CIBC*].

648 *LPRPDÉ,* annexe 1, principe 4.1.3.

649 Voir *infra* p. 23.

650 *State Farm, supra* note 624.

### *10.1.7.4. Renseignements personnels des employés*

Coordonnées, information bancaire, numéro d'assurance sociale voire parcours professionnel, situation familiale, renseignements médicaux, antécédents judiciaires[651], même. La liste peut apparaître vertigineuse des informations confidentielles dont le dévoilement s'impose au cours d'une relation de travail moderne. Pourtant, l'uniformité manque cruellement au Canada en la matière, tant en termes d'application des lois qu'au regard des obligations de l'employeur ou du syndicat.

La nécessité du consentement à la communication illustre bien les **disparités d'approche**[652]. Les employeurs albertains et britanno-colombiens, par exemple, ne sont pas tenus d'obtenir le consentement de leurs employés (ce qui comprend également les stagiaires, les bénévoles, les entrepreneurs et parfois les candidats) avant d'utiliser ou de transmettre de l'information personnelle à leur sujet, *sauf* là où une personne raisonnable estimerait qu'il devrait l'être[653]. Certains ont avancé que le même critère valait au Québec, où la loi ne crée pas de régime distinct pour les informations personnelles des employés[654]. De récentes remarques judiciaires laissent pourtant plutôt croire que rien dans la définition de «consentement» ne permet de présumer du consentement des employés[655].

Quoi qu'il en soit et par contraste, la LPRPDÉ exige le consentement de l'employé. Cependant, sa définition de «renseignements personnels» restreint son champ d'application aux seuls renseignements personnels des employés d'entreprises relevant de la **compétence fédérale** (p.ex., banques, compagnies maritimes, radiodiffuseurs). En outre, si certains estiment que cela signifie que la LPRPDÉ ne couvre aucunement les informations personnelles des employés du reste du secteur privé, d'autres croient que cela cesse d'être vrai dès que ces informations font l'objet d'une transaction commerciale, qu'il s'agisse de la vente de l'entreprise ou de l'externalisation de services comme le traitement de la paie ou les régimes de pension[656]. La même question peut se poser pour les activités commerciales des organismes de bienfaisance: normalement, ils sont exclus de la portée de la LPRPDÉ, mais qu'en est-il de leurs activités commerciales, qui constituent souvent une part importante de leurs revenus?

---

651 Mais seulement s'ils ont un lien avec l'emploi: *Québec (Commission des droits de la personne et des droits de la jeunesse)* c. *Maksteel Québec inc.*, 2003 CSC 68, [2003] 3 R.C.S. 228.

652 George Radwanski, alors commissaire à la protection de la vie privée du Canada avait d'ailleurs lourdement fait savoir qu'il estiment que le critère des lois albertaine et britanno-colombienne n'offrait pas une protection «essentiellement similaire» à celle de la LPRPDÉ: il a parlé des critères des lois provinciales comme «d'une faible épreuve et d'une piètre assurance pour les employés actuels ou éventuels qui se soucient de la protection de leur vie privée»: CPVPC, «Lettre à l'honorable Sandy Santorini, ministère des Services de gestion – Commentaire sur le projet de loi 38» (7 mai 2003), en-ligne: www.privcom.gc.ca/media/nr-c/2003/02_05_b_030508_f.asp [CPVPC, «Lettre»].

653 Lisa M. Austen, «Is Consent the Foundation of Fair Information Practices? Canada's Experience under PIPEDA», (2007) 56 U.T.L.J. 181, à la p. 183.

654 Ian Turbull, *Privacy in the Workplace*, 2e éd. (Toronto, CCH, 2009) [Turnbull], à la p. 54, citant *Laval (Ville) c. X.,* 2003 CanLII 44085 (C. du Q.), qui incorpore le test de proportionnalité de l'arrêt *R. c. Oakes*, [1986] 1 R.C.S. 103, ce que Turnbull interprète comme un critère de personne raisonnable analogue à celui des lois albertaine et britanno-colombienne.

655 *Syndicat de Autobus Terremont ltée (CSN) c. Autobus Terremont ltée,* 2010 QCCA 1050, le juge Léger ne se prononçant pas (au para. 70) et les juges Côté et Doyon (au para. 90) s'opposant à l'idée d'un consentement implicite à la communication vu le «caractère exigeant» de l'article 14 de la *L.priv. Qué.*

656 Turnbull, *supra* note 654, à la p. 358. Voir cependant *State Farm*, *supra* note 624.

Débat connexe, celui de savoir ce qui constitue un renseignement **personnel de l'employé**. Qu'en est-il des opinions professionnelles, des documents de travail? On pourrait avancer que les plans d'un architecte, les prescriptions d'un médecin[657] voire les notes de service des avocats sont des «données personnelles» puisqu'ils peuvent être rapportés à un individu en particulier. Seule la législature britanno-colombienne a cru bon d'exclure ces renseignements de manière explicite[658]. Et qu'en est-il de la surveillance des heures d'entrée dans un édifice[659] ou des relevés d'utilisation de l'Internet[660]? En droit du travail comme ailleurs, les technologies émergentes ont bousculé certains concepts[661].

## 10.2. Moyens d'action mis à la disposition des Canadiens pour que le respect de leurs droits

Le **droit d'accès** est le premier garant du respect de la législation sur la protection des données personnelles. À la consultation des renseignements figurant à son dossier le concernant, un individu pourra en évaluer l'exactitude et la pertinence et, le cas échéant, en **demander la correction, la mise à jour ou la suppression**. S'il se heurte à un refus, il peut porter plainte auprès du commissaire à la vie privée, qui instituera une enquête au terme de laquelle diverses avenues sont possibles, selon le régime applicable: amendes, ordonnances, recours en contrôle judiciaire, voire, recours devant les tribunaux. D'autres voies de droit existent, lorsque les manquements allégués aux obligations législatives dépassent ce cadre individuel. On trouvera à l'annexe C des diagrammes montrant le cheminement des plaintes dans certaines provinces.

### 10.2.1. Recours pour correction de renseignements erronés ou inexacts

Selon le principe d'exactitude des renseignements, tout individu devrait avoir le droit de rectifier une information erronée et, si la véracité de l'information est disputée, le droit d'en indiquer le caractère

---

657 Dans *Wyndowe c. Rousseau*, 2008 CAF 39 la Cour d'appel fédérale a jugé que les notes manuscrites rédigées par un médecin au cours de l'examen médical indépendant d'un assuré effectué en Ontario par ce médecin à la demande d'une compagnie d'assurances constituaient des renseignements personnels au sens de la *LPRPDÉ*. Cette décision fait l'objet d'un commentaire élaboré dans Colin H. H. McNairn, *A guide to the Personal Information Protection and Electronic Documents Act* (Markham, Ont., LexisNexis, 2010) [McNairn].

658 Turbull, *supra* note 654, à la p. 55

659 V.a. CVPCP, Résumé de conclusions d'enquêtes en vertu de la LPRPDÉ #279 –*La surveillance des employés au travail*, Résumé de conclusions d'enquête du CPVPC en vertu de la *LPRPDÉ* n$^{o}$ 279 (26 juillet 2004), 2004 CanLII 52849.

660 Dans *Johnson c. Bell Canada*, 2008 CF 1086, [2009] 3 R.C.F. 67 la Cour fédérale a jugé que les courriels entre employés étaient également des renseignements personnels, même s'ils étaient envoyés par le système de l'employeur. Le pourvoi a cependant été tranché en faveur de l'employeur, qui n'était pas soumis à la *LPRPDÉ*, la communication interceptée n'ayant pas été faite dans le cours d'une entreprise fédérale au sens du sous-paragraphe 4(1)b) de la *LPRPDÉ*. Cette décision est aussi commentée dans McNairn, *supra* note 657.

661 Voir généralement Melanie R. Bueckert, *The law of employee monitoring in Canada* (Markham, Ont., LexisNexis, 2009); Lyne Duhaime, «La protection des renseignements personnels en milieu de travail» dans Service de la formation continue du Barreau du Québec, Vie privée et protection des renseignements personnels (Cowansville, Qc, Yvon-Blais, 2006), 83.

litigieux. Ces modifications doivent également être transmises aux personnes à qui l'information initiale a été communiquée.

Le refus d'obtempérer ouvre généralement la voie aux **mêmes recours que le refus de communication** (cf. 10.1.5.). La législation fédérale fait cependant exception: si un refus de rectification peut faire l'objet d'une plainte et, partant, d'une enquête, elle ne peut être portée en révision devant la Cour fédérale. De l'avis de la CPVPC, cette lacune entraîne de nombreuses dépenses inutiles et une révision de la loi devrait y remédier[662].

### 10.2.2. Recours pour collecte ou communication illégale

Le plaignant peut également intenter un recours civil, pénal ou en jugement déclaratoire pour toute allégation de collecte à son insu ou d'utilisation ou de communication illégale[663]. Il peut le faire en son nom propre ou sous la forme d'un **recours collectif**[664].

Si le commissaire peut intervenir dans de telles actions, selon les règles d'attraction habituelle, il ne peut en revanche les intenter lui-même, personnellement ou *ès* qualité[665].

### 10.2.3. Initiatives des autorités de protection

De surcroît, les commissaires peuvent pratiquer des **vérifications ponctuelles** des pratiques d'un secteur ou d'un organisme donné. Ils disposent à cette fin des mêmes pouvoirs que pour une enquête sur plainte et leurs conclusions ont la même force.

On ne saurait finalement trop insister sur le **rôle de médiateur et de conciliateur** des commissaires à la vie privée. Au-delà des allégations de pratiques illégales, ils peuvent se pencher sur des griefs «qui ne correspondent à aucune catégorie juridique ordinaire, mais qui n'en sont pas moins réelles»[666], par exemple, des allégations de traitement inéquitable, hasardeux ou inélégant. S'inscrivant dans une optique de résolution alternative des différents, ses pouvoirs ne visent alors pas tant la réparation formelle que la prévention et l'apaisement[667].

---

662 *Ibid.*

663 Ces allégations ne peuvent faire l'objet d'un recours en révision judiciaire aux termes de la loi fédérale: *X. c. Canada (Ministre de la Défense)*, [1991] 1 C.F. 670 (1re inst.), *Statham c. Société Radio-Canada*, 2009 CF 1028.

664 Il est assez courant que la procédure de recours collectif soit amorcée à la suite de conclusions défavorables d'un commissariat à la vie privée. P.ex., *Waters v. Daimlerchrysler Financial* Services *Canada Inc.*, 2009 SKQB 263; *Speevak v. Canadian Imperial Bank of Commerce*, 2010 ONSC 1128. Des ententes interviennent généralement en cours de route, ou alors elles sont abandonnées. On pourra encore évoquer le recours collectif lance contre Facebook le 2 juillet 2010 à la suite du rapport du CPVPC, *supra* note 602 *in fine* ou encore le règlement de 751 750$ versé par le gouvernement fédéral, en 2009, à 4000 des 120 000 personnes dont des renseignements personnels avaient potentiellement été divulgués après le vol, en 2003, de six ordinateurs non protégés par encryptions, dans des bureaux de l'Agence de Revenu du Canada.

665 *Canada (Privacy commissioner) v. Canada (Attorney general),* [2003] 9 W.W.R. 242 (B.C.S.C.); *Rankin (Re)*, [1991] 1 C.F. 226 (1re inst.).

666 William Wade, *Administrative Law*, 5e éd. (Oxford, OUP, 1982), à la p. 73, cité avec approbation dans *Friedmann*, à la p. 461; v.a. *Lavigne,* aux para. 38-39.

667 *Ibid.*

## 10.3. Organisation de l'autorité de protection nationale

### 10.3.1. Mandat

Sauf au fédéral où il s'agit de deux bureaux distincts, toutes les juridictions canadiennes possèdent un **commissariat d'accès à l'information et de protection de la vie privée** (cf. en détail pour le Québec : 10.6.1.). Ces commissions ont pour mandat d'assurer le respect des lois en vigueur en matière d'accès à l'information et de protection des renseignements personnels. On a dit des commissaires à la vie privée qu'ils pouvaient, dans l'exercice de leurs fonctions, être amenés à «accompli[r] sept rôles connexes, à savoir les rôles d'ombudsman, de vérificateur, de consultant, de pédagogue, de conseiller en matière d'établissement de politiques, de négociateur et de responsable de l'application des lois»[668] et, dans certaines provinces, celui de décideur.

