Monday, October 19
2:30 pm–4:00 pm

303 The Evolution of Laws and Regulations in Privacy Matters and its Impact on Organizations Doing Business Outside the United States: An Overview of Canadian and Other International Jurisdictions

Christine Carron
Senior Partner
Ogilvy Renault LLP

Lukasz Granosik
Partner
Ogilvy Renault LLP

Vincent Kou
Director of Legal Services, China/Asia
Rio Tinto Alcan

Olivier Niggli
Attorney CFO/ Director of Legal Affairs
World Anti-Doping Agency (WADA)

Faculty Biographies

Christine Carron

Christine Carron is a senior partner at Ogilvy Renault, in their Montreal office. She practices primarily in corporate and commercial litigation and in the areas of banking, privacy, product liability, consumer protection, and e-commerce. She is chair of their privacy and access to information team. She has been involved in a wide range of commercial litigation, including the defense of class actions in the financial services, retail, and tobacco industries and represents corporate clients in disputes involving damages for breach of commercial contracts or for latent defects and in shareholder disputes. Ms. Carron also acts as defense counsel in major class actions. She has represented clients in parliamentary commissions on the adoption and amendment of Quebec's privacy legislation for the private sector and participated in the consultation process for Quebec's legislation on new technologies.

Her distinctions and recognitions include: advocatus emeritus by the Quebec Bar; fellow of the American College of Trial Lawyers; the best lawyers in Canada, corporate and commercial litigation, class action litigation; leader in the field of dispute resolution (Quebec), Chambers Global: The World's Leading Lawyers; leading lawyer in class action litigation, Lexpert American Lawyer Guide to the leading 500 lawyers in Canada; One of Canada's top 25 women lawyers, Lexpert Magazine; one of "Les 101 Femmes entrepreneurs," Magazine Entreprendre; consistently recommended in litigation - class actions; repeatedly recommended in litigation - corporate and commercial, The Canadian Legal Directory Lexpert.

Lukasz Granosik

Lukasz Granosik is a partner at Ogilvy Renault where he practices employment and labor law in Montreal. Mr. Granosik advises and represents employers, with a focus on collective bargaining and grievance arbitration, labor standards, individual contracts of employment, administrative law, and occupational health and safety matters. He has particular expertise in human rights issues and acts in numerous matters involving discrimination, medical examinations, employee surveillance, and protection of personal information.

Mr. Granosik is a member of the Canadian Bar Association, and has served as president of the Quebec Branch. He is a member of the disciplinary committee of the Quebec bar, serves on the Canada-Poland Chamber of Commerce, and is an assessor for the Human Rights Tribunal. He is the director of the Canadian Bar Insurance Association. In addition, Mr. Granosik lectures on labor law.

Mr. Granosik received a BS from Université de Montréal, and is a graduate of the Université de Sherbrooke School of Law.

Vincent Kou

Vincent H. Kou is chief counsel for Rio Tinto Alcan in Asia. He is currently based in Singapore. Before his relocation to Singapore, his was based in Beijing and Shanghai as director of legal services and mergers and acquisitions and chief representative for Alcan (now part of Rio Tinto Group). His work in China included negotiating, structuring and drafting legal documents related to mergers and acquisitions projects and other forms of direct investments, joint ventures, divestitures, greenfield projects, and he played a leading role in corporate initiatives including the creation of Alcan's regional headquarter in Shanghai. He also provided legal support to Rio Tinto Alcan's businesses operating in China and South East Asia, including drafting and reviewing of commercial contracts, advising on labor and employment matters and compliance with Chinese statutory requirements.

Prior to joining Rio Tinto Alcan, Mr. Kou was an associate with two Canadian national law firms in Montreal. His work in private practice includes securities law, mergers and acquisitions, venture capital financing, corporate and commercial law, and investments in PRC.

He is a past board member and vice-chairman of Canada-China Business Council, Beijing chapter.

Mr. Kou received his LLB from University of Sherbrooke.

Olivier Niggli

Olivier Niggli is the chief financial officer and legal director of the World Anti Doping Agency, an international organization with Swiss statutes and headquarters in Montreal Canada. He is in charge of overseeing all legal matter for the agency including all anti-doping prosecution and legislation. He is currently involved in on going discussion with the EU on the implications of the fight against doping for data protection.

Prior to that Olivier Niggli was a practicing lawyer in Switzerland with the firm Carrad&Associes. He was active in sports law, arbitration, and commercial matters.

Olivier Niggli has a law degree from Lausanne University in Switzerland and a LLM from the London School of Economics (LSE) in the UK. He also holds an MBA from McGill University in Canada.

CANADA

- Jurisdictional Issues
- Legislative Framework
  - Constitutional Protection
  - Federal Statutes
  - Provincial Statutes

2009 Annual Meeting October 18–21 Boston Don't just survive. Thrive!

CANADA

- PIPEDA
  - Territorial scope (Declaration of laws substantially similar to PIPEDA)
  - 10 Governing Principles
  - Definition of Personal Information
  - Consent

2009 Annual Meeting October 18–21 Boston Don't just survive. Thrive!

CANADA

- PIPEDA
  - Transfer and Disclosure of Personal Information
  - Privacy Commissioner's Guidelines Regarding Processing Personal Date Across Borders

2009 Annual Meeting October 18–21 Boston Don't just survive. Thrive!

CANADA

- PIPEDA
  - Case Summary #313 : Bank's notification to customers triggers PATRIOT Act concerns; complaint not well-founded

CANADA

- PIPEDA
  - Case Summary #365 : Responsibility of Canadian financial institutions in SWIFT's disclosure of personal information to US authorities; complaints not well-founded

CANADA

- PIPEDA
  - Case Summary #394 : Outsourcing of email services to US-based firm; complaint not well-founded

CANADA

- PIPEDA
  - Case concerning Facebook inc. : some of complaints well-founded.

2009 Annual Meeting October 18–21 Boston Don't just survive. Thrive!

CANADA

- QUÉBEC
  - Legislative Framework
    - Québec Charter
    - Civil Code of Québec
    - Protection of Personal Information Act in the Private Sector

2009 Annual Meeting October 18–21 Boston Don't just survive. Thrive!

CANADA

- QUÉBEC
  - Protection of Personal Information Act in the Private Sector
    - Definition of Personal Information
    - Consent
    - Notion of « Enterprise »
    - Access to Information Commission

2009 Annual Meeting October 18–21 Boston Don't just survive. Thrive!

ACC Association of Corporate Counsel

PRIVACY LAWS IN CANADA

- QUÉBEC
  - Transfer of Personal Information Outside Québec
  - Nominative lists and marketing issues

2009 Annual Meeting October 18–21 Boston Don't just survive. Thrive!

ACC Association of Corporate Counsel

CANADA

- OTHER CANADIAN JURISDICTIONS
  - Alberta
  - British Columbia
  - Ontario
  - Other Canadian Provinces

2009 Annual Meeting October 18–21 Boston Don't just survive. Thrive!

ACC Association of Corporate Counsel

EUROPE

- BACKGROUND
  - WADA is a Swiss foundation with headquarters in Canada
  - WADA's mandate is to fight against doping worldwide
  - WADA needs to collect and process personal data in order to have an efficient fight against doping
  - WADA has developed an electronic system to deal with this information

2009 Annual Meeting October 18–21 Boston Don't just survive. Thrive!

EUROPE

- BACKGROUND
  - The situation today is much more secure than it was 5 years ago, but the development of an electronic system has attracted the attention of the EU and European authorities
  - WADA is not directly subject to EU law, but must deal with it!!!

2009 Annual Meeting October 18–21 Boston Don't just survive. Thrive!

APPLICABLE LAWS - WADA

- EU Data Protection Directive 95/46/EC
- National Legislation of each EU Member State (27 states)
- Canadian Federal Law and Quebec Law
- Swiss Law

2009 Annual Meeting October 18–21 Boston Don't just survive. Thrive!

APPLICABLE LAWS - WADA

- Any other country where parties may have access to some personal information, either on athletes or other participants

2009 Annual Meeting October 18–21 Boston Don't just survive. Thrive!

EUROPE

- THE AUTHORITIES
  - WADA has been dealing since the year 2000 directly with individual countries and the Council of Europe
  - The European Commission has no jurisdiction over sport (for the moment) and only became involved last year

2009 Annual Meeting October 18–21 Boston Don't just survive. Thrive!

EUROPE

- THE AUTHORITIES
  - Suddenly, without informing WADA, the European Union became very interested in the subject of personal information collected for anti-doping purposes
  - The Working Party 29 (WP29) was invited by the European Commission to comment on a privacy standard that WADA had prepared

2009 Annual Meeting October 18–21 Boston Don't just survive. Thrive!

EUROPE

- THE AUTHORITIES
  - The WP29 went well beyond its mandate to critique the entire fight against doping

2009 Annual Meeting October 18–21 Boston Don't just survive. Thrive!

EUROPE

- THE PROCESS
  - WADA never heard from the WP29 until July 2008, despite 2 rounds of worldwide consultation on a draft Privacy Standard
    - WADA called the WP29 Secretariat in June and told to wait for the opinion

EUROPE

- THE PROCESS
  - The WP29 rendered a rather "negative" opinion on 1st August 2008 (on an outdated draft of the Standard)
  - WADA was never heard by the WP29 before they released their first opinion

EUROPE

- THE PROCESS
  - The WP29 had no understanding of WADA's activities and of the fight against doping
  - The opinion harmed WADA's operation and weakened the fight against doping

EUROPE

- THE PROCESS CONTINUED…
  - In April 2009, the WP29 rendered a second opinion.
  - Before then:
    - WADA invited to discuss "Standard" with WP29 sub-group in November, but then questioned on other issues
    - WADA told in January to respond in 2 weeks to long list of questions

2009 Annual Meeting October 18–21 Boston Don't just survive. Thrive!

EUROPE

- THE PROCESS CONTINUED…
  - Requests for an oral hearing were denied
  - The 2nd WP29 opinion (once again) reflected a lack of understanding about WADA's activities and the legal framework for the fight against doping

2009 Annual Meeting October 18–21 Boston Don't just survive. Thrive!

EUROPE

- THE PROCESS CONTINUED…
  - Only after the release of the 2nd opinion did the WP29 agree to meet WADA in June 2009
  - WP29 still probably does not understand the big picture….

2009 Annual Meeting October 18–21 Boston Don't just survive. Thrive!

ACC Association of Corporate Counsel

EUROPE

- THE ISSUES
  - Process
    - Who do you engage with and who do you complain to?
      - European Commission? (Secretariat of the WP29)
      - The WP29 itself? (its President?; its Members?; its Sub-group?)
      - National DPAs?

2009 Annual Meeting October 18–21 Boston Don't just survive. Thrive!

ACC Association of Corporate Counsel

EUROPE

- THE ISSUES
  - Can you control the process or does it control you? Can you play the interested parties against one another?
    - Go on the offensive or be passive?
    - DPAs against each other; Commission v. DPAs?
  - What approach is the most likely to produce a favorable outcome?
    - Friendly, neutral or combative?

2009 Annual Meeting October 18–21 Boston Don't just survive. Thrive!

ACC Association of Corporate Counsel

EUROPE

- THE ISSUES
  - How do you educate the authorities about the nature of your business and the rationale for the collection of data?
    - Lobbying? (resources required)
    - Presentation? (need invitation)
    - Building relationship? (takes time)

2009 Annual Meeting October 18–21 Boston Don't just survive. Thrive!

ACC Association of Corporate Counsel

EUROPE

- THE ISSUES
  - Merits
    - Legal basis for collection of data
      - WP29 adopted a very narrow - and questionable - interpretation of the EU directive:
        - Do not recognize consent
          - Consent is expressly allowed for by the EU directive
        - It is fundamental to the practice of sport

2009 Annual Meeting October 18–21 Boston Don't just survive. Thrive!

ACC Association of Corporate Counsel

EUROPE

- THE ISSUES
  - Do not accept public interest?
    - Doping is recognized by all governments as a public health issue
  - Ask for specific legal basis (i.e., national law) when such a basis does not exist!
    - Unrealistic in a short time frame
  - WP29 interpretation of the directive is not shared by all DPAs
    - Makes it very difficult for the companies and the end user to know who to believe

2009 Annual Meeting October 18–21 Boston Don't just survive. Thrive!

ACC Association of Corporate Counsel

EUROPE

- THE ISSUES
  - International Transfer of Data
    - Limited to countries with adequacy recognition (very limited in number; Switzerland, Canada (Canadian Federal Law), Argentina…)
    - No recognition yet of Quebec's provincial law despite its obvious adequacy

2009 Annual Meeting October 18–21 Boston Don't just survive. Thrive!

ACC Association of Corporate Counsel

EUROPE

- THE ISSUES
  - Lack of proper administrative process from the EU Commission to drive the process
  - Question of further transfers outside of Canada

2009 Annual Meeting October 18–21 Boston Don't just survive. Thrive!

ACC Association of Corporate Counsel

EUROPE

- SOLUTIONS
  - Keep dialog open
    - Expensive, time consuming, sometimes frustrating
    - Explain your business as much as you can and get them to see the bigger picture (if there is one)

2009 Annual Meeting October 18–21 Boston Don't just survive. Thrive!

ACC Association of Corporate Counsel

EUROPE

- SOLUTIONS
  - Look for alternative solutions that you can propose
    - Don't come empty handed to meetings and be prepared
  - Be ready to defend your position in court
    - Sometimes the best defense is a good offence

2009 Annual Meeting October 18–21 Boston Don't just survive. Thrive!

CHINA
BACKGROUND – Rio Tinto Alcan (RTA)

- RTA is the global leader in the aluminum industry -- one of the product groups operated by Rio Tinto
- Over 26,000 employees with operations in six continents and 29 countries and global headquarter based in Montreal

2009 Annual Meeting October 18–21 Boston Don't just survive. Thrive!

CHINA
BACKGROUND – Rio Tinto Alcan (RTA)

- All stages of aluminum process:
  - Mining bauxite
  - Refining bauxite into alumina
  - Smelting alumina to produce aluminum
  - Manufacturing a large variety of fabricated, semi-fabricatred aluminum and composites products

2009 Annual Meeting October 18–21 Boston Don't just survive. Thrive!

CHINA
BACKGROUND – Rio Tinto Alcan (RTA)

- Rio Tinto also owns downstream aluminum businesses under RTA which consist of Engineered Products and Alcan Packaging (both businesses have been identified to be divested) headquartered in Paris

2009 Annual Meeting October 18–21 Boston Don't just survive. Thrive!

CHINA
BACKGROUND – Rio Tinto Alcan (RTA)

- Together with Engineered Products and Alcan Packaging, RTA has strong operations and commercial presence in China with over 3,500 employees located in more than 10 sites dispersed over several different regions of China including a RHQ based in Shanghai

2009 Annual Meeting October 18–21 Boston Don't just survive. Thrive!

CHINA
BACKGROUND – Rio Tinto Alcan (RTA)

- Like most of the businesses in China, we do have to deal with risk associated with potential violation of privacy rights

2009 Annual Meeting October 18–21 Boston Don't just survive. Thrive!

CHINA

- APPLICABLE LAWS
  - What does privacy really mean in the context of the Chinese legal system?
  - No comprehensive national privacy or data protection legislation in place in PRC

2009 Annual Meeting October 18–21 Boston Don't just survive. Thrive!

ACC Association of Corporate Counsel

CHINA

- APPLICABLE LAWS
  - Privacy or data protection is vaguely and indirectly protected in some provisions of law scattered in different specific laws, the key ones include:
    - Constitution Law
    - Civil Law
    - Labor Law
    - Criminal Law
    - Local legislation

2009 Annual Meeting October 18–21 Boston Don't just survive. Thrive!

ACC Association of Corporate Counsel

CHINA

- PRIVACY PROTECTION
  - Under Constitution Law
    - Prohibition of physical search or invasion of a person's residence without legal cause or without due process
    - Citizen's right to freedom and privacy of correspondence is recognized

2009 Annual Meeting October 18–21 Boston Don't just survive. Thrive!

ACC Association of Corporate Counsel

CHINA

- PRIVACY PROTECTION
  - Under Constitution Law
    - Exception to this constitutional right:
      - National security
      - Criminal investigation
    - What constitutes "national security"?

2009 Annual Meeting October 18–21 Boston Don't just survive. Thrive!

CHINA

- PRIVACY PROTECTION
  - Under Civil Law
    - Right of privacy is not listed under the General Principles of Civil Law
    - No specific prohibition of disclosure of personal information under Civil Law
    - Privacy protection is recognized by civil law in the form of the traditional right against defamation or right to reputation
    - Change of direction with the Judicial Interpretation of 2001 and other recent court cases

2009 Annual Meeting October 18–21 Boston Don't just survive. Thrive!

CHINA

- PRIVACY PROTECTION
  - Under Civil Law
    - Draft Tort Liability Law
      - Recognizing the independent right of privacy

2009 Annual Meeting October 18–21 Boston Don't just survive. Thrive!

CHINA

- PRIVACY PROTECTION
  - Under Labor Law
    - Employer is restricted in asking for private information that is not relevant to the employment position
    - Information obtained on employee must be kept confidential
    - It implies that any disclosure requires employee's consent
  - *Specific Case of Medical Examination of Employees*

2009 Annual Meeting October 18–21 Boston Don't just survive. Thrive!

CHINA

- PRIVACY PROTECTION
  - Under Criminal Law
    - The 7th Amendment to the Criminal Law which came into force on February 28, 2008, provides that it is a criminal offense:
      - for employees of government or private organizations in the financial, telecommunication, transportation, education or medical sector to sell or otherwise illegally provide to third parties the personal information of any citizen obtained in the course of performing their duties
      - for any person to obtain such personal data by any unlawful means

2009 Annual Meeting October 18–21 Boston Don't just survive. Thrive!

CHINA

- PRIVACY PROTECTION
  - Under Criminal Law
    - If the *nature of such violation is serious* the person found guilty of either offense will be subject up to three (3) years imprisonment and/ or be fined

2009 Annual Meeting October 18–21 Boston Don't just survive. Thrive!

CHINA

- PRIVACY PROTECTION
  - Under Criminal Law
    - Any corporate entity that commits either offense will be liable to a fine and the officers in charge may be personally liable for such criminal offense
    - Uncertainty regarding the interpretation of or what constitutes "*nature of the violation is serious*" – need to wait for interpretations of the Supreme People's Court

2009 Annual Meeting October 18–21 Boston Don't just survive. Thrive!

CHINA

- MITIGATING RISK
  - How do we mitigate the risk associated with any potential violation of privacy right?
    - Put in place or customize the employee handbook to deal with China specifics and align with your global code of conduct
    - Build robust confidentiality and non-disclosure clause in the employment contract

2009 Annual Meeting October 18–21 Boston Don't just survive. Thrive!

CHINA

- MITIGATING RISK
  - How do we mitigate the risk associated with any potential violation of privacy right?
    - Strong employment contract is not enough -- be mindful of the cultural aspect and set up strong internal system to prevent disclosure and provide training to both management team and relevant employees

2009 Annual Meeting October 18–21 Boston Don't just survive. Thrive!

CHINA

- MITIGATING RISK
  - How do we mitigate the risk associated with any potential violation of privacy right?
    - Extremely careful in sharing personal information between your corporate functions (HR, Legal and Finance)
    - Do you have a good office/worksite security practice in China?

2009 Annual Meeting October 18–21 Boston Don't just survive. Thrive!

ACC Association of Corporate Counsel

CHINA

- MITIGATING RISK
  - How do we mitigate the risk associated with any potential violation of privacy right?
    - Don't deviate from your Western practices or requirements – same or more robust measures or standards should apply in your businesses and operations in China
    - Continue to monitor the progress of adoption of the comprehensive Personal Information Protection Law

2009 Annual Meeting October 18–21 Boston Don't just survive. Thrive!

ACC Association of Corporate Counsel

CHINA

- THE FUTURE
  - The National Privacy Law
    - Where are we in relation to the draft recommended national Personal Information Protection Law?
    - What are the key elements of this long waited law?

2009 Annual Meeting October 18–21 Boston Don't just survive. Thrive!

The Evolution of Laws and Regulations in Privacy Matters and its Impact on Organizations Doing Business Outside the United States: An Overview of Canadian and Other International Jurisdictions

Christine Carron *
Lukasz Granosik *
Érika Bergleron-Drolet **

* Partners, Ogilvy Renault S.E.N.C.R.L., s.r.l. / LLP
** Articling student, Ogilvy Renault S.E.N.C.R.L., s.r.l. / LLP

TABLE OF CONTENTS

PAGE

INTRODUCTORY REMARKS....1
CANADA....3
PRELIMINARY REMARKS....3
I. FEDERAL PERSONAL INFORMATION PROTECTION REGIME....3
A. Legislative Framework....3
1. Constitutional Protection....3
2. General Remarks on the Federal Personal Information Protection Regime....3
3. Purpose of PIPEDA....4
4. Scope of PIPEDA....4
a) Entities and Purposes Covered (s. 4)....*4*
(1) Organizations and purposes covered by PIPEDA (s. 4(1))....4
(2) Organizations and purposes not covered by PIPEDA (s. 4(2))....5
b) Territorial Scope....*5*
(1) Application where provincial legislation is substantially similar to PIPEDA....5
(2) Application in other provinces....6
(3) Application beyond Canada....6
5. Definition of "Personal Information"....7
a) General definition....*7*
b) Interpretative guidelines about what constitutes personal information:....*7*
c) Examples of what constitutes "personal information" for the purposes of PIPEDA....*8*
(1) General examples....8
(2) Specific examples from case law....8
d) Distinction between "personal information" and "work product"....*9*
(1) Workings of the distinction....9
(2) Examples from case law....9
6. Governing Principles of PIPEDA....10
7. Consent of the individual concerned....11
a) Requirements for consent to be valid....*11*
b) Circumstances where the data subject's consent is required....*12*

8. Highlights of the Canadian Federal Data Protection Regime (under PIPEDA) 12
B. Personal Information Transfers / Outsourcing 13
1. General remarks 13
2. Principle 4.1.3: Accountability 13
a) Responsibility for the personal information transferred *13*
b) Obligation to provide a "comparable level of protection" *14*
(1) Meaning of "comparable level of protection" 14
(2) Assessing the "comparable level of protection" 14
(3) Means of ensuring a "comparable level of protection" 14
3. Principe 4.3: Consent 15
4. Principle 4.8: Openness 15
C. Significant Case Law on Data Protection 16
1. *Wyndowe v. Rousseau*, 2008 FCA 39 16
2. Commissioner's Finding: PIPEDA Case Summary #2005-313: Bank's notification to customers triggers PATRIOT Act concerns 16
3. Commissioner's Finding: PIPEDA Case Summary #2007-365: Responsibility of Canadian financial institutions in SWIFT's disclosure of personal information to US authorities considered 17
II. BRIEF OVERVIEW OF PROVINCIAL PERSONAL INFORMATION PROTECTION REGIMES 18
A. Comprehensive Privacy Laws 18
B. Health Information Acts 18
C. Common Law Torts 19
D. Statutory torts 20
E. The Specific Case of Quebec 20
1. Legislative framework 20
a) Protection under the Charter of Human Rights and Freedoms *20*
b) Protection under the Civil Code of Quebec (C.c.Q.) *20*
c) The Act Respecting the Protection of Personal Information in the Private Sector *21*
2. Scope of the Act 21
a) General remarks *21*
b) The notion of enterprise *21*
c) Exclusions *22*

d) Information held by professional orders *22*
e) Territorial scope *22*
3. Definition of "personal information" 22
4. Consent of the individual concerned 23
a) Requirements for consent to be valid *23*
b) Circumstances where the data subject's consent is required *23*
5. Highlights of the Act 23
6. Transfer of personal information outside Québec 24
7. Significant case law on the protection of personal information 25
a) Deschesnes c. Groupe Jean Coutu (P.J.C.) Inc *25*
b) Congrégation des témoins de Jéhovah d'Issoudun-Sud c. Mailly *25*
c) Stébenne c. Assurance-vie Desjardins Laurentienne inc. *26*
EUROPE 27
I. EU DATA PROTECTION REGIME 27
A. Preliminary Remarks 27
B. Legislative framework 28
1. 1980: *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* 28
a) General Remarks *28*
b) Principles of the OECD Guidelines *28*
(1) Principles of national application 28
(2) Principles of international application 29
c) Impact of the OECD Guidelines and further developments *29*
2. 1981: *Convention for the protection of individuals with regard to automatic processing of personal data* 30
3. 1995: Directive 95/46: The main piece of legislation on data protection in the European Union 30
a) General remarks *30*
b) Purpose of the Directive (art. 1) *31*
c) Definition of "personal data" (art. 2(a)) *31*
d) Data subject's consent *32*
(1) Definition of "the data subject's consent" 32
(2) Circumstances where the data subject's consent is required 33

e) Scope – subject matter (art. 3) *33*

f) Scope – territorial (art. 4) *33*

g) General Rules On The Lawfulness Of The Processing Of Personal Data *34*

(1) Principles relating to data quality (article 6) 34

(2) Criteria for making data processing legitimate (art. 7) 35

(3) Processing of sensitive data (art. 8) 35

(4) Rights of the data subjects 35

(5) Other obligations of the data controller 37

(6) Additional requirements for data processing to be lawful 37

(7) Exemptions and limitations 37

h) Judicial remedies, liability and sanctions (art. 22-24) *38*

i) Data transfers to third countries (art. 25-26) *38*

j) Codes of conduct (art. 27) *40*

k) Supervisory authority (art. 28) *40*

l) Working Party (art. 29-30) *40*

4. Directives 2002/58 and 2006/24: Specific Directives in the telecommunications sector 41

a) Directive 2002/58 ..... *41*

b) Directive 2006/24 ..... *41*

5. 2000: *Charter of Fundamental Rights of the European Union* 42

a) General remarks and relevant provisions *42*

b) Legal status of the Charter *43*

C. INTERNATIONAL DATA TRANSFERS (TO THIRD COUNTRIES) 43

1. Definition of international data transfer 43

2. Requirements for an international data transfer to be lawful (art. 25 of Directive 95/46) 43

3. Assessment of the adequacy of the level of protection ensured by a third country 44

a) Entities entitled to make such an assessment *44*

b) Elements to consider *44*

(1) Core content principles 45

(2) Procedural/enforcement requirements 46

c) Third countries that have been considered to provide an adequate level of protection by the European Commission *46*

4. Circumstances under which personal data can be transferred to a country that does not provide an adequate level of protection (art. 26 Directive 95/46) 47

(1) The transfer falls within one of the *6 exceptions* listed in art. 26(1) 47

(2) "The data controller *adduces adequate safeguards* with respect to the protection of privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights" (art. 26(2)) 48

5. Standard Contractual Clauses ("SCCs") (art. 26(4) of Directive 95/46).....48

a) Definition and purpose of SCCs *49*

b) Types of SCCs.....*49*

c) Possibility for the parties to amend a SCC.....*49*

d) Effect of the SCC.....*50*

6. Binding Corporate Rules ("BCRs").....50

a) Definition of BCRs.....*50*

b) Scope of BCRs.....*50*

c) Content of BCRs *51*

d) Effect of the adoption of BCRs.....*51*

e) Enforcement.....*51*

7. Safe Harbor Framework ("Safe Harbor").....52

a) General information about the Safe Harbor *52*

b) Functioning of the Safe Harbor.....*52*

c) Effects of the adhesion to the Safe Harbor *53*

D. Significant case law from the European Court of Justice on data protection.....53

1. C-101/01 (judgment of November 6, 2003) / Reference for a preliminary ruling from the *Göta hovrätt (Sweden): Bodil Lindqvist*.....53

2. Joined Cases C-317/04 and C-318/04 (judgment of May 30 2006) / *European Parliament v. Council of the European Union and Commission of the European Communities* 55

3. C-553/07 (judgement of May 7, 2009) / *College van burgemeester en wethouders van Rotterdam v M.E.E. Rijkeboer Netherlands* 56

NATIONAL DATA PROTECTION REGIMES 58

Preliminary Remarks 58

FRANCE.....58

Legislative framework 58

Constitutional protection.....*58*

Implementation of Directive 95/46 .....*58*

Implementation of Directive 2002/58 ..... *59*
National supervisory authority *59*
Definition of "personal data" 59
Data subject's consent 60
Requirements for consent to be valid *60*
Circumstances where the data subject's consent is required *60*
Highlights of the French data protection regime (under the DPA) 60
Significant case law on data protection 61
Henri S. / SCPP, Cour d'appel de Paris 13ème chambre, section A Arrêt du 15 mai 2007 ..... *61*
Marc W., Asesif et autres / Cnil, Cour de cassation Chambre criminelle 28 septembre 2004 ..... *62*
Microsoft Corporation / Marko K. et AOL France / Marko K. Tribunal de commerce de Paris 8ème chambre Jugement du 05 mai 2004 ..... *62*
Le Ministère public et Mademoiselle S. / Monsieur F. Tribunal de grande instance de Privas Jugement correctionnel du 3 septembre 1997 ..... *63*
GERMANY 63
Legislative framework 63
Constitutional protection *63*
Implementation of Directive 95/46 ..... *64*
Implementation of Directive 2002/58 ..... *64*
National supervisory authority *64*
Definition of "personal data" 65
Data subject's consent 65
Requirements for consent to be valid *65*
Circumstances where the data subject's consent is required *66*
Highlights of the German Data Protection Regime (under the FDPA) 66
Significant case law on data protection 67
Volkszählungsurteil, Federal Constitutional Court, December 15, 1983 (BverfGE, 1 BvR 209/83) *67*
Ruling of the Federal Constitutional Court, October 23, 2006 (1 BvR 2027/02) on the rights of insured persons (notice of consent on standard forms) *68*
Ruling of the Federal Constitutional Court, February 23, 2007 (1 BvR 421/05) on covertly obtained genetic expertise *68*

ITALY 68
Legislative framework 68
Constitutional protection *68*
Implementation of Directive 95/46 ..... *69*
Implementation of Directive 2002/58 ..... *69*
National supervisory authority *69*
Codes of conduct *69*
Definition of "personal data" 70
Data subject's consent 70
Requirements for consent to be valid *70*
Circumstances where the data subject's consent is required *71*
Highlights of the Italian Data Protection Regime (under the Code) 71
Significant case law on data protection 72
Ruling of the Supreme Court of Cassation, February 2004, on evaluation data *72*
Ruling of the Supreme Court of Cassation, June 2004, on unstructured data *73*
Ruling of the Supreme Court of Cassation, 2000, on the right of rectification and exception for journalistic purposes *73*
THE NETHERLANDS 73
Legislative framework 73
Constitutional protection *73*
Implementation of Directive 95/46 ..... *74*
Implementation of Directive 2002/58 ..... *74*
National supervisory authority *74*
Definition of "personal data" 75
Data subject's consent 76
Requirements for consent to be valid *76*
Circumstances where the data subject's consent is required *77*
Highlights of the Dutch Data Protection Regime (under the WBP and the Decree) 77
Significant case law on data protection 78
Ruling of the Supreme Court, June 29, 2007 on three cases involving Dexia and HBU regarding the scope of the right of access *78*
Decision of the DPA, July 20, 2001, no. 2001-0784, regarding the international data transfer between eBay and iBazar *79*

SPAIN 79
Legislative framework 79
Constitutional Protection *79*
Implementation of Directive 95/46 ..... *80*
Implementation of Directive 2002/58 ..... *80*
National Supervisory Authority *81*
Ibero-American Data Protection Network (Red Iberoamericana de Protección de Datos) *81*
Definition of "personal data" 81
Data subject's consent 82
Requirements for consent to be valid *82*
Circumstances where the data subject's consent is required *84*
Highlights of the Spanish Data Protection Regime (under the LOPD and the Decree) 84
Significant case law on data protection 85
Ruling of the Spanish Supreme Court, judgment of April 17, 2007, STS 2778/2007, on the protection of sensitive personal data by a television production company *85*
Ruling of the Spanish Constitutional Court, judgment of November 30, 2000, STC 292/2000, recognizing an autonomous fundamental right to the protection of personal data *86*
Ruling of the Supreme Court, April 27, 2005, on the duty to inform and the registration of data files that do not meet the requisite security standards *86*
SWEDEN 87
Legislative framework 87
Constitutional protection *87*
Implementation of Directive 95/46 ..... *88*
Implementation of Directive 2002/58 ..... *88*
National supervisory authority *88*
Definition of "personal data" 89
Data subject's consent 89
Requirements for consent to be valid *89*
Circumstances where the data subject's consent is required *89*
Highlights of the Swedish Data Protection Regime (under the PDA) 90
Significant case law on data protection 91