L'homogénéité de la protection au Canada et la similitude des rôles des commissaires n'ont toutefois pas emporté l'identité organisationnelle des autorités de protection et **deux grands modèles** coexistent sur le territoire[669], l'un dotant les commissaires de pouvoirs décisionnels et l'autre restreignant les conclusions de leurs enquêtes au format de recommandation.

### 10.3.2. Garantie d'indépendance

#### *10.3.2.1. Conditions de nomination et garanties d'indépendance*

Nommés à titre inamovible, pour un **mandat fixe**, généralement renouvelable, d'une durée de deux[670] à sept ans[671], les commissaires sont des officiers des législatures. C'est devant leur **assemblée législative**, le cas échéant; qu'ils prêtent serment, c'est à elle qu'ils se rapportent et c'est elle seule qui peut, en cas de mauvaise conduite, les relever de leurs fonctions. C'est à elle qu'ils présentent leurs rapports annuels ainsi que, lorsque la situation en commande la considération immédiate, leurs rapports spéciaux. Ils ne sont pas tenus de faire approuver leurs publications et communiqués à quelqu'autre bureau du gouvernement[672].

Leur **rémunération** est généralement comparable à celle des magistrats et il leur est interdit d'occuper d'autres fonctions. Cela s'entend d'abord des postes de confiance auprès de l'administration, des offices publics et du mandat de député, mais certaines lois prévoient également l'interdiction de posséder une entreprise[673]. Énoncée trop strictement, cette exigence paraît problématique dans le cas,

---

668 Colin J. Bennett, «The Privacy Commissioner of Canada: Multiple Roles, Diverse Expectations and Structural Dilemmas», (2003) 46 Adm. publ. du Can. 218, à la p. 237, trad. off. dans *Heinz*, au para. 87.

669 *Heinz,* au para. 105.

670 À Terre-Neuve, *L.pub. T.-N.*, art. 42.2.

671 Au fédéral, *LPRP*, art. 53(2).et, parfois, en Nouvelle-Écosse (où le mandat est de cinq à sept ans), *L.pub. N.-É.*, art. 53.

672 Graham Fraser, «Hauts fonctionnaires du Parlement: Leur rôle au Canada» Notes pour une allocution devant des étudiants de la School of Public Policy and Administration de l'Université Carleton (Ottawa, le 26 octobre 2009), en-ligne: www.ocol-clo.gc.ca/html/speech_discours_26102009_f.php [Fraser].

673 P.ex., *L.pub. T.-N.*, art. 42.1(3), *L.pub. N.-B.*, art. 52-53.

certes de plus en plus rare, où le commissaire est nommé à temps partiel[674]. Formulation plus souple, certaines lois disposent plutôt l'interdiction de conflit d'intérêts[675].

S'ils sont astreints à diverses **obligations de confidentialités et d'impartialité**, les commissaires jouissent également des **privilèges des hauts fonctionnaires** et autres protecteurs du citoyen[676], notamment d'une immunité quant aux actes posés dans le cadre de leurs activités, particulièrement en ce qui a trait à la diffamation. Ils ne peuvent être contraints à témoigner (art. 66). De plus, entraver une de leurs enquêtes constitue une infraction pénale.

Les commissaires adjoints, s'ils existent (et dans certaines provinces, en Ontario par exemple, ils le doivent), sont généralement nommés aux mêmes conditions qu'eux.

De fait, cela suffit globalement à garantir l'indépendance de la personne du commissaire[677]. Dans l'ensemble du reste, les commissaires ne se trouvent généralement pas empêchés de critiquer les pratiques gouvernementales ou d'émettre des réserves à leur égard. Force est néanmoins de constater que, au plan théorique du moins, ce modèle organisationnel révèle certaines **failles au chapitre de l'indépendance**. Outre la question de la permanence du poste déjà évoquée, les questions de la dotation financière, de l'embauche du personnel et de l'empiétement de certains ministères prêtent flanc à la critique.

#### *10.3.2.2. Éventuelles sources de conflit*

C'est sans conteste le traitement de **l'enveloppe budgétaire** qui a suscité les plus grands appels à la réforme. Afin d'assurer non seulement une indépendance mais également une apparence d'indépendance[678], à l'instar des commissaires, le budget des commissions devrait relever de la législature directement. Or, si c'est bien le cas de certaines[679], d'autres continuent soit de relever de l'enveloppe budgétaire d'un ministère de tutelle[680], soit de devoir négocier leur budget sur une base annuelle de la même manière que les ministères et organismes d'État[681].

---

674 Comme c'est le cas au Yukon ou à l'Île-du-Prince-Édouard. Les commissaires dans cette situations n'ont pas manqué de demander la permanence du poste, et l'ont parfois obtenu, comme à Terre-Neuve en 2008 ou au Nouveau-Brunswick en 2010. Sur les contraintes que cela peut emporter, voir OIPC PEI, *Annual Report of the Office of the Information and Privacy Commissioner 2008* (Charlettown, Éd. off, 2009), aux pp. 8-9.

675 P.ex., *L.pub.Qué.,* art. 112.

676 Mary A. Marshall et Linda C. Reif, «The Ombudsman: Maladministration and Alternative Dispute Resolution», (1995) 34 *Alta. L. Rev*. 215.

677 *VALENTE C. LA REINE,* [1985] 2 R.C.S. 673.

678 *Renvoi relatif à la rémunération des juges de la Cour provinciale de l'Île-du-Prince-Édouard; Renvoi relatif à l'indépendance et à l'impartialité des juges de la Cour provinciale de l'Île-du-Prince-Édouard*, [1997] 3 R.C.S. 3; *idem,* [1998] 1 R.C.S. 3 et *idem,* [1998] 2 R.C.S. 443 [collectivement, *Renvois relatifs à l'indépendance*].

679 C'est le cas par exemple en Alberta, en Colombie-Britannique, à l'Île-du-Prince-Édouard ou en Nouvelle-Écosse, où les propositions budgétaires des commissariats sont présentées directement au Comité permanent sur les finances de l'assemblée.

680 C'est le cas de la Commission d'accès à l'information du Québec.

681 De sa création jusqu'en 2006, le CPVPC a ainsi été contraint de négocier directement avec le secrétariat du Conseil du Trésor.

Dans un cas comme dans l'autre, bien qu'il ne semble pas que les commissions aient fait l'objet de pressions indues, elles n'ont pas manqué de s'inquiéter de l'apparence de conflit de tels arrangements pouvaient engendrer[682], appelant à l'octroi d'un financement stable à long terme et à une révision des budgets et besoins par le truchement d'un intermédiaire neutre[683]. En 2006, le gouvernement fédéral, prenant acte de ces inquiétudes, a mis sur pied un **groupe consultatif** chargé d'assurer la liaison entre les hauts fonctionnaires du Parlement et le Conseil du trésor[684]. Si ce projet-pilote s'est pour l'instant déroulé sans heurt, quelques commentateurs se sont interrogés sur l'utilité d'un tel médiateur, la décision finale se trouvant prise de la même manière qu'auparavant[685].

L'organisation du budget d'un commissariat peut également avoir une incidence sur **l'embauche de son personnel**. En effet, généralement[686], ses employés sont membres de la fonction publique et recrutés comme tels. Cela signifie que, contrairement aux commissaires, ils relèvent de l'administration. Cette pratique n'est pas inhabituelle au Canada –le personnel des tribunaux, par exemple, relève également de la fonction publique et non de ses propres allocations budgétaires[687]–, et bien que la difficulté soit demeurée théorique pour l'instant, il n'en demeure pas moins qu'il y a là un risque d'apparence de conflit.

Finalement, des **conflits d'attribution** se dessinent à l'occasion entre commissariats et ministères. Les complications apportées par de telles rivalités trouvent illustration dans le différent qui oppose depuis plusieurs années Industrie Canada, sur la recommandation duquel le gouverneur en conseil reconnaît le caractère «essentiellement similaire» d'une loi provinciale visant le secteur privé, et le CPVPC, qui estime que les critères retenus par le ministère de l'Industrie n'offrent pas un niveau de protection suffisant[688]. Ce n'est pas l'indépendance à proprement parler qui est remise en question ici mais plutôt le bon déroulement ou l'utilité du travail de commissaire. Par contre, il y a un accroc dans l'autonomie

---

682 Jennifer Stoddart, «Discours à l'occasion de l'ouverture des travaux de la Commission parlementaire de la culture chargée d'étudier les recommandations du rapport quinquennal de la Commission d'accès à l'information» (25 septembre 2003), en-ligne: www.cai.gouv.qc.ca/05_communiques_et_discours/discours_25_09_03.html [NB. Jennifer Stoddart n'était alors pas alors CPVPC]; Jennifer Stoddart, «Mécanismes de financement destinés aux agents du Parlement», Allocution devant le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique (Ottawa, 10 février 2005), en-ligne: www.priv.gc.ca/speech/2005/sp-d_050210_f.cfm [Stoddart, «Mécanismes»].

683 À l'automne 2004, la CPVPC avait saisi de la question le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique: Kristen Douglas et Nancy Holmes, «Le financement des hauts fonctionnaires du Parlement», (2005) 35 Rev. parl. can. 13 [Douglas-Holmes].

684 Douglas-Holmes, *ibid.* à la p. 15; David Chatters, «Un nouveau mécanisme de financement pour les hauts fonctionnaires du parlement», rapport du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique (mai 2005), en-ligne: www2.parl.gc.ca/content/hoc/Committee/381/ETHI/Reports/RP1828347/ethirp04/ethirp04-f.pdf.

685 Jack Stilborn, «Le financement des hauts fonctionnaires du Parlement: l'expérience canadienne» (2010) 40 Rev. parl. can. 13.

686 Sauf au Yukon (*Loi sur l'ombudsman,* L.R.Y. c. 163, art. 7) et au Nouveau-Brunswick (*L.pub. N.-B.*, art. 58).

687 *Renvois relatifs à l'indépendance, supra* note 678, aux para. 118 *et s.*

688 Sur cette question, voir *supra,* p. 12.

de la Commission d'accès à l'information lorsqu'elle doit faire déposer son rapport dû à l'Assemblée nationale par le biais d'un ministère[689].

Nous n'estimons pas que le recours par l'appareil étatique à l'expertise du commissaire aux fins d'études constitue un pareil cas de conflit d'attribution. Il s'agit plutôt d'un exemple de coopération, d'ailleurs à l'occasion prévu par la loi[690]. De même, le choix de certains commissariats de se conformer à l'approche de la fonction publique en matière de planification et de rendement et de déposer et défendre chaque année divers plans stratégiques et rapports d'avancement[691] nous semble plutôt louable. Ils ne doivent cependant pas y être tenus, ce que certains exécutifs ont d'ailleurs récemment concédé[692].

### 10.3.3. Fonctions et pouvoirs.

Les commissaires, on l'a dit, ont pour mandat **d'assurer le respect des lois en vigueur**. Cette mission s'articule autour de deux grands axes, d'une part, la promotion de la loi, d'autre part, les fonctions de surveillance.

#### *10.3.3.1. Mission éducative*

Qu'il l'exerce *de facto*[693] ou qu'il s'agisse d'une exigence prévue par la loi, le commissaire est appelé à jouer ce **rôle de conseil** à la fois auprès du grand public et des organisations détentrices de données. Il lui revient ainsi de faire la promotion de la protection du droit à la vie privée et d'expliquer les tenants et aboutissants de la législation en matière de renseignements personnels. Cela peut se faire par le biais de conférences, de dépliants, de documents d'information, de séminaires, de reportages, de service de formation ou de consultation, voire de concours.

Les commissariats financent également des **projets de recherche** et en diffusent les résultats. Ces recherches peuvent être menées par des chercheurs indépendants, des chercheurs affiliés au commissariat ou à la demande d'un ministère.

Ils veillent aussi au **développement de codes de pratique**, de lignes directrices, de protocoles d'impartition et d'accords de principe, qu'ils les proposent ou qu'ils en encouragent l'élaboration par les organisations elles-mêmes. Dans la même veine, ils sont parfois amenés à prendre part à des initiatives intergouvernementales, symposiums, colloques de recherche.

Enfin, il leur revient souvent de se **prononcer sur des politiques en vigueur**, à commenter des projets de loi et à exercer, au besoin, le rôle de conseil auprès de l'administration ou de l'industrie.

---

689 Comeau, «Autorités», *supra* note 624, à la p. 31, n. 74; Comeau, «Protection», *supra* note 516, à la p. 26 et *infra* p. 39.

690 L'article 60 *LPRP* par exemple, permet au ministère de la Justice de commander des études spéciales au CPVPC.

691 Pour le fédéral, voir Stoddart, «Mécanismes», *supra* note 682.

692 Fraser, *supra* note 672.

693 Comme c'est le cas en vertu de la *LPRP*, la CPVPC recommandant fortement une modification législative pour refléter l'état des faits, CPVPC, *Recommandations 2009*, *supra* note 628, à la recommandation n$^{o}$ 4.

### *10.3.3.2. Pouvoirs de surveillance*

Ceci étant, c'est la fonction de surveillance qui canalise l'essentiel des ressources des commissariats[694]. Elle s'exerce principalement par le biais de **l'enquête**. Le terme «enquête» est ici employé au sens large et peut couvrir les enquêtes *stricto sensu*, qui font suite à des plaintes formulées par un particulier, les inspections initiées de l'initiative du commissaire, les vérifications ponctuelles, les examens de conformité d'un ministère ou d'un secteur ainsi que les investigations déclenchées par l'assemblée législative. Ce traitement global est possible car même si la terminologie varie d'une loi à l'autre, les pouvoirs associés à la démarche, eux, restent foncièrement les mêmes.

Ces **pouvoirs** sont appréciables, pour dire le moins. En premier lieu, le commissaire jouit d'un **droit d'accès** large aux documents. Il ne saurait à vrai dire en aller autrement pour lui permettre de s'acquitter de ses fonctions de gardien de la pertinence de leur contenu. Ce droit d'accès dépasse celui des particuliers, puisqu'il s'étend à des dossiers dont des considérations d'ordre public dictent qu'ils ne soient pas accessibles à ceux qu'ils concernent au premier chef[695]. À l'instar d'une commission d'enquête publique ou du vérificateur général, le commissaire a également accès, à certaines conditions, à des documents qui seraient inadmissibles en preuve devant un tribunal judiciaire.

Les enquêteurs disposent en outre de certains **moyens de contrainte** afin de s'assurer l'accès à des documents: droit de visite, droit de perquisition, droit de s'entretenir avec toute personne, droit d'ordonner la production de documents ou le témoignage, droit d'assermenter. Le commissaire ne possède pas «l'arsenal de contrainte d'un tribunal[696]» –notamment, les déclarations de culpabilité pour l'infraction sommaire d'entrave à l'exercice de ses fonctions sont du ressort des seules cours de justice–, la loi a tout de même prévu de «solides»[697] pouvoirs pour lui permettre d'obtenir les documents qu'il juge nécessaires à la poursuite de ses enquêtes.

Le droit d'accès du commissaire n'est cependant pas absolu. Les **limites** qu'il connaît varient selon les juridictions, aussi faut-il se reporter à la loi habilitante, mais on pourra généralement évoquer les documents confidentiels de l'assemblée législative, du gouverneur général, du lieutenant-gouverneur, des tribunaux, du conseil exécutif ou des archives nationales, soit que l'exception soit prévue comme tel par la loi, soit que ces instances se trouvent hors du champ d'application de la loi[698].

---

694 De nombreux commissaires faisant état, dans leurs rapports annuels, de ce que leurs ressources, humaines ou financières limitées, les obligent à mettre de côté cet aspect pour parvenir à traiter les plaintes dans les délais prévus par la loi. V. p.ex., Saskatchewan Information and Privacy Commissioner, *2009-2010 Annual Report* (Régina, Éd. off, 2010), en-ligne: www.oipc.sk.ca/Annual%20Reports/Annual%20Report%202009-2010%20FINAL.pdf, à la p. 6 et p. 42 (96% du budget étant alloué à la fonction de surveillance, 2% à la recherche et 2% à la sensibilisation).

695 Pour le détail des exceptions au droit d'accès des particuliers, voir *infra* p. 35.

696 Comeau, «Autorités», *supra* note 624, à la p. 15.

697 Gérard V. La Forest*, Les commissariats à l'information et à la vie privée: fusion et questions connexes,* Rapport du conseiller spécial auprès du ministre de la Justice (15 novembre 2005) (Ottawa, Éd. off, 2005), en-ligne: qww.justice.gc.ca/fra/ip/rap-rep.pdf [Rapport LaForest].

698 S'il faut en croire la Cour suprême (*Canada (Chambre des communes) c. Vaid*, [2005] 1 R.C.S. 667), les organes, en l'espèce législatifs, créés en vertu de la Constitution ne sont pas «des enclaves à l'abri de l'application du droit commun du pays» (au para. 1) et n'ont droit qu'à «l'indispensable immunité […] [qui] leur permett[e] d'effectuer leur travail législatif» (au para. 4). Pour Nancy Holmes, «Le droit à la vie privée et le Parlement» (22 février 2006), doc. n$^{o}$ PRB 05-85F du Service d'information et de recherche parlementaire, en-ligne: http://dsp-psd.pwgsc.gc.ca/Collection-R/LoPBdP/EB-f/prb0585-f.pdf, à la p. 2, cela signifie que

De manière plus commune, la question de savoir si un enquêteur peut avoir l'accès à des documents qui seraient protégés par une **immunité** en vertu du droit commun de la preuve a fait l'objet d'une jurisprudence intéressante. Au fédéral, par exemple, il existe une importante différence rédactionnelle entre la LPRP et la LPRPDÉ: l'article 34(2) LPRP pose en toutes lettres le droit d'accès du CPVPC à *tout* renseignement d'une institution fédérale, quel qu'en soit la forme ou le support, nonobstant toute autre loi fédérale ou immunité reconnue par le droit de la preuve (à l'exception des renseignements confidentiels du Conseil privé de la Reine pour le Canada). Cela signifierait que le commissaire peut avoir accès à des documents couverts, par exemple, par le privilège avocat-client ou le secret médical. On ne retrouve pas d'équivalent dans la LPRPDÉ: s'agit-il d'une omission du législateur ou d'une restriction volontaire du pouvoir du commissaire? Si la Cour suprême a refusé de trancher formellement, elle a néanmoins laissé entendre que l'on pouvait en tirer une inférence négative quant à l'accès du CPVPC aux documents couverts par le secret professionnel d'un avocat du secteur privé[699].

Dans d'autres provinces, au Québec[700] ou en Colombie-Britannique par exemple, le législateur s'est prononcé en faveur d'un droit d'accès du commissaire à ces documents. Sans doute a-t-il estimé que les obligations de confidentialité auxquelles sont assujettis les inspecteurs suffisent à le protéger, comme d'ailleurs leur inadmissibilité devant une cour de justice advenant l'institution de procédures civiles ou pénales[701].

#### *10.3.3.3. Pouvoirs décisionnels*

On a évoqué plus haut l'existence, au Canada, de deux écoles quant à la valeur des conclusions des enquêtes. Pour l'une, elles doivent rester à l'état de **recommandations** –c'est l'ombudsmodèle–, pour l'autre, elles ne sont efficaces que s'il est obligatoire d'y donner suite et les décisions du commissaire s'en trouvent revêtues de force exécutoire –c'est le modèle **quasi judiciaire**.

Traditionnellement –c'est là l'envers de son rôle de médiateur–, un ombudsman ne dispose que d'un **pouvoir de recommandation** à la suite de ses enquêtes[702]. Même s'il conclut au bien-fondé d'une

---

«bien que le Parlement ait cru bon de ne pas s'assujettir à l'application de la LPRP fédérale, il serait judicieux, en principe et en pratique, que, à titre d'institution publique tenue de rendre des comptes au public, il s'efforce de régler sa propre conduite sur celle qu'il exige d'autrui sur ce point.»

V.a. Saskatchewan Information and Privacy Commissioner, *Report on the Overarching Personal Information Privacy Framework For Executive Government* par Gary Dickson (15 juin 2004), en-ligne: www.oipc.sk.ca/Reports/ReporttoAssembly.pdf.

699 *Canada (Commissaire à la protection de la vie privée) c. Blood Tribe Department of Health*, 2008 CSC 44, [2008] 2 R.C.S. 574, aux para. 28-29.

700 Où le secret professionnel a pourtant une portée plus large que dans les juridictions de common law: *Société d'énergie Foster Wheeler ltée c. Société intermunicipale de gestion et d'élimination des déchets (SIGED) inc.*, 2004 CSC 18, [2004] 1 R.C.S. 4 au para 28; v.a. Jean-K. Samson et Marie-Ève Vézina «L'assujettissement des ordres professionnels au régime d'accès à l'information», dans Service de la formation professionnelle du Barreau du Québec, *Développements récents en déontologie, droit professionnel et disciplinaire 2007* (Cowansville, Qc, Yvon-Blais, 2007), 61.

701 Barbara McIsaac, Rick Shields, *The Law of Privacy in Canada*, 2e éd. (Toronto, Carswell, 2004), à la p. X.

702 *British Columbia Development Corporation c. Friedmann (Ombudsman),* [1984] 2 R.C.S. 447 [*Friedmann*], aux pp. 458-459:

plainte, il ne peut contraindre l'organisation visée à rectifier sa pratique, sauf si elle s'engage à y donner suite, ni imposer des mesures de protection intérimaires, de telles ordonnances devant nécessairement émaner d'un tribunal. Le commissaire doit miser ici sur l'ascendant moral afférent à sa fonction pour matérialiser tout changement qu'il propose[703]. À défaut, le législateur l'a aussi fourbi d'une autre arme, soit la **publicité**, le commissaire peut en effet dénoncer publiquement toute pratique qu'il juge inadéquate. La Saskatchewan, le Manitoba, les trois territoires, les quatre provinces maritimes, plusieurs législatures sont restées fidèles à cette vision plus classique de la fonction – d'ailleurs, au Yukon et au Manitoba, le commissariat à la vie privée se présente comme une division du bureau l'ombudsman de la province, plus ou moins intégrée à la conduite de la surveillance générale de l'administration[704]. Le commissariat fédéral participe également de l'ombudsmodèle encore qu'il s'écarte un peu des racines parlementaires de l'institution d'ombudsman en ce qu'il police également les agissements du secteur privé[705].

À l'inverse de ce modèle conciliateur, les législatures du Québec, de l'Ontario, de la Colombie-Britannique, de l'Alberta et de l'Île-du-Prince-Édouard ont plutôt choisi d'investir leur commissaire du pouvoir de rendre des **décisions définitives**. Au terme de ses enquêtes, le commissaire peut, s'il l'estime opportun, ordonner la communication d'un dossier, la correction de renseignements y figurant ou la modification des pratiques d'un organisme donné. La décision devient exécutoire sur dépôt auprès de la Cour supérieure et l'organisation doit s'y conformer, sauf à se pourvoir en contrôle judiciaire.

Il y a lieu de signaler que ce pouvoir est généralement exercé avec parcimonie, les commissaires préférant une **approche plus conciliatrice**, tout en reconnaissant que l'efficacité des approches informelles est hautement tributaire de l'éventuelle utilisation de leur pouvoir décisionnel[706]. Ceci étant, certains auteurs sont d'avis que le fait d'investir les commissaires d'un tel pouvoir améliore leur indépendance en les obligeant à agir davantage comme des arbitres que lorsqu'ils n'ont qu'un pouvoir de recommandation, auquel cas ils auraient tendance à faire avancer des politiques précises, voire à faire preuve d'antagonisme face à l'État[707].