Ruling of the Court of Appeal (Göta hovrätt), April 2004, on the internet publication of personal information about volunteers of a church (Lindqvist) *91*

Ruling of the Supreme Administrative Court, 2002, on the disclosure of information by the National Board of Student Aid for the purpose of direct marketing *91*

Ruling of the Supreme Court (Högsta domstolen), judgment of June 12, 2001, Case B 293-00, on the publication of derogatory comments on the Internet *92*

UNITED KINGDOM ("UK") 92

Legislative framework 92

Constitutional protection *93*

Implementation of Directive 95/46 ..... *93*

Implementation of Directive 2002/58 ..... *94*

National supervisory authority *94*

Tort of breach of confidence *94*

Definition of "personal data" 95

Data subject's consent 96

Requirements for consent to be valid *96*

Circumstances where the data subject's consent is required *96*

Highlights of the UK Data Protection Regime (under the DPA) 96

Significant case law on data protection 97

Durant v Financial Services Authority [2003] EWCA Civ 1746 ..... *97*

Johnson v Medical Defence Union [2007] EWCA Civ 262 ..... *98*

Campbell v MGN Ltd. [2004] UKHL 22 ..... *98*

ASIA-PACIFIC REGION 100

I. MAIN REGIONAL INITIATIVES 100

A. Preliminary Remarks 100

B. APEC Privacy Framework 100

1. General remarks 100

2. Definition of "personal information" under the Framework 101

3. Consent of the individual concerned 101

a) Requirements for consent to be valid *101*

b) Circumstances where the data subject's consent is required *101*

4. APEC information privacy principles 102
5. Guidance for domestic and international implementation 103
6. Pathfinder Projects 103
7. Weaknesses and criticisms of the Framework 104
C. ASSOCIATION OF SOUTH EAST ASIAN NATIONS (ASEAN) HARMONIZATION 104
II. NATIONAL DATA PROTECTION REGIMES 104
A. Preliminary Remarks 105
B. Countries That Have Adopted Privacy Legislation 105
1. AUSTRALIA 105
a) Constitutional protection 105
b) The main piece of legislation: the Privacy Act 1988 105
(1) Definition of "personal information" under the Act 106
(2) Consent of the individual concerned 106
(3) National Privacy Principles 106
(4) Highlights of the Act 107
c) Protection under Privacy Codes 107
d) Protection under the common law 108
2. HONG KONG 108
a) Constitutional protection 108
b) Main piece of legislation : the Personal Data (Privacy) Ordinance 108
(1) General information 108
(2) Definition of "personal data" under the Ordinance 109
(3) Data subject's consent 109
(4) Highlights of the Ordinance 109
c) Protection under sector-specific laws and codes of conduct 110
d) Common law torts 110
3. JAPAN 110
a) Constitutional protection 110
b) Main piece of legislation: the Act on the Protection of Personal Information 111
(1) General remarks 111
(2) Definition of "personal information" under the APPI 111

(3) Consent of the individual concerned 111
(4) Highlights of the APPI....112
c) Protection under sector-specific laws 112
d) Privacy Trustmark Scheme....113
4. MACAO 113
a) Constitutional protection....113
b) Main piece of legislation: the Personal Data Protection Act....113
(1) General remarks....113
(2) Definition of "personal data" under the PDPA....114
(3) Data subject's consent 114
(4) Highlights of the PDPA....114
5. NEW ZEALAND 115
a) Constitutional protection....115
b) Main piece of legislation: the Privacy Act 1993 115
(1) General remarks....115
(2) Definition of "personal information" under the Act....115
(3) Consent of the individual concerned 115
(4) The Information Privacy Principles....116
(5) Highlights of the Act: 117
(6) Project of assessment by the European Commission as providing an "adequate level of protection" 117
c) Protection under sector-specific laws and codes of practice 117
d) Protection under the common law....118
6. SOUTH KOREA 118
a) Constitutional protection....118
b) Main piece of legislation: the Act on Promotion of Information and Communication Network Utilization and Information Protection....119
(1) General remarks....119
(2) Moderately limited scope 119
(3) Definition of "personal information" under the APICNUIP 119
(4) Consent of the individual concerned 119
(5) Highlights of the APICNUIP....120
c) Protection under sector-specific laws 121

d) Self-regulatory initiative: the Privacy mark labeling *121*

e) Projects for reform *121*

7. TAIWAN 122

a) Privacy and data protection under the Constitution and the Codes *122*

b) Main piece of legislation: the Computer-processed Personal Data Protection Act *122*

(1) General remarks 122

(2) Limited Scope 122

(3) Definition of "personal data" 122

(4) Consent of the individual concerned 123

(5) Other highlights of the CPPDPA 123

(6) Legislative reform under way 124

C. COUNTRIES THAT ARE IN THE PROCESS OF DRAFTING PRIVACY LEGISLATION 124

1. CHINA 124

a) Constitutional protection *124*

b) Protection under sector-specific laws *124*

c) Drafting of a comprehensive data protection law *125*

2. MALAYSIA 126

a) Constitutional protection *126*

b) Final stages of the drafting of the Personal Data Protection Bill *126*

c) Protection under sector-specific laws *126*

3. THE PHILIPPINES 127

a) Constitutional protection *127*

b) Drafting of a comprehensive law on data protection *127*

4. THAILAND 128

a) Constitutional protection *128*

b) Drafting of a comprehensive law on data protection *128*

c) Protection under sector-specific laws *128*

D. COUNTRIES THAT ONLY HAVE PRIVACY PROVISIONS IN SECTOR-SPECIFIC LAWS 129

1. INDONESIA 129

a) Constitutional protection *129*

b) Protection under sector-specific law *129*
2. SINGAPORE 130
a) Constitutional protection *130*
b) Self-Regulation: Model Data Protection Code *130*
c) Protection under sector-specific laws and at common law *130*
3. VANUATU 131
4. VIETNAM 131
a) Constitutional protection *131*
b) Protection under the Civil Code *131*
c) Protection under sector-specific laws *132*
d) Sanctions *133*
E. COUNTRIES THAT DO NOT HAVE PRIVACY LEGISLATION 133
F. Outside the Asia-Pacific Region : The Case of India 134
1. Constitutional protection 134
2. Main piece of legislation: the Personal Data Protection Bill 134
(1) General remarks 134
(2) Definition of "personal data" 134
(3) Highlights of the Bill 135
3. Protection under sector-specific laws 135
CASES IN THE NEWS AND OTHER CASES OF INTEREST 136
I. CANADA 136
A. Facebook Contravenes PIPEDA 136
B. Loss Of A File Containing Customer Information Of Talvest Mutual Funds (CIBC Subsidiary) 136
C. Large Scale Credit Card Fraud At TJX Companies Inc., Operator Of Winners Merchant International L.P. 137
II. INTERNATIONAL 137
A. Google Street View Raises Privacy Concerns 137
B. Indian Government Demands Research in Motion to Provide Security Agencies With a Way Around the Encryption Used by the BlackBerry Network 138
C. US-EU: SWIFT and the Terrorist Tracking Finance Programme 138

INTRODUCTORY REMARKS

Canada's federal personal information protection regime in the private sector is mainly governed by the *Personal Information Protection and Electronic Documents Act* ("**PIPEDA**").[1] Some provinces have also enacted personal information protection laws, which are substantially similar to the federal legislation (Alberta, British Columbia, Québec; Ontario has enacted privacy legislation but only with regard to personal health information).

Member States of the European Union ("**EU**")[2] have all adopted comprehensive data protection laws, following the enactment of *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data* ("**Directive 95/46**").[3] Directive 95/46 sets forth general principles and fundamental requirements concerning the processing of personal data. It applies to both the private and public sectors. Major European countries (France, Germany, Italy, the Netherlands, Spain, Sweden and the United Kingdom) have fairly similar data protection regimes. Nevertheless, there are some differences in the way these countries have implemented the principles and requirements set out in Directive 95/46.

Countries of the Asia-Pacific region do not have a uniform data protection regime. The *Asia-Pacific Economic Cooperation* ("**APEC**") *Privacy Framework*,[4] an international instrument that sets forth basic principles for the processing of personal information, has failed to achieve a EU-like harmonization of personal information protection laws in the APEC Member economies. The countries of the region are at very different stages of their legal, social, economic and cultural development. This is reflected in their respective privacy laws. Some countries have adopted privacy legislation (Australia, Hong Kong, Japan, Macao, New Zealand, South Korea and Taiwan), while others are in the process of drafting it (China, Malaysia, the Philippines and Thailand). Finally, there are countries that only have privacy provisions in sector-specific legislation (Indonesia, Singapore, Vanuatu, and Vietnam), and others that simply do not have any privacy laws (Brunei, Cambodia, Laos, Myanmar and the majority of the small Pacific Island countries). India, which is outside of the Asia-Pacific region, is in the final stages of the enactment of its first comprehensive law on data protection.

---

1 *Personal Information Protection and Electronic Documents Act* (2000, c. 5) http://laws.justice.gc.ca/en/ShowFullDoc/cs/P-8.6//20090714/en.

2 The Member States of the EU are: Austria, Belgium, Bulgaria, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, the United Kingdom.

3 *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:NOT.

4 *APEC Privacy Framework;* available for download at: http://www.apec.org/apec/news___media/fact_sheets/apec_privacy_framework.html.

There is a difference in privacy terminology used in Europe, Asia and Canada. In Europe, the protection of personal information is referred to as “data protection”. A distinction is made between the right to privacy and the right to data protection. In Canada, the expression “protection of personal information” is used. It is directly linked to the right of privacy. In Asia, the terminology varies greatly from one country to another.

CANADA

PRELIMINARY REMARKS

Canada has a patchwork of legislation governing the protection of personal information in the private sector both federally and provincially.

In this section, we will address the federal regime (part **I**). We will outline the legislative framework (section **A**), the rules governing the transfer of personal information to third countries (section **B**), and significant case law in the field of data protection (section **C**). We will also briefly address the provincial data protection regimes (part **II**).

I. FEDERAL PERSONAL INFORMATION PROTECTION REGIME

A. LEGISLATIVE FRAMEWORK

1. Constitutional Protection

The Supreme Court has confirmed that the right to privacy, including the right to informational privacy, deserves constitutional protection. In *R. v. Dyment*,[5] La Forest J. wrote that the right to privacy, including informational privacy, was "[g]rounded in man's physical and moral autonomy" and "essential for the well-being of the individual" (para. 17).

2. General Remarks on the Federal Personal Information Protection Regime

At the federal level, the protection of personal information in the private sector is governed by the *Personal Information Protection and Electronic Documents Act* ("**PIPEDA**"),[6] which was implemented over a three-year period beginning on January 1, 2001. The drafting of PIPEDA was inspired by the *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*.[7]

---

5 *R. v. Dyment* [1988] 2 S.C.R. 417 http://www.canlii.org/en/ca/scc/doc/1988/1988canlii10/1988canlii10.html.

6 PIPEDA, see note 1.

7 *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html. See p. 28 for an overview of the OECD Guidelines.

The body responsible for compliance with PIPEDA is the Privacy Commissioner of Canada ("**PCC**").[8]

There are also other sector-specific laws that are relevant to the protection of personal information in the private sector (e.g. the *Bank Act*[9]).

Please note that there are also federal laws regarding the protection of personal information in the public sector: the *Privacy Act*[10] and the *Access to information Act*.[11]

In this section, we will only focus on PIPEDA.

3. Purpose of PIPEDA

The purpose of Part I of PIPEDA on the Protection of Personal Information is defined at s. 3 of PIPEDA. It is :

> to establish, in an era in which technology increasingly facilitates the circulation and exchange of information, rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.

4. Scope of PIPEDA

a) Entities and Purposes Covered (s. 4)

(1) Organizations and purposes covered by PIPEDA (s. 4(1))

PIPEDA applies in respect of information either:

*Collected, used or disclosed by an organization in the course of **commercial** activities.*

---

8 Office of the Privacy Commissioner of Canada, *Welcome*: http://www.priv.gc.ca/.

9 *Bank Act*, S.C. 1991, c. 46, http://www.canlii.org/en/ca/laws/stat/sc-1991-c-46/latest/sc-1991-c-46.html.

10 *Privacy Act*, R.S.C. 1985, c. P-21, http://www.canlii.org/en/ca/laws/stat/rsc-1985-c-p-21/latest/rsc-1985-c-p-21.html.

11 *Access to Information Act*, R.S.C. 1985, c. A-1, http://www.canlii.org/en/ca/laws/stat/rsc-1985-c-a-1/latest/rsc-1985-c-a-1.html.

- "Commercial activity" means "any particular transaction, act or conduct or any regular course of conduct that is of a commercial character, including the selling, bartering or leasing of donor, membership or other fundraising lists" (s. 2(1)).

- Non-profit organizations are not automatically excluded from the scope of PIPEDA, as they may also be engaged in commercial activities in certain given situations.[12]

or

Collected, used or disclosed by an organization about one of its ***employee****, in connection with the operation of a* ***federal work, undertaking or business****.*

- "Federal work, undertaking or business" refers to "any work, undertaking or business that is within the legislative authority of Parliament" (s. 2(1)). Concrete examples of federal works, undertakings and businesses included within this definition can be found at s. 2(1).

- PIPEDA does not apply to employers of provincially regulated business. Protection of personal information of employees is left to appreciation provincial privacy legislation, although, as noted above, not all provinces have such legislation.

(2) Organizations and purposes not covered by PIPEDA (s. 4(2))

PIPEDA does not apply to:

> (a) any government institution to which the Privacy Act applies;
>
> (b) any individual in respect of personal information that the individual collects, uses or discloses for personal or domestic purposes and does not collect, use or disclose for any other purpose; or
>
> (c) any organization in respect of personal information that the organization collects, uses or discloses for journalistic, artistic or literary purposes and does not collect, use or disclose for any other purpose.

b) Territorial Scope

(1) Application where provincial legislation is substantially similar to PIPEDA

PIPEDA does not apply to the collection, use or disclosure of personal information by organizations in the course of commercial activities wholly within provinces that have enacted privacy laws declared substantially similar to PIPEDA.

---

12 PIPEDA Case Summary #2005-309: Daycare denied parent access to his personal information, http://www.priv.gc.ca/cf-dc/2005/309_20050418_e.cfm. and *Rodgers v. Calvert*, 2004 CanLII 22082 (ON S.C.) http://canlii.org/en/on/onsc/doc/2004/2004canlii22082/2004canlii22082.html.

The following Acts have been declared substantially similar to PIPEDA:

- Alberta : *Personal Information Protection Act*[13]
- British Columbia : *Personal Information Protection Act*[14]
- Québec : *An Act Respecting the Protection of Personal Information in the Private Sector*[15]
- Ontario: *Personal Health Information Protection Act*,[16] only with respect to the collection, use or disclosure of personal health information by health information custodians in Ontario.

PIPEDA nonetheless applies in Alberta, British Columbia, Quebec and Ontario when:

- the organization is a federal work, undertaking or business, or
- the personal information is disclosed outside of a province in the course of a commercial activity.

(2) Application in other provinces

PIPEDA applies to an organization's commercial activities in all other provinces. It also applies nationwide with respect to the personal information of employees of federal works, undertakings and businesses.

In the Northwest Territories, the Yukon and Nunavut, all organizations are considered federal works, undertakings or businesses. Therefore, all employee personal information is covered by PIPEDA.

(3) Application beyond Canada

PIPEDA may apply to foreign entities if:

- The foreign entity collects either receives or transmits communications to and from Canada, or discloses personal information about individuals in Canada;[17]

---

13 *Personal Information Protection Act*, S.A. 2003, c. P-6.5, http://www.canlii.org/en/ab/laws/stat/sa-2003-c-p-6.5/latest/sa-2003-c-p-6.5.html.

14 *Personal Information Protection Act*, S.B.C. 2003, c. 63, http://www.canlii.org/en/bc/laws/stat/sbc-2003-c-63/latest/sbc-2003-c-63.html.

15 *An Act respecting the Protection of personal information in the private sector*, R.S.Q. c. P-39.1, http://www.canlii.org/en/qc/laws/stat/rsq-c-p-39.1/latest/rsq-c-p-39.1.html.

16 *Personal Health Information Protection Act*, 2004, S.O. 2004, c. 3, Sch. A RSS http://www.canlii.org/en/on/laws/stat/so-2004-c-3-sch-a/latest/so-2004-c-3-sch-a.html.

- The foreign entity is engaged in a commercial activity within Canada, according to real and substantial connecting factors.[18]

The application of PIPEDA to foreign entities depends on the specific circumstances of each case.

5. Definition of "Personal Information"

a) General definition

Pursuant to s. 2(1) of PIPEDA, "personal information" refers to "information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization" (s. 2(1) PIPEDA).

An "identifiable individual" refers to a physical person, not a moral person.

b) Interpretative guidelines about what constitutes personal information:

1. Information will be about an "identifiable individual" where there is a serious possibility that an individual could be identified through the use of that information, alone or in combination with other information (*Gordon v. Canada (Health)*, 2008 FC 258 (CanLII).

2. Information need not be recorded for it to constitute personal information. It is sufficient that the information be about an identifiable individual even if the information is not in a recorded form, such as oral conversations, biological samples and real time video surveillance. While the absence of a recording may go to the issue of collection, it does not change the fact that the information is personal information (*Morgan v. Alta Flights Inc*. (2006) FCA 121, affirming (2005) FC 421).

---

17 *Lawson c. Accusearch* Inc. (C.F.), 2007 CF 125, http://www.canlii.org/en/ca/fct/doc/2007/2007fc125/2007fc125.html. Office of the Privacy Commissioner of Canada, "Leading by Example: Key Developments in the First Seven Years of the *Personal Information Protection and Electronic Documents Act* (PIPEDA)", p. 14, available for download at: http://www.priv.gc.ca/information/pub/lbe_080523_e.cfm.

18 PIPEDA Case Summary #2007-365: Responsibility of Canadian financial institutions in SWIFT's disclosure of personal information to US authorities considered, http://www.priv.gc.ca/cf-dc/2007/365_20070402_e.cfm. In this Case, the Assistant Commissioner found that SWIFT was engaged in a commercial activity within Canada based on the following connecting factors: SWIFT collected personal information from and disclosed it to Canadian banks; SWIFT charged the Canadian banks a fee for its services; 14 of SWIFT's shareholders were Canadian; one of SWIFT's directors was from a Canadian bank; the vast majority of the cross-border transfers of personal information to and from Canadian banks were transmitted by SWIFT; and SWIFT was an integral part of the Canadian financial system.

3. The same information can be personal to more than one individual, where, for example, it contains the views of one individual about another individual, or where the same information reveals something about two identifiable individuals (*Wyndowe v. Rousseau*, 2008 FCA 39 (CanLII)).

4. Information will still be personal information even if it is publicly available within the meaning of the regulations, and is exempt from applicable consent requirements (*Englander v. TELUS Communications Inc*., 2004 FCA 387 (CanLII)).

5. Subjective information about an individual may still be personal information even if it is not necessarily accurate (*Lawson v. Accusearch Inc.* 2007 FC 125).[19]

c) Examples of what constitutes "personal information" for the purposes of PIPEDA

(1) General examples

Personal information includes: Name, opinions about the individual, birth date, income, physical description, medical history, gender, religion, address, political affiliations and beliefs, education, employment, visual images such as photographs, and videotape where individuals may be identified.[20]

(2) Specific examples from case law

- Photographs of apartment units taken by a property manager for insurance purposes have been considered personal information, as they revealed information about the unit dweller's standard of living, and ensured that each photograph could be traced back to the individual living in the unit (the address was written under each photograph – individuals were then "identifiable").[21]

- Business email addresses have been held to be personal information, as they are not specifically listed in the exceptions in s. 2(1) of PIPEDA.[22] This decision, however, has

---

19 Office of the Privacy Commissioner of Canada, *Interpretations (Personal Information)*: http://www.privcom.gc.ca/leg_c/interpretations_02_e.cfm. This webpage also provides interpretative guidelines about the meaning of "personal information" in different contexts, such as the business and professional context, the employment context, the health context, the financial context, and the technological context.

20 The items of this list were taken from Office of the Privacy Commissioner of Canada, *Questions and Answers regarding the application of PIPEDA, Alberta and British Columbia's Personal Information Protection Acts*: http://www.privcom.gc.ca/fs-fi/02_05_d_26_e.cfm.

21 PIPEDA Case Summary #2006-349: Photographing of tenant's apartments without consent for insurance purposes http://www.priv.gc.ca/cf-dc/2006/349_20060824_e.cfm.

22 PIPEDA Case Summary #2005-297: Unsolicited email for marketing purposes http://www.priv.gc.ca/cf-dc/2005/297_050331_01_e.cfm. This finding by the Commissioner has been heavily criticized.

been widely criticized by jurists and it remains to be seen weither it will stand the test of time.

- Identification numbers used to refer to an employee are considered to be personal information.[23]

- IP addresses are considered personal information where they can be associated with an identifiable individual, i.e. the ISP subscriber.[24]

d) Distinction between "personal information" and "work product"

(1) Workings of the distinction

It is important to distinguish information about a person that amounts to "personal information" under PIPEDA, and information that merely represents an individual's "work product". The simple fact that information is produced in the workplace does not mean that it is not personal information under PIPEDA. Contextual elements, such as how and for what purposes the information was produced, its intended use, industry practices, must be taken into account.[25]

In *Wyndowe v. Rousseau*[26] (see summary at p. 16), the Federal Court of Appeal refused to read in an implicit exception to the term "work product" in the definition of "personal information".

(2) Examples from case law

- Sales statistics of individual telemarketers were considered to be their personal information.[27]

- The number of houses sold in one year by a named estate broker was considered to be his personal information.[28]

---

23 PIPEDA Case Summary #2003-149: Individual denied access to personal information http://www.priv.gc.ca/cf-dc/2003/cf-dc_030409_2_e.cfm.

24 PIPEDA Case Summary #2005-315: Web-centred company's safeguards and handling of access request and privacy complaint questioned http://www.priv.gc.ca/cf-dc/2005/315_20050809_03_e.cfm, PIPEDA Case Summary #2005-319: ISP's anti-spam measures questioned http://www.priv.gc.ca/cf-dc/2005/319_20051103_e.cfm. *BMG Canada Inc. v. Doe*, 2005 FCA 193 http://canlii.org/en/ca/fca/doc/2005/2005fca193/2005fca193.html at para. 37.

25 Office of the Privacy Commissioner of Canada, "Leading by Example: Key Developments in the First Seven Years of the *Personal Information Protection and Electronic Documents Act* (PIPEDA)" (2008), p. 7, see note 17.

26 *Wyndowe v. Rousseau*, 2008 FCA 39, http://canlii.org/en/ca/fca/doc/2008/2008fca39/2008fca39.html.

27 PIPEDA Case Summary #2003-220: Telemarketer objects to employer sharing her sales results with other employees http://www.priv.gc.ca/cf-dc/2003/cf-dc_030915_e.cfm.

6. Governing Principles of PIPEDA

Schedule I of PIPEDA incorporates the "Principles set out in the National Standard of Canada entitled Model Code for the Protection of Personal information, CAN/CSA-Q830-96" (the "**Principles**"). These principles are supplement to provisions of PIPEDA, although in cases of doubt it is PIPEDA that prevails. The principles are as follows (please note that only the opening paragraph was reproduced. See Schedule I of PIPEDA for more details on the application and exceptions to the Principles):

> Principle 1 — Accountability: An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.
>
> Principle 2 — Identifying Purposes: The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.
>
> Principle 3 — Consent: The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.
>
> Principle 4 — Limiting Collection: The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.
>
> Principle 5 — Limiting Use, Disclosure, and Retention: Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.
>
> Principle 6 — Accuracy: Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.
>
> Principle 7 — Safeguards: Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.
>
> Principle 8 — Openness: An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

---

28 PIPEDA Case Summary #2005-303: Real estate broker publishes names of top five sales representatives in a city http://www.priv.gc.ca/cf-dc/2005/303_20050531_e.cfm.

> Principle 9 — Individual Access : Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.
>
> Principle 10 — Challenging Compliance : An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.

7. Consent of the individual concerned

a) Requirements for consent to be valid

The PIPEDA sets out guidelines to determine whether consent is validly obtained:

- Typically, consent should be sought **at the time of the collection**. Consent for use or disclosure of personal information must be sought before the use or disclosure (Principle 4.3.1).

- For consent to be meaningful, the organization must **make a reasonable effort to ensure that the individual is informed** of the purposes for which the information will be used and disclosed (Principle 4.3.2).

- The **form of the consent** sought by the organization, as well as the **way in which an organization seeks consent** may vary depending on the circumstances, the type of information, and the reasonable expectations of the individual with regard to the subsequent use of his personal information (Principles 4.3.4 – 4.3.6). For example, an organization should seek express consent when the information is sensitive, whereas implied consent may be sufficient if the information is not so sensitive (Principle 4.3.4).

- There are **several ways by which an individual may express his consent**. For example, he may consent in writing by filling in an application form, or by checking off a box in a form. The individual may also give his consent verbally when information is collected over the phone, or at the time of the use of a product or service (Principle 4.3.7).

- Consent might not be obtained through **deception** (Principle 4.3.5).

- An organization may not make the **supply of a product or a service** conditional on the individual's consent to the collection, use, or disclosure of information beyond that required to achieve the legitimate and explicitly specified purposes (Principle 4.3.3).

- Consent may be given by an **authorized legal representative** (Principle 4.3.6).

Please note that consent may be **withdrawn** by the individual at any time with reasonable notice, subject to legal or contractual restrictions (Principle 4.3.8).

b) Circumstances where the data subject's consent is required

As a general rule, the individual must know and consent to the collection, use or disclosure of personal information. The knowledge and consent of the individual is not required if it is inappropriate in the circumstances, namely for legal, medical or security reasons (e.g. information collected for the detection and prevention of fraud or for law enforcement; the individual is a minor, seriously ill or mentally incapacitated) (Principle 4.3). Section 7 of PIPEDA also defines cases in which personal information may be collected, used or disclosed without the knowledge or consent of the individual concerned.

When personal information is to be used for a purpose different from the one for which it was collected for, the data subject must give his consent to the new purpose before information can be used for that purpose (Principle 4.2.4).

The use or disclosure of personal information for purposes other than those for which it was initially collected is only admissible if the individual has consented to it, or if the use or disclosure is required by law (Principle 4.5).

8. Highlights of the Canadian Federal Data Protection Regime (under PIPEDA)

- As previously mentioned, the protection of personal information in the private sector is governed by the Principles of Schedule I of PIPEDA. Division I of Part I on the Protection of Personal Information provides certain exceptions to the Principles. For example:
    - Personal information may be collected, used and disclosed by an organization only for **appropriate purposes**, from the standpoint of a reasonable person (s. 5(3)).
    - Their are circumstances where information may be **collected** (s. 7(1)), **used** (s. 7(2)) **or disclosed** (s. 7(3)) **without consent**.
- Before a complainant may have its **case heard by a Court**, he must file a **complaint** with the PCC, and wait for it to investigate the complaint and prepare a report (s. 11-15).
    - The Court may, in addition to any other remedies, order the organization in violation of PIPEDA to modify its practices and publish a notice of the actions taken in this regard.
    - The Court may also award damages to the complainant, including damages for humiliation suffered.
- The Commissioner may **audit** the personal information management practices of an organization if it has reasonable ground to believe that the organization contravenes to PIPEDA.

- Part 2 of PIPEDA (s. 31-51) addresses the **use of electronic alternatives** where federal laws contemplate the use of paper to record or communicate information or transactions (s. 32).

B. PERSONAL INFORMATION TRANSFERS / OUTSOURCING[29]

1. General remarks

Transfers of personal information to third parties are governed by the Principles of PIPEDA. The most salient principles in this specific context are Principle 4.1.3 on accountability, Principle 4.3 on consent, and Principle 4.8 on openness.

Please note that PIPEDA makes no distinction between domestic and international transfers of personal information. All transfers to third parties are governed by the same principles.

2. Principle 4.1.3: Accountability

Principle 4.1.3 of Schedule I to PIPEDA provides that:

> An organization is **responsible** for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a **comparable level of protection** while the information is being processed by a third party.

This principle has two main consequences for the transferring organization: a) responsibility for the personal information transferred and; b) an obligation to provide a comparable level of protection.

a) Responsibility for the personal information transferred

Transfers of personal information to third parties follow an organization-to-organization approach, based on the principle of accountability of transferring organizations.[30]

This entails that an organization will be held accountable under each individual outsourcing agreement for the information held by third party processors. While organizations are free to

---

29 This section was based on two main documents: Office of the Privacy Commissioner of Canada, "Leading by Example: Key Developments in the First Seven Years of the *Personal Information Protection and Electronic Documents Act* (PIPEDA)", p. 11-15 (see note 17) and Office of the Privacy Commissioner of Canada, "Guidelines for Processing Personal Data Across Borders" (2009): http://www.priv.gc.ca/information/guide/2009/gl_dab_090127_e.cfm.

30 This approach contrasts with the State-to-State approach of the EU, set out in Directive 95/46.

transfer personal information to organizations outside Canada, they must nevertheless ensure that the information transferred is adequately safeguarded ("comparable level of protection").

b) Obligation to provide a "comparable level of protection"

(1) Meaning of "comparable level of protection"

The expression "comparable level of protection" means that the level of protection provided by the third party must be comparable to the level of protection that the personal information would have been provided with had it not been transferred. For levels of protection to be comparable, they need not be identical across the board. A general equivalence is sufficient to meet the requirement.

(2) Assessing the "comparable level of protection"

When evaluating whether levels of protection are comparable, organizations must take into consideration all elements surrounding the transaction. For example, it is important to consider the political, economical and social situation of the country in which the information is to be transferred. The nature of the information transferred is equally important, as some information may be considered too sensitive to be transferred to another jurisdiction.

In short, organizations are expected to undertake a due diligence process that takes into account any element that might be relevant in assessing the level of risk of the transaction.

(3) Means of ensuring a "comparable level of protection"

Principle 4.1.3 provides that a comparable level of protection can be ensured through contract, or any other means. Organizations must take all reasonable steps to ensure that the personal information under its control is protected from unauthorized uses and disclosures while held by a third party. Moreover, organizations must:

> be satisfied that the third party has policies and processes in place, including training for its staff and effective security measures, to ensure that the information in its care is properly safeguarded at all times. It should also have the right to audit and inspect how the third party handles and stores the personal information, and exercise the right to audit and inspect when warranted.[31]

A question arose as to whether such safeguards were possible for transfers of personal information to the United States ("US"), given the provisions of the US Patriot Act. The Privacy Commissioner of Canada has ruled, however, that notwithstanding the Patriot Act, personal

---

31 Office of the Privacy Commissioner of Canada, "Guidelines for Processing Personal Data Across Borders" (2009), see note 29.

information transferred to the US can benefit from protection similar to that enjoyed in Canada. The US allows for disclosure, without consent, of this information for national security reasons.[32]

3. Principe 4.3: Consent

Principle 4.3 provides that "[the] knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate".

According to the case law, consent is only needed when an individual first applies for a service or product. Additional consent is not needed where the third-party processor offers services directly related to the primary purposes for which the personal information was collected.[33]

4. Principle 4.8: Openness

Organizations must be transparent about their personal information handling practices and policies. Principle 4.8 provides that an "organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information." Pursuant to this principle, organizations must inform their customers that:

- Their personal information may be processed in another jurisdiction;
- While in another jurisdiction, their information may be available to courts, law enforcement agencies and national security authorities.[34]

---

32 PIPEDA Case Summary #2005-313: Bank's notification to customers triggers PATRIOT Act concerns http://www.priv.gc.ca/cf-dc/2005/313_20051019_e.cfm.; PIPEDA Case Summary #2007-365, see note 18. For more information about this case from the US-EU angle, see p. 138.

33 Idem, see note 32.

34 This is the case when information is transferred to the United States, since the enactment of the *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001* HR 3162 RDS, 107th CONGRESS, http://epic.org/privacy/terrorism/hr3162.html.

C. SIGNIFICANT CASE LAW ON DATA PROTECTION

1. *Wyndowe v. Rousseau,* 2008 FCA 39[35]

Facts : Dr. Wyndowe, a psychiatrist, performed an independent medical examination ("**IME**") of Mr. Rousseau (the insured person) at the request of Maritime Life (the insurer). Wyndowe took notes during the IME. He later sent a formal report to Maritime Life. Maritime Life terminated Rousseau's long-term benefits because of Wyndowe's report. Rousseau requested to access the Wyndowe's formal report, as well as the notes he had taken during the IME. Maritime Life gave him access to the report, but Wyndowe refused to disclose his notes. Rousseau complained to the PCC with respect to Wyndowe's refusal to disclose the notes. The Federal Court ordered Wyndowe to give Rousseau access to his notes. Wyndowe appealed this decision.