---

Au début, l'ombudsman suédois devait être le surveillant parlementaire de l'administration, mais par la suite la nature de l'institution s'est progressivement modifiée. Finalement, l'ombudsman en est venu à avoir pour fonction principale d'enquêter sur des plaintes de mauvaise administration pour le compte de citoyens lésés et de recommander des mesures correctives aux fonctionnaires ou ministères gouvernementaux visés.

703 Comeau, «Autorités», *supra* note 624, à la p. 15; Comeau, «Protection», *supra* note 516, à la p. 28.

704 C'était encore récemment le cas au Nouveau-Brunswick. Cependant, à la suite de l'ajout à son mandat de la défense des enfants et de la jeunesse, on a cru bon de retirer à son application les lois portant sur l'accès à l'information et la protection de la vie privée. Cet été, le gouvernement annonçant la nomination de la première commissaire à l'information et à la vie privée de la province: Nouveau-Brunswick, Bureau du Conseil exécutif, «Me Anne Bertrand est nommée commissaire à l'accès à l'information et à la protection de la vie privée», communiqué de presse (15 juillet 2010).

705 Sur cette question, voir Jennifer Stoddart, «Distinguer le seigle du blé: réorientation de l'actuel débat sur la fonction d'ombudsman telle que définie dans la *LPRPDÉ*» (Ottawa, 21 octobre 2005), en-ligne: www.priv.gc.ca/information/pub/omb_051021_f.cfm.

706 Rapport LaForest, *supra* note 697, à la p. 56.

707 Alasdair Roberts, «New Strategies for Enforcement of the *Access to Information Act*» (2002), 27 Queen's Law Journal 647, aux pp. 662-663.

Dans ce modèle, il faut signaler la structure particulièrement **formaliste du Québec**, qui s'est doté à la fois d'un organe de surveillance et d'un tribunal administratif. Cette structure particulière a été adoptée afin d'accroître l'indépendance décisionnelle de la commission[708]. Nous aurons l'occasion d'y revenir en seconde partie[709].

## 10.4. Rôle des organisations protectrices

La législation canadienne ne prévoit pas, à notre connaissance, de règles spéciales pour les organisations protectrices des consommateurs. Toutefois, la pratique récente montre que les organisations protectrices peuvent jouer un rôle important dans le domaine de la protection des données. Ainsi, c'était sur plainte d'une organisation (Clinique d'intérêt public et de politique d'Internet du Canada (CIPPIC)) qu'une enquête sur Facebook a eu lieu.[710] Le recours collectif est donc un **outil important** dans la mise en œuvre de la protection des donnés (cf. également supra, 10.2.2.).

Enfin, il faut relever que Le Commissariat à la Protection à la Vie Privée joue, d'une certaine mesure, le rôle d'organisation protectrice.

## 10.5. Mögliche und vorgeschriebene Aktivitäten der Datenbearbeiter

Die folgenden Ausführungen beschränken sich auf die Beschreibung der LPRPDE, welche für die anderen Regulierungen einen Beispielcharakter hat. Die LPRPDE übernimmt dabei die **10 Prinzipien der Datenbearbeitung** (10.1.2.2.) und erklärt deren Beachtung für Datenbearbeiter als grundsätzlich obligatorisch (Art. 5 LPRDE), wobei sowohl Verfahrensvorschriften als auch Ausnahmen im Gesetz selbst vorgesehen sind (Art. 6 – 9 LPRDE). Ausnahmen betreffen insbesondere Fälle der Datensammlung und –verarbeitung ohne Zustimmung der betroffenen Person.

### 10.5.1. Datenschutzzertifizierung

Es besteht soweit ersichtlich keine Datenschutzzertifizierung.

### 10.5.2. Meldung von Datensammlungen

Es besteht keine Pflicht zur Meldung von Datensammlungen. Vielmehr wird in der Gesetzgebung der Grundsatz des Einverständnisses der betroffenen Personen mit einer Datenverarbeitung hervorgehoben.

### 10.5.3. Bestellung betrieblicher Datenschutzbeauftragter

Für die Aktivitäten der Datenbearbeiter erscheint insbesondere relevant, dass unter dem ersten Prinzip der Verantwortung eine Verpflichtung zur Bestimmung einer für die Datenbearbeitung zuständigen Person vorgesehen ist, welche die Befolgung der Datenschutzbestimmung durch

---

708 Jacques Saint-Laurent, «Le rôle de la Commission d'accès à l'information au lendemain d'une modernisation attendue du régime québécois d'accès à l'information» dans Service de la formation permanente du Barreau du Québec, *Le droit à l'information: le droit de savoir!* (Cowansville, Qc, Yvon-Blais, 2006), 105, à la p. 115.

709 *Infra* p. 39

710 E. Denham, Rapport de copnclusions de l'enquuête menée à la suite de la plainte déposée par la Clinique d'intérêt public et de politique d'Internet du Canada contre Facebook Inc., disponible sous http://www.priv.gc.ca/cf-dc/2009/2009_008_0716_f.cfm#plainte (15.11.2010).

organisatorische Massnahmen ermöglichen soll.[711] Das kanadische Recht sieht damit eine Pflicht zur **Bestellung betrieblicher Datenschutzbeauftragten** vor.

### 10.5.4. Datenbrief

Es besteht soweit ersichtlich keine Verpflichtung zur regelmässigen unaufgeforderten Information der Betroffenen.

### 10.5.5. Selbstregulierung

Selbstregulierung spielt eine erhebliche Rolle und steht am Anfang der heutigen Regelung, basieren doch die heutigen gesetzlichen Pflichten auf einer nicht gesetzgeberischen Initiative (s. oben, 10.1.2.2.). Sektorielle Gesetzgebung scheint jedoch lange ebenfalls eine gewisse Bedeutung zu haben (s. zum Gesundheitssektor, 10.4.4.).

### 10.5.6. Privacy by Design

Unter dem Prinzip der Verantwortung ist vorgesehen, dass die Organisationen die Umsetzung der Datenschutzpolitik ermöglichen müssen, indem sie Schutzvorkehrungen bei der Datenbearbeitung sowie Mechanismen zum Empfang und zur Beantwortung von Anfragen und Beschwerden einrichten. Im Weiteren muss das Personal im Datenschutzbereich ausgebildet und über die internen Verfahren informiert werden.[712] Dies entspricht dem Konzept der „privacy by design“, welches in Kanada eine besondere Bedeutung hat (s. oben, 10.1.2.).

## 10.6. Régimes particuliers.

Les commentaires qui précèdent ont cherché à dresser un portrait d’ensemble de la protection des données personnelles au Canada dont, au final, malgré plusieurs régimes, la nature et la portée ne varient guère. Sans revenir généralement sur les caractéristiques évoquées, les particularités ou les innovations présentées par **quatre régimes** méritent que l’on s’y attarde. Il s’agit du régime québécois, eu égard à son statut de pionnier et à la structure hautement définie de sa commission, du régime fédéral, à cause de son ampleur, du régime visant le secteur privé en Colombie-Britannique et en Alberta, vu les améliorations qu’ils consacrent par rapport au modèle de la *LPRPDÉ* et finalement de la législation touchant le domaine de la santé.

### 10.4.1. Le Québec, un défricheur

Le Québec a fait figure de pionnier en matière de protection des renseignements personnels[713]. Consacrant le droit à la vie privée de manière quasi constitutionnelle dès 1975[714], il a été le premier

---

711 Annex 1, 4.1.1. LPRDE.

712 Annexe 1, 4.1.4. LPRDE.

713 Paul-André Comeau et Maurice Couture, «Accès à l’information et renseignements personnels: le précédent québécois » (2003), 46 Adm. publ. du Can. 364 [Comeau-Couture], à la p. 365.

714 *Charte* québécoise, *supra* note 526, art. 5.

État nord-américain[715] à se doter de législation portant sur la protection des renseignements personnels. Dans le sillage de la réforme de son code civil, dont les articles 35 à 41 protègent désormais la vie privée, la province **étend les exigences** de protection des renseignements personnels **au secteur privé**.

C'est la province du Québec qui, la première, a doté son organe de protection, la **Commission d'accès à l'information** (CAI), de **pouvoirs décisionnels**. Le modèle «collégial, complexe et pluriel»[716] de la CAI se présente d'ailleurs comme une figure singulière au Canada,

D'abord, l'Assemblée nationale nomme, sur proposition du premier ministre, non pas un mais au moins **cinq commissaires**, qui doivent être élus par résolution des deux tiers des députés[717]. Les candidats doivent en sus satisfaire aux exigences du règlement du Bureau de l'Assemblée nationale et aussi établir un code de déontologie, mesures dont d'aucun croit qu'elles aviveront leur indépendance et leur prestige[718].

Ce sont des officiers de la législature et c'est devant son président qu'ils doivent prêter leur serment d'office. La CAI relève cependant à plusieurs égards du ministre délégué à la réforme des institutions démocratiques, depuis quelques années le ministère des Affaires intergouvernementales canadiennes, des Affaires autochtones, de la Francophonie canadienne, de la Réforme des institutions démocratiques et de l'accès à l'information. C'est ce ministère qui est chargé de la révision quinquennale des lois sur la protection des renseignements personnels ainsi que de la formation des responsables institutionnels des organismes publics (regroupés dans l'Association de l'accès et de la protection de l'information); c'est encore de lui dont émane le budget de la CAI et c'est lui qui transmet à l'Assemblée nationale le rapport annuel qu'elle lui doit. Cette intégration institutionnelle d'un organe censé être indépendant a parfois été soulignée[719].

La structure de la CAI a fait l'objet d'une importante modernisation en 2006[720] et elle se présente depuis peu en deux branches distinctes[721]. Il y a d'abord la **section de surveillance** qui fait à la fois office d'organe de consultation et d'organe de contrôle. Quant à sa fonction de conseil, il est loisible à la CAI de se prononcer sur tout projet de loi ou de règlement ou protocole de transfert de renseignements. Elle est même tenue de le faire dans certains cas, p.ex., en ce qui a trait à l'échange de renseignements personnels entre différentes institutions gouvernementales ou à la création de bases de données biométriques. Ces avis ne lient pas le gouvernement, mais en cas de rejet, ils doivent être publiés à la *Gazette officielle du Québec*. La CAI peut également établir diverses normes de fonctionnement ou de tenues des dossiers.

---

715 Comeau-Couture, *supra* note 713.

716 Comeau, «Autorités», *supra* note 624, à la p. 34.

717 En pratique, la proposition du premier ministre est également présentée au chef de l'opposition officielle et l'élection se fait à l'unanimité. Voir: Comeau, «Autorités», *supra* note 624, à la p. 31.

718 Saint-Laurent, *supra* note 708, à la p. 115.

719 *Supra* note 689.

720 *La Loi modifiant la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels et d'autres dispositions législatives,* L.Q. 2006, c. 22, sanctionnée le 14 juin 2006 marquait l'aboutissement d'une longue période de réflexion sur le rôle et la structure de la CAI, amorcée avec le dépôt de CAI, *Quatrième rapport quinquennal, supra* note 587. Pour une présentation des modifications, voir Saint-Laurent, *supra* note 708.

721 Sur la séparation des organes de surveillance et des tribunaux administratifs réunis au sein d'une même entité, voir *2747-3174 Québec Inc. c. Québec (Régie des permis d'alcool),* [1996] 3 R.C.S. 919.

Quant à sa fonction de contrôle, si ses inspecteurs disposent des pouvoirs d'enquête habituels, ces pouvoirs se trouvent bonifiés de ce qu'ils peuvent *ordonner* la communication, la rectification ou la suppression d'un renseignement au terme d'une enquête. La CAI peut également autoriser le transfert de l'information.

La **section juridictionnelle** entre en jeu lorsqu'il y a demande de révision (secteur public) ou demande d'examen de mésententes (secteur privé). Si la médiation échoue –et la section a pour pratique d'y renvoyer les parties dès que possible[722]–, il y a alors débat contradictoire selon les règles d'équité procédurale habituelles, devant un tribunal administratif. Les décisions de la CAI peuvent être portées en appel sur une question de droit seulement devant les juges de la Cour du Québec désignés à cette fin, dont les décisions sont finales et exécutoires, sauf révision judiciaire. Cette «passerelle vers le système judiciaire» a permis le développement dans la province d'une importante jurisprudence en matière d'accès à l'information et de protection des renseignements[723].

### 10.4.2. Le modèle fédéral

Le gouvernement fédéral est, on l'a dit, le plus grand administrateur de données personnelles au pays. Cette ampleur explique certainement l'abondance des commentaires doctrinaux qu'il a suscités. Le modèle fédéral est lui aussi unique en son genre. Aux observations formulées en première partie du présent document, il faut ajouter d'abord, que seul le fédéral a jugé opportun de **séparer les offices de Commissaire à la vie privée et de Commissaire à** l'accès **à l'information**. Dans la mesure où l'on a souvent reconnu l'identité des finalités de la Loi sur l'accès à l'information et de la LPRP[724] –il s'agit dans les deux cas de réglementer la divulgation de renseignement à des tiers, le principe de protection de la vie privée contenue dans la LPRD devenant l'exception au principe de divulgation et d'accès prévu par la Loi sur l'accès à l'information[725]– et dans la mesure où il existe déjà une certaine synergie administrative[726], on peut s'interroger sur l'opportunité d'offices distincts. L'éventualité d'une fusion est d'ailleurs prévue[727] et la possibilité a été examinée par divers gouvernements soucieux de réduire la taille de l'appareil de l'État[728]. Le dernier rapport en date s'est toutefois fortement positionné à

---

722 Comeau, «Protection», *supra* note 516, à la p. 26.

723 *Ibid.*

724 *Canada (Commissaire à l'information) c. Canada (Commission de l'immigration et du statut de réfugié)*, [1997] A.C.F. n° 1812 (QL), aux para. 34-35:

> Le préambule que constitue l'article 2 de la *Loi sur la protection* des renseignements personnels a dans l'ensemble le même effet que le paragraphe 2(1) de la Loi sur l'accès à l'information. La *Loi sur la protection* des renseignements personnels a pour objet de donner accès aux renseignements personnels conservés par le gouvernement. Les règles d'interprétation décrites plus haut s'appliquent en l'occurrence. Les exceptions nécessaires au droit d'accès doivent être interprétées de manière stricte.
>
> V.a. Comeau, «Protection», *supra* note 516, qui semble trouve que c'était un défi législatif que d'assurer la cohérence des deux objectifs (p. 18) et «procéder de façon cohérente, à l'inévitable arbitrage entre les deux droits insérés dans une seule législation» (p. 25).

725 *Loi sur l'accès à l'information,* L.R.C. 1985, c. A-1 [*LAI*]. Sur la relation entre les deux lois, voir *Dagg, supra* note 536, au para. 48.

726 Qui a pu varier selon les époques, Rapport LaForest, *supra* note 697, aux pp. 22-23.

727 *LPRP*, art. 55.

728 Pour un aperçu des initiatives en la matière, voir Rapport LaForest, *supra* note 697, aux pp. 21-22.

l'encontre d'une telle mesure, en partie étant donné le fonctionnement adéquat de la structure actuelle, en partie par crainte de conflit d'application des deux mandats[729].

Même sans cette attribution combinée, c'est le plus occupé des commissariats[730]. On l'a dit, le CPVPC surveille à la fois le **secteur public fédéral** et une bonne part du **secteur privé**. C'est également lui qui convoque et préside aux réunions bisannuelles des commissaires à la vie privée et à l'information du Canada et c'est à lui qu'il revient de coordonner les efforts canadiens et internationaux[731].

Alors que la tendance au Canada est à l'adoption de loi dans le secteur privé et le secteur de la santé, les **efforts de réforme législative** du CPVPC se sont, ces dernières années, plutôt concentrés sur la modernisation de la LPRP*,* jugée trop permissive*.* Un rapport a d'ailleurs été déposé, qui a fait l'objet de débats en comité parlementaire[732]. Certaines propositions cherchent plus ou moins l'uniformisation des obligations de la LPRP et celles de la LPRPDÉ: on a déjà évoqué le remplacement du critère du «lien direct» de la LPRP par un critère de nécessité[733], on pourra ajouter l'application de la LPRP aux renseignements personnels enregistrés mais non consignés[734]. D'autres propositions ont plutôt pour objet la facilitation du travail du CPVPC –pouvoir discrétionnaire d'abandonner une enquête, souplesse administrative accrue, inscription législative d'un examen périodique obligatoire de la LPRP[735]. Les dernières enfin concernent plutôt l'alignement des termes de la loi avec les pratiques développées depuis son adoption. Ainsi, y aurait-il lieu d'y insérer le mandat de sensibilisation du public[736], d'y consacrer les directives du Conseil du Trésor quant à la procédure d'avis en cas d'atteinte à la protection des données[737] ou d'y inscrire les obligations imposées à l'ensemble de l'administration par le programme d'évaluation des facteurs de risque relatifs à la vie privée, mis en œuvre depuis 2002[738]. Ce programme, le premier en son genre, prévoit que la modification ou la création de tout programme qui pourrait avoir un impact sur la vie privée des citoyens canadiens doit faire l'objet d'une étude d'impact et de faisabilité soumise au commissaire à la vie privée pour commentaires[739].

Une dernière évolution éventuelle est à souligner: le processus de **nomination du CPVPC** pourrait prendre un tournant davantage public, le premier ministre du Canada ayant en effet envisagé d'instaurer un processus d'audition parlementaire préalable à la nomination des hauts fonctionnaires. En l'occurrence, le candidat au poste de CPVPC serait entendu par Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique[740].

---

729 *Ibid.*

730 Comeau, «Protection», *supra* note 516, aux annexes.

731 Comeau, «Autorités», *supra* note 624, à la p. 17.

732 CPVPC, *Recommandations 2009*, *supra* note 628; Rapport Szabo, *supra* note 639.

733 *Ibid.,* à la recommandation n° 1.

734 *Ibid.*, à la recommandation n° 7.

735 *Ibid.,* aux recommandations n$^{os}$ 5, 6 et 8.

736 *Ibid.,* à la recommandation n° 4.

737 *Ibid.,* à la recommandation n° 12

738 *Ibid.,* à la recommandation n° 3.

739 Secrétariat du Conseil du Trésor*, Directive sur l'évaluation des facteurs relatifs à la vie privée* (1$^{er}$ avril 2010), en-ligne: qww.tbs-sct.gc.ca/pol/doc-fra.aspx?id=18308, remplaçant Secrétariat du Conseil du Trésor, *Politique d'évaluation des facteurs relatifs à la vie privée* (2 mai 2002), en-ligne: qww.tbs-sct.gc.ca/pol/doc-fra.aspx?id=12450.

740 Comeau, «Protection», *supra* note 516, à la p. 27.

### 10.4.3. Les lois de deuxième génération pour le secteur privé

De nombreuses similarités traversent les **lois albertaine et britanno-colombienne** en matière de protection des renseignements. Elles visent à la fois le secteur public et le secteur privé, y compris les organismes à but non lucratif. Elles augmentent les pouvoirs des commissaires en leur permettant d'émettre certaines amendes et ordonnances de conformité à la loi. Si les lois visant le secteur public sont virtuellement identiques à celles en vigueur dans le reste du Canada, quatre particularités des lois visant le secteur privé méritent d'être soulevées.

D'abord, ces lois sont **plus précises**. Certains les ont d'ailleurs qualifiées de lois de «deuxième génération» pour cette raison[741]. Ainsi, elles renferment une section sur ce qui constitue un «**consentement»** –principe cardinal–, et en présentent les diverses modalités: consentement exprès, implicite, présumé, révocable, etc. Elles clarifient également certaines exceptions en la matière. Par exemple, les transferts d'information découlant de négociations portant sur l'achat ou la fusion d'entreprises sont permis, mais assortis de lourdes exigences de confidentialité. Aussi, comme on l'a évoqué, ces deux lois opèrent une distinction quant au niveau de consentement requis de la part des employés et de celle des clients: si seuls les renseignements qu'une personne raisonnable estimerait acceptables peuvent être emmagasinés dans le cours de ses transactions commerciales, une entreprise peut recueillir, utiliser et transmettre toute information que ce soit au sujet de ses employés sans leur consentement, pourvu que cela soit fait à une **fin raisonnable** (for *«reasonable purpose»*) dans la gestion de leur relation. Certains se sont demandé en quoi cette exception au principe de consentement servait les objectifs de protection des renseignements personnels[742].

La loi albertaine pose en outre certaines règles quant à la conservation ou à la destruction des renseignements personnels recueillis pendant le processus de recrutement d'un candidat[743].

Finalement, les deux lois possèdent une **clause de droit acquis**, qui permet aux entreprises de conserver les renseignements personnels recueillis avant leur entrée en vigueur même sans le consentement des parties. La mesure a été dénoncée par certains organismes de défense des intérêts publics[744], qui estiment qu'il eût été préférable d'accorder aux entreprises un délai pour se conformer à la loi, de même que par le Commissaire à la privée du Canada[745], qui s'est objecté à la déclaration de similarité faite par Industrie Canada[746].

---

741 Canada, Chambre des communes, *Examen, prévu par la loi, de la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDÉ)*, Quatrième Rapport du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique, par Tom Wappel et al. (mai 2007), 39e législature, 1re session, en-ligne: www2.parl.gc.ca/content/hoc/Committee/391/ETHI/Reports/RP2891060/ethirp04/ethirp04-f.pdf [Wappel, *Examen*], aux pp. 1 et 17.

742 Le CPVPC, *Deuxième Rapport au Parlement relativement aux lois provinciales essentiellement similaires* (juin 2003), en-ligne: www.priv.gc.ca/legislation/leg-rp_030611_f.pdf, à la p. 11, a lourdement critiqué cette «forme faible» de consentement qu'est le consentement implicite de l'employé.

743 Sandra M. Anderson, « Alberta's Statutory Privacy Regime and Its Impact on the Workplace» (2005-2006) 43 Alta. L. Rev. 647.

744 B.C. Freedom of Information and Privacy Association, «Lettre à l'honorable Sandy Santorini, ministère des Services de gestion – Commentaire sur le projet de loi 38» (15 mai 2002), en-ligne: http://fipa.bc.ca/library/Law_Reform_Activities/LETTERS/May_15_2003_Sandy_Santori.doc.

745 CPVPC, «Lettre», *supra* note 652

746 CPVPC, *Rapport au Parlement relativement aux lois provinciales essentiellement similaires* (Ottawa, Éd. off, 2003), en-ligne: www.priv.gc.ca/legislation/leg-rp_030611_f.pdf, à la p. 11.

### 10.4.4. Le secteur de la santé

Le secteur de la santé peut faire l'objet de dispositions particulières au sein d'une loi générale sur la vie privée[747]. C'est le cas des lois fédérales, britanno-colombienne visant le secteur public[748]. À l'inverse, la vie privée peut faire l'objet de dispositions particulières dans des lois sur la provision des services de santé, comme c'est le cas au Québec[749] ou au Yukon[750].

Il se dégage cependant au Canada une nette tendance législative à mettre en place un **régime distinct** pour l'ensemble du domaine de la santé. À ce jour, six provinces ont recouru à ce mécanisme et une septième l'envisage[751]. Plusieurs raisons peuvent expliquer cette réglementation propre. D'abord, la santé est un secteur important de l'économie canadienne[752], qui draine une part considérable des ressources des provinces. Ensuite, c'est un domaine lourdement fragmenté entre ses divers intervenants, participant à la fois du public (hôpitaux, médecins, infirmières, régies de la santé, ministères) et du privé (cliniques privées, pharmacies, physiothérapeutes, etc.)[753]. Finalement, il s'agit d'un domaine «fortement axé sur l'information»[754], une information sensible, dont l'exactitude conditionne l'efficacité des soins et traitements[755].

---

747 Sur les avantages de cette approche, voir: David Loukidelis, Health Information Privacy - The British Columbia Experience, allocution au Canadian Institute Conference (Toronto, 19 juin 2001), en-ligne: qww.oipc.bc.ca/publications/speeches_presentations/speech_04.html.