Issue : Are the handwritten notes of a doctor, taken during an IME of an insured person performed in Ontario at the request of an insurance company, personal information under the PIPEDA ? (para. 1)

Decision: The Court ruled that:

> (…) there are in the notes information which is personal to Mr. Rousseau and information which is not, it may be said that in the end, Mr. Rousseau has a right of access to the information he gave the doctor, and to the final opinion of the doctor in the form of the report to the insurer. In accordance with Principle 4.9.1. of Schedule I to the PIPED Act, this enables Mr. Rousseau to correct any mistakes in the information he gave the doctor or which the doctor noted, as well as any mistakes in the doctor's reasoned final opinion about his medical condition. But the process of getting to that final opinion from the initial personal information of Mr. Rousseau belongs to the doctor (para. 49).

2. Commissioner's Finding: PIPEDA Case Summary #2005-313: Bank's notification to customers triggers PATRIOT Act concerns[36]

Facts: In the fall of 2004, CIBC sent a notice to its VISA customers to amend its credit cardholder agreement. CIBC informed them that it used a service provider based in the US, where their personal information would be processed. CIBC added that the customers' personal information could be accessed by US law enforcement or regulatory agencies under American law, namely the *Patriot Act*.[37]

---

35 *Wyndowe v. Rousseau*, 2008 FCA 39, see note 26.

36 PIPEDA Case Summary #2005-313, see note 32.

37 *Patriot Act,* see note 34.

Complaint: VISA customers objected to the possibility for US authorities to scrutinize their personal information. There was also a consent issue, as customers could not "opt-out" from having their data processed in the US.

Finding*:* The CIBC acted in accordance with its obligations under PIPEDA.

In accordance with Principle 4.1.3, the CIBC's contract with its US service provider ensured a comparable level of protection with regard to the handling of personal information. Moreover, the outsourcing arrangement had been approved by the Office of the Superintendent of Financial Institutions. The arrangement set out in detail the requirements regarding the safeguards, confidentiality and security of customer account information. There were also other terms related to monitoring, oversight, audit, custody and control.

In accordance with Principle 4.8, the CIBC duly notified its customers about its personal information handling practices, and that their information may be accessed by the US government or its agencies under the *Patriot Act*.

The Assistant Commissioner expressed that the real issue was the prospect of a foreign government accessing Canadians' personal information. However, neither PIPEDA nor contractual arrangements can effectively prevent the American authorities from accessing the personal information of Canadians once that information is in the US. Moreover, no contract for the transfer of personal information can override a foreign country's national law.

Furthermore, the Assistant Commissioner stated that there is a comparable legal risk that the personal information of Canadians held by any organization can be obtained by government agencies, whether through the provisions of U.S. law or Canadian law.

With regard to the issue of consent (principle 4.3), the Assistant Commissioner followed the Office's position that a company is not required to provide customers with the choice of opting out where the third-party processor provides services directly related to the primary purposes for which the personal information was collected. CIBC only needed to obtain the consent of its customers when they first applied for the service or product. CIBC was only notifying the customers that, because of the place where it is processed, their personal information could be made available to US authorities.

3. Commissioner's Finding: PIPEDA Case Summary #2007-365: Responsibility of Canadian financial institutions in SWIFT's disclosure of personal information to US authorities considered

Facts*:* In 2006, six complaints were filed with the Office of the Privacy Commissioner of Canada with regard to the mass disclosure of personal banking information by Society for Worldwide Interbank Financial Telecommunication ("**SWIFT**"), a Belgium-based service provider, to US authorities pursuant to the US legislation. Canadian banks had agreements with SWIFT for the processing of foreign-bound financial messages.

Complaint: The complainant was of the view that the Canadian banks were responsible for the personal information transferred to SWIFT, and that the exceptions to consent (art. 7(3)(c) and 7(3)(c.1) of PIPEDA) did not apply.

Finding: The Assistant Commissioner found that the Canadian banks had discharged their duties under PIPEDA. The arrangements between SWIFT and the Canadian banks met the requirements of PIPEDA by ensuring a comparable level of protection (principle 4.1.3). The customers were duly notified of the Banks' practices with regard to the handling of personal information, and of the possibility that their information could be accessed by foreign authorities (principle 4.8). Under the arrangement between SWIFT and the Canadian banks, SWIFT has absolute discretion with respect to the manner in which it handles subpoenas or other lawful processes by a court or other competent authority. Finally, the Assistant Commissioner reiterated the finding issued in Case summary #313 to the effect that a Canadian organization that outsources the processing of personal information to a US firm can not prevent it from being lawfully accessed by US authorities .

II. BRIEF OVERVIEW OF PROVINCIAL PERSONAL INFORMATION PROTECTION REGIMES

A. COMPREHENSIVE PRIVACY LAWS

Three provinces have enacted comprehensive privacy legislation in the private sector, which have all been declared substantially similar to PIPEDA:

- Alberta : *Personal Information Protection Act*[38]
- British Columbia : *Personal Information Protection Act*[39]
- Québec : *An Act Respecting the Protection of Personal Information in the Private Sector*[40]

B. HEALTH INFORMATION ACTS

Six provinces have enacted legislation governing the protection of personal health information. Among them, only the Ontario Act has been declared substantially similar to PIPEDA:

- Alberta : *Health Information Act*[41]

---

38 *Personal Information Protection Act*, see note 13.

39 *Personal Information Protection Act*, see note 14.

40 *An Act respecting the Protection of personal information in the private sector*, see note 15.

- British Columbia: *E-Health (Personal Health Information Access and Protection of Privacy) Act*[42]
- Manitoba: *Personal Health Information Act*[43]
- Newfound Land and Labrador: *Personal Health Information Act*[44]
- Ontario : *Personal Health Information Protection Act*[45]
- Saskatchewan: *Health Information Protection Act*[46]

Please note that there many sector-specific laws that include provisions dealing with the protection of personal information, notably with regard to consumer credit reporting.

C. COMMON LAW TORTS

At common law, there is no independent right to privacy, and thus, no tort of invasion of privacy *per se*. Other torts, like nuisance, trespass, defamation and breach of confidence are relied upon by courts to protect the private life of individuals. Some relationships also entail a duty of confidentiality (e.g. banker-client, accountant-client).[47]

---

41 *Health Information Act*, R.S.A. 2000, c. H-5 http://www.canlii.org/en/ab/laws/stat/rsa-2000-c-h-5/latest/rsa-2000-c-h-5.html.

42 *E-Health (Personal Health Information Access and Protection of Privacy) Act*, S.B.C. 2008, c. 38 http://www.canlii.org/en/bc/laws/stat/sbc-2008-c-38/latest/sbc-2008-c-38.html.

43 *Personal Health Information Act*, C.C.S.M. c. P33.5 http://www.canlii.org/mb/laws/sta/p-33.5/20090324/whole.html.

44 *Personal Health Information Act*, S.N.L. 2008, c. P-7.01 http://www.canlii.org/nl/laws/sta/p-7.01/20090324/whole.html.

45 *Personal Health Information Protection Act*, see note 16.

46 *Health Information Protection Act*, S.S. 1999, c. H-0.021 http://www.canlii.org/en/sk/laws/stat/ss-1999-c-h-0.021/latest/ss-1999-c-h-0.021.html.

47 William Charnetski et al, "The Personal Information Protection And Electronic Documents Act: a comprehensive guide"Aurora: Canada Law Book nic., 2001, p.16.

D. STATUTORY TORTS

Four provinces have adopted laws setting out the statutory tort of invasion of privacy. These laws make it a tort for a person to violate the privacy of another willfully and without claim of a right. This tort is actionable without proof of damage.

- British Columbia: *Privacy Act*[48]
- Saskatchewan: *Privacy Act*[49]
- Newfoundland and Labrador: *Privacy Act*[50]
- Manitoba: *Privacy Act*[51]

E. THE SPECIFIC CASE OF QUEBEC

1. Legislative framework[52]

a) Protection under the Charter of Human Rights and Freedoms

The right to private life is guaranteed under s. 5 of the *Charter of human rights and freedoms*: "[every] person has a right to respect for his private life".[53]

b) Protection under the Civil Code of Quebec (C.c.Q.)

The *Civil Code of Quebec* ("**C.c.Q.**")[54] reaffirms the right to private life, and requires the consent of the individual concerned to invade his privacy, unless authorized by law (s. 35 C.c.Q.) It also

---

48 *Privacy Act*, R.S.B.C. 1996, c. 373 http://canlii.org/en/bc/laws/stat/rsbc-1996-c-373/latest/rsbc-1996-c-373.html.

49 *Privacy Act*, R.S.S. 1978, c. P-24 http://canlii.org/en/sk/laws/stat/rss-1978-c-p-24/latest/rss-1978-c-p-24.html.

50 *Privacy Act*, R.S.N.L. 1990, c. P-22 http://canlii.org/nl/laws/sta/p-22/20090324/whole.html.

51 *Privacy Act*, C.C.S.M. c. P125 http://canlii.org/mb/laws/sta/p-125/20090324/whole.html.

52 This section was mainly based on Karl Delwaide and Antoine Aylwin, "*Learning from a Decade of Experience: Québec's Private Sector Privacy Act*" (2005), available at: http://www.priv.qc.ca/information/pub/dec_050816_e.cfm.

53 *Charter of human rights and freedoms*, R.S.Q. c. C-12, http://canlii.org/en/qc/laws/stat/rsq-c-c-12/latest/rsq-c-c-12.html.m.

54 *Civil Code of Québec* (C.C.Q.), S.Q. 1991, c. 64, http://www.canlii.org/en/qc/laws/stat/sq-1991-c-64/latest/sq-1991-c-64.html.

sets out rules for the collection of personal information, as well as the rights of the individuals concerned (see s. 36-41).

The Civil Code sets out the general regime for the protection of personal information.

c) The Act Respecting the Protection of Personal Information in the Private Sector

Québec was the first Canadian province to enact a comprehensive law on the protection of personal information in the private sector : the *Act Respecting the Protection of Personal Information in the Private Sector* (the "**Act**").[55] The Act entered into force in 1994. It is substantially similar to PIPEDA.

The Act establishes particular rules for the exercise the rights conferred by articles 35-40 of the C.c.Q (s. 1).

The body responsible for compliance with the Act is the Commission d'accès à l'information du Québec.[56]

2. Scope of the Act

a) General remarks

The Act applies to "personal information relating to other persons which a person collects, holds, uses or communicates to third persons in the course of carrying on an enterprise within the meaning of article 1525 of the [C.c.Q.]" (s. 1(1) of the Act).

b) The notion of enterprise

The notion of "enterprise" is quite broad. The carrying on of an enterprise refers to "[the] carrying on by one or more persons of an organized economic activity, whether or not it is commercial in nature, consisting of producing, administering or alienating property, or providing a service" (art. 1525(3) C.c.Q.).

This definition covers non-profit organizations, professionals, artisans and agricultural activities.[57]

---

55 *Act Respecting the Protection of Personal Information in the Private Sector*, see note 15.

56 Commission d'accès à l'information du Québec, *Welcome*: http://cai.gouv.qc.ca/index-en.html.

57 Karl Delwaide and Antoine Aylwin, "*Learning from a Decade of Experience: Québec's Private Sector Privacy Act*", p.5, see note 52.

The interpretation of "enterprise" varies depending on the legal field in which it is applied. In the context of privacy legislation, the notion of "enterprise" benefits from a wide and liberal interpretation in order to achieve the purposes of the Act.[58] (p. 6)

c) Exclusions

The Act does not apply to:

- Public bodies, to which the *Act respecting Access to documents held by public bodies and the Protection of personal information applies*, or information held on behalf of a public body (s. 3(1)).

- Journalistic, historical or genealogical data collected, held, used or communicated for the legitimate information of the public (s. 3(2)).

d) Information held by professional orders

The Act applies to personal information held by a professional order only when the information is not held for the purpose of supervising the practice of the profession (s. 108.2 of the *Professional Code*). Otherwise, the *Act respecting Access to documents held by public bodies and the Protection of personal information*[59] will apply (s. 108.1 of the *Professional Code*).

e) Territorial scope

The Act applies to every enterprise that conducts business in Québec, regardless of the location of its place of business and where the information is stored.[60]

3. Definition of "personal information"

"Personal information" under the Act refers to "any information which relates to a natural person and allows that person to be identified" (s. 2). The nature of the medium and the form in which the information is accessible does not matter. It could be either written, graphic, taped, filmed, computerized, or other (s. 1(2)).

The Act only applies to information about natural persons, not legal entities.

---

58 Karl Delwaide and Antoine Aylwin, "*Learning from a Decade of Experience: Québec's Private Sector Privacy Act*", p.6, see note 52.

59 *Act respecting Access to documents held by public bodies and the Protection of personal information*, see note 15.

60 Karl Delwaide and Antoine Aylwin, "*Learning from a Decade of Experience: Québec's Private Sector Privacy Act*", p. 7, see note 52.

4. Consent of the individual concerned

a) Requirements for consent to be valid

For consent to be valid, it must be manifest, free, enlightened and given for a specific object (s. 14 (1)). Therefore, implicit consent is not valid under the Act.[61]

The consent is only valid for the length of time necessary to fulfill the purpose for which it was requested (s. 14 (1)).

Section 15 provides that "[consent] to the communication of personal information by a third person may be given by the person concerned to the person who collects the information from the third person".

b) Circumstances where the data subject's consent is required

Information may be collected solely from the person concerned, unless the latter consents to the collection of this information from third persons, or another exception applies (s. 6).

The consent of the person concerned is necessary to continue using his personal information once the object for which the consent was obtained was achieved (s. 12).

Consent of the individual concerned is required when the person carrying on an enterprise wishes to communicate personal information to a third person, or use it for purposes that are not relevant to the object of the file (s. 13).

There are several exceptions to this principle, namely when information is disclosed to attorneys (s. 18(1)), detectives and security agencies (s. 18(4)), archival agencies (s. 18.2), authorized employees, mandataries, agents or any party to a contract for work or services, on the condition that it is needed to perform their duties (s. 20), for research purposes if authorized by the CAI (s. 21), for philanthropic or commercial prospection purposes when the information is part of a nominative list (s. 22-24). A nominative list is a list of names, telephone numbers, geographical addresses of natural persons or technological addresses where a natural person may receive communication of technological documents or information (s. 22).

5. Highlights of the Act

- The Act is governed by **four main principles**:

    1. A person carrying on an enterprise may only open a file on another person for a serious and legitimate reason, and for a specified purpose. The information gathered must be relevant to the stated objective. (art. 37 C.c.Q., s. 4 of the Act).

---

61 Karl Delwaide and Antoine Aylwin, "*Learning from a Decade of Experience: Québec's Private Sector Privacy Act*", p. 18, see note 52.

- Only information that is necessary (and not merely useful) for the purpose of the file may be collected (s. 5 of the Act).

2. Every individual must have the right to access any file containing his personal information, unless it impairs the right of third parties, or there is a serious and legitimate reason for refusing access (art. 38-39 C.c.Q., s. 37 of the Act).

3. Every individual must have the right to correct incomplete, equivocal or inaccurate information that concerns him held by another person, or have obsolete and unjustified information deleted from his file (art. 40-41 C.c.Q., s. 28 of the Act).

4. Every person carrying on an enterprise that opens a file about another person must keep confidential the personal information collected, and must not communicate to third parties any personal information collected without the individual's consent unless otherwise authorized by law (art. 37 C.c.Q., ss. 10 and 13 of the Act).

- Specific rules apply to the **access to credit reports** by a person carrying on an enterprise that has as its object the lending of money (s. 19).

- The activities of **personal information agents** are governed by additional provisions under the Act. A personal information agents is "[any] person who, on a commercial basis, personally or through a representative, establishes files on other persons and prepares and communicates to third parties credit reports bearing on the character, reputation or solvency of the persons to whom the information contained in such files relates" (s. 70 *et s*.).

- The Act contains several **penal provisions** (s. 91 *et sec.*)and fines of up to $100,000 may be imposed under the Act.

6. Transfer of personal information outside Québec

Generally speaking, transfers of personal information outside Québec may be made under circumstances similar to those under the PIPEDA. Section 17 of the Act provides that the person who communicates the information to a recipient outside Québec must take all reasonable steps to ensure:

> 1) that the information will not be used for purposes not relevant to the object of the file or communicated to third persons without the consent of the persons concerned, except in cases similar to those described in sections 18 and 23;
>
> 2) in the case of nominative lists, that the persons concerned have a valid opportunity to refuse that personal information concerning them be used for purposes of commercial or philanthropic prospection and, if need be, to have such information deleted from the list.

The person who communicates the information has a duty to refuse to transfer personal information if he considers that it will not receive the above-mentioned protection.

While Québec's Commission d'accès à l'information has not ruled on whether transfers of personal information to the US is permissible, given the US Patriot Act, one would expect a result similar to that under PIPEDA, since both the Québec legislation and PIPEDA contain similar provisions with respect to disclosure for law enforcement purposes.

7. Significant case law on the protection of personal information

a) Deschesnes c. Groupe Jean Coutu (P.J.C.) Inc[62]

Facts: M. Deschesnes filed a complaint with the CAI for an alleged violation of the Act against the Groupe P.J.C. (the "**Group**"), a Pharmacist affiliated to the Group (the "**Pharmacist**"), Bayer inc. and Diabetes Quebec (collectively referred to as the "**respondents**"). M. Deschesnes complained about the fact that the Group and the Pharmacist included his name in a list of people suffering from diabetes without obtaining his prior consent, or giving him the opportunity to refuse that the personal information contained in his pharmaceutical file be used for commercial solicitation purposes. The list in question was used to send invitations by mail for special activities about diabetes held by Bayer Inc. and Diabetes Quebec.

Issue: Were the respondents in violation of the Act ?

* The complaint against Bayer inc. and Diabetes Quebec was withdrawn by Mr. Deschesnes, as the CAI held that they were not involved in any violation of the Act.

Decision: The CAI found that the Group and the Pharmacist had acted in violation of s. 13 of the Act by communicating personal information contained in Mr. Deschesnes' pharmaceutical file (name, address and health status) without his consent for purposes irrelevant to the object of the file. The Pharmacist and the Group could only have communicated to a third party Mr. Deschesnes' personal information for commercial prospection if the information had been part of a nominative list (s. 22-24). However, only names, telephone numbers and addresses may be part of a nominative list, not health status. Therefore, the nominative list exception did not apply. The CAI also found that the Pharmacist and the Group did not take adequate security measures to ensure the protection of the personal information disclosed (s. 10).

b) Congrégation des témoins de Jéhovah d'Issoudun-Sud c. Mailly[63]

Facts: Mailly was expelled by an internal ecclesiastical tribunal from the Congregation of the Jehovah Witness of Issoudun-South (the "**Congregation**"). She requested that the Congregation

---

62 *Deschesnes c. Groupe Jean Coutu (P.J.C.) Inc* [2000] C.A.I. 216 (C.A.I.)

63 *Congrégation des témoins de Jéhovah d'Issoudun-Sud c. Mailly* [2000] C.A.I. 427, REJB 2000-20159 (C.Q.).

communicate to her certain documents regarding herself, by invoking s. 1 and 27 of the Act. The Congregation refused. Mailly filed a complaint with the CAI, which decided that the Act applied to the Congregation. The CAI ordered the Congregation to communicate certain documents to Mailly. The Congregation appealed from the CAI's decision.

Issue: Is the Congregation an "enterprise" within the meaning of art. 1525(3) C.c.Q., and therefore covered by the Act ?

Decision: The Court came to the conclusion that the Congregation was not an "enterprise" within the meaning of art. 1525 (3) C.c.Q. and therefore fell outside the scope of the Act. The Court stated that if the carrying of an enterprise always involved an organized economic activity, the opposite was not true. Though the Congregation carried an organized economic activity, it was not its main purpose. Rather, it was ancillary onto its mission to carry on religious activities.

c) Stébenne c. Assurance-vie Desjardins Laurentienne inc.[64]

Facts: Mr. Stébenne requested a copy of documents regarding himself held by Assurance-vie Desjardins ("**Desjardins**"). Desjardins gave Mr. Stébenne a copy of his disability insurance and pension fund files, but refused to provide him with the internal administrative notes and office memos concerning him. Desjardins argued that there was a serious and legitimate reason for its refusal (s. 39), namely that access would violate the freedom of expression of its employees. It also invoked that the said notes and memos were not personal information pursuant to the Act, as they were only opinions and comments made by employees. Mr. Stébenne filed a complaint with the CAI.

Issue: Whether the internal administrative notes and office memos written by the Desjardins employees in Mr. Stébenne's file constituted personal information under the Act; and whether Desjardins could deny Mr. Stébenne's request for access to his personal information.

Decision: The Court found that the notes and memos were personal information under the Act, but only those that allowed the identification of Mr. Stébenne and concerned him directly. They were part of the file, and therefore accessible to Mr. Stébenne. The Court confirmed the CAI's decision that any exception to the right of access had to be interpreted restrictively and that only the interests mentioned in s. 37-41 of the Act were to be considered serious and legitimate enough to refuse someone access to documents containing his personal information.

---

64 *Stébenne c. Assurance-vie Desjardins Laurentienne inc*., [1995] C.A.I 14, [1995] C.A.I. 416, EYB 1995-72354 (C.Q.), confirmed by *Assurance-vie Desjardins Laurentienne inc. c. Boissonnault* [1998] C.A.I. 562, J.E. 98-995 (C.S.), appeal rejected: [2002] C.A.I. 459, REJB 2001-27130 (C.A.)

EUROPE

Please note that the technical terms used in this section refer to the definitions of Directive 95/46 (personal data, data subject, processing of personal data, personal data filing system, controller, processor, third party, recipient, data subject's consent).

I. EU DATA PROTECTION REGIME

A. PRELIMINARY REMARKS

The European Union has developed a very sophisticated data protection regime with stringent standards. Directive 95/46[65] sets out the general principles with regard to the processing of personal data, which are now implemented in the national law of every EU Member State. The underlying principles of Directive 95/46 were largely based on those of international bodies, like the *Organization for Economic Cooperation and Development's* ("**OECD**") *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*,[66] and the Council of Europe's *Convention for the protection of individuals with regard to automatic processing of personal data.*[67] Other Directives were also adopted to regulate data protection in telecommunications industry.

In this section, we will address the legislative framework of the EU data protection regime (part **B**); the rules governing international data transfers (part **C**); and the major case law of the European Court of Justice (part **D**).

---

65 *Directive 95/46*, see note 3.

66 *OECD Guidelines*, see note 7.

67 *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*; for more information about the 1981 Convention, see http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=108&CM=8&DF=11/07/2009&CL=ENG.

B. LEGISLATIVE FRAMEWORK

1. 1980: *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*

a) General Remarks

On September 23, 1980, the OECD[68] issued the *Recommendations of the Council Concerning Guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data*, most commonly referred to as the *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* ("**OECD Guidelines**").[69] The OECD Guidelines were the first international initiative to create a comprehensive data protection system between and within the OECD Member Countries. Member Countries were encouraged to enact into their domestic legislation the principles governing the protection of privacy and individual liberties set forth in the OECD Guidelines.

b) Principles of the OECD Guidelines

(1) Principles of national application

The OECD Guidelines are based on eight principles of national application (art. 7-14):

1. *Collection Limitation principle:* Personal data should be obtained by lawful and fair means, with the knowledge or consent of the data subject where appropriate (art. 7);

2. *Data Quality Principle:* Personal data should be relevant for the purposes of its use, as well as accurate, complete and up-to-date to the extent necessary for those purposes (art. 8);

3. *Purpose Specification Principle:* The purposes for which personal data is collected should be specified before or at the time of the collection. Personal data can only be used for specified purposes, or for uses that are not incompatible with the specified purposes (art. 9);

4. *Use Limitation Principle:* Personal data should not be disclosed to a third party for purposes other than those specified, except with the consent of the data subject, or with the authorization of the law (art. 10);

---

68 There were 24 OECD Member Countries at the time of the adoption of the OECD Guidelines: Australia, Austria, Belgium, Canada, Denmark, Finland, France, Germany, Greece, Iceland, Ireland, Italy, Japan, Luxembourg, Netherlands, New Zealand, Norway, Portugal, Spain, Sweden, Switzerland, Turkey, United Kingdom, United States.

Since then, six countries have joined the OECD: Czech Republic, Hungary, Korea, Mexico, Poland, Slovak Republic. *Ratification of the Convention on the OECD*, http://www.oecd.org/document/58/0,3343,en_2649_201185_1889402_1_1_1_1,00.html.

69 *OECD Guidelines*, see note 7.

5. *Security Safeguards Principle:* Personal data should be adequately protected by reasonable security measures (art. 11);

6. *Openness Principle:* Information about the policies and practices pertaining to personal data should be readily available (art. 12);

7. *Individual Participation Principle:* An individual should have the right to be informed of personal data relating to him (art. 13);

8. *Accountability Principle:* Data controllers should be accountable for complying with the national measures implementing the above-mentioned principles (art. 14).

(2) Principles of international application

The OECD Guidelines also define basic principles of international application concerning the free flow of personal data and legitimate restrictions (art. 15-18). For example, a Member country should not restrict the transborder flow of personal data between itself and another Member country, except if the latter does not substantially observe the OECD Guidelines, or where the re-export of such data would go against its national privacy legislation (art. 17).

c) Impact of the OECD Guidelines and further developments

Although the OECD Guidelines are not binding, they remain very influential almost 30 years following their conception. For example, the principles set forth in the OECD Guidelines largely inspired the drafting of Directive 95/46.[70]

Since 1980, the OECD has adopted several documents of interest, based on the OECD Guidelines. For example:

- 1992: *OECD Guidelines for the Security of Information Systems*[71]
- 2002: *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*[72]
- 2007: *OECD Recommendation on Cross-Border Co-operation in the Enforcement of Laws Protecting Privacy*[73]

---

70 *Directive 95/46*, see note 3.

71 *OECD Guidelines for the Security of Information Systems*, http://www.oecd.org/document/19/0,3343,en_2649_34255_1815059_1_1_1_1,00.html.

72 *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security;* available for download at: http://www.oecd.org/document/42/0,3343,en_2649_34255_15582250_1_1_1_1,00.html.

2. 1981: *Convention for the protection of individuals with regard to automatic processing of personal data*

The *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* ("**1981 Convention**")[74] was the first binding international instrument asserting the right to the protection of personal data. It also sought to regulate international personal data transfers. The 1981 Convention was adopted by the Council of Europe (the "**Council**") on January 28, 1981, and entered into force in 1985. So far, 41 countries have ratified it.[75]

The 1981 Convention sets forth general principles governing the collection and processing of personal data. It enshrines the individual's right to know what information is stored on him, as well as the right to correct it. The 1981 Convention also prohibits the processing of sensitive personal data (data concerning racial origin, political opinions or religious or other beliefs, health, sexual life, criminal convictions) unless adequate safeguards are provided.

3. 1995: Directive 95/46: The main piece of legislation on data protection in the European Union

a) General remarks

Directive 95/46 (only referred to as the "**Directive**" in this section)[76] is the main European piece of legislation with regard to personal data protection. It was adopted on October 24, 1995 by the European Parliament and the Council.

The Directive aims at implementing a harmonized legal framework for the protection of personal data within the EU. Its principles are largely inspired by those of the OECD Guidelines and the 1981 Convention. The Directive promotes a comprehensive approach to data protection, by opposition to the sectoral approach adopted by the US. It applies to both private and public bodies.

---

73 *OECD Recommendation on Cross-Border Co-operation in the Enforcement of Laws Protecting Privacy*; available for download at: http://www.oecd.org/document/60/0,3343,en_2649_34255_38771516_1_1_1_1,00.html.

74 *1981 Convention*, see note 67.

75 The 41 ratifying countries of the 1981 Convention are: Albania, Andorra, Austria, Belgium, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Georgia, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Moldova, Monaco, Montenegro, Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, the former Yugoslav Republic of Macedonia, United Kingdom.

76 *Directive 95/46*, see note 3.

The Directive sets forth the minimum protections that national law statutes must provide, as well as guidelines for their implementation. The Directive prescribes the result to be archived but leans the means of archiving the results. It is up to the Member States.[77] The Directive expressly provides that Member States shall define for themselves the precise conditions under which the processing of data protection will be considered lawful (art. 5).

All of the 27 Member States of the EU,[78] as well as the three European Free Trade Association ("**EFTA**") countries[79] which are part of the European Economic Area ("**EEA**") have implemented the Directive into their national law pursuant to article 32 of the Directive.

b) Purpose of the Directive (art. 1)

The Directive is meant to prevent Member States from restricting the free flow of information between them, while protecting the fundamental rights and freedoms of natural persons (in particular their right to privacy with respect to the processing of personal data).

c) Definition of "personal data" (art. 2(a))

For the purposes of the Directive, "personal data" means "any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity" (art. 2). Date "controller" means: "the natural or legal person, public authority, agency or another body which, alone or jointly with others, determines the purposes and means of the processing of personal date (…)"

In *Opinion N° 4/2007 on the concept of personal data*,[80] the Article 29 Data Protection Working Party (the "**Working Party**") specifies what is meant by "personal data" under the Directive. It also provides detailed examples taken from the practice of the Member States. The Working Party breaks down the definition of "personal data" into four elements, and comes to the following conclusions:

---

77 Kennedy, C., *The Business Privacy Law Handbook*, (Boston: Artech House, 2008), p. 101.

78 For a list of the 27 EU Member States, see note 2.

79 The three EFTA countries that have implemented the Directive are Iceland, Liechtenstein and Norway.

80 Working Party, *Opinion N° 4/2007 on the concept of personal data, 20 June 2007*, WP 136; available for download at http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/index_en.htm. See this document for a series of detailed examples on what is considered personal data.

(1) "**Any information**": This element calls for a broad interpretation of the concept. It refers to both:

- the nature of the information, which can be objective (statement of fact) or subjective (opinion or assessment);
- the technical format (e.g. alphabetical, numerical, graphical, photographical or acoustic) in which the information is presented.

(2) "**Relating to**": This element determines the scope of the concept. The information does not need to focus directly on the person. Information is said to relate to a person when at least one of the following links exist:

- "Content": The information is *about* a person, regardless of the purpose of the data controller or the impact of the information on the person. This should be evaluated with regard to all the circumstances of the case.
    - E.g. Results of a medical analysis relate to the patient; information contained in a company's folder under the name of a person relates to this person.
- "Purpose": The information is likely to be used by the data controller for the purpose of evaluating, treating in a certain way or influencing the status or behavior of a person.
- "Result": The use of the data is likely to have an impact on a person's rights and interests, with regard to all of the surrounding circumstances.

(3) "**Identified or identifiable**":

- A person is identified when: he is distinguished from the members of a group of persons.
- A person is identifiable when: it is possible to identify/single out the person directly or indirectly (by a unique combination of identifiers). All reasonable means available to the data controller or another person to identify the person should be taken into account.

(4) "**Natural person**": The data subject must be a living individual. However, information about dead persons, unborn children or legal entities may be considered personal data if it "relates to" a natural person, and indirectly reveals information about that person. Moreover, nothing prevents Member States from extending the scope of the Directive to dead persons, unborn children or legal entities.

d) Data subject's consent

(1) Definition of "the data subject's consent"

The Directive defines "the data subject's consent" as "any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed" (art. 2(h)).

(2) Circumstances where the data subject's consent is required

As a general rule, for data processing to be legitimate, the data subject must give unambiguous consent prior to the processing, unless an exception applies (art. 7).

Sensitive data may only be processed if the data subject has given his explicit consent to it, or if another exception applies (art. 8 (2)(a)).

An international data transfer to a country that does not ensure an adequate level of protection may take place if the data subject has given his unambiguous consent to the proposed transfer, or if another exception applies (art. 26 (1)(a)). (see below, section i))

e) Scope – subject matter (art. 3)

The Directive **applies** to:

- The processing of personal data wholly or partly by automatic means, and to
- The processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system.