748 Afin d'assurer le respect de certaines obligations constitutionnelles, la jurisprudence a conféré à la notion de «secteur public de la santé» une portée assez large qui comprend, à certains égards, le secteur privé, lorsqu'il accomplit des actes «de nature intrinsèquement gouvernementale»: *Eldridge c. Colombie-Britannique (Procureur général),* [1997] 3 R.C.S. 624.

749 *Loi sur les services de santé et les services sociaux,* L.R.Q., c. S-4.2, art. 17 à 27.3 (qui ont préséance sur la *L.pub. Qué.*), 161 *et s.*, *Loi sur l'assurance maladie*, L.R.Q. c. A-29, art. 9.0.1.1., 63 *et s.* Voir Marie-Nancy Paquet, «Le principe de l'exception: la confidentialité dans la *Loi sur les services de santé et les services sociaux*» dans Barreau du Québec, *La protection des personnes vulnérables* (Cowansville, Qc, Yvon-Blais, 2010), 51 [Paquet].

750 *Loi sur la santé*, L.R.Y. 2002, c. 106 telle que modifiée par la *Loi modifiant la loi sur l'accès à l'information et la protection de la vie privée*, L.Y. 2009, c. 13.

751 Soient l'Ontario, le Manitoba, la Saskatchewan, l'Alberta, Terre-Neuve-et-Labrador et, tout récemment, le Nouveau-Brunswick. Une loi similaire est à l'étude en Nouvelle-Écosse, *Bill no. 64 – Personal Health Information Act* (61e législature, 1re session) (2009) 58 Elizabeth II). Si ces provinces mettent toutes de l'avant un modèle semblable, seule la loi ontarienne a fait l'objet d'une reconnaissance d'équivalence de la part d'Industrie Canada, la portion relevant du privé du secteur de la santé de cette province se trouvant du coup retranché du champ d'application de la *LPRPDÉ*. Aucune demande de reconnaissance d'équivalente ne semble avoir été présentée par les autres provinces: «Législation en matière de protection des renseignements personnels - caractère "essentiellement similaire"», courriel de Jean-François Boudreau, agent du Centre de service Web d'Industrie Canada (30 septembre 2010).

752 Finn-Malone, *supra* note 594, à la p. 7 rapportent qu'il représente environ 10% du PIB canadien; Willison, *supra* note 609.

753 Finn-Malone, *ibid.,* aux pp. 6-7.

754 *Ibid.*, aux pp. 6 et 12 qui rapportent, à la p. 7 que «chaque minute, plus de 2000 activités nécessitant l'échange de renseignements sont effectuées dans le cadre du système de soins de santé du Canada» soit un volume «comparable au volume de transactions au sein des établissements bancaires du pays.»

755 *Ibid.*, à la p. 9; v.a. *L.s. Man.*, préambule; *Livre blanc, supra* note 611, aux pp. 7, 35-36.

On a alors jugé que la protection des renseignements personnels se trouverait enrichie de la réunion d'obligations éparses en un seul instrument qui reflète la réalité des intervenants d'un secteur complexe[756]. Les fondements de la protection ne sont nullement remis en question, il y a plutôt contextualisation et réalignement des objectifs à la pratique du domaine de la santé: d'une part, la loi impose de **nouvelles obligations de conservation et de traitement** pour mieux garantir la protection d'une information jugée particulièrement sensible, d'autre part, elle aménage de **nouvelles exceptions** afin d'accroître l'efficacité la prestation des services de santé et la gestion des dossiers.

Le régime, donc, ne modifie pas les principes de consentement liés à la collecte de l'information. Il assouplit plutôt certaines règles quant à la transmission. Essentiellement, les lois créent une **nouvelle catégorie d'individus**, les «dépositaires de renseignements sur la santé», qui disposent d'une **autorisation implicite** de prendre connaissance et de divulguer les renseignements acquis. Les dépositaires sont ceux qui, dans le cours des services de santé qu'ils fournissent à un patient, sont appelés à obtenir ou à contrôler certaines informations personnelles le concernant. On compte parmi eux les autorités publiques, ministères et régies de la santé, les professionnels de la santé, médecins, infirmiers, ambulanciers, pharmaciens, techniciens de laboratoire et de prélèvement, les opérateurs de centre de soins et, dans certains cas, les travailleurs sociaux, les conseillers aux incapables, certains centres de recherche et leurs mandataires. La définition exclut cependant généralement les ordres professionnels et conseils de discipline, les compagnies d'assurances, la direction de la protection de la jeunesse, les employeurs et les commissions du travail[757].

L'autorisation ne vaut que pour la **divulgation** faite **entre dépositaires** –dans le jargon, on parle de «cercle des soins»–, elle se limite aux renseignent nécessaires pour le traitement ou la logistique de la fourniture de soins. Elle peut être retirée en tout temps par le patient, de façon complète ou à l'égard de certains seulement –on parle alors de «coffre-fort» (*lock-box*).

Les règles de protection demeurent pour le reste inchangées: l'information doit être assujettie aux plus strictes **exigences de confidentialité**, mais sa gestion doit être ouverte et transparente et le patient doit pouvoir être informé des pratiques de tenue des dossiers[758]. En principe, tout particulier a le **droit de connaître** l'information dont dispose une organisation sur son compte, sauf dans les cas où cette information concerne également un tiers ou lorsque sa communication pourrait être préjudiciable. On pourrait croire que cette dernière exception sera plus fréquemment invoquée dans par les professionnels de la santé[759].

Le patient dispose également du **droit de faire rectifier** toute information erronée à son dossier. Les dépositaires de renseignements sur la santé ne sont cependant pas obligés de modifier leurs opinions professionnelles, bien qu'elles puissent être touchées par une déclaration de désaccord.

Il importe de souligner que si les lois couvrent les renseignements sur la santé, qu'il s'agisse d'informations liées à l'état de santé de cette personne ou à son rapport au système de santé, elles ne protègent que ceux qui pourraient servir à **identifier une personne**. Les renseignements anonymisés

---

[756] *Ibid.*, aux pp. 12 et 19.

[757] Ces dernières sont parfois aussi visées par leur propre règlement d'exemption, p.ex., *Disclosure of Information Regulations,* N.S. Reg. 220/86.

[758] Voir à cet égard les pratiques préconisées par l'Association canadienne de normalisation, dont s'inspirent en large part les lois en la matière (*ibid.*, à la p. 42).

[759] Martin Hébert, *Aspects juridiques du dossier de santé et de services sociaux* (Québec, Association québécoise des archivistes médicales, feuilles mobiles), à la p. 107; Paquet, *supra* note 749, à la p. 57.

peuvent ainsi faire l'objet de transmission. Sont considérés comme identificatoires tant le détail des consultations, des traitements ou des ordonnances, l'historique de maladie d'un individu, son information génétique et ses antécédents familiaux que sa couverture d'assurance-maladie, ses fournisseurs de soin ou l'existence d'un mandataire.

La question de savoir si les renseignements doivent être consignés pour être protégé constitue un point de divergence entre les différentes lois provinciales: dans certaines, comme l'Alberta, la Saskatchewan et la Colombie-Britannique, les informations «orales» sont exclues, dans d'autres, comme au Nouveau-Brunswick[760] et à Terre-Neuve, elles sont incluses, l'Ontario et le Manitoba, finalement, ne précisent pas ce qu'il en est.

Quoi qu'il en soit, d'autres initiatives sont à prévoir dans le domaine de la santé. Il est ainsi souvent question de **constitutions de banques de recherche** ou de dématérialisation des dossiers de santé. Des lois ont déjà été adoptées à ce dernier sujet et d'autres sont à l'étude, mais il s'agit de considérations assez théoriques, de cadres de mise en œuvre future, car aucune province canadienne ne connaît de base de dossiers médicaux centralisée, bien qu'il existe, au sein de certaines régies, des projets-pilotes en ce sens[761].

---

760 Malgré l'avis des Commissaires, qui estimaient que, bien que les deux formes de renseignements soient également dignes de protection, la couverture des renseignements oraux était impraticable, voir Finn-Malone, à la p. 14.

761 Voir *supra* titre 10.1.5. , à la p. 21.

# 11. Datenschutz und Technologieentwicklung in den USA

The U.S. approach to privacy protection, unlike that in Europe, relies on **industry-specific legislation, regulation and self-regulation**. It is therefore extremely difficult, if not impossible, to provide a comprehensive overview of data protection legislation in the United States. To add to the complexity, it should be remembered that legislation may – and does – exist on both the Federal and the State levels. Such legislation may vary significantly from one state to another. We therefore present a brief discussion of certain aspects of data protection in two states: Massachusetts, because it has a recent law concerning data protection that addresses some of the issues posed by the new technologies, and California, because this state has taken a multi-pronged approach to the area, with emphasis on consumer education.

## 11.1 California

### 11.1.1. Institutional Framework

California is the first state in the United States to have an agency dedicated to promoting and protecting the privacy rights of consumers. The **Office of Privacy Protection**, part of the State and Consumer Services Agency, was created by legislation in 2000 and opened in 2001. Its mission is to identify consumer problems in the privacy area and encourage the development of fair information practices.[762] It provides information and assistance on privacy issues to individuals and recommends privacy practices to businesses and other organizations. In particular it:

- Assists individuals with **identity theft** and other privacy-related concerns.
- Coordinates with local, state and federal law enforcement on identity theft investigations.
- Provides **consumer education** and information on privacy issues.
- **Recommends policies and practices** that protect individual privacy rights.

The web-site of the Office provides **information and practical advice** concerning identity theft, online privacy, privacy at work, freezing credit ratings, etc. It also provides links to relevant laws as well as proposed and pending legislation. In the area of internet, the Office forms the Coalition on Children's Internet Safety in order to foster collaboration between stakeholders and experts and facilitating the safe and legal use of the Internet by children.[763]

### 11.1.2. Legislation in the Area of New Technologies

In Kalifornien besteht eine Vielzahl von Regelungen zu Aspekten des Datenschutzes beim Einsatz neuer Technologien. Dabei handelt es sich jeweils um sehr spezifische, auf einen bestimmten Aspekt sowie in der Regel einen bestimmten Wirtschaftsbereich gerichtete Rechtsakte. Die folgende Übersicht soll einen Eindruck über Regelungsgebiete und –technik ermöglichen.

Ein grosses Anliegen und Gegenstand kürzlicher Gesetzgebung ist der „Identitätsdiebstahl" (***identity theft***), wie sich bereits aus obigen Ausführungen ergeben hat. Dabei besteht einerseits ein „*Criminal Identity Theft Registry*", bei welchem sich eine Einzelperson über eine Gratistelefonnummer melden kann, sofern deren Namen mit Kriminalität in Verbindung als Folge des Gebrauchs durch einen Kriminellen bei Begehung einer Straftat, Festgnahme, Strafverfolgung oder Verurteilung. Dabei kann die Unschuld mittels einer Telefonnummer und eines PIN bestätigt werden.[764] Nochmehr auf das Internet ausgerichtet ist die am 25. September 2010 genehmigte

---

762 http://www.privacy.ca.gov/Default.htm (21.10.2010).

763 http://www.cybersafety.ca.gov/coalition.htm. (21.10.2010).

764 For more information see : http://www.privacy.ca.gov/res/docs/pdf/cis8englsih.pdf (21.10.2010).

*Senate Bill 1411*[765], welche die Personifizierung durch Internet unter Strafe stellt. Bereits vorher war es strafbar, eine andere Identität zu verkörpern und ohne Genehmigung zum Zwecke der Täuschung oder Bereicherung Daten abzurufen und zu verändern. Nach dem neuen Gesetz wird die glaubhafte wissentliche Verkörperung einer anderen Person (ohne deren Zustimmung) auf einer Internetseite oder durch andere elektronische Mittel zum Zweck der Verletzung, Einschüchterung oder zu betrügerischen Zielen unter Strafe gestellt, wobei auch ein zivilrechtlicher Schadenersatzanspruch vorgesehen ist. Zur Verfolgung von *identity theft* sowie von Kriminalität im Technologiebereich wurde zudem ein besonderes Programm lanciert (*High Technology Theft Apprehension and Prosecution Program*), das auch die Schaffung spezialisierte Strafverfolgungseinheiten beinhaltet (*Identity Theft Unit, High Technology Regional Crimes Task Force, High Technology Crime Advisory Committee*). **[766]**.