The Directive **does not apply** to the processing of personal data:

- In the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning:
  - Public security;
  - Defense;
  - State security (including the economic well-being of the State when the processing operation relates to State security matters);
  - the activities of the State in areas of criminal law.
- By a natural person in the course of a purely personal or household activity.

f) Scope – territorial (art. 4)

The National provisions adopted by the Member States pursuant to the Directive apply where:

- The processing is carried out in the context of the activities of an establishment of the controller in the territory of the Member State;
    - *When the same controller is established on the territory of several Member States,* in such case, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable;
- The controller is not established on the Member State's territory, but in a place where its national law applies by virtue of international public law;
- The controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.
    - *In this latter case, the controller must designate a representative established in the territory of the Member State without prejudice to legal action which could be initiated against the controler*.

g) General Rules On The Lawfulness Of The Processing Of Personal Data

(1) Principles relating to data quality (article 6)

General principles related to the quality of data must be followed:

- Processing must be fair and lawful;
- The collection has to be done for specified, explicit and legitimate purposes, and not further processed in a way that is incompatible with those purposes (*there may be exceptions for processing of data for historical, statistical or scientific purposes if appropriately safeguarded*);
- The data must be adequate, relevant and not excessive in relation to the purposes for which they were collected or processed;
- The data must be accurate and kept up to date where necessary. Accordingly, every reasonable step must be taken to erase or rectify inaccurate or incomplete data.
- The data must be kept in a form which permits identification of data subjects no longer than necessary (*Member States may lay down safeguards for personal data stored longer for historical, statistical or scientific use*).

(2) Criteria for making data processing legitimate (art. 7)

The process must be legitimate. This means that the data subject must have given his consent unambiguously, or the processing must be necessary for one of the following reasons:

- The performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract;
- Compliance with a legal obligation to which the controller is subject;
- In order to protect the vital interests of the data subject;
- The performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or
- The purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under art. 1(1).

**** The data subject has a right to object on a legitimate ground to the processing of personal data related to the individual concerned in, at least, the two last instances (art. 14(a)).*

(3) Processing of sensitive data (art. 8)

The processing of sensitive data is prohibited, unless it falls in one of the exceptions specified in the Directive and strict safeguards are provided.

- The standard types of sensitive data are personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, or concerning health or sex life.

(4) Rights of the data subjects

The data subject must benefit from the following rights (which also correspond to obligations for the data controller):

- Article 10: Right to be informed of, at least,
  - The *identity of the controller*
  - The *purpose of the processing* for which the data are intended

- Any *further information* (e.g. the recipients or categories of recipients of the data whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply, the existence of the right of access to and the right to rectify the data concerning him)

- Article 12: Right of access to the personal data relating to the individual concerned, which includes:
  - The right to be informed by the data controller about the circumstances surrounding the processing of the personal data relating to the individual;
  - The right to obtain appropriate rectification, erasure or blocking of data which are unlawfully processed (*in particular, if it is inaccurate or incomplete*);
  - The right to obtain notification of modifications made under the previous item to third parties to whom the data have been disclosed, unless it involves an unreasonable effort.
    - *This right may be restricted when data are processed solely for scientific purposes or are kept in personal form for a period which does not exceed the period necessary for the sole purpose of creating statistics. This restriction may only apply where there is clearly no risk of breaching the privacy of the data subject. (art. 13 (2))*

- Article 14: Right to object to the processing of personal data related to the individual:
  - If the individual has not consented to the processing of personal data, but the data could nevertheless be processed because of the exceptions related to public interest or legitimate purpose (art. 7).
    - Member States can choose to expand the right to object to more exceptions.
  - If the controller anticipates that the personal data will be processed or disclosed to third parties for the purposes of direct marketing.

- Article 15: Right not to be subject to a decision based solely on automated processing of data:
  - When the decision produces legal effects concerning him or significantly affects the individual; *and*
  - When the processing of data is intended to evaluate certain personal aspects relating to the individual, such as his/her performance at work, creditworthiness, reliability, conduct, etc.
  - *Except in circumstances specified by law where there are sufficient safeguards. (art. 15 (2) (b))*

- Article 23: Right to be compensated if damages are suffered as a result of unlawful processing.

(5) Other obligations of the data controller

The data controller must also uphold the following duties:

- Ensure the confidentiality and security of personal data processing (art. 16-17)
- Notify the national supervisory authority before carrying out in whole or in part an automatic processing operation or set of such operations intended to serve a single purpose or several related purposes (art. 18-19)
    - *Member States may exempt the data controller from its duty to notify, or simplify the procedure in specific circumstances, notably if an independent Personal Data Representative is appointed*.

(6) Additional requirements for data processing to be lawful

The data protection system should provide for:

- Prior checking by the supervisory authority (as established by each Member State following art. 28)of processing operations likely to present specific risks to the rights and freedoms of data subjects (art. 20).
- Publicity of processing operations in a register kept by the supervisory authority pursuant to the data controller's duty of notification, except under certain circumstances (art. 21).

(7) Exemptions and limitations

- The processing of personal data carried out solely for journalistic purposes or for the purpose of artistic or literary expression must benefit from exemptions and derogations in order to harmonize the right to privacy with the freedom of expression (art. 9).
- The scope of certain obligations and rights may be restricted when it is necessary to safeguard (art. 13):
    - National security;
    - Defense;

- Public security;
- The prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;
- An important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters;
- A monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e);
- The protection of the data subject or of the rights and freedoms of others.

h) Judicial remedies, liability and sanctions (art. 22-24)

Remedies (art. 22): Member States shall grant every person a right to a judicial remedy for any breach of the rights guaranteed to the individual by the national law applicable to the processing in question.

- The remedy should be sought before the supervisory authority, prior to referral to the judicial authority.

Liability (art. 23): Any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive is entitled to receive compensation from the controller for the damage suffered.

- *Unless* the controller proves that he/she is not responsible for the event giving rise to the damage.

Sanctions (art. 24): Member States must lay down sanctions for infringement of the national protection adopted pursuant to the Directive and adopt measures to ensure the full implementation of the provisions of the Directive.

i) Data transfers to third countries (art. 25-26)[81]

Article 25 provides that international transfers of personal data from the EU/EEA to a third country may only take place if the third country ensures an adequate level of protection. Article 26 sets out exceptions under which an international data transfer to a third country could be allowed, even if this third country does not ensure an adequate level of protection:

---

81 For more information about international data transfers, see section of B of this part entitled “International Data Transfers (To Third Countries)”, at p. 43.

"**Article 26 Derogations**

By way of derogation from Article 25 and save where otherwise provided by domestic law governing particular cases, Member States shall provide that a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2) may take place on condition that:
(a) the data subject has given his consent unambiguously to the proposed transfer; or
(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request; or
(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or
(d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or
(e) the transfer is necessary in order to protect the vital interests of the data subject; or
(f) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation" are fulfilled in the particular case.

Without prejudice to paragraph 1, a Member State may authorize a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2), 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.

The Member State shall inform the Commission and the other Member States of the authorizations it grants pursuant to paragraph 2.
If a Member State or the Commission objects on justified grounds involving the protection of the privacy and fundamental rights and freedoms of individuals, the Commission shall take appropriate measures in accordance with the procedure laid down in Article 31 (2).
Member States shall take the necessary to comply with the Com mission's decision.

Where the Commission decides, in accordance with the procedure referred to in Article 31 (2), that certain standard contractual clauses offer sufficient safeguards as required by paragraph 2, Member States shall take the necessary measures to comply with the Commission's decision."

j) Codes of conduct (art. 27)

The drawing up of codes of conduct in specific sectors is encouraged under the Directive.

k) Supervisory authority (art. 28)

Every Member State must create or entrust an existing public authority with the responsibility for monitoring the application of the national provisions adopted pursuant to the Directive. The supervisory authority must carry out its functions independently.

Powers: The supervisory authority is endowed with investigative powers, effective powers of intervention, and the power to engage in legal proceedings where the national provisions adopted pursuant to the Directive are violated.

Duties:

- Duty to hear claims concerning the protection of rights and freedoms with regard to the processing of personal data.
- Duty to draw up a report regularly and make it public.
- Duty to cooperate with other supervisory authorities to the extent necessary for the performance of their duties, in particular by exchanging all useful information
- Duty of professional secrecy with regard to confidential information to which they have access (*even after employment, for the members and staff of supervisory authority*). (art. 28 (71))

l) Working Party (art. 29-30)

The Directive creates the Working Party, an independent advisory entity composed of a representative of the supervisory authority or authorities designated by each Member State and of a representative of the authority or authorities established for the Community institutions and bodies, and of a representative of the European Commission (art. 29).

Notably, the Working Party examines any question covering the application of the national measures adopted pursuant to the Directive. It also gives opinions and makes recommendations in this regard. Moreover, the Working Party draws up an annual report on the situation of the protection of natural persons in connection with the processing of personal data in the Community and in third countries. This report is made public, and transmitted to the European Commission, the European Parliament and the Council (art. 30).

4. Directives 2002/58 and 2006/24: Specific Directives in the telecommunications sector

a) Directive 2002/58

On July 12, 2002, the European Parliament and the Council adopted *Directive 2002/58 of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)* ("**Directive 2002/58**").[82] This Directive repealed and replaced *Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector* ("**Directive 97/66**").[83] Directive 97/66 was the first Directive to translate the principles set out in Directive 95/46 into specific rules for the telecommunications sector.

Directive 2002/58 is part of the "Telecoms Package," a legislative framework intended to unify the Member States' laws in the telecommunications sector. This Directive complements and particularizes Directive 95/46.

Directive 2002/58 addresses specific issues related to the right of privacy in the context of the development of new technologies, such as the Internet and electronic messaging services. It applies to the processing of personal data in connection with the provision of publicly available electronic communications services.

The highlight of Directive 2002/58 is the introduction of an opt-in approach to unsolicited commercial electronic communications (i.e. spam). Pursuant to art. 13, subscribers must have previously given their consent before unsolicited messages (e.g. emails or SMS text messages) can be sent to them.[84]

b) Directive 2006/24

On March 2006, the European Parliament and the Council adopted *Directive 2006/24 of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or*

---

82 *Directive 2002/58 of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications),* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:NOT

83 *Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector*, http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31997L0066&model=guichett.

84 Europe – Summaries of EU Legislation, *Data protection in the electronic communications sector*, http://europe.eu/legislation_summaries/internal_market/single_market_services/124120_eu_htm.

processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58 ("**Directive 2006/24**").[85]

Directive 2006/24 harmonizes the Member States' provisions concerning the obligations of providers of publicly available electronic communications services or of public communications networks with respect to the retention of certain data which is generated or processed by them. Its purpose is to ensure that the data is available for the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law (art. 1(1)).

Directive 2006/24 sets out the obligation to retain data, the categories of data to be retained, the periods of retention, and storage requirements for retained data.

5. 2000: *Charter of Fundamental Rights of the European Union*

a) General remarks and relevant provisions

Following a recommendation by the Article 29 Data Protection Working Party,[86] the *Charter of Fundamental Rights of the European Union*[87] ("**Charter**"), proclaimed in 2000, protects the fundamental right to data protection:

> **Article 8 (Protection of personal data)**
>
> 1. Everyone has the right to the protection of personal data concerning him or her.
>
> 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
>
> 3. Compliance with these rules shall be subject to control by an independent authority.

---

85 *Directive 2006/24 of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58,* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:EN:NOT.

86 Working Party, *Recommendation 4/99 on the inclusion of the fundamental right to data protection in the European catalogue of fundamental rights,* 7 September 1999, WP 26; available for download at http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/1999_en.htm.

87 *Charter of Fundamental Rights of the European Union;* available for download at: http://ec.europa.eu/justice_home/unit/charte/index_en.html.

The Charter also protects private and family life:

> **Article 7 (Respect for private and family life)**
>
> Everyone has the right to respect for his or her private and family life, home and communications.

b) Legal status of the Charter

To this date, the Charter is without legal effect. The Charter was first introduced as a part of the *Treaty establishing a Constitution for Europe* ("**TCE**")[88] in 2005. The TCE never came into force because French and Dutch voters rejected it by referendum. The Charter was later introduced by reference in the *Treaty of Lisbon*[89] in 2007. This Treaty never came into force as it was rejected in Ireland by way of a referendum. Negotiations and modifications to the *Treaty of Lisbon* have been made since then, and the Irish government will hold a second referendum on October 2, 2009. If the referendum is successful, the *Treaty of Lisbon* will enter into force. The rights, freedoms and principles set forth in the Charter will then take full legal effect and be binding on EU institutions and the Member States when implementing EU law.

C. INTERNATIONAL DATA TRANSFERS (TO THIRD COUNTRIES)

1. Definition of international data transfer

An international data transfer refers to "the act of sending or transmitting personal data from one country to another, for instance by sending paper or electronic documents containing personal data by post or email. [It also includes] cases where a controller takes action in order to make personal data available to a third party located in a third country".[90] However, the simple fact of uploading personal data via the internet is not an international data transfer just because the personal information is thereby made available to individuals in third countries.

The expression "third countries" refers to countries that are not members of the EU/EEA.

2. Requirements for an international data transfer to be lawful (art. 25 of Directive 95/46)

---

88 *Treaty establishing a Constitution for Europe*, http://eur-lex.europa.eu/JOHtml.do?uri=OJ:C:2004:310:SOM:en:HTML.

89 *Treaty of Lisbon*, http://eur-lex.europa.eu/JOHtml.do?uri=OJ:C:2007:306:SOM:EN:HTML.

90 European Commission, "Frequently asked questions relating to transfers of personal data from the EU/EEA to third countries", p. 18; available for download under the heading "European Commission FAQ": http://www.datainspektionen.se/in-english/in-focus-transfer-of-personal-data/.

- The collection and processing of personal data must be lawful (in accordance with the national data protection laws applicable to the data controller).

- The third country must ensure an adequate level of protection (art. 25(1)), or a rule of derogation has to be satisfied (art. 26).

- Depending on the Member State, data controllers might have to inform and/or obtain the authorization of the data subject or the national supervisory authority prior to the transfer.

3. Assessment of the adequacy of the level of protection ensured by a third country

a) Entities entitled to make such an assessment

The Member State or the European Commission may assess the adequacy of the level of protection ensured by a third country. The decisions of the Commission regarding the level of adequacy of a third country are binding upon the Member States.

The Member States and the European Commission shall inform each other of the countries that do not ensure an adequate level of protection (art. 25(3) of Directive 95/46).

b) Elements to consider

The adequacy of the level of protection shall be assessed in light of the circumstances surrounding the transfer. Article 25(2) provides elements that should be given special attention in that regard: nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures that are complied with in that country.

In *Working Document: Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive*,[91] the Working Party gave additional guidance on the elements to consider when assessing the adequacy of a third country's level of protection. The minimum requirements for protection to be considered adequate are a set of core content principles, and procedural/enforcement requirements.

---

91 Working Party, *Working Document: Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive,* 24 July 1998, WP 12; available for download at: http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/index_en.htm#general_issues

(1) Core content principles

To be considered adequate, a data protection system should at least reflect the core principles of Directive 95/46. These principles are:

1) **the purpose limitation principle** - data should be processed for a specific purpose and subsequently used or further communicated only insofar as this is not incompatible with the purpose of the transfer. The only exemptions to this rule would be those necessary in a democratic society on one of the grounds listed in Article 13 of the directive.

2) **the data quality and proportionality principle -** data should be accurate and, where necessary, kept up to date. The data should be adequate, relevant and not excessive in relation to the purposes for which they are transferred or further processed.

3) **the transparency principle -** individuals should be provided with information as to the purpose of the processing and the identity of the data controller in the third country, and other information insofar as this is necessary to ensure fairness. The only exemptions permitted should be in line with Articles 11(2) and 13 of the directive.

4) **the security principle -** technical and organisational security measures should be taken by the data controller that are appropriate to the risks presented by the processing. Any person acting under the authority of the data controller, including a processor, must not process data except on instructions from the controller.

5) **the rights of access, rectification and opposition -** the data subject should have a right to obtain a copy of all data relating to him/her that are processed, and a right to rectification of those data where they are shown to be inaccurate. In certain situations he/she should also be able to object to the processing of the data relating to him/her. The only exemptions to these rights should be in line with Article 13 of the directive.

6) restrictions on onward transfers - further transfers of the personal data by the recipient of the original data transfer should be permitted only where the second recipient (i.e. the recipient of the onward transfer) is also subject to rules affording an adequate level of protection. The only exceptions permitted should be in line with Article 26(1) of the directive.

Examples of additional principles to be applied to specific types of processing are:

1) **sensitive data -** where 'sensitive' categories of data are involved (racial or ethnic origin, political opinion, religious or philosophical belief, or trade union membership, data concerning health and sex life and data relating to offences, criminal convictions or security measures), additional safeguards should be in place, such as a

requirement that the data subject gives his/her explicit consent for the processing.

2) **direct marketing -** where data are transferred for the purposes of direct marketing, the data subject should be able to 'opt-out' from having his/her data used for such purposes at any stage.

3) **automated individual decision -** where the purpose of the transfer is the taking of an automated decision in the sense of Article 15 of the directive, the individual should have the right to know the logic involved in this decision, and other measures should be taken to safeguard the individual's legitimate interest.[92]

(2) Procedural/enforcement requirements

In order to meet the adequacy requirement of the European Commission, a data system must also provide a means for enforcing the core principles. In that regard, it should:

- Deliver a good level of compliance: Data controllers should be aware of their obligations, and the means of exercising them. Other measures may be taken, such as effective and dissuasive sanctions, systems of direct verification by authorities, auditors or independent data protection officials.

- Provide support and help individual data subjects in the exercise of their rights: For example, there should be an institutional mechanism allowing for complaints and independent investigations. In all cases, the data subject must be able to enforce his right quickly, effectively and without prohibitive cost.

- Provide appropriate redress to the injured data subject: An independent adjudication or arbitration system must exist in order to allow compensation and impose sanctions.[93]

c) Third countries that have been considered to provide an adequate level of protection by the European Commission

The European Commission has made an adequacy finding in 7 cases:

- Switzerland (July 2000),

- Canada, for personal data subject to PIPEDA (December 2001),

---

92 Working Party, *Working Document: Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive*, p. 6-7; see note 91.

93 Working Party, *Working Document: Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive*, p. 7, see note 91.

- Argentina (June 2003);
- the Bailiwick of Guernsey (November 2003);
- the Isle of Man (April 2004);
- the US Department of Commerce's Safe Harbor Privacy Principles of the US Department of Commerce (July 2000); and
- the Bailiwick of Jersey (2008).[94]

Several countries are currently changing their data protection laws with a clear view to obtain an adequacy finding, such as Australia, Hong Kong, Japan, China, New Zealand, the Philippines and several Latin American countries (Chile, Columbia, Mexico, Uruguay).[95]

4. Circumstances under which personal data can be transferred to a country that does not provide an adequate level of protection (art. 26 Directive 95/46)[96]

Personal data may nevertheless be transferred to a third country which does not ensure an adequate level of protection if one of the rules of derogation is satisfied. The transfer must either fall within one of the 6 exceptions listed in art. 26(1), or be adequately safeguarded by the data controller (art. 26(2)).

(1) The transfer falls within one of the *6 exceptions* listed in art. 26(1)

(1) the data subject has given his consent unambiguously to the proposed transfer;

(2) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request;

(3) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party;

---

94 Data Protection – European Commission, *Commission decisions on the adequacy of the protection of personal data in third countries*: http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm

95 Michael D. Birnhack, "The EU Data Protection Directive: An engine of global regime" (2008) 24 Computer Law & Security Report 508 at pp. 515-517.

96 For more information about derogations, see European Commission, "Frequently asked questions relating to transfers of personal data from the EU/EEA to third countries", p. 48-54, see note 90.

(4) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims;

(5) the transfer is necessary in order to protect the vital interests of the data subject; or

(6) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.

(2) "The data controller *adduces adequate safeguards* with respect to the protection of privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights" (art. 26(2))

The safeguards are considered adequate when:

(a) The contract between the data controller and the data importer contains a EU-approved standard contractual clause (art. 26(4)).[97]

(b) The national supervisory authority of the data controller's Member State has approved the transfer (e.g. it decided that the self-drafted contract clauses were adequate).

(c) The data controller and data importer are entities of the same multinational corporation, which has adopted binding corporate rules.[98]

When more than one means is available to ensure that the transfer is lawful, the solution ensuring the highest level of protection should prevail. For example, if a transfer can either be performed by obtaining express consent or by using a standard contractual clause, the latter solution should prevail.[99]

5. Standard Contractual Clauses ("SCCs") (art. 26(4) of Directive 95/46)[100]

---

97 For more information about standard contractual clauses, see p. 48.

98 For more information about Binding Corporate Rules, see p. 50.

99 European Commission, "Frequently asked questions relating to transfers of personal data from the EU/EEA to third countries", p. 22, see note 90.

100 For more information about Standard Contractual clauses, see Data Protection – European Commission, *Model Contracts for the transfer of personal data to third countries:* http://ec.europa.eu/justice_home/fsj/privacy/modelcontracts/index_en.htm. See also the documents adopted by the Article 29 Working Party, namely: Working Party, *Opinion 3/2009 on the Draft Commission Decision on standard contractual clauses for the transfer of personal data to processors established in*

a) Definition and purpose of SCCs

SCCs can be defined as:

> (…) contractual clauses that include obligations for personal data controllers who wish to transfer data to third countries, as well as obligations for those controllers or personal data processors who receive the data. The clauses also regulate other aspects in connection with the transfer, such as the data subjects' rights and dispute resolution. The contractual clauses aim at providing adequate safeguards for the protection of individuals' rights when personal data is transferred to countries without an adequate level of protection.[101]

The European Commission has the power to decide that a SCC provides adequate safeguards within the meaning of art. 26(2). SCCs are based on the same principles as those of the Directive 95/46.[102]

b) Types of SCCs

There are three sets of SCCs:

- Sets I and II apply to transfers from EU/EEA data controllers to *controllers* in third countries.
- Set III applies to transfers from EU/EEA data controllers to *processors* in third countries

c) Possibility for the parties to amend a SCC

Parties may supplement a SCC as long as they do not contradict it or impair the fundamental rights of the data subjects. However, if they wish to modify it, the national data protection authority must approve the modified clause prior to the transfer, pursuant to art. 26(2) of Directive 95/46. This is the logical conclusion, as the clause used is no longer "standard".[103]

---

third countries, under Directive 95/46/EC (data controller to data processor), 5 March 2009, WP 161, and Working Party, *Opinion 8/2003 on the draft standard contractual clauses submitted by a group of business assocations,* 17 December 2003, WP 84; available for download at http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/index_en.htm. See also European Commission, "Frequently asked questions relating to transfers of personal data from the EU/EEA to third countries", p. 23-38, see note 90.

101 Datainspektionen, *What are standard contractual clauses?*: http://www.datainspektionen.se/in-english/in-focus-transfer-of-personal-data/#12.

102 The Principles of Directive 95/46 are listed at p. 45 (core content principles) and p. 46 (procedural / enforcement requirements).

103 European Commission, "Frequently asked questions relating to transfers of personal data from the EU/EEA to third countries", p.28, see note 90.

d) Effect of the SCC

The introduction of a SCC in an international data transfer contract makes lawful a transfer to a third country that otherwise would not ensure a sufficient level of protection. It also prevents the national supervisory authority from blocking such a transfer, except in exceptional circumstances.[104]

6. Binding Corporate Rules ("BCRs")[105]

a) Definition of BCRs

BCRs are defined as a:

> (…) code of practice based on European data protection standards, which multinational organizations draw up and follow voluntarily to ensure adequate safeguards for transfers or categories of transfers of personal data between companies that are part of a same corporate group and that are bound by these corporate rules.[106]

b) Scope of BCRs

BCRs apply to data transfers within a corporate group world-wide. They do not cover transfers to an external entity. Such transfers remain possible if the requirements outlined in art. 25 and 26 of Directive 95/46 are met.

BCRs must apply "generally throughout the corporate group, irrespective of the place of establishment of the companies involved in transfers of personal data or the nationality of the individuals whose personal data is being processed or any other criteria or consideration."[107]

---

104 For a list of the circumstances under which a national data protection authority may block a transfer involving a SCC, see European Commission, "Standard contractual clauses for the transfer of personal data to third countries - Frequently asked questions" (2005): http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/05/3&format=HTML&aged=1&language=EN&guiLanguage=fr.

105 For more information about Binding Corporate Rules, see the documents adopted by the Working Party on this matter, namely: Working Party, *Working Document on Frequently Asked Questions (FAQs) related to Binding Corporate Rules*, 24 June 2008, WP 155 rev.4; Working Party, *Working Document Setting up a framework for the structure of Binding Corporate Rules*, 24 June 2008, WP 154; Working Party, *Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules*, 24 June 2008, WP 153; available for download at http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/index_en.htm. See also European Commission, "Frequently asked questions relating to transfers of personal data from the EU/EEA to third countries", p. 38-47, see note 90.

106 European Commission, "Frequently asked questions relating to transfers of personal data from the EU/EEA to third countries", p. 38, see note 90.

107 Working Party, *Working Document on Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers*, 3

c) Content of BCRs

The following should be included in BCRs:

- *Substantial content principles:* BCRs should provide details on how the basic principles of Directive 95/46 are to be implemented.
- *Guarantees of compliance and enforcement:* BCRs should contain provisions on the means that will be taken to guarantee a satisfactory level of compliance within the organization; audits; complaint handling; the duty to co-operate with data protection authorities; liability rules; jurisdiction rules and transparency.[108]

d) Effect of the adoption of BCRs

The adoption of BCRs allows the transfer of personal data from one entity to another within a corporate group, when the recipient entity is located in a third country that does not otherwise provide an adequate level of protection. It is important to keep in mind that each entity must comply with the applicable national data protection laws. Most of the time, the national supervisory authority for each entity must approve the BCRs.

e) Enforcement

BCRs are binding in nature. This means that, in practice, members of the corporate group and the employees within it are compelled to comply with the rules.

BCRs are also legally enforceable. Data subjects and national protection authorities should be entitled to enforce compliance with the rules by lodging a complaint or by bringing the case before a competent court.[109]

June 2003, WP 74, p. 8; available for download at: http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/index_en.htm.

108 Idem, pp.14-20

109 Idem, pp.10-13.

7. Safe Harbor Framework ("Safe Harbor")[110]

a) General information about the Safe Harbor

The Safe Harbor is recognized by the European Commission as providing an adequate level of protection, pursuant to art. 26(2) of Directive 95/46. It regulates international data transfers between the EU and the US.

The Safe Harbor was developed by the US Department of Commerce in consultation with the European Commission. It was approved by the latter in the year 2000.

The *Commission Decision of 26 July 2000 pursuant to Directive 95/46 of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce* (the "**Decision**")[111] sets out the general framework and requirements of the Safe Harbor.

b) Functioning of the Safe Harbor

The Safe Harbor creates a voluntary mechanism allowing US organizations to qualify as offering adequate protection to transfer data with a Member State of the EU. To enter the Safe Harbor, organizations must:

- Comply with the Safe Harbor's requirements*:* Organizations may join a self-regulatory program that complies with the requirements of the Safe Harbor, or develop their own. The Safe Harbor requirements to be complied with are:
  - *Seven principles* on which the Safe Harbor is based. They pertain to notice (duty of the organization to notify and provide specific information to the data subject), choice (duty of the organization to let the data subject opt out in certain cases), onward transfer (on the disclosure of information to third parties), security, data integrity, access and enforcement. These principles are in line with those of the Directive 95/46 (Annex I of the Decision).
  - *Frequently asked questions* ("**FAQs**"), that provide guidance for the implementation of the Principles issued by the Government of the United States on July 21, 2000 (Annex II of the Decision).

---

110 This section is mainly based on Export.gov, *Welcome to the Safe Harbor:* http://www.export.gov/safeharbor/index.asp, and the Working Party on the Safe Harbor, namely Working Party, *Working document on functioning of the Safe Harbor Agreement*, 2 July 2002, WP 62; available for download at: http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/index_en.htm.

111 *Commission Decision of 26 July 2000 pursuant to Directive 95/46 of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce;* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000D0520:EN:NOT.

- Publicly declare that they do so: Organizations must annually self-certify with the Department of Commerce. They must guarantee in writing that they adhere to the Safe Harbor requirements, and disclose such in their privacy policy. Since this is a self-certification mechanism, no prior authorization or confirmation from the Department of Commerce is required.

The Department of Commerce maintains a list of all the organizations that file self-certification letters. This list must be made available to the public.[112]

c) Effects of the adhesion to the Safe Harbor

Organizations that adhere to the Safe Harbor will be deemed to provide an adequate level of protection for international data transfers with the EU. Member States are bound to recognize this, and may not block data transfers involving Safe Harbor participants.

Enforcement of the Safe Harbor is ensured by the dispute resolution body designated by the organization in its privacy policies. The Government may also intervene depending on the industry sector.

D. SIGNIFICANT CASE LAW FROM THE EUROPEAN COURT OF JUSTICE ON DATA PROTECTION[113]

1. C-101/01 (judgment of November 6, 2003) / Reference for a preliminary ruling from the *Göta hovrätt (Sweden): Bodil Lindqvist*[114]

This is a major case on the interpretation of the Directive 95/46, perhaps the most referred to in the literature and subsequent case law.

Facts: Bodil Lindqvist, an employee in a church, published personal information about her colleagues on a webpage. The webpage was meant to provide useful information to the children of the parish about the church volunteers in an easy and humorous way (such as names, jobs, hobbies, family circumstances and telephone numbers). Ms. Lindqvist also disclosed that one of her colleagues had a foot injury and was on part-time medical leave. She had not asked her colleagues for their consent, nor had she informed the Datainspektionen (Swedish supervisory

---

112 For a list of the companies that have adhered to the Safe Harbor Framework, see US Department of Commerce, *Safe Harbor List*: http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list.

113 For more cases of the European Court of Justice on Data Protection, see Data Protection – European Commission, *Case Law*: http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm#caselaw.

114 C-101/01 (judgment of November 6, 2003) / *Reference for a preliminary ruling from the Göta hovrätt (Sweden): Bodil Lindqvist;* available for download at http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm#caselaw.

authority) before publishing the data. Ms. Lindqvist removed the webpage after colleagues told her that it was not appreciated.

Ms. Lindqvist was criminally charged with violation of the Swedish law on the protection of personal data for (1) processing data without notifying the Datainspektionen; (2) processing sensitive data (foot injury) without authorization; (3) transferring personal data to a third country without authorization.

Issue: The questions referred to the interpretation of Directive 95/46. The major issues were:

(1) Whether referring to various persons and identifying them by their name and other personal information on a webpage constituted personal data processing within the meaning of Article 3(1) of Directive 95/46;

(2) Whether reference to the fact that an individual has injured her foot constituted sensitive personal data for the purposes of art. 8(1) of Directive 95/46;

(3) Whether storing information on a webpage that could be consulted in other countries constituted a transfer of personal data to a third country within the meaning of art. 35 of Directive 95/46;

(4) Whether the provisions of Directive 95/46 brought about a restriction conflicting with the general principles of freedom of expression or other freedoms and rights which are applicable within the European Union;

(5) Whether Member States could extend the scope of the national legislation implementing the provisions of Directive 95/46 to areas that are not covered by it.

Decision: **(1)** Referring to various persons and identifying them by their name and other personal information on a webpage, constitutes a processing of personal data within the meaning of Article 3(1) of Directive 95/46;

(2) The reference to the fact that an individual has injured her foot constitutes sensitive personal data for the purposes of art. 8(1) of Directive 95/46;

(3) Storing information on an internet page that can be consulted in other countries does not constitute a transfer of personal data to a third country within the meaning of art. 25 of Directive 95/46;

(4) The provisions of Directive 95/46 do not bring about a restriction which conflicts with the general principles of freedom of expression or other freedoms and rights. It is for the national authorities and courts to ensure a fair balance between fundamental rights;

(5) Member States may extend the scope of the national legislation implementing the provisions of Directive 95/46 to areas that are not covered by Directive 95/46. They may do so only to the extent that no other provision of Community law precludes it, and that the measures taken by Member States are consistent both with the provisions and the underlying objectives of Directive 95/46.

Decision of the Swedish Court of Appeal (April 2004):

Pursuant to the findings of the ECJ on the interpretation of Directive 95/46, the Swedish Court of Appeal (Göta hovrätt) found that Mrs. Lindqvist had indeed contravened certain provisions of the PDA by publishing personal information without the consent of the individuals concerned. However, the Court ruled that the offence was so trivial that no sentence should be imposed on Mrs. Lindqvist (s. 49 of PDA).[115]

2. Joined Cases C-317/04 and C-318/04 (judgment of May 30 2006) / *European Parliament v. Council of the European Union and Commission of the European Communities*[116]

Background and facts: In response to the terrorist attacks of September 11, 2001, the US enacted legislation obliging air carriers operating flights to, from, or across the US to grant access to US customs authorities to the "Passenger Name Records" ("**PNR**"). PNR refers to the data contained in the air carriers' automated reservation and departure control systems. A large number of airlines from the EU complied with this new law. In 2004, two decisions were issued in that regard:

- The European Commission Decision 2004/535/EC of May 14, 2004 holding that there was adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the United States Bureau of Customs and Border Protection.

- The Council decision 2004/496/EC of May 17, 2004 approving the Agreement between the European Community and the United States of America on the processing and transfer of PNR data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection.

Issue: The European Parliament sought the annulment of these two decisions.

Decision: The Court annulled the European Commission Decision on the adequacy of the protection of PNR data. The Court found that the European Commission had no power to render such a decision on the basis of Directive 95/46, as PNR data fell outside the scope of Directive 95/46 pursuant to art. 3(2). Rather, it fell within a framework established by public authorities concerning public security, to which the Directive does not apply. The fact that the data was

---

115 *Ruling of the Court of Appeal (Göta hovrätt), April 2004, on the internet publication of personal information about volunteers of a church (Lindqvist).* Summary based on the Working Party, *Eighth Annual Report on the situation regarding the protection of individuals with regard to the processing of personal data in the European Union and in third countries - covering the year 2004*, pp. 103-104; available for download at: http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/annual_reports_en.htm.

116 Joined Cases C-317/04 and C-318/04 (judgment of May 30, 2006) / *European Parliament v. Council of the European Union and Commission of the European Communities;* available for download at http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm#caselaw

collected by private air carriers for commercial purposes, and that they were in charge for organizing the transfer, did not change the Court's conclusion.

The Court also annulled the Council Decision, as the article 95 of the *Treaty establishing the European Community*[117] did not give the Council competence to conclude such an agreement.

** Please note that since then, there has been several agreements between the EU and the US on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS).*[118]

3. C-553/07 (judgement of May 7, 2009) / *College van burgemeester en wethouders van Rotterdam v M.E.E. Rijkeboer Netherlands*[119]

This case is a reference to a preliminary ruling made by the Raad van State (Dutch Council of State) concerning the interpretation of art. 12(a) of Directive 95/46.

Facts: The reference was made in the context of proceedings between Mr. Rijkeboer and a local authority, the *College van burgemeester en wethouders van Rotterdam* (the "**College**").

The lawsuit was initiated by Mr. Rijkeboer under the *Law on personal data held by local authorities* (*Wet gemeentelijke basisadministratie persoongegevens, Stb.* 1994, No 494).[120] Art. 103(1) provided that the College must notify, on request, a data subject in writing, within four weeks, whether data relating to him from the local authority personal records have, in the year preceding the request, been disclosed to a purchaser or to a third party. Art. 110 provided that the College must retain details of any data communication for one year following the communication. After a year, this information was automatically deleted.

The College had refused to grant Rijkeboer access to information on the disclosure of his personal data to third parties during the two years preceding his request.

Questions at issue: Pursuant to the Directive, and in particular to Article 12(a) thereof, may an individual's right to access information on the recipients of personal data regarding him, and on

---

117 *Treaty establishing the European Community:* http://eur-lex.europa.eu/en/treaties/dat/12002E/htm/C_2002325EN.003301.htm.

118 The agreements and relevant decisions concerning the transfer of PNR data between the EU and the US are available at Data Protection – European Commission, *Commission decisions on the adequacy of the protection of personal data in third countries:* http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm.

119 C-553/07 (judgement of May 7, 2009) / *College van burgemeester en wethouders van Rotterdam v M.E.E. Rijkeboer Netherlands*; available for download at: http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm#caselaw

120 *Law on personal data held by local authorities* (*Wet gemeentelijke basisadministratie persoongegevens,* Stb. 1994, No 494): unavailable in English or French.

the content of the data communicated, be limited to a period of one year preceding his request for access ?

Decision (operative part):

> (1) Article 12(a) of the Directive requires Member States to ensure a right of access to information on the recipients or categories of recipient of personal data and on the content of the data disclosed not only in respect of the present but also in respect of the past. It is for Member States to fix a time-limit for storage of that information and to provide for access to that information which constitutes a fair balance between, on the one hand, the interest of the data subject in protecting his privacy, in particular by way of his rights to object and to bring legal proceedings and, on the other, the burden which the obligation to store that information represents for the controller.
>
> (2) Rules limiting the storage of information on the recipients or categories of recipient of personal data and on the content of the data disclosed to a period of one year and correspondingly limiting access to that information, while basic data is stored for a much longer period, do not constitute a fair balance of the interest and obligation at issue, unless it can be shown that longer storage of that information would constitute an excessive burden on the controller. It is, however, for national courts to make the determinations necessary.

NATIONAL DATA PROTECTION REGIMES

PRELIMINARY REMARKS

Since the 27 Member States of the European Union have adopted legislation to implement Directives 95/46 and 2002/58 into their national law, the domestic data protection regime of all European countries has become quasi-uniform. The purpose and scope of the legislation, the requirements governing data processing, and the rules pertaining to data transfers to third countries are all essentially aligned with those of the Directives.

In this section, we will address (**1**) the general legislative framework; (**2**) the concept of personal data as defined in each jurisdiction; (**3**) the notion of consent; (**4**) the highlights of each national data protection regime (what is distinctive about the way the principles of Directive 95/46 are implemented); (**5**) the significant case law.

We only highlight each national data protection regime in relation to the Directive 95/46, and not Directive 2002/58.

FRANCE

Legislative framework

Constitutional protection

The right to privacy is not constitutionally enshrined in France. However, it is protected by article 9 of the *French Civil Code*:[121]

> **Art. 9 (Act n° 70-643 of 17 July 1970)**
>
> Everyone has the right to respect for his private life.
>
> Without prejudice to compensation for injury suffered, the court may prescribe any measures, such as sequestration, seizure and others, appropriate to prevent or put an end to an invasion of personal privacy; in case of emergency those measures may be provided for by interim order.

Implementation of Directive 95/46

121 *French Civil Code* in article 9, Art. 9 (Act n° 70-643 of 17 July 1970): http://www.legifrance.gouv.fr/html/codes_traduits/code_civil_textA.htm#CHAPTER%20I%A0%20-%A0%20OF%20THE%20ENJOYMENT.

Directive 95/46 was transposed into French law by the *Law no. 2004-801 of 6 August 2004 relating to the protection of individuals against the processing of personal data*[122] and *Decree no. 2005-1309 of 20 October 2005*, as amended by *Decree no. 2007-451 of 25 March 2007*.[123] This legislation amended the *Act n°78-17 of 6 January 1978 on Data Processing, Data Files and Individual Liberties*[124] ("**DPA**") by effectively aligning the DPA with the Directive. The DPA is the main piece of legislation of the French data protection regime. Specific laws complement the general regime in some sectors.

Implementation of Directive 2002/58

Directive 2002/58 became part of French law under the *Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique*.[125]

National supervisory authority

The national supervisory authority is the Commission Nationale de l'informatique et des Libertés ("**Cnil**").[126]

Definition of "personal data"

For the purposes of the DPA, "personal data" refers to "any information relating to a natural person who is or can be identified, directly or indirectly, by reference to an identification number or to one or more factors specific to him. In order to determine whether a person is identifiable, all the means that the data controller or any other person uses or may have access to should be taken into consideration." (s. 2)

- The definition is similar to the one provided in the Directive.
- It applies only to physical persons, not legal entities.

---

122 *Law no. 2004-801 of 6 August 2004 relating to the protection of individuals against the processing of personal data:* http://www.legifrance.gouv.fr/affichTexte.do;jsessionid=4955714D70884E1A4F17991847A98415.tpdjo02v_2?cidTexte=LEGITEXT000005821923&dateTexte=20090713

123 *Decree no. 2005-1309 of 20 October 2005*, as amended by decree no. 2007-451 of 25 March 2007: http://www.legifrance.gouv.fr/affichTexte.do;jsessionid=4955714D70884E1A4F17991847A98415.tpdjo02v_2?cidTexte=LEGITEXT000006052581&dateTexte=20090713

124 *Act n°78-17 of 6 January 1978 on Data Processing, Data Files and Individual Liberties:* http://www.cnil.fr/en-savoir-plus/textes-fondateurs/loi78-17/.

125 *Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique,* http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000801164&dateTexte=#.

126 Commission Nationale de l'informatique et des Libertés, *Accueil*: http://www.Cnil.fr/.

Data subject's consent

Requirements for consent to be valid

The DPA does not define the requirements for a consent to be valid. In practice, the data subject's consent must be in French and given either in writing or by a click-through on a website.[127]

Circumstances where the data subject's consent is required

As a general rule, the data subject must consent to the processing of his personal data, unless another exception applies (s. 7).

S**ensitive personal data** may only be processed if the data subject gives his express consent, or if another exception applies. Please note that there are cases where the law upholds the prohibition against processing sensitive personal data despite of the data subject's consent (s. 8 (II) (1)).

An international data transfer to a country that does not ensure an adequate level of protection is admissible if the data subject has given consent unambiguously to the proposed transfer, or if another exception applies (s. 69).

There are **other specific instances** where express consent is necessary for data processing to be admissible. It is notably the case where personal data is obtained by providers of electronic certification services for purposes of delivery and storage of certificates in relation to electronic signatures (s. 33), or where medical research requires the collection of identifying biological samples (in this case, the consent must also be informed, s. 56).

Highlights of the French data protection regime (under the DPA)

- In certain instances, **prior authorization** of the Cnil, a minister or the "Conseil d'État" is required to process data (s. 25-29).
- **When a data controller violates the DPA**, the Cnil may order fines (up to 300,000 euros), injunctions or special emergency measures. The Cnil may also ask a competent court to order any measure deemed necessary (s. 45-49).
- The DPA also refers to articles 226-16 to 226-24 of the ***Penal Code*.**[128] These articles list specific offences for the violation of personal rights in relation to computer files or processes (s. 50).

---

127 Data Protected – Linklaters, *France: Personal data*: https://clientsites.linklaters.com/Clients/dataprotected/Pages/France.aspx#dataquality.

- **Impediment to the action of the Cnil** is punishable by a fine of 15,000 euros, as well as by one year of imprisonment (s. 51).

- There are **additional conditions for data processing** made for the purpose of medical research (s. 53-61), or for the purposes of evaluation or analysis of care and prevention practices or activities (s. 62-66).

- As regards **international data transfers** (s. 68-69), in practice, the Cnil considers that the consent of the data subject to the transfer is rarely sufficient in the case of an employee's personal data.

    - The Cnil has approved the use of binding corporate rules in France.[129]

Significant case law on data protection

Henri S. / SCPP, Cour d'appel de Paris 13ème chambre, section A Arrêt du 15 mai 2007[130]

Facts: Henri S. illegally downloaded music files. SCPP, a collecting company specialized in the assignment of rights in the music industry, sued Henri S. for infringement of copyright law, and under criminal provisions. Henri S. objected that the processing of his IP address, which had been used to identify him and link him to the downloaded files, was unlawful. He claimed that the SCPP should have requested the Cnil for its authorization to collect, extract and transmit his IP address.

Issue (exception raised by the defendant): Is an IP address personal data for the purposes of the DPA ?

Decision: IP addresses were not considered personal data for the purposes of the DPA. Henri S.' conviction was confirmed.

* Please note that the Cnil has appealed from this decision on the issue of the qualification of IP addresses. The case is still pending.

---

128 Articles 226-16 to 226-24 of the *Penal Code* are available at http://www.Cnil.fr/en-savoir-plus/textes-fondateurs/sanctions-penales/.

129 Data Protected – Linklaters, *France: Transfer of Personal Data to Countries Outside of the EEA:* https://clientsites.linklaters.com/Clients/dataprotected/Pages/France.aspx#transfer.

130 *Henri S. / SCPP*, Cour d'appel de Paris 13ème chambre, section A Arrêt du 15 mai 2007, http://legalis.net/jurisprudence-decision.php3?id_article=1955.

Marc W., Asesif et autres / Cnil, Cour de cassation Chambre criminelle 28 septembre 2004[131]

Facts: The Spiritual Association of the Church of Scientology of Île-de-France (the "**Association**") failed to remove the personal information of a person (the "**complainant**") from its files despite an explicit request. In 1997, the Cnil intervened. The Association subsequently guaranteed that this complainant's personal data had been duly removed from its files. In March and April 2000, the complainant received various letters and publications from a third party related to the Association bearing the same ID number as the mail received in 1997.

The Association was charged with violating the DPA, notably for its failure to notify a third party of the data subject's objection (s. 38). This constitutes a criminal offence pursuant to art. 226-18 of the Penal Code. The Association was also found guilty of impeding the action of the Cnil. Both the Paris Court (May 17, 2002) and the Court of Appeal (October 13, 2003) fined the Association accordingly.

Claim: The Association appealed from the decision before the Court of Cassation. It argued that the complainant had not lawfully exercised his right to object to the processing of his data, as he had not provided a legitimate ground.

Decision: The Court of Cassation upheld the decisions of the Paris Court and the Court of Appeal. The complainant had lawfully exercised his right to object, pursuant to s. 38 of the DPA. No formalism was required in the exercise of this right. The Court also confirmed that, as a general principle, data subjects do not need to invoke a legitimate ground to exercise their right to object to the processing of data when it is related to the processing of files resulting from the exercise of an individual liberty, especially as regards political, philosophical or religious matters.

Microsoft Corporation / Marko K. et AOL France / Marko K. Tribunal de commerce de Paris 8ème chambre Jugement du 05 mai 2004[132]

Facts: Mr. K, the owner of a French company selling football merchandise by correspondence, sent spam emails via the numerous AOL and MSN Hotmail accounts of the company.

Claim: AOL France and Microsoft Corporation sued Mr. K in damages for breach of contract

Decision : The Court found Mr. K guilty of a breach of contract and was thus condemned to pay damages to AOL and Microsoft (5,000 euros each).

---

131 *Marc W., Asesif et autres / Cnil*, Cour de cassation Chambre criminelle 28 septembre 2004, http://legalis.net/jurisprudence-decision.php3?id_article=1350.

132 *Microsoft Corporation / Marko K. et AOL France / Marko K.* Tribunal de commerce de Paris 8ème chambre Jugement du 05 mai 2004, http://legalis.net/jurisprudence-decision.php3?id_article=1203.

** Please note that this decision was rendered pursuant to the general rules governing civil liability of the French Civil Code (s. 1147 on contractual liability). Nevertheless, it was referred to, in the* Eighth Annual Report on the situation regarding the protection of individuals with regard to the processing of personal data in the European Union and in third countries - covering the year 2004*, as a landmark case.*[133]

Le Ministère public et Mademoiselle S. / Monsieur F. Tribunal de grande instance de Privas Jugement correctionnel du 3 septembre 1997[134]

Facts: Florent G. uploaded pornographic photographs of Sarah B. on his personal Internet account without her consent.

Claim: Florent G. was charged under articles 226-19 and 226-31 of the Penal Code for the violation of Sarah B.'s privacy right through the conservation of a computerized memory of her photographs. Sarah B. also claimed damages for moral prejudice.

Decision: The Court found Florent G. guilty of violation of personal rights resulting from computer files or processes under articles 226-19 and 226-31 of the Penal Code. The Court ruled that the photograph constituted sensitive data, as it indirectly gave information about Sarah B.'s sexual life. The Court condemned Florent G. to eight months of imprisonment, a fine of 5,000 francs, and ordered him to pay 20,000 francs in damages to Sarah B.

GERMANY

Legislative framework

Constitutional protection

Basic Law for the Federal Republic of Germany of 1949 (*Grundgesetz*),[135] protects the protection human dignity (art. 1), and the rights of liberty (art. 2):

> ***Article 1*** **(Protection of human dignity).**
> (1) The dignity of man inviolable. To respect and protect it is the duty of all state authority.
> (2) The German people therefore acknowledge inviolable and inalienable

133 Working Party, *Eighth Annual Report*, p. 40, see note 115.

134 *Le Ministère public et Mademoiselle S. / Monsieur F.* Tribunal de grande instance de Privas Jugement correctionnel du 3 septembre 1997, http://legalis.net/jurisprudence-decision.php3?id_article=159.

135 *Basic Law for the Federal Republic of Germany of 1949 (Grundgesetz):* http://www.iuscomp.org/gla/statutes/GG.htm.

> human rights as the basis of every community, of peace and of justice in the world.
> (3) The following basic rights shall bind the legislature, the executive, and the judiciary as directly applicable law.
>
> ***Article 2* (Rights of liberty).**
> (1) Everyone has the right to the free development of his personality insofar as he does not violate the rights of others or offend against the constitutional order or the moral code.
> (2) Everyone has the right to life and to inviolability of his person. The freedom of the individual is inviolable. These rights may only be encroached upon pursuant to a law.

The right of privacy of communications is also constitutionally protected :

> ***Article 10* (Privacy of letters, posts, and telecommunications).**
> ***(amended 24 June 1968)***
> (1) Privacy of letters, posts, and telecommunications shall be inviolable.
> (2) Restrictions may only be ordered pursuant to a statute. Where a restriction serves to protect the free democratic basic order or the existence or security of the Federation, the statute may stipulate that the person affected shall not be informed of such restriction and that recourse to the courts shall be replaced by a review of the case by bodies and auxiliary bodies appointed by Parliament.

Implementation of Directive 95/46

Directive 95/46 was implemented into German law by the *Federal Data Protection Act* (*Bundesdatenschutzgesetz*) (the "**FDPA**"),[136] which came into force on May 23, 2001. The German States have also enacted state legislation.

Implementation of Directive 2002/58

The Directive 2002/58 was implemented into German law by the *Telecommunications Act* (*Telekommunikationsgesetz*) of June 22, 2004,[137] and the *Act Against Unfair Competition* (*Gesetz gegen den unlauteren Wettbewerb*) of July 7, 2004.[138]

National supervisory authority

---

136 *Federal Data Protection Act (Bundesdatenschutzgesetz)*: http://www.iuscomp.org/gla/statutes/BDSG.htm.

137 *Telecommunications Act (Telekommunikationsgesetz)*: http://www.iuscomp.org/gla/statutes/TKG.htm.

138 *Act Against Unfair Competition (Gesetz gegen den unlauteren Wettbewerb)*: the Act is not available in English or French, but a review of the Act in English is available at: Jan Peter Heidenreich, The New German Act Against Unfair Competition: http://www.iuscomp.org/gla/literature/heidenreich.htm

There are 20 different federal and regional supervisory authorities that monitor the implementation of the data protection regime. The federal supervisory authority is the Federal Commissioner for Data Protection and Freedom of Information.[139]

Definition of "personal data"

Personal data means "any information concerning the personal or material circumstances of an identified or identifiable individual (the data subject)" (s. 3(1)).

- The German definition of "personal data" differs slightly from the *Opinion Nº 4/2007 on the concept of personal data, 20 June 2007* of the Working Party.[140] In German law, whether or not an individual is identifiable must be considered from the point of view of the data controller only. Information held by third parties is not relevant in determining whether the controller could identify the data subject, contrary to the opinion of the Working Party.

- The concept of personal data applies only to individuals and not to legal entities.

- Personal data processed solely for personal or family activities falls outside of the scope of the FDPA (s. 1(2)3).

- Personal data subject to professional or special official secrecy (s. 39), or used by research institutes (s. 40) or by the media (s. 41) is subject to special provisions.

Data subject's consent

Requirements for consent to be valid

The FDPA defines **specific requirements** for consent to be valid (s. 4a):

- Consent must be based on the data subject's free will;

- The data subject must be informed of the purpose of the collection, processing or use and, in so far as the circumstances of the individual case permit it or at his request, of the consequences of withholding consent;

---

139 Federal Commissioner for Data Protection and Freedom of Information, *Homepage*: http://www.bundesdatenschutz.de/.

140 Working Party, *Opinion Nº 4/2007 on the concept of personal data*, see note 80. See this document for a series of detailed examples on what is considered personal data.

- Consent must be given in writing, except where special circumstances justify any other form;

    - In the field of *scientific research*, a special circumstance is deemed to exist where the defined purpose of research would be impaired considerably if consent were obtained in writing. In such a case, the required information must be recorded in writing, together with the reasons for which considerable impairment of the defined purpose of research arises.

- Consent must be made distinguishable from other written declarations given at the same time.

- When sensitive data is collected, processed or used, the consent must refer expressly to the said data.

Circumstances where the data subject's consent is required

As a general rule, "[the] collection, processing and use of personal data shall be admissible only if permitted or prescribed by this Act or any other legal provision or if the data subject has consented" (s. 4(1)).

Sensitive data may not be collected, except where the data subject has given his consent, or another exception applies (s. 13 (2) 2.)

A **transfer of personal data** is admissible, even where the recipient does not guarantee an adequate level of protection, if the data subject has given his consent or another exception applies (s. 4c(1)1.).

Storage, modification or use for other purposes than those for which the data was collected is admissible if the data subject has consented or another exception applies (s. 14(2) 2).

Bodies conducting scientific research may publish personal data only if the data subject has given his consent, or if this is indispensable for the presentation of research findings on contemporary events. (s. 40 (3)).

Consent is required in **other circumstances**, such as a waiver of the requirement for prior registration (s. 4d(3)) or for prior checking (s. 4d(5)).

Highlights of the German Data Protection Regime (under the FDPA)

- The appointment in writing of a **Data protection official** is mandatory for every public and private body of more than nine employees that processes personal data automatically (s. 4f).

- With regard to **international data transfers**, the FDPA makes a distinction between transfers which fall within and outside the scope of the law of the European

Communities (s. 4b). There is no obligation to notify the supervisory authority of an international data transfer.

- Data processors must take **technical and organizational safety measures** (s. 9). These measures concern access control, transmission control, input control, job control, availability control and separation of data (Annex to the FDPA).

- **A violation of the provisions of the FDPA** may constitute an administrative (s. 43) or a criminal offence (s. 44). Administrative offences are punishable by fines up to 250,000 euros (s. 43(3)).

Significant case law on data protection

Volkszählungsurteil, Federal Constitutional Court, December 15, 1983 (BverfGE, 1 BvR 209/83) [141]

Facts: German citizens brought a petition to the constitutional court in order to oppose a population census. They feared that the personal data collected and stored in the context of the census would allow the state to spy on them.

Decision: The Court recognized for the first time the *right to informational self-determination*, derived from article 1 (human dignity) and article 2 (personality right) of the German Constitution. This notion gives an individual the right to decide if and under which conditions his personal information should be communicated to others. It is based on the idea of self-determination. The Court noted that the development of technology required increased protection of the right to informational self-determination. The Court also stated that the right to data privacy could only be restricted in the case of a predominant, well justified public interest. However, any restriction must comply with procedural safeguards.

Based on these principles, the Court established conditions on the processing of personal data for the purpose of the census. It ruled that evaluations programs for statistical purposes could only be carried out if it was impossible to distinguish certain people by recording dates.[142]

---

141 *Volkszählungsurteil*, The summary of this case is also based on: Sjaak Nouwt, Berend R. de Vries and Corien Prins, eds., *Reasonable Expectations of Privacy?* (The Hague: Information Technology & Law Series, 2005), pp. 213-215; Cora Zeugmann, *The Trade-Off between Civil Liberties and Security in the United States and Germany after 9/11/01 – An analysis*, Diplom.de, Hamburg Diplomica – Verl., 2008, pp. 49-50: (http://books.google.ca/books?id=crvwPASwqjUC&pg=PA49&lpg=PA49&dq=Volksz%C3%A4hlungsurteil+federal&source=bl&ots=Cuz2-B7v0P&sig=VF2-Okhp3mkMhedp6TaGrsMoFto&hl=en&ei=jwVVSrK6MI37tgeZ_qWmCA&sa=X&oi=book_result&ct=result&resnum=1); Dataprotection.eu, *The census decision and the second generation of data protection norms:* http://www.dataprotection.eu/pmwiki/pmwiki.php?n=Main.SecondGeneration; Sebastian Meissner, *Country Report Germany, Austria, Switzerland:* http://www.fidis.net/resources/deliverables/privacy-and-legal-social-content/d133-study-on-id-number-policies/doc/15/.

Ruling of the Federal Constitutional Court, October 23, 2006 (1 BvR 2027/02) on the rights of insured persons (notice of consent on standard forms)[143]

The Court held that a general notice of release from the pledge of secrecy in insurance contracts violated the data subject's right to informational self-determination. The notice was in a standard form, and worded very broadly, which made it impossible to determine what information could be obtained by whom.

Ruling of the Federal Constitutional Court, February 23, 2007 (1 BvR 421/05) on covertly obtained genetic expertise[144]

The Court ruled that covertly obtained genetic expertise on parentage could not be used as evidence, as it violated the child's right to informational self-determination. The legislature has yet to provide an appropriate procedure to satisfy the father's right to information about whether the child is of his descent. The Court balanced the right of the child to the non-disclosure of his data, with the father's right to information. This decision reinforces the right to informational self-determination.

ITALY

Legislative framework

Constitutional protection

---

142 Sjaak Nouwt, Berend R. de Vries and Corien Prins, eds., *Reasonable Expectations of Privacy?*, p. 214, see note 141.

143 *Ruling of the Federal Constitutional Court on the rights of insured persons (notice of consent on standard forms),* October 23, 2006 (1 BvR 2027/02). Summary based on the Google translation of the judgment (hereby attached), and the Working Party, *10th Annual Report on the situation regarding the protection of individuals with regard to the processing of personal data in the European Union and in third countries - covering the year 2006,* p. 45; available for download at: http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/annual_reports_en.htm.

144 *Ruling of the Federal Constitutional Court on covertly obtained genetic expertise*, February 23, 2007 (1 BvR 421/05). Summary based on the Google translation of the judgment, and the Working Party, *11th Annual Report on the situation regarding the protection of individuals with regard to the processing of personal data in the European Union and in third countries - covering the year 2007*, p. 49; available for download at:http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/annual_reports_en.htm.

The right to privacy is not expressly protected in Italy's Constitution.[145] It only protects the privacy of communications:

> **Article 15 [Freedom of Correspondence]**
> (1) Liberty and secrecy of correspondence and other forms of communication are inviolable.
> (2) Limitations may only be imposed by judicial decision stating the reasons and in accordance with guarantees defined by law.

Implementation of Directive 95/46

Directive 95/46 was first implemented into Italian law by *Act No. 675 of 31 December 1996*,[146] which was supplemented by a series of subsequent acts. On January 1st, 2001, the *Italian Data Protection Code* (Legislative Decree no. 196 of 30 June 2003) (the "**Code**")[147] entered into force, replacing all previous laws and regulations, and consolidating them under the same piece of legislation.

The Code expressly introduces the right to the protection of personal data (s. 1).

Implementation of Directive 2002/58

Directive 2002/58 was also implemented under the Code, namely title X, sections 121 to 133 which concern electronic communications.

National supervisory authority

The supervisory authority is the *Garante per la protezione dei dati personali* (the "**Garante**")[148].

Codes of conduct

The Garante has adopted six codes of conduct, which can be found in Annex A of the Code:

- *Code of practice concerning the processing of personal data in the exercise of journalistic activities* (1998);

---

145 *Constitution of Italy*: http://www.servat.unibe.ch/icl/it00000_.html.

146 *Act No. 675 of 31 December 1996:* http://www.privacy.it/legge675encoord.html.

147 *Italian Data Protection Code (Legislative Decree no. 196 of 30 June 2003)*; available for download under the heading "DataProtectionCode2003_ Consolidated Text in Force.pdf" at: http://www.garanteprivacy.it/garante/navig/jsp/index.jsp?folderpath=Normativa%2FItaliana%2FIl+Codice+in+materia+di+protezione+dei+dati+personali.

148 Garante per la protezione dei dati personali, *Home*: http://www.garanteprivacy.it/garante/navig/jsp/index.jsp.

- *Code of conduct and professional practice regarding personal data for historical purposes* (2001);
- *Code of conduct and professional practice applying to the processing of personal data for statistical and scientific research purposes within the framework of the national statistical system* (2002);
- *Code of conduct and professional practice applying to processing of personal data for statistical and scientific purposes* (2004);
- *Code of conduct and professional practice applying to information systems managed by private entities with regard to consumer credit, reliability and timeliness of payments* (2005);
- Code of practice applying to the processing of personal data performed with a view to defence investigations (2008).

Definition of "personal data"

The Code defines "personal data" as "any information relating to natural or legal persons, bodies or associations that are or can be identified, even indirectly, by reference to any other information including a personal identification number" (s. 4.1a)).

- It is important to take notice of the fact that this definition covers both natural and legal persons.
- IP addresses are not considered to be personal data for the purposes of the Code.[149]

Personal data processed in specific sectors is subject to distinct rules, laid out in Part II of the Code. This Part addresses, namely, data processed by banking, financial and insurance systems (title IX), and journalism, literary and artistic expression (title XII).

Data subject's consent

Requirements for consent to be valid

For the consent of the data subject to be effective, it must satisfy **several requirements** (s. 23):

- Consent must be express.
- Consent may refer either to the processing as a whole or to one or more of the operations thereof.

149 Data Protected – Linklaters, *What is personal data?:* https://clientsites.linklaters.com/Clients/dataprotected/Overview/Pages/Index.aspx.

- Consent must be given freely, specifically with regard to a clearly identified processing operation.
- Consent must be documented in writing.
- The data subject must have been provided with the information referred to in s. 13 of the Code.
- Consent must be given in writing if the processing pertains to sensitive data.

The Code provides for **simplified arrangements** regarding information and consent (Chapter II), which may only be applied by public health care bodies, other private health care bodies and health care professionals or by the other public entities referred to in s. 80 (s. 77).

Circumstances where the data subject's consent is required

As a general rule, express consent of the data subject is needed for the processing of personal data by private entities or profit-seeking public bodies (s. 23). However, there are circumstances where no consent is required for data processing (e.g. where the processing is necessary to comply with an obligation imposed by law) (s. 24).

The **processing of sensitive data** requires the data subject's written consent to be allowed, except for specific types of processing (s. 26).

A **data transfer to a third country** may only take place in specific circumstances, including when the data subject has expressly consented (if the transfer concerns sensitive personal data, consent must be given in writing) (s. 43).

The data subject must consent to the processing of **personal health data** by health professionals and public health care bodies (s. 76).

Highlights of the Italian Data Protection Regime (under the Code)

- The Code may **apply to the processing of personal data carried out for purely personal purposes** if the data is intended for systematic communication or discrimination (s. 5.3).
- There is a **strict liability rule** for damages caused as a consequence of the processing of data (s. 15).
- The Code provides specific rules for the **termination** of processing operations (s. 16).
- **Processing operations carrying certain risks** are subject to specific rules (s. 17).
- **No consent is required** for the processing of data relating to economic activities that are processed in compliance with the legislation in force applicable to business and industrial secrecy (s. 24.1d)).

- **The processing of sensitive data** requires the consent of the data subject (in writing) and the prior authorization of the Garante. There are some exceptions. (s. 26).

- The Code lays out the **specific technical, logical and organisational minimum security measures** that must be complied with (s. 33-36). These measures are specified in Annex B. The failure to adopt the minimum security measures required under s. 33 shall be punished by imprisonment of up to two years or a fine between 10,000 and 50,000 euros (s. 169).

- Data controllers only need to **notify the Garante** prior to the processing of sensitive data (s. 37).

- With regard to **internal data transfers**, the data controller does not need to notify the Garante if the third country ensures an adequate level of protection.

    - If contractual safeguards are used in a contract for the transfer of data to a country that does not ensure an adequate level of protection, prior authorization of the Garante is needed (s. 44).

    - The use of binding corporate rules has not yet been approved by the Italian Legislator. The Garante suggested that Parliament amend the Code in order to allow the use of binding corporate rules.[150]

- The **sanctions** that can be imposed under the Code are heavy. Significant fines can be imposed for administrative offences (see s. 161-166). For criminal offences, substantial fines and imprisonment sentences of up to three years may be imposed (see 167-172).

Significant case law on data protection

Ruling of the Supreme Court of Cassation, February 2004, on evaluation data[151]

An employee requested to have access to his evaluation data, which was controlled by his employer. The employer denied the employee's request on the grounds that the data was not "personal data" under the Code. The *locus standi* of the Garante, who wished to defend the decision he had previously rendered in this case, was also at issue. The Court stated that:

- Evaluation data is personal data and may be accessed by the data subject at any step of its processing.

---

150 Data Protected – Linklaters, *Italy: Transfer of Personal Data to Countries Outside of the EEA:* https://clientsites.linklaters.com/Clients/dataprotected/Pages/Italy.aspx#transfer.

151 *Ruling of the Supreme Court of Cassation, February 2004, on evaluation data*. Summary based on the Working Party, *Eighth Annual Report*, p. 52, see note 115.

- The Garante has *locus standi* when his decisions are appealed, so as to protect the public interest.