Eine Reihe von Gesetze besteht auch zur Verhinderung oder Einschränkung vom **Sammeln von Daten** durch technologische Mittel. Dabei handelt es sich teilweise um öffentliche Überwachung (Electronic Eavesdropping by State Law Enforcement Officials – Penal Code sections 629.50-629.98; Notwendigkeit der Genehmigung durch einen höheren Richter sowie Information nach Abschluss der Überwachung)**[767]**, vor allem aber um Verhinderung von Überwachung durch Privatpersonen. Dabei ist mit wenigen Ausnahmen das Aufzeichnen oder Überwachen von privaten Gesprächen allgemein sowie das Überwachen des Benutzerverhaltens verboten (Electronic Eavesdropping - Penal Code sections 630-638[768], per Telefon, Funktelefon, Kabel oder andere, besonders auch durch Fernsehbetreiber), oder das Ermitteln der Identität durch Lektüre der durch RFID-Technologie ausgerüstete Ausweise (Eavesdropping or Skimming RFID – Civil Code section 1798.79)[769]. Spezifischer sind Vorschriften, welche das Implantieren von identifizierenden Geräten unter Strafe stellen[770] oder bei Verletzungen der Privatsphäre durch Photographie, Tonaufnahme oder andere Aufnahme eine Schadenersatzpflicht (inkl. punitive damages) begründen.[771]

Im Bereich der **Automobilindustrie** besteht eine Vielzahl von sehr spezifischen Vorschriften, z.B. eine Informationspflicht bei der Installation von Aufzeichnungsgeräten (*event data recorders / black boxes*) sowie Vorschriften zur Aufzeichnung und Gebrauch der Daten (Einwilligung, gerichtliche Verfügung, Zweck des Strassenverkehrs, Reparatur; Zweckgebundenheit, Anonymisierung)[772]; ein Verbot der Beschaffung und des Gebrauchs von Daten über den Gebrauch von Mietwagen durch im Mietwagen installierte Überwachungstechnologie (ausser mit Einverständnis des Mieters)**[773]**, oder auch Vorschriften, welche den Zugang und die Veränderung durch Autohersteller und –verteiler zu

---

765 http://www.leginfo.ca.gov/pub/09-10/bill/sen/sb_1401-1450/sb_1411_bill_20100219_introduced.pdf (21.10.2010).

766 Penal Code Sections 13848-13848.6, verfügbar unter http://www.leginfo.ca.gov/cgi-bin/displaycode?section=pen&group=13001-14000&file=13848-13848.6 (21.10.2010) w.

767 See http://www.leginfo.ca.gov/cgi-bin/displaycode?section=pen&group=00001-01000&file=629.50-629.98 (21.10.2010) for the text of the law.

768 See http://www.leginfo.ca.gov/cgi-bin/displaycode?section=pen&group=00001-01000&file=630-638 (21.10.2010) for the text of the law.

769 See http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=01001-02000&file=1798.79-1798.795 (21.10.2010) for the text of the law.

770 Prohibition on Bodily Implanting of Identification Devices, Civil Code section 52.7, verfügbar unter http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=00001-01000&file=43-53 (21.10.2010).

771 Physical & Contructive Invasions of Privacy, Civil Code section 1708.8, verfügbar unter http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=01001-02000&file=1708-1725 (21.10.2010).

772 Vehicle Code section 9951, verfügbar unter http://www.leginfo.ca.gov/cgi-bin/displaycode?section=veh&group=09001-10000&file=9950-9955 (21.10.2010).

773 Civil Code section 1936, verfügbar unter http://law.onecle.com/california/civil/1936.html (21.10.2010).

computersierten Daten von Autoverkäufern beschränken, soweit keine Zustimmung besteht und keine Informationssicherheit gewährleistet wird.[774]

Auch in **anderen Bereichen** des Wirtschaftslebens bestehen besondere Vorschriften zu Beschaffen, Gebrauch und Weitergabe / Veröffentlichung (*disclosure*) von Daten. So werden im Versicherungsbereich Standards zur Datenbearbeitung definiert und die Weitergabe ist nur bei Zustimmung und Notwendigkeit erlaubt.[775] Im Bereich der Telekommunikation ist das Offenlegen des Gebraucherverhaltens ohne Zustimmung grundsätzlich verboten (ausser bei gerichtlicher Anordnung oder im Zusammenhang mit der Eintreibung von Schulden) und es besteht eine Hinweispflicht auf die Möglichkeit der Aufzeichnung bei Anruf auf gewisse Nummern.[776] Es bestehen zudem Regeln, welche unaufgeforderte Anrufe einschränken (*do not call list*)[777], das Zusenden von Werbetexten auf Telefone verbieten[778]. Im medizinischen Bereich darf keine medizinische Information zum Zweck der Direktvermarktung beschafft werden, sofern keine Zustimmung vorliegt und der Zweck nicht klar dargelegt ist[779]. Wohl angesichts der kontroversen Natur der Fortpflanzungsmedizin besteht zudem ein Verbot, Adresse, Telefonnummern oder Bilder von Patienten, Angestellten und Freiwilligen in diesem Bereich tätigen Personen zu veröffentlichen.[780] Damit soll die Sicherheit der betroffenen Personen geschützt werden. Ein weiterer, eigener Wirtschaftsbereich sind die Agenturen, welche das Verhalten von Konsumenten für Drittpersonen (Arbeitgeber, Versicherungen) aufzeichnen. Auch hier bestehen spezifische Regulierungen.[781]

Ein regelrechtes Arsenal von Gesetzgebung besteht im Zusammenhang mit **Computern, e-mail und Internet**. Zu erwähnen sind z.B. der *Anti-Phising Act von 2005* (Verbot sich als Firma oder Verwaltungsbehörde auszugeben, um persönliche Informationen zu erhalten)[782], das Verbot der Installation von Software, welche das Sammlen von persönlicher Information erlaubt (spyware)[783], eine Schadenersatzpflicht bei Spam (Verwendung von rreführenden oder gefälschten Titel oder Informationen beim Versand von Spam, wobei auch der Attorney General klageberechtigt ist;

---

774 Vehicle Code section 11713.3 und 11713.25, verfügbar unter http://www.leginfo.ca.gov/cgi-bin/displaycode?section=veh&group=11001-12000&file=11700-11740 (21.10.2010).

775 Insurance Code Section 791, verfügbar unter http://www.leginfo.ca.gov/cgi-bin/displaycode?section=ins&group=00001-01000&file=791-791.28 (21.10.2010).

776 Public Utilities Code sections 2891-2894.10, verfügbar unter http://www.leginfo.ca.gov/cgi-bin/displaycode?section=puc&group=02001-03000&file=2891-(21.10.2010) 2894.10.

777 Business and Professions Code sections 17590-17594, verfügbar unter http://www.leginfo.ca.gov/cgi-bin/displaycode?section=bpc&group=17001-18000&file=17590-17594 (21.10.2010).

778 Business and Professions Code section 17538.41, verfügbar unter http://www.leginfo.ca.gov/cgi-bin/displaycode?section=bpc&group=17001-18000&file=17530-17539.6 (21.10.2010).

779 Civil Code section 1798.91, verfügbar unter http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=01001-02000&file=1798.91 (21.10.2010).

780 Government Code section 6218, verfügbar unter http://www.leginfo.ca.gov/cgi-bin/displaycode?section=gov&group=06001-07000&file=6218-6218.05 (21.10.2010).

781 Investigative Consumer Reporting Agencies Act, California Civil Code sections 1786-1786.60, verfügbar unter http://www.privacy.ca.gov/icraa.htm (21.10.2010).

782 Business and Professions Code sections 22948-22948.3, verfügbar unter http://www.leginfo.ca.gov/cgi-bin/displaycode?section=bpc&group=22001-23000&file=22948-22948.3 (21.10.2010).

783 Business and Professions Code sections 22947, verfügbar unter http://www.leginfo.ca.gov/cgi-bin/displaycode?section=bpc&group=22001-23000&file=22947-22947.6 (21.10.2010).

Klagerecht des e-mail Providers).[784] Oft führen Gesetze eine Hinweispflicht („privacy policy“) sowie eine Schadenminderungspflicht ein, so z.B. für Wireless-Geräte,[785] für kommerzielle Web-Sites (Hinweis auf die Art der identifizierenden Information, welche gesammelt wird, sowie auf Dritte, mit welchen Daten ausgetauscht werden)[786] und für Verwaltungsbehörden (Hinweis, Zustimmung vor Weiterleitung der Daten)[787]. Gegenüber der Öffentlichkeit des Internets haben zudem gewählte oder ernannte Beamte (*officials*) das Recht, schriftlich die Nichtveröffentlichung der Privatadresse und Telefonnummer zu verlangen.[788]

Besondere Regeln bestehen ebenfalls im Zusammenhang mit der **Sicherheit von computerisierten Datensammlungen**. Dabei müssen Firmen und Verwaltungseinheiten, welche unverschlüsselte persönliche Informationen beinhalten, die betroffene Person benachrichtigen, sofern eine nicht berechtigte Person die persönliche Information erhalten hat (oder zu haben scheint) [789]

Als neuste gesetzgeberische Initiative im Informatikbereich ist die momentan debattierte Regulierung von **sozialen Netzwerken** zu erwähnen (*Social Networking Privacy Act*), wobei den Betreibern die Veröffentlichung der Adresse und Telefonnummer von Benutzern unter 18 Jahren verbietet.[790]

---

784 Business and Professions Code sections 17529 ff. und 17538.45, verfügbar unter http://www.leginfo.ca.gov/cgi-bin/displaycode?section=bpc&group=17001-18000&file=17529-17529.9 (21.10.2010) und http://www.leginfo.ca.gov/cgi-bin/displaycode?section=bpc&group=17001-18000&file=17530-17539.6 (21.10.2010).

785 Business and Professions Code sections 22948.5-22948.7, verfügbar unter http://www.leginfo.ca.gov/cgi-bin/displaycode?section=bpc&group=22001-23000&file=22948.5-22948.7 (21.10.2010).

786 Online Privacy Protection Act 2003, Business and Professions Code sections 22575-22579, verfügbar unter http://www.leginfo.ca.gov/cgi-bin/displaycode?section=bpc&group=22001-23000&file=22575-22579 (21.10.2010).

787 Government Code 6254.21, verfügbar unter http://www.leginfo.ca.gov/cgi-bin/displaycode?section=gov&group=10001-11000&file=11000-11019.10 (21.10.2010).

788 Government Code 6254.21, verfügbar unter http://www.leginfo.ca.gov/cgi-bin/displaycode?section=gov&group=06001-07000&file=6250-6270 (21.10.2010).

789 Civil Code sections 1798.29, 1798.82, 1798.84, verfügabr unter http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=01001-02000&file=1798.25-1798.29 (21.10.2010) and http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=01001-02000&file=1798.80-1798.84 (21.10.2010). Siehe auch Office of Privacy Protection’s Recommended Practices.

790 Senate Bill 1361, verfügbar unter http://e-lobbyist.com/gaits/text/1749 (25.10.2010).

## 11.2 Massachusetts

The New Massachusetts Data Protection Regulation 201 CMR 17.00 aims to insure the security and confidentiality of customer information in a manner fully consistent with industry standards; protect against anticipated threats or hazards to the security or integrity of such information; and protect against unauthorized access to or use of such information that may result in substantial harm or inconvenience to any consumer.[791] It imposes a duty to protect personal information and to adopt a **written plan of detailed administrative, technical, and physical safeguard measures** to be taken in order to do so.[792]

---

791 201 CMR 17.01(1).

792 201 CMR 17.03. This section contains a non-exclusive list of such measures:

(2) Without limiting the generality of the foregoing, every comprehensive information security program shall include, but shall not be limited to:

(a) Designating one or more employees to maintain the comprehensive information security program;

(b) Identifying and assessing reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, including but not limited to:

1. ongoing employee (including temporary and contract employee) training;
2. employee compliance with policies and procedures; and
3. means for detecting and preventing security system failures.