Ruling of the Supreme Court of Cassation, June 2004, on unstructured data[152]

Television journalists and a broadcasting company complained that a publisher of a daily newspaper had published material disclosing information on the said journalists. They had previously requested the elimination of their personal data on the ground that the processing was unlawful. The Court allowed the journalists' claim and stated that:

- the Code aims at protecting the fundamental right of individuals. These rights may be breached merely by disseminating information, regardless of the fact that the information is part of a structured filing system.

- the Code applies to unstructured data contained in a database, as well as information taken from public sources. The rules for processing personal data set out in the Code must be complied with, even though publicly available information is at stake (the only difference is that explicit consent is not required for processing, s. 24.1c)). This is justified by the fact that an entity processing the data may add informational value and violate the subject's dignity.

Ruling of the Supreme Court of Cassation, 2000, on the right of rectification and exception for journalistic purposes[153]

In the press, a third party improperly referred to the name of an individual. The person wanted her name to be corrected. The main issue was the applicability of the Act No. 675 of 31 December 1996,[154] to the processing of data for journalistic purposes. The Court ruled that the data subject had the right to request correction of data allowing her to be accurately identified.

THE NETHERLANDS

Legislative framework

Constitutional protection

---

152 *Ruling of the Supreme Court of Cassation, June 2004, on unstructured data.* Summary based on the Working Party, *Eighth Annual Report*, p. 52, see note 115.

153 *Ruling of the Supreme Court of Cassation, 2000, on the right of rectification and exception for journalistic purposes.* Summary based on the Working Party, *Fifth Annual Report on the situation regarding the protection of individuals with regard to the processing of personal data and privacy in the European Union and in third countries - covering the year 2000*, p. 41; available for download at: http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/annual_reports_en.htm.

154 *Act No. 675 of 31 December 1996*, see note 146.

The right to privacy, including the privacy of correspondence, is protected by the *Dutch Constitution:*[155]

> **Article 10 [Privacy]**
>
> (1) Everyone shall have the right to respect for his privacy, without prejudice to restrictions laid down by or pursuant to Act of Parliament.
> (2) Rules to protect privacy shall be laid down by Act of Parliament in connection with the recording and dissemination of personal data.
> (3) Rules concerning the rights of persons to be informed of data recorded concerning them and of the use that is made thereof, and to have such data corrected shall be laid down by Act of Parliament.
>
> **Article 13 [Secrecy of Communication]**
>
> (1) The privacy of correspondence shall not be violated except, in the cases laid down by Act of Parliament, by order of the courts.
> (2) The privacy of the telephone and telegraph shall not be violated except, in the cases laid down by Act of Parliament, by or with the authorization of those designated for the purpose by Act of Parliament.

Implementation of Directive 95/46

The Directive 95/46 was implemented into Dutch law by the *Personal Data Protection Act* (*Wet Bescherming Persoonsgegevens*, "**WBP**").[156] It entered into force in September 2001.

The *Exemption Decree* ("**Decree**") of May 7, 2001 completes the WBP by providing exemptions and simplifications to the notification duty for certain categories of data.[157]

Implementation of Directive 2002/58

Directive 2002/58 was implemented mainly through an amendment to the *Telecommunications Act* (*Wet implementatie Europees regelgevingskader voor de elektronische communicatiesector 2002*)[158]. The amended version of the Act came into force in May 2004.

National supervisory authority

---

155 *Dutch Constitution*: http://www.servat.unibe.ch/icl/nl00000_.html.

156 *Personal Data Protection Act;* available for download at: http://www.dutchdpa.nl/indexen/en_ind_wetten_wbp_wbp.shtml.

157 *Exemption Decree of 7 May 2001*: as cited by Data Protected – Linklaters, https://clientsites.linklaters.com/Clients/dataprotected/Pages/TheNetherlands.aspx#.

158 *Telecommunications Act (Wet implementatie Europees regelgevingskader voor de elektronische communicatiesector 2002)*: Only available in Dutch.

The national supervisory authority is the Dutch Data Protection Authority (*College bescherming persoonsgegevens*) (the "**DPA**").[159]

Definition of "personal data"[160]

"Any information relating to an identified or identifiable natural person" is considered personal data for the purposes of the WBP (s. 1a)). This definition is in line with the definition of the Directive.

- A person is identifiable when her identity can be established reasonably, without disproportionate efforts.
- Data concerning legal entities is not usually considered personal data. Nevertheless, data concerning companies or organizations can be personal data if it contributes to the way in which a person is judged or treated in a social or economic setting.
    - Ex.: The profit of a sole proprietorship is personal data as it represents the income of the proprietor, which tells about his socio-economic position.
- Data regarding items or objects can also be treated as personal data depending on the context. The issue is whether the data contribute to the way a person is judged or treated in a socio-economic context.
    - Ex.: The value of a car constitutes personal data when it is processed in the context of a car insurance company, as it sometimes establishes the approximate income of the owner of the car. However, the value of a car is not personal data when the price is listed (e.g. car dealer).
- The DPA considers that IP addresses can sometimes be regarded as personal data, depending on the circumstances of the case.[161]
- The DPA also expressed the view that digital pictures of public areas, including detailed pictures of individual houses, are to be considered personal data when (1) the data is used for purposes that affect the interests of the individual home owners, such as taxation or real estate; and (2) the owners are identifiable natural persons.[162]

---

159 Dutch Data Protection Authority, *News of the Dutch DPA*: http://www.dutchdpa.nl/.

160 Based on Ministry of Justice, "Guidelines for personal data processors – Personal Data Protection Act" (2001) p. 12-13 available for download at: http://www.dutchdpa.nl/indexen/en_ind_wetten_wbp.shtml.

161 Working Party, *Sixth Annual Report on the situation regarding the protection of individuals with regard to the processing of personal data and privacy in the European Union and in third countries - covering the year 2001*, p. 57, http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/annual_reports_en.htm.

162 Working Party, *Sixth Annual Report*, p. 57, see note 161.

Personal data processed in specific situations mentioned in the WBP, such as in the course of a purely personal or household activity (s. 2), or for exclusively journalistic, artistic or literary purposes (s. 3 – certain conditions apply) does not fall within the scope of the WBP.

Data subject's consent

Requirements for consent to be valid

The WBP **defines** the "consent of the data subject" as "any freely-given, specific and informed expression of will whereby data subjects agree to the processing of personal data relating to them" (s. 1).

For consent to be valid, **specific requirements** must be met:

- The consent must consist in the free expression of the data subject's will. The consent will be invalid if there is no free will (e.g. the data subject gives his consent under pressure or his position of dependence towards the data controller was exploited to obtain his consent).

- The consent must be aimed at a specific data processing.

- The consent must be unambiguous. This means that the data controller must not have any doubt as to the content and scope of the data subject's consent.

    - For this purpose, the data controller may *obtain a separate confirmation of consent*.

    - The data controller may also *rely on the data subject's behavior*. For example, consent is apparent when the data subject leaves his business card with the data controller, if the data to be processed is on the business card.

- Regardless, the data controller must keep in mind that the *burden of proof* for obtaining consent unambiguously rests on his shoulders.

- Moreover, the data controller must *adequately inform* the data subject about the processing procedure.

- The consent **no longer needs to be in writing**, though a written consent may always be helpful for evidentiary purposes.[163]

Where the **data subject is less than 16 years old**, or has been placed under legal restraint or in the care of a mentor, it is the consent of his legal representative that is required (s. 5(1)).

---

163 Ministry of Justice, "Guidelines for personal data processors – Personal Data Protection Act" (2001), pp. 21-22, see note 160.

Consent may be **withdrawn** at any time by the data subject or his legal representative (s. 5(2)).

Circumstances where the data subject's consent is required

As a **general rule**, personal data may only be processed when the data subject has unambiguously given his consent to the processing, or where the processing is necessary in the circumstances defined in the WBP (s. 8).

Sensitive data concerning a person's religion, philosophy of life, political persuasion or trade union membership may only be supplied to third parties with the consent of the data subject (s. 7 (3), 19(3) and 20(2)).

- The prohibition on the processing of sensitive personal data does not apply if the data subject has given his express consent, or if another exception applies (s. 23).

A **personal data transfer** to a country that does not ensure an adequate level of protection is admissible if the data subject has unambiguously consented to it, or if another exception applies (s. 77 (1) a)).

Highlights of the Dutch Data Protection Regime (under the WBP and the Decree)

- The **data controller** must comply with the WBP, and the **data processor** has an independent responsibility to comply with the provisions concerning data processing (s. 4 of WBP).
- The Decree exempts certain categories of data from the **notification obligation**, such as the processing of data as part of salary and/or personnel administration. This exemption does not apply in the context of an international data transfer.[164]
- The **legitimate interests condition** is available when the data subject has not expressly consented to the processing (s. 8f of WBP).
- **Special (or sensitive) data** includes, in addition to the standard types of sensitive data, personal data connected with a person's criminal behavior or with unlawful or objectionable conduct for which a ban has been imposed (s. 16 of WBP).
    - The DPA considers as sensitive biometric information indicating health and racial or ethnic origin.[165]

---

164 Data Protected – Linklaters, *The Netherlands: National Regulatory Authority:* https://clientsites.linklaters.com/Clients/dataprotected/Pages/TheNetherlands.aspx#nra.

165 Data Protected – Linklaters, *The Netherlands: Sensitive Personal Data:* https://clientsites.linklaters.com/Clients/dataprotected/Pages/TheNetherlands.aspx#sensitive.

- The **data subject's right of access** under art. 35 is very broad (see the *Ruling of the Supreme Court, June 29, 2007 on three cases involving Dexia and HBU regarding the scope of the right of access,*[166] summarized at p. 78).

- In some cases, the Minister may issue a permit for **international data transfers** if the third country to which data is transferred does not otherwise guarantee an adequate level of protection, nor falls in any of the exceptions (necessity of explicit consent) (s. 77.2 of WBP).

    - The use of binding corporate rules is recognized by the DPA.[167]

- The **sanctions** that can be imposed under the WBP range from administrative fines (s. 66 of WBP) to penal sanctions, which include a prison sentence for a maximum of six months (s. 75 of WBP).

Significant case law on data protection

Ruling of the Supreme Court, June 29, 2007 on three cases involving Dexia and HBU regarding the scope of the right of access[168]

Facts: Following the stock market crash of 2000-2001, customers that had a securities-lease agreement with Dexia Bank Nederland N.V. ("Dexia") or investors in the funds of HBU requested permission to access their files. The financial institutions refused, invoking that it could harm their position in legal procedures and lead to disproportionate administrative costs.

Issue: What is the extent of the right of access under art. 35 of the WBP ? Does it require Dexia and HBU to allow the data subjects to inspect their files and obtain a copy of all their personal data (including transcripts of telephone conversations) ?

---

166 *Ruling of the Supreme Court, June 29, 2007 on three cases involving Dexia and HBU regarding the scope of the right of access.* Summary based on the Working Party, *9th Annual Report on the situation regarding the protection of individuals with regard to the processing of personal data in the European Union and in third countries - covering the year 2005,* p. 86-87; available for download at: http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/annual_reports_en.htm. Also based on Mark Turner and Dominic Callaghan, "The Regular article tracking developments at the national level in key European countries in the area of IT and communications – Co-ordinated by Herbert Smith LLP and contributed to by firms across Europe" (2007) 23 Computer Law & Security Report 404 at p. 406.

167 Alonso Blas LL.M., D., "Policy paper on transfers of personal data to third countries in the framework of the new Dutch Data Protection Act (Wbp)" (February 2003), p. 12, available for download at: http://www.dutchdpa.nl/documenten/en_int_policy_paper.shtml?refer=true&theme=purple.

168 *Ruling of the Supreme Court, June 29, 2007 on three cases involving Dexia and HBU regarding the scope of the right of access.* See note 166.

Decision: The Court ruled that the financial institutions must provide the data subjects with most of the information requested. The data controller should provide all relevant and specific information, and not just a rough overview. The data controller should also provide copies of the relevant documents, but this does not mean that data subjects have an automatic right to receive copies. The data controller may fulfill his duty by other means. It may provide a summary or extracts, or allow inspection. The data subject does not need to invoke a specific justification to exercise his right under art. 35 of WBP.

The Court may refuse to grant the data subject access to their files if the administrative burden is disproportional, or its rights and freedoms are infringed or threatened to be infringed. Accordingly, the Court did not allow the request to provide copies of the telephone conversations.

Decision of the DPA, July 20, 2001, no. 2001-0784, regarding the international data transfer between eBay and iBazar[169]

The DPA provided an opinion on the transfer of consumer data from iBazar, a company operating auction websites in various EU countries, to eBay, an American company. The transfer occurred after eBay took over iBazar. The DPA based its opinion on the Directive 95/26/EC, as the WBP was not in force at that time (hence, the permit system was not available).

At that time, eBay was not a part of the Safe Harbor framework, so the data transfer to the US constituted a transfer to a third country that did not provide an adequate level of protection. Accordingly, the unambiguous consent of the data subjects was needed for the transfer to be lawful. The DPA suggested that in this regard, providing the data subjects with an option to "opt-out" was not sufficient, as a voluntary act of will was needed to consent.

The DPA recommended two options to eBay: (1) join the Safe Harbor framework agreement; (2) set up a system where all customers must "opt-in" in order to consent to the transfer. This had been done for the data transfer from iBazar France. Ultimately, eBay chose the second option.

SPAIN

Legislative framework

Constitutional Protection

The right to privacy is guaranteed under the *Spanish Constitution*:[170]

---

169 *Decision of the DPA, July 20, 2001, no. 2001-0784, regarding the international data transfer between eBay and iBazar*. Summary based on the Working Party, *Sixth Annual Report*, p. 57, see note 161. See also Alonso Blas LL.M., D., "Policy paper on transfers of personal data to third countries in the framework of the new Dutch Data Protection Act (Wbp)" p. 34, see note 167.

> **Article 18 [Honor, Privacy, Home, Secrecy of Communication]**
> (1) The right of honor, personal, and family privacy and identity is guaranteed.
> (2) The home is inviolable. No entry or search may be made without legal authority except with the express consent of the owners or in the case of a *flagrante delicto*.
> (3) Secrecy of communications, particularly regarding postal, telegraphic, and telephone communication, is guaranteed, except for infractions by judicial order.
> (4) The law shall limit the use of information, to guarantee personal and family honor, the privacy of citizens, and the full exercise of their rights.

Implementation of Directive 95/46

Directive 95/46 was incorporated into Spanish law under *Organic Law 15/1999 of 13 December on the Protection of Personal Data* (*Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal*, "**LOPD**").[171]

The *Royal Decree 1720/2007 of 21 December which approves the Regulation Implementing Organic Law 15/1999, of 13 December, on the Protection of Personal Data* (the "**Decree**")[172] consolidates the regulation already in place to implement the LOPD, as well as the precedents established by the national supervisory authority. The Decree also details each aspect of the data protection regime in Spain. It came into force on April 19, 2008.

Specific and regional laws complement the general Spanish data protection regime.

Implementation of Directive 2002/58

Directive 2002/58 was implemented by several acts, notably the *Act 34/2002 of 11 July on Information Society Services and Electronic Commerce*[173] as amended by *Act 32/2003 of 3*

---

170 *Spanish Constitution:* http://www.servat.unibe.ch/icl/sp00000_.html.

171 *Organic Law 15/1999 of 13 December on the Protection of Personal Data (Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal)* available for download at https://www.agpd.es/portalweb/english_resources/regulations/index-iden-idphp.php##.

172 *Royal Decree 1720/2007 of 21 December which approves the Regulation Implementing Organic Law 15/1999, of 13 December, on the Protection of Personal Data;* available for download at https://www.agpd.es/portalweb/english_resources/regulations/index-iden-idphp.php##.

173 *Act 34/2002 of 11 July on Information Society Services and Electronic Commerce;* extracts of the relevant articles are available for download at: https://www.agpd.es/portalweb/english_resources/regulations/index-iden-idphp.php##.

November (State Telecommunications Act),[174] the *Law 56/2007 on measures to boost the information society*.[175]

National Supervisory Authority

The *Agencia Española de Protección de Datos* (the "**AEPD**") is the national data protection supervisory authority.[176]

Ibero-American Data Protection Network (Red Iberoamericana de Protección de Datos)[177]

Spain participates in the Ibero-American Data Protection Network (the "**Network**"). The purpose of the Network is to achieve mutual cooperation and permanent dialogue in the field of data protection between Ibero-American countries. In 2007, at the Annual Summit in Cartagena de Indias, Columbia, the Network issued *Directives for the Harmonization of Data Protection in the Ibero-American Community*.[178]

Definition of "personal data"

The LOPD defines "personal data" as "any information concerning identified or identifiable natural persons" (s. 3 of LOPD). It is closely based on the definition of Directive 95/46.

In the Decree, personal data is defined as "any alphanumeric, graphic, photographic, acoustic or any other type of information pertaining to identified or identifiable natural persons" (s. 5f) of Decree). The Decree introduces or confirms several exceptions to the application of the system of protection of personal data:

- Data regarding legal entities (s. 2.2 of Decree)

---

174 *Act 32/2003 of 3 November (State Telecommunications Act)*; extracts of relevant articles regarding personal data protection are available for download at: https://www.agpd.es/portalweb/english_resources/regulations/index-iden-idphp.php##.

175 *Law 56/2007 on measures to boost the information society;* only available in Spanish at: http://www.glin.gov/download.action?fulltextId=177635&documentId=205409&glinID=205409

176 Agencia Española de Protección de Datos, *English Resources:* https://www.agpd.es/portalweb/english_resources/index-iden-idphp.php.

177 For more information about the structure and purpose of the Ibero-American Data Protection Network, see Ibero-American Data Protection Network, *Strategy document for the Red Iberoaméricana de Protección de Datos*; available for download at: https://www.agpd.es/portalweb/english_resources/regulations/index-iden-idphp.php##.

178 Ibero-American Data Protection Network, *Directives for the harmonization of data protection in the Ibero-American Community*: document available for download at: https://www.agpd.es/portalweb/english_resources/regulations/index-iden-idphp.php##.

- The "business card exception", which excludes the name, functions or jobs performed, as well as the postal or email address and professional telephone and fax numbers of individuals providing services in legal entities(s. 2.2 of Decree).

- Data relating to sole traders, when referring to them as traders, industrialists or ship owners (s. 2.3 of Decree).

- Data regarding the deceased. However, relatives of the deceased may contact the data controller of the deceased's data to inform him of the death. They have to provide sufficient documentary proof and request, where appropriate, erasure of the data (s. 2.4 of Decree).

Email addresses held by individuals (outside of the scope of the business card exception) are personal data for the purposes of the LOPD. The fact that the address may not match the name or country of the holder is not relevant. The rationale behind this qualification is that the individual is easily identifiable. In fact, it would only be necessary to consult the server that manages the service to find out the identity of the owner of an email address, which is linked to a specific domain.[179]

IP addresses are considered personal data for the purposes of the LOPD, following the ECJ decision in *Productores de Música de España (Promusicae) v Telefónica de España SAU*.[180]

Files either maintained by natural persons in the exercise of purely personal or household activities; subject to the legislation on the protection of classified materials; or established for the investigation of terrorism and serious forms of organized crime do not fall within the ambit of the Act (s. 2 of LOPD and s. 13 of Decree). Other types of files are governed by specific provisions (s. 3 of LOPD).

Data subject's consent

Requirements for consent to be valid

Both the LOPD and the Decree **define** the "data subject's consent" as "any free, unequivocal, specific and informed indication of his wishes by which the data subject consents to the processing of personal data relating to him" (s. 3 h) of LOPD; s. 5 (1) d) of the Decree).

Both the LOPD and the Decree set out **specific requirements** for consent to be valid:

---

179 Working Party, *10th Annual Report*, p. 106, see note 143.

180 Case C-275/06 (Judgment of 29 January 2008) /*Reference for a preliminary ruling from the Juzgado de lo Mercantil No 5 de Madrid — Spain/ Productores de Música de España (Promusicae) v Telefónica de España SAU*, available at http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm#caselaw.

- **When requesting the consent of the data subject**, the data controller must include precise information, such as the specific processing or series of processes, the purpose for which the data is collected and the other conditions applying to the processing or series of processes (s. 12 (1) of the Decree).

- **When requesting the consent of the data subject for the assignment of his data**, the must receive the necessary information to unequivocally understand the purpose for which the relevant data is collected and the type of activity performed by the recipient. Otherwise, consent will be considered null and void (s. 12 (2) of the Decree).

- **When the data subject is less than fourteen years old**, the consent of his parents or guardians is required. Other rules apply to the consent for the processing of data of minors (s. 13 of the Decree).

- **When consent is requested for the communication of personal data to third parties**, the data controller must inform the data subject of the purpose for which the data will be used or the type of activity practiced by the person to whom the data is to be communicated. Otherwise, the consent is null and void (s. 11 (3) of LOPD). The consent may be revoked (s. 11(4) LOPD).

- **When consent is required for the processing of sensitive data,** the data subject must be informed that he has the right to deny consent. The consent must be explicit and in writing (s. 7 of LOPD).

- Section 14 of the Decree sets out a **specific procedure for obtaining consent**. Pursuant to this procedure, the data controller may contact the data subject, provide him with specific information and grant him 30 days to object to the processing.

- Special conditions apply to the **request for consent within a contractual relationship** for purposes that have no direct link with the contractual relationship (s. 15 of the Decree), as well as for the processing or disclosure of traffic data in electronic communication services (s. 16 of the Decree).

Other important considerations with regard to consent must be kept in mind:

- The data controller must **prove the fulfillment of his duty to inform** the data subject, and preserve the support on which compliance with the duty to inform is recorded (s. 18 of the Decree).

- The data subject may **revoke** his consent when justifiable grounds for doing so exist. The revocation does not have a retroactive effect (s. 6(3) of LOPD). The revocation must be done through free and simple means, and must not imply payment to the data controller. The data controller must cease the processing of data within ten days from the receipt of the revocation of consent (s. 17 of the Decree).

- The **burden of proving the existence of the data subject's consent** rests with the data controller (s. 12 (3) of the Decree).

Circumstances where the data subject's consent is required

As a general rule, personal data may only be processed or assigned if the data subject has previously given his unambiguous consent, or if another exception applies (e.g. where the data is publicly available) (s. 6 of LOPD and s. 10 of the Decree).

Sensitive data may only be processed if the data subject has given his explicit and written consent to the processing, or if another exception applies (s. 7 of LOPD).

The communication by the data controller to third persons of the personal data subjected to processing is allowed if the data subject has given his consent, or if another exception applies (e.g. the transfer is authorized by law) (s. 11 of LOPD).

An international data transfer to a country that does not provide an adequate level of protection is only admissible if the data subject gives his unambiguous consent to the said transfer, or if another exception applies (s. 34 e) of LOPD).

It is a **serious infringement** to collect personal data without obtaining the explicit consent of the data subject where it is requires (s. 44 (3)c) of LOPD). It is a **very serious infringement** to obtain and process sensitive personal data without the explicit consent of the data subject (s. 44 (4) c) of LOPD).

Highlights of the Spanish Data Protection Regime (under the LOPD and the Decree)

- Both the **data controller** and the **data processor** are responsible for compliance with the LOPD (s. 2 of LOPD) and are subject to the penalties set out in the LOPD (s. 43 if LOPD).
- Any person intending to create or modify files containing personal data must **notify the AEPD**. There is **no exemption to the duty to notify** the AEPD prior to processing the data. (s. 26 of LOPD).
- **Sanctions** for the violation of the LOPD are among the most stringent in the entire EU. They involve heavy fines (s. 45 of LOPD).
    - The LOPD distinguishes between minor, serious, and very serious infringements (s. 44 of LOPD).
- **Sensitive data** may only be processed with the explicit consent of the data subject. Depending on the nature of the data, written consent may be required (s. 7 of LOPD).
    - It remains prohibited to create files solely for the purposes of storing sensitive personal data (s. 7.4 of LOPD).

- With regard to **international data transfers**, prior authorization of the AEPD is needed where a transfer is made to a country that does not ensure an adequate level of protection (s. 33 of LOPD).

- The Decree establishes **very specific security measures.** There are three security levels: basic, medium and high (s. 80 of Decree).

  - When data processing requires medium and high security level, the data controller must **appoint a security officer** (s. 95 of Decree).

- The Decree recognizes **international transfers** using binding corporate rules (s. 70.4 of Decree) and Model Contract clauses (s. 70.2 of Decree). The prior authorization of the AEPD is still needed.

  - The prior authorization of the AEPD is also needed when Model Contract clauses are used.[181]

Significant case law on data protection

Ruling of the Spanish Supreme Court, judgment of April 17, 2007, STS 2778/2007, on the protection of sensitive personal data by a television production company[182]

Facts: In January 2001, the AEPD imposed the highest fine ever given for a violation of the LOPD to Zeppelin Television S.A., the television production company responsible for making *Gran Hermano*, the Spanish version of *Big Brother*. The fine amounted to €1,081,822. For the purposes of selecting the candidates on the show, Zeppelin had collected a significant amount of personal information about each applicant, including sensitive personal data (tastes, ideologies, religious beliefs, race, health, sex life), without obtaining their consent before processing it. Moreover, Zeppelin had assigned the processing of the information to other firms, without ensuring adequate security measures by contract.

Decision: In a judgment of the April 17, 3007, the Supreme Court of Spain judged that the fine had been lawfully imposed. The Court confirmed that Zeppelin had violated:

---

181 On international data transfers in Spain, see also *INSTRUCTION 1/2000, of 1 December 2000 issued by the Data Protection Agency on the rules governing international data movements*; available for download at https://www.agpd.es/portalweb/english_resources/regulations/index-iden-idphp.php##.

182 *Ruling of the Spanish Supreme Court, judgment of 17 April 2007, STS 2778/2007, on the protection of sensitive personal data by a television production company*; Spanish text can be found on the Website of the Spanish Supreme Court: http://www.poderjudicial.es/search/index.jsp; An English Summary is provided in the Working Party, *11th Annual Report*, p. 101, see note 144.

- S. 5 of LOPD for not adequately informing the data subjects about the specifics of the collection and processing of their personal data;
- S. 6 of LOPD for not obtaining proper consent to collect and process the information, especially with regard to sensitive data (s. 7.3 of LOPD);
- S. 11 of LOPD for not obtaining the prior consent of the data subjects before communicating their personal data to third parties (this is a very serious infringement pursuant to 44.4b) of LOPD);
- S. 9 of LOPD for not adopting adequate security measures for the processing of personal information (this is a serious infringement pursuant to 44.3h) of LOPD).

Ruling of the Spanish Constitutional Court, judgment of November 30, 2000, STC 292/2000, recognizing an autonomous fundamental right to the protection of personal data[183]

Facts: The Ombudsman challenged the constitutional validity of specific paragraphs in two sections of the LOPD: s. 21.1 about the communication of data between public administrations; and s. 24. The articles in their original form provided for more exceptions to the right of data subjects in an administrative context. The Ombudsman argued that these provisions violated art. 18.4 of the Spanish Constitution.

Decision: The Constitutional Court found that the paragraphs of the articles at issue were unconstitutional. They were declared null and void. Most notably, the Court recognized the fundamental right to personal data protection as an autonomous right, independent from the right of privacy:

> "the subject protected by the fundamental right to data protection is not solely limited to an individual's private and personal data, but to any kind of personal data, whether strictly private or not, knowledge or use of which by a third party may affect his or her rights, fundamental or otherwise, because it does not solely concern individual privacy, which is protected by Article 18.1 of the Spanish Constitution, but personal data."

Ruling of the Supreme Court, April 27, 2005, on the duty to inform and the registration of data files that do not meet the requisite security standards[184]

---

183 *Ruling of the Spanish Constitutional Court, judgment of November 30, 2000, STC 292/2000, recognizing an autonomous fundamental right to the protection of personal data;* Spanish text can be found on the Website of the Spanish Constitutional Tribunal: http://www.tribunalconstitucional.es/fr/jurisprudencia/Pages/Sentencia.aspx?cod=7467; an English Summary is provided in the Working Party,*Fifth Annual Report*, p. 50, see note 153.

184 *Ruling of the Supreme Court, 27 April 2005, on the duty to inform and the registration of data files that do not meet the requisite security standards*; Summary based on the Working Party, *9th Annual Report*, p. 106, see note 166.

The Court ruled that for the data controller to discharge his duty to inform the data subject under s. 5 of LOPD, a written report was needed. Verbal information was found to be insufficient, in light of the fact that the duty to inform is an inherent part of the fundamental right to data protection.

In this case, security measures were also insufficient, in violation of s. 9 of LOPD.

SWEDEN

Legislative framework

Constitutional protection

Chapter 2 on fundamental rights and freedoms of the *Instrument of Government* (SFS 1974:152)[185] contains provisions that are relevant to the right of privacy:

> **Art. 2.** Every citizen shall be protected in his relations with the public institutions against any *coercion to divulge* an opinion in a political, religious, cultural or other such connection. He shall furthermore be protected in his relations with the public institutions against any coercion to participate in a meeting for the formation of opinion or a demonstration or other manifestation of opinion, or to belong to a political association, religious community or other association for opinion referred to in sentence one.
>
> **Art. 3**. No record in a public register concerning a citizen may be based without his consent solely on his political opinions.
>
> Every citizen shall be protected, to the extent set out in more detail in law, against any *violation of personal integrity resulting from the registration of personal information by means of automatic data processing*.
>
> **Art. 6.** Every citizen shall be protected in his relations with the public institutions against any physical violation also in cases other than cases under Articles 4 and 5. He shall likewise be protected against body searches, house searches and other such *invasions of privacy, against examination of mail or other confidential correspondence, and against eavesdropping and the recording of telephone conversations or other confidential communications.*
>
> **Art. 13.** Freedom of expression and freedom of information may be restricted having regard to the security of the Realm, the national supply

185 Chapter 2 on fundamental rights and freedoms of the *Instrument of Government* (SFS 1974:152); http://www.riksdagen.se/templates/R_PageExtended____6319.aspx.

> of goods, public order and public safety, the good name of the individual, *the sanctity of private life*, and the prevention and prosecution of crime. Freedom of expression may also be restricted in commercial activities. Freedom of expression and freedom of information may otherwise be restricted only where particularly important grounds so warrant.
>
> In judging what restrictions may be introduced by virtue of paragraph one, particular regard shall be had to the importance of the widest possible freedom of expression and freedom of information in political, religious, professional, scientific and cultural matters.
>
> The adoption of provisions which regulate in more detail a particular manner of disseminating or receiving information, without regard to its content, shall not be deemed a restriction of the freedom of expression or the freedom of information.

Implementation of Directive 95/46

In 1998, the Swedish Parliament enacted the *Personal Data Act* (1998:204) ("**PDA**"),[186] which implements Directive 95/46. The *Personal Data Ordinance* (1998:1191) (the "**Ordinance**"),[187] enacted the same day, completes the PDA. The Ordinance names the Data Inspection Board (*Datainspektionen*) (the "**Board**") as the supervisory authority referred to in the PDA. It also delegates to the Board the power to decide some exemptions from the provisions of the PDA, namely with regard to transfers of data to third countries, notification, and prior checking.[188]

Implementation of Directive 2002/58

The *Electronic Communications Act* (2003:389)[189] implements Directive 2002/58. Chapter 6 addresses data protection in the telecommunications sector. The supervisory authority of this act is the National Post and Telecom Agency.

Amendments to the *Marketing Practices Act* (1995:450)[190] were made in order to implement Article 13 of Directive 2002/58 on unsolicited emails. The implementation of the *Marketing Practices Act* is supervised by the Consumer Agency.

National supervisory authority

---

186 *Personal Data Act* (1998:204); available for download at: http://www.datainspektionen.se/in-english/legislation/the-personal-data-act/.

187 *Personal Data Ordinance* (1998:1191); available for download at: http://www.datainspektionen.se/in-english/legislation/the-personal-data-act/.

188 Datainspektionen, *About Us*: http://www.datainspektionen.se/in-english/about-us/,

189 *Electronic Communications Act* (2003:389); http://www.pts.se/upload/Documents/EN/The_Electronic_Communications_Act_2003_389.pdf.

190 *Marketing Practices Act* (1995:450): http://www.wipo.int/clea/en/text_html.jsp?lang=EN&id=3635.

The national supervisory authority is the *Datainspektionen* (Data Inspection Board, the "**DIB**").[191]

Definition of "personal data"

"Personal data" refers to "[all] kinds of information that directly or indirectly may be referable to a natural person who is alive." (s. 3 PDA). This definition is based on the Directive's definition.

- It only applies to living individuals – not legal entities or dead persons.
- It has been interpreted broadly by the Courts.[192] It includes IP addresses.[193]
- Personal data in unstructured material, or processed by a natural person in the course of activities of a purely private nature does not fall within the ambit of the PDA.

Data subject's consent

Requirements for consent to be valid

The PDA **defines** "consent" as "[every] kind of voluntary, specific and unambiguous expression of will by which the registered person, after having received information, accepts processing of personal data concerning him or her" (s. 3).

Consent may **either be in writing, or verbal**.[194]

Consent may be **revoked** at any time (s. 12).

Circumstances where the data subject's consent is required

As a general rule, personal data may only be processed if the data subject has given consent to the processing, or if the processing is necessary for purposes defined in the PDA (s. 10).

---

191 Datainspektionen, *About Us*: http://www.datainspektionen.se/in-english/about-us/, see note 188

192 Data Protected – Linklaters, *Sweden: Personal Data*, https://clientsites.linklaters.com/Clients/dataprotected/Pages/Sweden.aspx#dataquality.

193 Working Party, *11th Annual Report*, p. 106-107, see note 144.

194 Datainspektionen, "Personal Data Protection: Information on the Personal Data Act", p. 11. This document is available for download under "Personal Data Protection Fact Brochure" at http://www.datainspektionen.se/in-english/legislation/the-personal-data-act/.

Sensitive data may only be processed if the data subject has explicitly consented to the processing, or publicized the information in a clear manner (s. 15).

Personal data transfers to third countries that do not ensure an adequate level of protection may take place if the data subject has given his consent to the transfer, or if the transfer is necessary for purposes defined in the PDA (s. 34).

Highlights of the Swedish Data Protection Regime (under the PDA)

- The PDA expressly provides that its provisions will not apply to the extent that they would limit an authority's obligation under Chapter 2 of the *Freedom of the Press Act*[195] to provide personal data (s. 8), or contravene the provisions concerning the **freedom of the press and freedom of expression** contained in the *Freedom of the Press Act or the Fundamental Law on Freedom of Expression*[196] (s. 7).

- With regard to **international data transfers**, the PDA provides that they are permitted if the data is transferred for use only in a state that has acceded to the 1981 Convention (s. 34(2)).

    - The Government (or the supervisory authority) may decide in individual cases on exemptions from the prohibition of transfer of personal data to third countries that do not guarantee an adequate level of protection (s. 35(3)).

- The data subject is entitled to **compensation** from the controller for damages and for the violation of personal integrity that the processing of personal data in contravention of the PDA has caused (s. 48).

- "A **sentence** shall not be imposed in petty cases" (s. 49).

- As of January 1st, 2007, the **"Unstructured Material Rule"** applies. This rule renders most of the provisions of the PDA inapplicable when unstructured material is processed. "Unstructured material" refers to personal data that is not included in or not intended to form part of a structured collection of personal data that is available for searching or compilation according to specific criteria (e.g. sound or images, emails, texts published on the Internet, short or long memoranda, other documents produced with word processing software).[197]

---

195 *Freedom of the Press Act*; http://www.riksdagen.se/templates/R_Page____8908.aspx.

196 *Freedom of the Press Act or the Fundamental Law on Freedom of Expression,* http://www.riksdagen.se/templates/R_Page____8909.aspx.

197 Data Protected – Linklaters, *Sweden,* https://clientsites.linklaters.com/Clients/dataprotected/Pages/Sweden.aspx.

- The provisions of the PDA on security measures apply (s. 30-32).
- It is not necessary to apply the provisions on fundamental requirements for processing personal data (s. 9), permitted processing of personal data (s. 10), information to the person who is registered (s. 23-29) and transfer of personal data to a third country (s. 33-35).
- The main guideline for the processing of unstructured material is that it must not entail a violation of the integrity of the data subject.[198]

Significant case law on data protection

Ruling of the Court of Appeal (Göta hovrätt), April 2004, on the internet publication of personal information about volunteers of a church (Lindqvist) [199]

In 2003, this case was brought before the ECJ for a preliminary ruling on the interpretation of several provisions of Directive 95/46. See p. 53 for full facts, issues, and findings of the ECJ.

Decision: The Swedish Court of Appeal found that Mrs. Lindqvist had indeed contravened to certain provisions of the PDA by publishing personal information without the consent of the individuals concerned. However, the Court ruled that the offence was so trivial that no sentence should be imposed on Mrs. Lindqvist (s. 49 of PDA).[200]

Ruling of the Supreme Administrative Court, 2002, on the disclosure of information by the National Board of Student Aid for the purpose of direct marketing[201]

Facts: The National Board of Student Aid refused to disclose the names and addresses of university students to a company who wanted to send them discount cards. The company

198 Other guidelines may be found in Datainspektionen, "Personal Data Protection: Information on the Personal Data Act", p. 14, see note 194.

199 C-101/01 (judgment of November 6, 2003) / *Reference for a preliminary ruling from the Göta hovrätt (Sweden): Bodil Lindqvist*, see note 114.

200 *Ruling of the Court of Appeal (Göta hovrätt), April 2004, on the internet publication of personal information about volunteers of a church (Lindqvist).* Summary based on the Working Party, *Eighth Annual Report*, p. 103-104, see note 115.

201 *Ruling of the Supreme Administrative Court, 2002, on the disclosure of information by the National Board of Student Aid for the purpose of direct marketing.* Summary based on the Working Party, *Seventh Annual Report on the situation regarding the protection of individuals with regard to the processing of personal data in the European Union and in third countries - covering the year 2004*, pp. 78-79; available for download at: http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/annual_reports_en.htm.

complained to the DIB. The DIB found that the processing of the students' information by the company would be unlawful under s. 10(f) of the PDA, as the students' interest of privacy outweighed the company's commercial interest. The County Administrative Court and the Administrative Court of Appeal were of the same opinion.

Issue: Should the National Board of Student Aid disclose the names and addresses of students for direct marketing purposes ?

Decision: The Supreme Administrative Court decided that the National Board of Student Aid should disclose the names and addresses of the students for direct marketing purposes. In fact, the marketing literature was only sent two times a year, and the personal data asked for was not sensitive. The Court added that the students can always oppose the direct marketing under s. 11 of the PDA.

Ruling of the Supreme Court (Högsta domstolen), judgment of June 12, 2001, Case B 293-00, on the publication of derogatory comments on the Internet[202]

Facts : A businessman published insulting assessments on his website about particular Swedish banks and several named individuals working in these banks. This was part of a campaign he initiated to spread information about alleged malpractice in the Swedish banking system.

Both the City Court of Stockholm and the Court of Appeal sentenced the man primarily for having transmitted personal data to foreign countries by publishing it on his website, in violation of s. 33 of PDA.

Issue: Did the publishing of highly derogatory comments by the businessman on his website constitute a violation of the PDA, or was it covered by the exemption for journalistic purposes or artistic or literary expression (s. 7 of PDA) ?

Decision: The journalistic purposes exception provided for in s. 7 of PDA was found to apply. The Supreme Court unanimously judged that the purpose of the website was to inform, criticize and raise awareness on societal questions that are of larger significance for the general public. The fact that the businessman was not a professional journalist did not matter, as there was a journalistic purpose to the publishing.

UNITED KINGDOM ("UK")

Legislative framework

---

202 *Ruling of the Supreme Court (Högsta domstolen), judgment of June 12, 2001, Case B 293-00, on the publication of derogatory comments on the Internet.* Summary based on Lee A Bygrave, "Balancing data protection and freedom of expression in the context of website publishing — recent Swedish case law" (2001) PLPR 40; available at: http://www.austlii.edu.au/au/journals/PLPR/2001/40.html and the Working Party, *Sixth Annual Report*, p. 67, see note 161.

Constitutional protection

Since the UK does not have a written constitution, the generic concept of a "constitutional right" was not recognized until the adoption of the *Human Rights Act* ("**HRA**")[203] in 1998.[204] The HRA came into force on October 2, 2000. It incorporates the *European Convention on Human Rights*[205] into UK Law. Articles 8 and 10 of the HRA are relevant:

> **Article 8 Right to respect for private and family life**
>
> 1. Everyone has the right to respect for his private and family life, his home and his correspondence.
>
> 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.
>
> **Article 10 Freedom of expression**
>
> 1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.
>
> 2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.

Implementation of Directive 95/46

---

203 *Human Rights Act*; http://www.opsi.gov.uk/ACTS/acts1998/plain/ukpga_19980042_en.

204 Hendrickx, F., *Employment Privacy Law in the European Union: Surveillance and Monitoring*, (New York: Intersentia, 2002), p. 257.

205 *European Convention on Human Rights*; http://conventions.coe.int/treaty/en/Treaties/Html/005.htm.

Directive 95/46 was transposed into UK law by the *Data Protection Act 1998* ("**DPA**"),[206] which came into force on March 1, 2000. The DPA also implements the principles of the OECD Guidelines,[207] and the 1981 Convention.[208]

The DPA only sets out the general principles of the Directive. There is extensive secondary legislation that details the UK data protection regime.

Implementation of Directive 2002/58

The *Privacy and Electronic Communication Regulations*[209], which came into effect on December 11, 2003, implemented the Directive 2002/58 into UK law.

National supervisory authority

The national supervisory authority is the Information Commissioner.[210]

Tort of breach of confidence

- The tort of breach of confidence applies to the misuse of private information. A duty of confidence arises when "the party subject to the duty is in a situation where he knows or ought to know that the other person can reasonably expect his privacy to be protected."[211]

A useful practical test to determine whether information is private consists in asking whether a reasonable person with ordinary sensitivity would find the disclosure or observation of information or conduct highly offensive. The simple fact that the activity is not done in public does not automatically make it private.[212] This test does not apply when the information is obviously of a private nature.

---

206 *Data Protection Act 1998*; http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1.

207 *OECD Guidelines*, see note 7.

208 *1981 Convention*, see note 67.

209 *Privacy and Electronic Communication Regulations*; http://www.opsi.gov.uk/si/si2003/20032426.htm.

210 Information Commissioner's Office, *ICO*: http://www.ico.gov.uk/.

211 *Campbell v MGN Ltd.*, [2004] UKHL 22, para. 85; http://www.bailii.org/uk/cases/UKHL/2004/22.html. See summary of this case at p. 98.

212 Gleeson CJ in *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 185 ALR 1 p. 11-12, paras 34-35, quoted at para. 93; *Campbell v. MGN Ltd* see note 211.

Definition of "personal data"

Even though the DPA's definition of "personal data" is closely based on the definition found in Directive 95/46, the UK is said to be out of step in practice.[213]

> Article 1
>
> "data" means information which—
>
> (a) is being processed by means of equipment operating automatically in response to instructions given for that purpose,
> (b) is recorded with the intention that it should be processed by means of such equipment,
> (c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system, or
> (d) does not fall within paragraph (a), (b) or (c) but forms part of an accessible record as defined by section 68;
>
> "personal data" means data which relate to a living individual who can be identified—
>
> (a) from those data, or
> (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,
> and 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;

Certain types of personal data benefit from exemptions under the Act, such as personal information processed for the purpose of national security (s. 28), crime and taxation (s. 29), health, education and social work (s. 30), regulatory activity (s. 31), journalism, literature and art (s. 32), research, history and statistics (s. 33); domestic activities (s. 36); information available to the public by or under enactment (s. 34); and disclosures required by law or made in connection with legal proceedings (s. 35).

In *Durant v. Financial Services Authority*,[214] the Court took a narrow approach to the concept of personal data.

The Information Commissioner subsequently adopted a much broader view of the concept of personal data.[215]

---

213 Data Protected – Linklaters, *What is Personal Data ?*, see note 149.

214 *Durant v Financial Services Authority*, [2003] EWCA Civ 1746 http://www.bailii.org/ew/cases/EWCA/Civ/2003/1746.html.

215 For more information on the definition of personal data for the purposes of the DPA, see two documents published by the Information Commissioner on this matter: Information Commissioner's Office, "Determining what is Personal Data" (2007) and Information Commissioner, "Determining what

Data subject's consent

Requirements for consent to be valid

The Act does not define the notion of consent.

Circumstances where the data subject's consent is required

As a general rule, the processing of any personal data may only take place if the data subject consents to the processing, or if the processing is necessary for the purposes defined in the Act (Schedule 2, s. 1 and 2 of the Act).

The same rule applies to the **processing of sensitive personal data** (Schedule 3 of the Act), and the **transfer of personal information** to countries that do not ensure an adequate level of protection (Schedule 4 of the Act).

Highlights of the UK Data Protection Regime (under the DPA)

- The DPA sets out additional exceptions under which **sensitive data** (defined at s. 2) may be processed, such as the processing of sensitive data as to ethnic or racial origin for the purpose of reviewing equal treatment opportunities (Schedule III).
- **The data subject's right of access** is limited where the data controller is a credit reference agency (s. 9).
- **The "right to prevent"** (right to object to the processing of personal data) can be exercised if the processing is likely to cause damage or distress, or if the processing is made for the purposes of direct marketing (s. 10-11).
- A data subject may obtain the **rectification, blocking, erasure and destruction** only if a court is satisfied that the data is inaccurate (s. 14).
- The Information Commissioner does not need to be notified of or to give his consent to **international data transfers**, and to the use of Model Contract Clauses.
    - The use of binding corporate rules in the UK has been approved by the Information Commissioner.[216]

Information is Data for the purposes of the DPA" (2009), both available for download at http://www.ico.gov.uk/about_us/news_and_views/current_topics/what_is_data_DPA_purposes.aspx.

216 See Information Commissioner's Office, "Binding Corporate Rules Authorisation" (2009); available for download at: http://www.ico.gov.uk/tools_and_resources/document_library/data_protection.aspx.

- **Violations of the DPA** may entail civil liability or criminal sanctions, including unlimited fines.
    - Breaching a data principle is not a criminal offence, but may result in an Enforcement Notice, the breach of which is a criminal offence (s. 40).
    - Amendments to the DPA have been made to increase the sentence to two years of imprisonment for unlawfully obtaining or disclosing personal data. They also allow the Information Commissioner to impose an administrative fine in serious cases. These amendments are not yet in force.[217]

Significant case law on data protection

Durant v Financial Services Authority [2003] EWCA Civ 1746[218]

Facts: Mr. Durant sought disclosure of what he claimed to be personal data related to him, held by the Financial Services Authority ("**FSA**"). The request was made under s. 7 of the DPA, and concerned information that was contained in both manual and electronic files. The information pertained to a litigation between Mr. Durant and a bank. The FSA provided the information held in the electronic files, but not in the manual files. The FSA claimed that the information held in the manual files was not personal data for the purposes of the PDA.

Issue: Four issues were dealt with, but only the first two deserve special attention: **(1)** What is personal data for the purposes of s. 1(1) of the PDA ? **(2)** What is meant by "relevant filing system" in s. 1(1) of the PDA ?

Decision: (1) The Court adopted a narrow approach to the definition of personal data, which excludes the information sought by Mr. Durant. The Court ruled that to constitute personal data, the information must be (a) biographical in a significant sense; (b) focused on the data subject rather than on some other person. In short, the information should affect the person's privacy, whether in his personal or family life, business or professional capacity (para. 26).

(2) The manual files in this case were not part of a "relevant filing system", so they fall outside of the scope of the DPA. To be a relevant filing system, "a manual filing system must: 1) relate to individuals; 2) be a "set" or part of a "set" of information; 3) be structured by reference to individuals or criteria relating to individuals; and 4) be structured in such a way that specific information relating to a particular individual is readily accessible" (para. 46).

* Leave to appeal to the House of Lords was refused, thereby confirming the decision of the Court of Appeal.[219]

---

217 Data Protected – Linklaters, *United Kingdom: Enforcement*: https://clientsites.linklaters.com/Clients/dataprotected/Pages/UnitedKingdom.aspx#enforcement.

218 *Durant v Financial Services Authority*, see note 214.

Johnson v Medical Defence Union [2007] EWCA Civ 262[220]

Fact: Mr. Johnson claimed damages for the allegedly unfair withdrawal of his insurance cover and professional support, previously enjoyed under his membership with the Medical Defence Union ("**MDU**"). It was admitted, as a matter of contract and domestic law that the MDU had complete discretion over the termination of Mr. Johnson's membership. However, since the information was held on a computer, Mr. Johnson claimed damages under the DPA. In fact, Mr. Johnson did not contest the decision of the MDU itself. Rather, he argued that the processing by the MDU of the information that led to the decision to terminate his membership was unfair. The specific act of processing claimed to be unfair was "[selecting] the information contained in the personal data and thereby presenting a false picture of the situation" (para. 21). It is important to note that this claim is only possible because the information was held on a computer.

Issue: Does the DPA apply ?

Decision: *Lord Justice Buxton:* The selection of data from Mr. Johnson's file did not constitute a processing of data for the purposes of the DPA. Even if it did, the processing was not unfair. Further, even if the processing had been unfair, it would not have affected the MDU's decision to revoke Mr. Johnson's membership. If Mr. Johnson had had a right to damages under s. 13 of the DPA, he could only have been granted distress damages corresponding to a pecuniary loss.

Lady Justice Arden : The selection and presentation of personal data about Mr Johnson constituted processing under the PDA. However, the processing was not unfair.

Lord Justice Longmore : The DPA does not extend to the selection of personal information by a human being, even if this information is put into an automated system.

Campbell v MGN Ltd. [2004] UKHL 22[221]

Facts: The *Mirror* newspaper published photographs of Naomi Campbell as she came out of a Narcotics Anonymous meeting. The accompanying article revealed details about Ms. Campbell's drug addiction and treatment. Ms. Campbell had previously made public statements, denying her drug addiction. Ms. Campbell initiated proceedings against MGN Ltd, the publisher of the *Mirror*. The *Mirror* responded by publishing offensive articles.

Ms. Campbell claimed damages for breach of confidence and compensation under the DPA. The High Court awarded her £2,500 plus £1,000 aggravated damages in respect of both claims.[222] The Court of Appeal reversed the judgment.[223]

---

219 Out-Law.com, *House of Lords ends Durant's data protection saga:* http://www.out-law.com/page-6405.

220 *Johnson v Medical Defence Union* [2007] EWCA Civ 262: http://www.bailii.org/ew/cases/EWCA/Civ/2007/262.html.

221 *Campbell v MGN Ltd*. see note 211.

Issue: Is MGN Ltd liable for breach of confidence for the publication of photographs and disclosure of details about Ms. Campbell's treatment ?

* The fact that the journalists disclosed that Ms. Campbell had a drug addiction was not at issue, as journalists have the right to set the record straight when people make public statements.

Decision: The House of Lords allowed Ms. Campbell's appeal by a majority of 3 (Lords Hope of Craighead and Carswell, and the Baroness Hale of Richmond) to 2 (Lord Nicholls of Birkenhead and Hoffmann). The decision of the High Court was restored.

The *majority* decided that the information about Ms. Campbell's treatment was private, and entailed a duty of confidence for the *Mirror*. To make this determination, the Court emphasized that it was important to take the context into account, which meant considering the sensitivities of a drug addict receiving treatment. Disclosure of information and public scrutiny may disrupt the treatment. The Court found that Ms. Campbell's right under s. 8 of the HRA (right to privacy) had been infringed, and that it could not be justified by MGN Ltd.'s right under s. 10 of the HRA (freedom of expression). Accordingly, the majority found that MGN Ltd. was liable for breach of confidence.

The *dissenting* judges found that the details about Ms. Campbell's treatment were in the public domain, since it was already publicly known that she had a drug addiction. At most, the intrusion in Ms. Campbell's life was minor. The interest of the journalists was also found to prevail over Ms. Campbell's right to privacy.

---

222 *Campbell v Mirror Group Newspapers*, [2002] EWHC 499 (QB): http://www.bailii.org/ew/cases/EWHC/QB/2002/499.html.

223 *Naomi Campbell v MGN Ltd.* [2002] EWCA Civ 1373: http://www.bailii.org/ew/cases/EWCA/Civ/2002/1373.html.

ASIA-PACIFIC REGION

I. MAIN REGIONAL INITIATIVES

A. PRELIMINARY REMARKS

There have been very few serious attempts to harmonize the data protection regime of the Asian-Pacific countries. The APEC Privacy Framework,[224] adopted in 2004, failed to unify the data protection standards in the APEC Member Economies. This instrument sets out general principles with regard to the protection of personal information. However, the actual impact of the APEC Privacy Framework is highly debatable (part **B**). The Association of South East Asian Nations has a project to develop a harmonized legal framework with regard to data protection in the field of e-commerce by 2015. However, only a limited number of countries are targeted by this initiative (part **C**).

B. APEC PRIVACY FRAMEWORK

1. General remarks

The APEC Privacy Framework (the "**Framework**")[225] was adopted in November 2004 at the APEC meeting in Santiago, Chile. The Framework was modified in September 2005 to address cross-border data transfers, at the second APEC Implementation Seminar held in Kyongju, South Korea. The Framework is divided into four parts: (i) preamble ; (ii) scope ; (iii) APEC information privacy principles (the "**Principles**"); (iv) implementation.

The Framework addresses personal information protection with a view to promoting electronic commerce throughout the Asia-Pacific region. It is modeled on the OECD Guidelines. It focuses both on the domestic and international implementation of the Principles.

The Framework promotes a flexible approach to privacy issues. It aims at providing clear guidance and direction to businesses in APEC economies. It is non-prescriptive.

The Framework accounts for the great disparities in the social, cultural, economic and legal backgrounds of the APEC economies. Section 12 specifies that there should be great flexibility in implementing the Principles set out by the Framework. Moreover, the Framework is not very restrictive when it comes to carving out exceptions to the Principles. Section 13 only provides that exceptions, including those relating to national sovereignty, national security, public safety

---

224 *APEC Privacy Framework,* see note 4.

225 *APEC Privacy Framework,* see note 4.

and public policy should be limited and proportional to meeting the objectives to which the exceptions relate, and be made known to the public or in accordance with the law.

There are 21 Member economies in the APEC.[226]

2. Definition of "personal information" under the Framework

Section 9 of the Framework defines "personal information" as "any information about an identified or identifiable individual".

- In the commentary to the section, it is specified that only the information about natural persons is concerned, and not information about legal entities.
- Information that does not meet this criteria alone, but which together with other information, would allow to identify an individual, is also covered.
- It is important to keep in mind that Member economies may make exceptions to this definition pursuant to s. 13.

3. Consent of the individual concerned

a) Requirements for consent to be valid

The Framework does not define the notion of consent. It is up for the Member economies to circumscribe the notion and set requirements for consent to be valid.

b) Circumstances where the data subject's consent is required

As a general rule, information should be collected with notice to, or with the consent of the individual concerned, but only where appropriate (s. 18).

Information may be used for **purposes that are incompatible or irrelevant to the ones for which it was collected if the individual concerned has consented**, if it is necessary to provide a service or a product at the request of the individual concerned, or if it is authorized by law (s. 19).

The controller of personal information should obtain the consent of the individual concerned before any **transfer of personal information**, whether domestic or international (s. 26).

---

226 The 21 Member economies of the APEC are: Australia, Brunei Darussalam, Canada, Chile, People's Republic of China, Hong Kong, China, Indonesia, Japan, Republic of Korea, Malaysia, Mexico, New Zealand, Papua New Guinea, Peru, The Philippines, Russia, Singapore, Chinese Taipei, Thailand, The United States, Viet Nam. List available at: http://www.apec.org/apec/member_economies.html.

4. APEC information privacy principles

The Principles set out in the Framework may be summarized as follows:

- Principle I: Preventing Harm. Personal information protection should be designed to prevent the misuse of such information. Remedies for privacy infringements are to be proportionate to the likelihood and severity of the risk of harm.

- Principle II: Notice. Personal information controllers should provide certain information about their practice and policies in a clear and accessible way. They must take all reasonable steps to provide notice to the individuals concerned before or at the time of the collection, or as soon after as is practicable.

- Principle III: Collection Limitation. The collection of information should be limited to what is relevant to the purposes of the collection. The collection should be performed using fair and lawful means and, when appropriate, with notice to or consent of the individual concerned.

- Principle IV: Uses of Personal Information. Personal information collected should be used only for the purposes of the collection and other compatible or related purposes. However, it may be used otherwise if: the individual concerned gives his consent, the use is necessary to provide a service or product requested by the individual, or it is prescribed by law.

- Principle V: Choice. Individuals should be provided with mechanisms to exercise choice with regard to the collection, use and disclosure of their personal information. An exception is made for publicly available information.

- Principle VI: Integrity of Personal Information. Personal information should be accurate and complete. It should also be kept up-to-date to the extent necessary for the purposes of the use.

- Principle VII: Security Safeguards. Personal information controllers should ensure appropriate safeguards, proportional to the risk and severity of harm, the sensitivity of the information and the context in which it is held.

- Principle VIII: Access and Correction. Individuals should be given rights to access their personal information, challenge its accuracy and have it corrected. Such rights may not be granted where it would be unreasonable to do so, where the information is confidential or where it would violate the privacy of others.

- Principle IX: Accountability. Personal information controllers are accountable to comply with measures implemented to give effect to the Principles. In the context of a domestic or international transfer of personal information, the controller should obtain the consent of the individual concerned and take reasonable steps to make sure that the recipient will protect the information in accordance with the Principles.

5. Guidance for domestic and international implementation

The Framework suggests ways in which the Principles could be implemented into the national law of the Member Economies. It calls for cooperation between public and private sectors for domestic implementation. It also encourages the cooperative development of Cross-Border Privacy Rules ("**CBPR**"). It is important to note that the Framework only provides suggestions, and no prescriptions for the implementation of the Principles.

6. Pathfinder Projects

The Framework is complemented by nine Pathfinder Projects, which were formally endorsed at the meeting in Sydney in September 2007. A "Pathfinder" is an APEC term referring to a plan to which all Member economies have agreed for the development and implementation of a specific project within or between all economies.

The nine Pathfinder Projects are:

1. Self-assessment guidelines for business;
2. Trust-mark (accountability agents) guidelines;
3. Compliance review process of CBPR;
4. Directories of compliant organizations;
5. Contact directories for data protection authorities and privacy contact officers within economies, as well as with accountability agents;
6. Templates for enforcement cooperation arrangements;
7. Templates for cross-border complaint handling forms;
8. Guidelines and procedures for responsive regulation in CBPR systems, and
9. A pilot program that can test and implement the results of the projects leading to the testing of a complete system.[227]

Six APEC economies have chosen not to participate in any of the nine Pathfinder Projects, namely Chile, Indonesia, Malaysia, Papua New Guinea, Russia and Brunei.

---

227 APEC Data Privacy Projects Implementation Work Plan: available at http//aimp.apec.org/documents/2008/ECSG/ESCG1/08_ecsgl_024.doc

7. Weaknesses and criticisms of the Framework

The Framework has been the subject of criticisms by many commentators.[228]

The Framework has been mainly criticized for setting standards that are too weak and potentially retrograde. For the APEC economies that already had privacy laws, the APEC Framework has been of no positive domestic significance (Australia, Canada, New Zealand, Hong Kong, Macao, Japan, South Korea). Moreover, the APEC economies which are currently drafting privacy laws use Directive 95/46 as a model, and not the Framework.

The non-prescriptive nature of the Framework was also denounced. In fact, the Framework exhorts the APEC economies to implement the Principles, without requiring any particular means of doing so. Moreover, no means of assessment has been developed.

The fact that the Framework has completely ignored the EU standards of adequacy in the context of international data transfers is also criticized.

C. ASSOCIATION OF SOUTH EAST ASIAN NATIONS (ASEAN) HARMONIZATION

The ASEAN is committed to the establishment of an integrated ASEAN Community (AEC) by 2015. Part of this project concerns the setting up of a harmonized legal infrastructure for e-commerce. The adoption of guidelines and best practices for data privacy is one of the targets.[229]

The members countries of the ASEAN are Brunei, Cambodia, Indonesia, Laos, Malaysia, Myanmar, Philippines, Singapore, Thailand and Vietnam.[230]

II. NATIONAL DATA PROTECTION REGIMES[231]

---

228 For critical evaluations of the Framework, see Graham Greenleaf, "Five years of the APEC Privacy Framework: Failure or Promise" (2009) 25 Computer Law & Security Review 28; Gabriela Kennedy, Sarah Doyle, Brenda Lui and Contributors, "Data Protection in the Asia-Pacific region" (2009) 25 Computer Law & Security Review 59; Chris Connolly, "Asia-Pacific Region at the Privacy Crossroads" (2008) Galexia; available for download at: http://www.galexia.com/public/research/assets/asia_at_privacy_crossroads_20080825/.

229 Association of Southeast Asian Nations, *Strategic Schedule for ASEAN Economic Community*, http://www.aseansec.org/21161.pdf.

230 Association of Southeast Asian Nations, *Member Countries*: http://www.aseansec.org/74.htm.

A. PRELIMINARY REMARKS

The personal information protection laws of Asian-Pacific countries are very disparate. This heterogeneity may be attributed to the fact that countries of this region are at very different stages of their legal, social, economic and cultural development. The increasing importance of e-commerce and of business outsourcing opportunities triggered a legislative proliferation in the field of personal information protection in Asia-Pacific countries.

In this section, we will address the legal framework surrounding to the protection of personal information in countries that have adopted privacy legislation (Australia, Hong Kong, Japan, Macao, New Zealand, South Korea and Taiwan) (part **B**); countries that are in the process of drafting privacy legislation (China, Malaysia, the Philippines and Thailand) (part **C**); countries that only have privacy provisions in sector-specific legislation (Indonesia, Singapore, Vanuatu, and Vietnam) (part **D**); and countries that do not have any privacy laws (Brunei, Cambodia, Laos, Myanmar and the majority of the small Pacific Island countries) (part **E**). We will also address the case of India, which is not an Asia-pacific country.

B. COUNTRIES THAT HAVE ADOPTED PRIVACY LEGISLATION

1. AUSTRALIA

a) Constitutional protection

There are no express provisions relating to privacy in the *Commonwealth of Australia Constitution Act*[232] nor the Constitutions of the six States and two Territories of Australia.[233]

b) The main piece of legislation: the Privacy Act 1988

Privacy protection in Australia is primarily governed by the *Privacy Act 1988* (the "**Act**").[234] Two sets of regulations have been issued under the Act.[235]

---

231 This section is mainly based on Gabriela Kennedy, Sarah Doyle, Brenda Lui and Contributors, "Data Protection in the Asia-Pacific region" and Chris Connolly, "Asia-Pacific Region at the Privacy Crossroads", see note 228; Freshfields Bruckheus Deringer "Data Privacy Protection Across Asia: a regional perspective" (2008), http://www.freshfields.com/publications/pdfs/2008/oct.08/24238.pdf.

232 *Commonwealth of Australia Constitution Act*: http://www.austlii.edu.au/au/legis/cth/consol_act/coaca430/.

233 Privacy International, *PHR2006-Australia*: http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-559550.

234 *Privacy Act 1988;* available for download at http://www.comlaw.gov.au/comlaw/Legislation/ActCompilation1.nsf/0/98DF083E9BFEA5CBCA2575C500021052?OpenDocument.

The national privacy regulator is the Privacy Commissioner.[236]

(1) Definition of "personal information" under the Act

For the purposes of the Act, "personal information" refers to "information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion" (s. 6).

Personal information related to employee records (s. 7B(3)), journalism (s. 7B(4)), or personal, family or household affairs (s. 16E) is exempt from the application of the privacy principles laid out in the Act.

(2) Consent of the individual concerned

Requirements for consent to be valid

The Act does not give many details about the requirements for consent to be valid. It only says that consent may be express or implied (s. 6).

Circumstances where the data subject's consent is required

Unless another exception applies, a record-keeper or an organization must obtain the consent of the individual concerned if it wishes to:

- Use the information for another purpose than the one for which it was collected (s. 14, Principle 10; Schedule 3, s. 2)
- Disclose the information to a third party (s. 14, Principle 11).
- Transfer the personal information to another country (Schedule 3, s. 9).
- Process sensitive information (Schedule 3, s. 10).

Specific consent requirements apply to small businesses or operators (s. 6D).

(3) National Privacy Principles

The Act was amended in 2001 to include ten National Privacy Principles ("**NPPs**") (Schedule 3 of the Act). These principles deal with collection, use and disclosure, data quality, data security,

---

235 For more information, see The Office of the Privacy Commissioner, *Privacy Act Regulations:* http://www.privacy.gov.au/act/Regulations/index.html.

236 Office of the Privacy Commissioner, *Australian Government – Office of the Privacy Commissioner:* http://www.privacy.gov.au/

openness, access and correction, identifiers, anonymity, transborder data flows and sensitive information.

(4) Highlights of the Act

- **Small businesses** benefit from many exemptions under the Act and only need to comply with certain parts of the Act. However, they may voluntarily decide to conform to the privacy coverage offered under the Act (s. 6EA).