(c) Developing security policies for employees relating to the storage, access and transportation of records containing personal information outside of business premises.

(d) Imposing disciplinary measures for violations of the comprehensive information security program rules.

(e) Preventing terminated employees from accessing records containing personal information.

(f) Oversee service providers, by:

1. Taking reasonable steps to select and retain third-party service providers that are capable of maintaining appropriate security measures to protect such personal information consistent with these regulations and any applicable federal regulations; and
2. Requiring such third-party service providers by contract to implement and maintain such appropriate security measures for personal information; provided, however, that until March 1, 2012, a contract a person has entered into with a third party service provider to perform services for said person or functions on said person's behalf satisfies the provisions of 17.03(2)(f)(2) even if the contract does not include a requirement that the third party service provider maintain such appropriate safeguards, as long as said person entered into the contract no later than March 1, 2010.

(g) Reasonable restrictions upon physical access to records containing personal information,, and storage of such records and data in locked facilities, storage areas or containers.

(h) Regular monitoring to ensure that the comprehensive information security program is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of personal information; and upgrading information safeguards as necessary to limit risks.

(i) Reviewing the scope of the security measures at least annually or whenever there is a material change in business practices that may reasonably implicate the security or integrity of records containing personal information.

(j) Documenting responsive actions taken in connection with any incident involving a breach of security, and mandatory post-incident review of events and actions taken, if any, to make changes in business practices relating to protection of personal information.

### 11.2.1. Scope of Application

The provisions of this regulation apply to all persons that own, license, receive, store, maintain, process, or otherwise has access to (referred to as "own or license") personal information about a resident of the Commonwealth in connection with the provision of goods or services or in connection with employment.[793] Personal information is defined as follows:

> a Massachusetts resident's first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident: (a) Social Security number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account; provided, however, that "Personal information" shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.[794]

The regulation applies to those engaged in commerce. More specifically, the regulation applies to those who collect and retain personal information in connection with the provision of goods and services or for the purposes of employment. The regulation does not apply, however, to natural persons who are not in commerce.[795]

No. 201 CMR 17.01 specifically excludes from the definition of "person" any "agency, executive office, department, board, commission, bureau, division or authority of the Commonwealth, or any of its branches, or any political subdivision thereof."

### 11.2.2. Security Provisions in connection with information stord through computer

#### *11.2.2.1 Risk-based approach*

Anyone who owns or licenses personal information must have a **written plan** detailing the measures adopted to safeguard such information. The regulation adopts a **risk-based approach** to information security. A risk-based approach is one that is designed to be flexible while directing businesses to establish a written security program that takes into account the particular business's size, scope of business, amount of resources and the need for security. For example, if a company has only employee data with a small number of employees, it should lock its files in a storage cabinet and lock the door to that room. It should permit access to only those who require it for official duties. Conversely, if the company has both employee and customer data containing personal information, then its security approach would be more stringent. If the company has a large volume of customer data containing personal information, then its approach would be even *more* stringent.

The level of monitoring necessary to ensure a business' information security program is providing protection from unauthorized access to, or use of, personal information, and effectively limiting risks will depend largely on the nature of the business, its business practices, and the amount of personal information it owns or licenses. It will also depend on the form in which the information is

---

793 201 CMR 17.01(2).

794 *Id.*

795 COMMONWEALTH OF MASSACHUSETTS OFFICE OF CONSUMER AFFAIRS AND BUSINESS REGULATION, FAQ, available at: http://www.mass.gov/Eoca/docs/idtheft/201CMR17faqs.pdf (consulted October 11, 2010).

kept and stored. Obviously, information stored as a paper record will demand different monitoring techniques from those applicable to electronically stored records. In the end, the monitoring that is put in place must be such that it is reasonably likely to reveal unauthorized access or use.

***11.2.2.2 Encryption***

Section 17.04 provides a non-exclusive list of **minimum precautions** to be taken in connection with information stored or transmitted through a computer.[796] The regulations require that businesses encrypt documents sent over the Internet or saved on laptops or flash drives, encrypt wirelessly transmitted data, and deploy up-to-date firewalls to create "an electronic gatekeeper" between the data and the outside world that only allows authorized users to access or transmit data.

The computer security provisions in 17.04 should be construed in accordance with the risk-based approach of the regulation. All of the computer security provisions apply to a business if they are **technically feasible**. The standard of technical feasibility takes reasonableness into account. “Technically feasible” means that if there is a reasonable means through technology to accomplish a required result, then that reasonable means must be used.

The regulation requires **encryption of portable devices** where it is reasonable and technically feasible. The definition of encryption has been amended to make it technology neutral so that as

---

[796] 201 CMR 1704 provides :

Every person that owns or licenses personal information about a resident of the Commonwealth and electronically stores or transmits such information shall include in its written, comprehensive information security program the establishment and maintenance of a security system covering its computers, including any wireless system, that, at a minimum, and to the extent technically feasible, shall have the following elements:
(1) Secure user authentication protocols including:
(a) control of user IDs and other identifiers;
(b) a reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices;
(c) control of data security passwords to ensure that such passwords are kept in a location and/or format that does not compromise the security of the data they protect;
(d) restricting access to active users and active user accounts only; and
(e) blocking access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system;
(2) Secure access control measures that:
(a) restrict access to records and files containing personal information to those who need such information to perform their job duties; and
(b) assign unique identifications plus passwords, which are not vendor supplied default passwords, to each person with computer access, that are reasonably designed to maintain the integrity of the security of the access controls;
(3)Encryption of all transmitted records and files containing personal information that will travel across public networks, and encryption of all data containing personal information to be transmitted wirelessly.
(4) Reasonable monitoring of systems, for unauthorized use of or access to personal information;
(5) Encryption of all personal information stored on laptops or other portable devices;
(6) For files containing personal information on a system that is connected to the Internet, there must be reasonably up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of the personal information.
(7) Reasonably up-to-date versions of system security agent software which must include malware protection and reasonably up-to-date patches and virus definitions, or a version of such software that can still be supported with up-to-date patches and virus definitions, and is set to receive the most current security updates on a regular basis.
(8) Education and training of employees on the proper use of the computer security system and the importance of personal information security.

encryption technology evolves and new standards are developed, this regulation will not impede the adoption of such new technologies. Only those portable devices that contain personal information of customers or employees need be encrypted and only where technically feasible The "technical feasibility" language of the regulation is intended to recognize that at this period in the development of encryption technology, there is little, if any, generally accepted encryption technology for most portable devices, such as cell phones, blackberries, net books, iphones and similar devices. While it may not be possible to encrypt such portable devices, personal information should not be placed at risk in the use of such devices. There is, however, technology available to encrypt laptops.

**Password protecting data** when storing it on a laptop and when transmitting it wirelessly is not enough to satisfy the encryption requirement. No. 201 CMR 17.00 makes clear that encryption must bring about a "*transformation* of data into a form in which meaning cannot be assigned" (emphasis added). This is to say that the data must be *altered* into an unreadable form. Password protection does not *alter* the condition of the data as required, and therefore would not satisfy the encryption standard.

**Backup** tapes must ordinarily be encrypted on a prospective basis only. However, if a backup tape is to be transported from current storage, and it is technically feasible to encrypt (i.e. the tape allows it) then it must be done prior to the transfer. If it is not technically feasible, then one should consider the sensitivity of the information, the amount of personal information and the distance to be traveled and take appropriate steps to secure and safeguard the personal information. For example, a large volume of sensitive personal information is to be transported, if might be appropriate to consider using an armored vehicle with an appropriate number of guards.

If it is not technically feasible to encrypt email containing personal information, then it is not necessary. However, best practices would entail not sending unencrypted personal information in an **email**. There are alternative methods to communicate personal information other than through email, such as establishing a secure website that requires safeguards such as a username and password to conduct transactions involving personal information.

#### *11.2.2.3 Third party service providers*

A person who owns or licenses personal information is responsible for the selection and retention of a third-party service provider who is capable of properly safeguarding personal information that such person owns or licenses. The third party service provider provision in 201 CMR 17.00 is modeled after the third party vendor provision in the Federal Trade Commission's Safeguards Rule.[797] Where state or federal law or regulation requires the use of a specific third party service provider, then the obligation to select and retain would effectively be met.

#### *11.2.2.4 Swipe technology*

If a legal person uses swipe technology only, and does not have actual custody or control over the personal information, then it would not own or license personal information with respect to *that* data, as long as such data is batched out in accordance with the Payment Card Industry (PCI) standards.[798]

#### *11.2.2.5 Retention*

How long a company can retain documents containing personal information is a business decision; there are no maximum periods specified in the law. However, good business practice would dictate limiting the amount of personal information collected to that reasonably necessary to accomplish the legitimate purpose for which it is collected and limiting the time such information is retained to

---

[797] Available at : http://www.ftc.gov/os/2002/05/67fr36585.pdf (consulted October 12, 2010).

[798] See https://www.pcisecuritystandards.org/index.shtml (consulted October 12, 2010).

that reasonably necessary to accomplish such purpose. Access should also be limited to those persons who are reasonably required to know such information.

Although it is not necessary to inventory all records, companies should perform a risk assessment and identify which of its records contain personal information in order to be able to handle and protect that information.

#### *11.2.2.6 Financial accounts*

A financial account is an account that if access is gained by an unauthorized person to such account, an increase of financial burden, or a misappropriation of monies, credit or other assets could result. Examples of a financial account are: checking account, savings account, mutual fund account, annuity account, any kind of investment account, credit account or debit account.

An insurance policy number qualifies as a financial account number if it grants access to a person's finances, or results in an increase of financial burden, or a misappropriation of monies, credit or other assets.

#### *11.2.2.7 Attorney-client privilege*

If an attorney owns or licenses personal information, he/she must comply with 201 CMR 17.00 regardless of privileged or confidential communications. The attorney must take steps outlined in 201 CMR 17.00 to protect the personal information taking into account the size of his/her firm, scope, resources, and need for security.

# IV. SCHLUSSFOLGERUNG

Ein detaillierter Vergleich mit dem schweizerischen Recht ist im Rahmen dieser Analyse nicht möglich. Ganz allgemein scheint jedoch das Schweizerische Recht dem europäischen Standard weitgehend zu entsprechen und teilweise darüber hinauszugehen, insbesondere was die Rechte der Betroffenen sowie die Aktivitäten der Datenschutzbeauftragten betrifft. Keine analogen Regelungen finden sich jedoch (unseres Wissens) im Gebiet der **elektronischen Kommunikation und der modernen Technologien**, wo die Richtlinie 2002/58/EG, das amerikanische Recht sowie deutsche und österreichische Regelungen zur Videoüberwachung allenfalls Beispielscharakter haben könnten. Die weitere Entwicklung lässt zudem weitere Initiativen insbesondere auf dem Gebiet der „social networks“ erwarten.

Auch im Hinblick auf die **Kompetenzen der Aufsichtsbehörde** geht das schweizerische Recht eher weniger weit als andere Rechtsordnungen. Auch wenn sich hier die verschiedenen Rechtsordnungen erheblich unterscheiden ist doch darauf hinzuweisen, dass die Mehrheit von Staaten der Behörde weitreichende Entscheidbefugnisse einräumen. Es bestehen aber auch gewisse Bedenken hinsichtlich (Rechtsstaatlichkeit, Verfahrensgarantien), welche durchaus ernst zu nehmen sind.

SCHWEIZERISCHES INSTITUT FÜR RECHTSVERGLEICHUNG

Dr. Lukas Heckendorn Urscheler
*Leiter der wissenschaftlichen Abteilung*

Dr. Josef Skala
*Wissenschaftlicher Mitarbeiter*

Benelux : Annelot Peters
Deutschland : Marit Mann
Frankreich : Marion Hervier
Italien : Giovanni Tamburrini
Kanada : Laurence Bich-Carrière
Norwegen und Österreich : Andreas Fötschl
Slowenien : Josef Skala
Spanien : Alberto Aronovitz
USA und Vereinigtes Königreich : Karen Jeanneret-Druckman