- **Transfers of personal data to foreign countries** is prohibited unless one of the 6 exceptions set out in s. 9 of Schedule 3 apply. For example, an organization may transfer data if the recipient of the information is bound by personal information handling principles similar to the NPPs.

    - Please note that, unlike in New Zealand, the transferring organization will not be held accountable for the protection of the personal information held by the recipient.

    - In its 2008 Report, the Australian Law Reform Commission suggested that a broad accountability requirement of the transferring organization should be introduced.[237]

- **Offences** under the Act are punishable by imprisonment for up to 12 months, and fines of up to $150,000.

c) Protection under Privacy Codes

Under the Act, companies may apply for approval of their Privacy Code. Once approved, the Privacy Code applies instead of the National Privacy Principles for the organizations bound by the Code (s. 16A). The following codes have been approved by the Privacy Commissioner:

- *Market and Social Research Privacy Code* (2003);[238]

- *Queensland Club Industry Privacy Code* (2002);[239]

- *Biometrics Institute Privacy Code* (2006).[240]

---

237 Australian Law Reform Commission, "ALRC Report 108 For Your Information: Australian Privacy Law and Practice" (2008) vol. 2 at para. 31-95: http://www.austlii.edu.au/au/other/alrc/publications/reports/108/31.html#Heading325

238 *Market and Social Research Privacy Code* (2003); available for download at: http://www.amro.com.au/index.cfm?p=2403.

239 *Queensland Club Industry Privacy Code* (2002); available for download at: http://www.clubsqld.com.au/www/index.cfm?itemid=224.

d) Protection under the common law

The tort of breach of confidence may also be relied upon.[241]

2. HONG KONG

a) Constitutional protection

The *Basic Law of the Hong Kong Special Administrative Region of the People's Republic of China*[242] provides some privacy protection:

> **Article 30**
>
> The freedom and privacy of communication of Hong Kong residents shall be protected by law. No department or individual may, on any grounds, infringe upon the freedom and privacy of communication of residents except that the relevant authorities may inspect communication in accordance with legal procedures to meet the needs of public security or of investigation into criminal offences.

b) Main piece of legislation : the Personal Data (Privacy) Ordinance

(1) General information

Hong Kong has established a comprehensive data protection regime in the *Personal Data (Privacy) Ordinance* (the "**Ordinance**").[243] It came into force on December 20, 1996. The Ordinance covers both the public and private sector.

The Ordinance is broadly aligned on Directive 95/46. However, it has not included any registration requirements for businesses.[244]

---

240 *Biometrics Institute Privacy Code* (2006); available for download at: http://www.biometricsinstitute.org/displaycommon.cfm?an=1&subarticlenbr=8.

241 Gabriela Kennedy, Sarah Doyle, Brenda Lui and Contributors, "Data Protection in the Asia-Pacific region" and Chris Connolly, "Asia-Pacific Region at the Privacy Crossroads", see note 228; Freshfields Bruckheus Deringer "Data Privacy Protection Across Asia: a regional perspective", see note 231.

242 *The Basic Law of the Hong Kong Special Administrative Region of the People's Republic of China*: http://www.basiclaw.gov.hk/en/basiclawtext/chapter_3.html

243 *Personal Data (Privacy) Ordinance*: http://www.pcpd.org.hk/english/ordinance/ordfull.html.

244 Gabriela Kennedy, Sarah Doyle, Brenda Lui and Contributors, "Data Protection in the Asia-Pacific region" and Chris Connolly, "Asia-Pacific Region at the Privacy Crossroads", see note 228; Freshfields Bruckheus Deringer "Data Privacy Protection Across Asia: a regional perspective", see note 231.

(2) Definition of "personal data" under the Ordinance

Section 2 of the Ordinance defines "personal data" as "any data

> (a) relating directly or indirectly to a living individual;
> (b) from which it is practicable for the identity of the individual to be directly or indirectly ascertained; and
> (c) in a form in which access to or processing of the data is practicable"

Personal information held by an individual for domestic purposes falls outside of the ambit of the Ordinance (s. 52). Other types of information are partly exempt from the application of certain provisions of the Ordinance, such as information relevant to staff planning (s. 53), personal references (s. 56), health (s. 59), legal professional privilege (s. 60), news (s. 61), statistics and research (s. 62) and human embryos (s. 63A). There are other partial exemptions relevant for the public sector (s. 57, 58, 58A).

(3) Data subject's consent

Requirements for consent to be valid

To be valid, consent must be express and given voluntarily (s. 1 (3)). Consent may be withdrawn by written notice (s. 1 (3)).

Circumstances where the data subject's consent is required

Before personal data may be used for a purpose other than the one for which it was originally collected or a directly related purpose, the data subject must give his consent (Schedule 1, s. 3).

Matching procedures may not be carried out, except with the consent of the data subjects or if another exception applies (s. 30).

A **personal data transfer** outside of Hong Kong may only take place if the consent of the individual is obtained, or if another exception applies (s. 33 (2) (c) – this provision is not yet in force).

(4) Highlights of the Ordinance

- The Ordinance establishes the **Privacy Commissioner for Personal Data** ("**PCPD**") as the national supervisory authority (s. 5).[245]

- S. 33 of the Ordinance on **international data transfers** is not yet in force. When it will come into effect, it will prohibit international data transfers to third countries unless, among other conditions, the data subject has given his consent, or the third country has

---

245 Office of the Privacy Commissioner for Personal Data, Hong Kong, *The Role of the PCPD*: http://www.pcpd.org.hk/english/about/role.html.

data protection laws which are substantially similar to, or serve the same purposes as, the Ordinance. The former Privacy Commissioner stated that s. 33 is still inoperative because is would be ‘‘rather imprudent for Hong Kong to ‘jump the gun’ on the matter of trans-border data flows and ‘go it alone’’’ [sic].[246]

- The Ordinance defines a variety of **offences**, which are sanctioned by fines and imprisonment of up to two years (s. 64-66).

c) Protection under sector-specific laws and codes of conduct

Various laws and codes of conduct supplement the Hong Kong data protection regime.

For example, in the banking sector, the *Hong Kong Monetary Authority Supervisory Policy Manual (Guideline IC-1)*[247] and the *Securities and Futures Commission's Management Supervision and Internal Control Guidelines*[248] contain relevant provisions with regard to data protection.

In the electronic communications sector, the *Unsolicited Electronic Messages Ordinance*[249] regulates the use of commercial electronic messages. It came into force in 2007.

d) Common law torts

The tort of breach of confidence may be invoked by data subjects when the conditions are met.

In the banking sector, there is a general common law rule that implies a term in contracts between banks and their customers which imposes a duty of confidentiality on the bank with regard to its customers' information. Liability may ensue from a breach of this implied term.[250]

3. JAPAN

a) Constitutional protection

---

246 Gabriela Kennedy, Sarah Doyle, Brenda Lui and Contributors, "Data Protection in the Asia-Pacific region", p. 63, see note 228.

247 *Hong Kong Monetary Authority Supervisory Policy Manual (Guideline IC-1):* http://www.info.gov.hk/hkma/eng/bank/spma/index.htm.

248 *Securities and Futures Commission's Management Supervision and Internal Control Guidelines:* www.sfc.hk/sfcRegulatoryHandbook/EN/displayFileServlet?docno=H196.

249 *Unsolicited Electronic Messages Ordinance*: http://www.hklii.org/hk/legis/en/ord/593/.

250 Gabriela Kennedy, Sarah Doyle, Brenda Lui and Contributors, "Data Protection in the Asia-Pacific region" and Chris Connolly, "Asia-Pacific Region at the Privacy Crossroads", see note 228; Freshfields Bruckheus Deringer "Data Privacy Protection Across Asia: a regional perspective", see note 231.

The right of privacy in Japan is based on general provisions of tort law and article 13 of the Constitution of Japan:[251]

> **Article 13**
> All of the people shall be respected as individuals. Their right to life, liberty, and the pursuit of happiness shall, to the extent that it does not interfere with the public welfare, be the supreme consideration in legislation and in other governmental affairs.

b) Main piece of legislation: the Act on the Protection of Personal Information

(1) General remarks

The main piece of legislation with regard to data protection in Japan is the *Act on the Protection of personal information* (the "**APPI**").[252] The APPI was enacted on May 30, 2003. It follows a comprehensive approach to personal information protection. It is based on the OECD Guidelines.[253]

Guidelines issued by relevant government agencies supplement the APPI. As of September 1st, 2007, there were as many as 35 sets of guidelines, covering 22 business areas.[254]

(2) Definition of "personal information" under the APPI

Under the APPI, personal information refers to "information about a living individual which can identify the specific individual by name, date of birth or other description contained in such information (including such information as will allow easy reference to other information and will thereby enable the identification of the specific individual)" (s. 2.1).

The handling of personal information for the purposes of journalism, academic studies, religious activities or political activities is not covered by Chapter 4 of the APPI on the duties of entities handling personal information (s. 50).

(3) Consent of the individual concerned

Requirements for consent to be valid

---

251 *Constitution of Japan*: http://www.solon.org/Constitutions/Japan/English/english-Constitution.html.

252 *Act on the Protection of personal information*: http://www5.cao.go.jp/seikatsu/kojin/foreign/act.pdf.

253 Gabriela Kennedy, Sarah Doyle, Brenda Lui and Contributors, "Data Protection in the Asia-Pacific region" and Chris Connolly, "Asia-Pacific Region at the Privacy Crossroads", see note 228; Freshfields Bruckheus Deringer "Data Privacy Protection Across Asia: a regional perspective", see note 231.

254 Jay Ponazecki, Daniel Levison, Toshihiro So, Morrison & Foerster, "Japan: Personal information privacy update" (December 2007) BNAI's World Data Protection Report, at p. 1: http://www.mofo.com/docs/pdf/WDPR1207_Privacy.pdf.

The Act does not define the requirements for consent to be valid.

Circumstances where the data subject's consent is required

Except if another exception applies, an entity handling personal information must obtain the prior consent of the individual concerned if it wishes to:

- **Use personal information beyond the scope necessary** for the achievement of the original purpose for which information was collected (s. 16(1)).
- Use personal information, when the entity handling the **personal information has acquired it as a result of, for example, a takeover in a merger** (s. 16(2)).
- Provide the personal information to a **third party** (s. 23) (1)).

(4) Highlights of the APPI

- With regard to **international data transfers**, Japan has adopted an approach similar to that of Canada. It is based on the accountability of organizations that transfer data to third parties. As a trustee of the personal information, the transferring organization will be found liable if it has failed to establish proper safeguards and that, as a result, the data subject suffers damages (s. 22-23).
- The APPI contains **penal provisions** for offences defined under the APPI (see Chapter 6). The sanctions that can be imposed are fines of no more than 300,000 yen, or up to six months of imprisonment.
    - There are no civil penalties, but the tort of infringement of the privacy of an individual may be used.[255]
- The APPI **does not introduce a single national supervisory authority**. Rather, the relevant ministers and government agencies are responsible for policing privacy compliance in each industry.[256]

c) Protection under sector-specific laws

Japan has enacted two anti-spam laws. It has also enacted the *Internet Provider Responsibility Law*[257] in 2001, that regulates the disclosure of customers' personal information by Internet service providers.[258]

---

255 Gabriela Kennedy, Sarah Doyle, Brenda Lui and Contributors, "Data Protection in the Asia-Pacific region", p. 63, see note 228.

256 Chris Connolly, "Asia-Pacific Region at the Privacy Crossroads", p. 28. see note 228.

257 *Internet Provider Responsibility Law*: unavailable in English or French.

d) Privacy Trustmark Scheme

Private enterprises based in Japan are eligible to receive certification for PrivacyMark. It is a voluntary privacy trustmark scheme that indicates compliance with Japan Industrial Standards (JIS Q 15001:2006 [Personal Information Protection Management System - Requirements]).[259]

4. MACAO

a) Constitutional protection

The *Basic Law of the Macao Special Administrative Region of the People' s Republic of China*[260] provides some privacy protection:

> **Article 30** The human dignity of Macao residents shall be inviolable. Humiliation, slander and false accusation against residents in any form shall be prohibited. Macao residents shall enjoy the right to personal reputation and the privacy of their private and family life.
>
> **Article 31** The homes and other premises of Macao residents shall be inviolable. Arbitrary or unlawful search of, or intrusion into, a resident's home or other premises shall be prohibited.
>
> **Article 32** The freedom and privacy of communication of Macao residents shall be protected by law. No department or individual may, on any grounds, infringe upon the freedom and privacy of communication of residents except that the relevant authorities may inspect communication in accordance with the provisions of the law to meet the needs of public security or of investigation into criminal offences.

b) Main piece of legislation: the Personal Data Protection Act

(1) General remarks

In 2005, Macao enacted a comprehensive law on data protection, the *Personal Data Protection Act* (Act 8/2005) (the "**PDPA**").[261] It is directly inspired by Directive 95/46, and contains very similar provisions and principles. In fact, it is expressly based on Portugal's data protection law.[262]

---

258 Yuko Kim, "Data Security, Privacy in Asia", the Seoul Times http://theseoultimes.com/ST/?url=/ST/dg/read.php?idx=6879%20.

259 PrivacyMark Office, *PrivacyMark System*, http://privacymark.org/index.html.

260 *Basic Law of the Macao Special Administrative Region of the People's Republic of China:* http://bo.io.gov.mo/bo/i/1999/leibasica/index_uk.asp.

261 *Personal Data Protection Act* (Act 8/2005): http://www.gpdp.gov.mo/cht/forms/lei-8-2005_en.pdf.

262 Graham Greenleaf, "Five years of the APEC Privacy Framework: Failure or Promise" p.32, see note 228.

The national data protection supervisory authority is the Office for Personal Data Protection.[263]

(2) Definition of "personal data" under the PDPA

The PDPA's definition of "personal data" refers to "any information of any type, irrespective of the type of medium involved, including sound and image, relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an indication number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity" (s. 4.1(1)).

Personal data processed by a natural person in the course of a purely household activity does not fall within the scope of the PDA, save those with the purposes of systematic communication and dissemination (s. 3.2).

The DPPA applies to video surveillance and other forms of capture, processing and dissemination of sound and images allowing persons to be identified provided the controller is domiciled or based in Macao (s. 3.3).

(3) Data subject's consent

Requirements for consent to be valid

The DPPA **defines** the "the data subject's consent" as "any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed" (s. 4.1(4)).

Circumstances where the data subject's consent is required

As a general rule, personal information may only be processed if the data subject gives his unambiguous consent to the processing, or if it is necessary for the purposes defined under the DPPA (s. 6).

The same rule applies to the processing of **sensitive data** (s. 7), and to the **transfer of personal information** to a country that does not ensure an adequate level of protection (s. 20).

(4) Highlights of the PDPA

- An **international data transfer** may only take place if the third country ensures an adequate level of protection. It is for the public authority to decide whether a country ensures an adequate level of protection (s. 19).

- "any individual may have **recourse to administrative and legal means** to guarantee compliance with legal provisions and statutory regulations in the area of personal data protection" (s. 28).

---

263 Office for Personal Data Protection, *Home*: http://www.gpdp.gov.mo/en/.

- PDPA defines **administrative offences** (s. 30-36) **as well as crimes** (s. 37-42) for violations of the PDPA. Administrative fines go up to MOP 100,000, and can be cumulative. Sanctions for crimes involve imprisonment sentences of up to two years, as well as fines.

5. NEW ZEALAND

a) Constitutional protection

A right to privacy was read in by Courts in section 21 of the *Bill of Rights Act*:[264]

> **Section 21 [Unreasonable Search and Seizure]**
> Everyone has the right to be secure against unreasonable search or seizure, whether of the person, property, or correspondence, or otherwise.

b) Main piece of legislation: the Privacy Act 1993

(1) General remarks

The primary data protection law in New Zealand is the *Privacy Act 1993* (the "**Act**").[265] It is a comprehensive law that covers both the public and the private sectors. It applies to almost every person and business in New Zealand. The Act entered into force on July 1st, 2001.

The national regulatory authority is the Privacy Commissioner.[266]

(2) Definition of "personal information" under the Act

For the purposes of the Act, "personal information" refers to "information about an identifiable individual; and includes information relating to a death that is maintained by the Registrar-General pursuant to the Births, Deaths, and Marriages Registration Act 1995, or any former Act" (s. 2).

Personal information relating to domestic affairs does not fall within the ambit of the Act (s. 56).

Please note that some types of information are exempt from the application of some privacy principles (listed below) (e.g. information collected, obtained, held, used or disclosed by, or disclosed to an intelligence organization is exempt from the application or principles 1-5, and 8-11 (s. 56)).

(3) Consent of the individual concerned

---

264 *Bill of Rights Act*: http://www.servat.unibe.ch/icl/nz01000_.html.

265 *Privacy Act 1993*: http://www.legislation.govt.nz/act/public/1993/0028/latest/DLM296639.html.

266 Privacy Commissioner (Te Mana Matapono Matatapu), *Home*: http://www.privacy.org.nz/.

The Act does not specifically address the issue of consent. However, it states that an agency must collect personal information directly from the individual concerned, which would seem to introduce a consent requirement. Please note that information may not be collected directly from the individual concerned in specific circumstances, namely where the information is publicly available, or doing so would not prejudice the interests of the individual concerned (s. 6, Principle 2).

(4) The Information Privacy Principles

The Act is based on 12 Information Privacy Principles ("**IPPs**"), defined in s. 6. Here is a brief summary of the IPPs:

(1) *Purpose of collection of personal information:* it must be lawful, connected with a function or activity of the agency, and necessary for that purpose.

(2) *Source of personal information:* the information concerning a person should be collected directly from that person, except in some circumstances.

(3) *Collection of information from subject:* the agency that collects information must take reasonable steps to make sure that the individual concerned is aware of a number of things related to the processing of his information.

(4) *Manner of collection of personal information:* personal information shall not be collected by unlawful means or by means that are unfair or that intrude to an unreasonable extent upon the personal affairs of the individual concerned.

(5) *Storage and security of personal information*: the agency that holds information shall ensure adequate security safeguards.

(6) *Access to personal information*

(7) *Correction of personal information*: the individual concerned is entitled to request the correction of his personal information.

(8) *Accuracy, etc, of personal information to be checked before use* by the agency that holds the information

(9) *Agency not to keep personal information for longer than necessary*

(10) *Limits on use of personal information:* the information collected for one purpose cannot be collected for another purpose unless an exception applies.

(11) *Limits on disclosure of personal information:* the agency that holds the information shall not disclose it to a third party unless one of the exceptions apply.

(12) *Unique identifiers:* an agency shall not assign a unique identifier to an individual unless it is necessary. Other rules apply to unique identifiers.[267]

(5) Highlights of the Act:

- IPPs apply to **information held overseas** by an agency, where that information has been transferred out of New Zealand. This means that, in the context of international transfers of personal information, the transferring organization remains responsible for the protection of the information transferred and held by a third party. This approach is similar to the one in Canada under PIPEDA (s. 10).

- When a **code of conduct** applies, every action done in compliance with the code is lawful, even if it would otherwise amount to a breach of an information privacy principle (s. 53).

- **Proceedings** for may be initiated before the Human Rights Review Tribunal either by the Director of Human Rights Proceedings or by an aggrieved individual (s. 82-83).

    - The **remedies** that may be sought are a declaration that the action of the defendant interferes with the privacy of an individual, a restraining order, damages, specific performance or other relief as the tribunal sees fit (s. 84-85).

- The Act sets out a limited number of **offences**, which are sanctioned by a fine not exceeding $2,000 (s. 127).

(6) Project of assessment by the European Commission as providing an "adequate level of protection"

The Act has been amended several times in the past years, with a view towards meeting the EU requirements for international data transfers. New Zealand is very eager to align its Act with Directive 95/46 in order to facilitate trade with the European Union, stimulate business opportunities and enhance the economic capability of the country. The Act is still under revision in order to obtain a finding from the European Commission that New Zealand law offers an "adequate level of protection" for data transfers.[268]

c) Protection under sector-specific laws and codes of practice

The *Unsolicited Electronic Messages Act*,[269] assented in 2007, embodies anti-spam legislation.

---

267 See note 257, Sec. 6.

268 Office of the Privacy Commissioner (Te Mana Matapono Matatapu), "Statement of Intent 2008/09" (2008) p. 11: http://www.privacy.org.nz/assets/Files/SOI-2008-09.pdf.

269 *Unsolicited Electronic Messages Act*; available for download at http://www.parliament.nz/en-NZ/PB/Legislation/Bills/1/d/f/00DBHOH_BILL6896_1-Unsolicited-Electronic-Messages-Bill.html

The Privacy Commissioner has issued several codes of practice, which may modify the operation of the Act for specific industries, agencies, activities or types of personal information. Codes of practice are a flexible means of regulation as they can be repealed at any time by the Privacy Commissioner. There are currently five codes of practice are in force:

- *Health Information Privacy Code* (1994);[270]
- *Justice Sector Unique Identifier Code* (1998);[271]
- *Superannuation Schemes Unique Identifier Code* (1995);[272]
- *Telecommunications Information Privacy Code* (2003).[273]
- *Credit Reporting Privacy Code* (2004).[274]

d) Protection under the common law

The torts of invasion of privacy and breach of confidence may also be relied upon.[275]

6. SOUTH KOREA

a) Constitutional protection

The *Constitution of the Republic of Korea*[276] explicitly protects the right to privacy:

> **Article 16 [Home, Search, Seizure]**
> All citizens are free from intrusion into their place of residence. In case

---

270 *Health Information Privacy Code* (1994); available for download at http://www.privacy.org.nz/health-information-privacy-code/.

271 *Justice Sector Unique Identifier Code* (1998) ; available for download at http://www.privacy.org.nz/justice-sector-unique-identifier-code/.

272 *Superannuation Schemes Unique Identifier Code* (1995) ; available for download at http://www.privacy.org.nz/superannuation-schemes-unique-identifier-code/

273 *Telecommunications Information Privacy Code* (2003); available for download at http://www.privacy.org.nz/telecommunications-information-privacy-code/.

274 *Credit Reporting Privacy Code* (2004); available for download at http://www.privacy.org.nz/credit-reporting-privacy-code/.

275 Gabriela Kennedy, Sarah Doyle, Brenda Lui and Contributors, "Data Protection in the Asia-Pacific region" and Chris Connolly, "Asia-Pacific Region at the Privacy Crossroads", see note 228; Freshfields Bruckheus Deringer "Data Privacy Protection Across Asia: a regional perspective", see note 231.

276 *Constitution of the Republic of Korea*, http://www.servat.unibe.ch/icl/ks00000_.html.

> of search or seizure in a residence, a warrant issued by a judge upon request of a prosecutor has to be presented.
>
> **Article 17 [Privacy]**
> The privacy of no citizen may be infringed.
>
> **Article 18 [Secrecy of Correspondence]**
> The secrecy of correspondence of no citizen may be infringed.

b) Main piece of legislation: the Act on Promotion of Information and Communication Network Utilization and Information Protection

(1) General remarks

Data protection in the private sector is governed by the *Act on Promotion of Information and Communication Network Utilization and Information Protection* (the "**APICNUIP**").[277] It came into force on July 1st, 2001.

(2) Moderately limited scope

The APICNUIP applies to personal data obtained by information and communication service providers (s. 1 and 3). The APICNUIP may also apply to any provider of goods or services who collects, provides or uses personal information (s. 58).

(3) Definition of "personal information" under the APICNUIP

The APICNUIP defines "personal information" as "the information concerning anyone living that contains the code, letter, voice, sound, and/or image, which allows for the possibility for that individual to be identified by name and resident registration number (including information which, if not by itself, allows for the possibility of identification when combined with other information)" (s. 2(6)).

(4) Consent of the individual concerned

Requirements for consent to be valid

When obtaining the consent of an individual, the service provider must provide the individual with **specific information** defined at s. 22:

> 1.The name, department, position, telephone number, and other communication means of a person in charge of administering the personal information;

---

277 *Act on Promotion of Information and Communication Network Utilization and Information Protection:* unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN025694.pdf

> 2.The objective of the collection and use of the personal information;
>
> 3.The identification, objective, and contents of the personal information to be provided to a third person if the personal information is provided to a third person;
>
> 4.The right of the user and his legal representative and the method of exercising this right under Articles 30 (1) and (2) and 31 (2);
>
> 5.Presidential Decree shall stipulate other requisite matters that protect personal information.

When the individual concerned is under 14 years old, his legal representative must provide his consent on his behalf (s. 31).

Circumstances where the data subject's consent is required

As a general rule, service providers must obtain the consent of the individual concerned before collecting and using his personal information, unless an exception applies (s. 22).

Digital documents may not be disclosed unless the consent of the individual concerned is obtained, or the law authorizes it (s. 21).

Sensitive data may only be collected if the individual concerned has given his consent, or it if it is authorized by law (s. 23).

Personal information may be **used for purposes other than the one specified at the time of the collection** if the individual has given his express consent, or if another exception applies (s. 24).

(5) Highlights of the APICNUIP

- The **Minister of Information and Communication** is the key regulatory authority under the APICNUIP. Other agencies are established under the APICNUIP:
    - The Personal Information Dispute Mediation Committee is established to mediate disputes concerning personal information (s. 33).
    - The Korea Information Security Agency is responsible for implementing the requisite protective steps securing information distribution (s. 52).
    - The Korea Association of Information and Telecommunications ("KAIT") is created to promote the use and protection of information and communications networks (s. 59).
- Service providers must obtain **consent** to disclose digital documents (s. 21), and collect personal information (s. 22). Additional restrictions apply to the gathering of **sensitive personal information** (political ideology, religion, medical record) (s. 23).

- Each service provider must **designate a person to administer personal information** and handle complaints with regard to the protection of personal information (s. 27).

- The **rights of the users** (data subject) are similar to those in Directive 95/46 (access, information, correction, objection) (s. 30). They also benefit from the right to a legal representative (s. 31) and to indemnification if harm is suffered as a result of a violation of the APICNUIP (s. 32).

- The APICNUIP contains **special provisions to protect juveniles** in information and communication networks (s. 41-44).

- The Minister of Information and Communication may require service providers to take **protective steps before transferring** major domestic industry, economy, science and technology information to foreign countries (s. 51).

- Service providers may only **transfer information** to countries where data protection standards are equal or higher than those set by the APICNUIP (s. 54).

- The APICNUIP contains **penal provisions** (art. 61-67). Sanctions consist in fines of up to 50 million won, as well as imprisonment sentences with prison labor of up to seven years.

c) Protection under sector-specific laws

The *Personal Credit Information Protection Act*[278] protects information provided to financial institutions. Prior written consent from the individuals concerned is required for the collection and use of any personal credit information. The information may only be used for pre-agreed financial transactions and credit assessment.[279]

d) Self-regulatory initiative: the Privacy mark labeling

The KAIT awards the "Privacy Mark" to on-line businesses and websites that have stringent requirements for information protection.[280]

e) Projects for reform

A legislative reform of privacy laws is under way. The Korean cabinet plans to heighten personal data protection.[281] It may lead to the drafting of a comprehensive law on data protection.

---

278 *Personal Credit Information Protection Act*: unavailable in French or English.

279 Freshfields Bruckhaus Deringer, "Data Privacy Protection across Asia: A regional perspective" (2008), p. 21, http://www.freshfields.com/publications/pdfs/2008/oct08/24238.pdf.

280 Dr Chang-Boem Yi and Dr Ki-Jin Ok, "Korea's personal information protection laws" (2003) PLPR 4, http://www.austlii.edu.au/au/journals/PLPR/2003/8.html.

281 Chris Connolly, "Asia-Pacific Region at the Privacy Crossroads", p. 29 see note 228.

7. TAIWAN

a) Privacy and data protection under the Constitution and the Codes

Taiwan does not have comprehensive legislation on data protection.

The Taiwanese Constitution[282] only recognizes a limited right to privacy:

> **Article 12**
> The people shall have freedom of privacy of correspondence.

The Civil Code and *Criminal Code of Taiwan* afford some data protection.[283]

b) Main piece of legislation: the Computer-processed Personal Data Protection Act

(1) General remarks

The main piece of legislation with regard to data protection in the private sector in Taiwan is the *Computer-Processed Personal Data Protection Act* (the "**CPPDPA**").[284] It was largely inspired by Directive 95/46.

(2) Limited Scope

The CPPDPA is quite restricted in scope. First, it only applies to computerized data processing. Second, the CPPDPA only covers a limited number of industries, like hospitals, schools, telecommunications companies, finance companies, security companies, insurance companies, mass media businesses, credit investigation companies, organizations or individuals engaged primarily in the business of collecting or processing computer data and companies in other designated industries.[285]

(3) Definition of "personal data"

---

282 The *Taiwanese Constitution*: http://www.servat.unibe.ch/icl/tw00000_.html.

283 Gabriela Kennedy, Sarah Doyle, Brenda Lui and Contributors, "Data Protection in the Asia-Pacific region", p. 64. see note 228.

284 *Computer-Processed Personal Data Protection Act:* http://www.winklerpartners.com/a/features/computerprocessed-personal-dat.php.

285 Freshfields Bruckhaus Deringer, "Data Privacy Protection across Asia: A regional perspective", p. 22 see note 279.

Under the CPPDPA, “personal data” refers to “a natural person's name, date of birth, national identification number, special features, fingerprints, marital [status], family, education, occupation, health, medical history and financial status, social activities and other data which is sufficient to identify that person” (s. 3.1).

Specific types of personal information fall outside of the ambit of the Act, but they are only relevant for the public sector (s. 11 of CPPDPA).

(4) Consent of the individual concerned

Requirements for consent to be valid

The Act only specifies that consent must be given in writing (s. 18(1) and 23(4) for information handled by a non-public agency).

Circumstances where the data subject’s consent is required

Unless another exception applies, a non-public agency must obtain the written consent of the individual concerned which will allow a non-public agency to:

- Engage in the collection or computerized processing of personal information (s. 18 (1)).
- Use personal information for a different purpose than the one that was specified at the time of the collection (s. 23 (4)).

(5) Other highlights of the CPPDPA

- The CPPDPA does not establish a national supervisory authority. It rather relies on **regulatory authorities** in each industry to ensure compliance with the CPPDPA.
- Organizations must **register** with the competent authority (s. 19 CPPDPA).
- The CPPDPA provides for **remedies** (s. 27-32 CPPDPA) and sets out the amount of damages that can be claimed by the injured party (may go up to 20,000,000 New Taiwan Dollars depending on what is claimed). The CPPDPA also sets out **penalties** for offences under the act (s. 33-41 CPPDPA), which include imprisonment sentences of up to three years, and fines.
- The competent authority for a specified industry may impose restrictions on **international data transfers** in specific cases (s. 24 CPPDPA).

(6) Legislative reform under way

Taiwan is currently engaging in an important reform of its data protection regime, which should involve bringing all non-public agencies under the scope of the CPPDPA.[286]

C. COUNTRIES THAT ARE IN THE PROCESS OF DRAFTING PRIVACY LEGISLATION

1. CHINA

a) Constitutional protection

The concept of privacy is not an organizing principle in China. The *Constitution of the People's Republic of China*[287] protects a limited right of privacy:

> Article 40. The freedom and privacy of correspondence of citizens of the People's Republic of China are protected by law. No organization or individual may, on any ground, infringe upon the freedom and privacy of citizens' correspondence except in cases where, to meet the needs of state security or of investigation into criminal offences, public security or procuratorial organs are permitted to censor correspondence in accordance with procedures prescribed by law.

It also prohibits physical search or invasion of a person's residence without legal cause or due process.

Is it important to note that government agencies have taken a broad view of what constitutes the "needs of state security".[288]

b) Protection under sector-specific laws

Data protection is provided under several sector-specific laws, notably:

- The *Employment Service and Employment Management Regulations* (2008) protects employee personal data, as employer is restricted in asking for private information, such information most be kept confidential and its disclosure requires employee's consent;[289]

---

286 Freshfields Bruckheus Deringer "Data Privacy Protection Across Asia: a regional perspective", see note 231.

287 *Constitution of the People's Republic of China*: http://english.people.com.cn/constitution/constitution.html.

288 Caslon Analytics privacy guide, *China and the Hong Kong SAR*: http://www.caslon.com.au/privacyguide6.htm#china.

- The *Municipal Interim Measures on Administration of the Collection of Personal Credits*[290] and the *Interim Measures on Administration on Personal Credit Information Fundamental database* which govern the collecting of personal credit data;[291]

- The *Insurance Law of the People's Republic of China* which imposes a duty of confidentiality on the insurer or re-insurance underwriter;[292]

- The *Regulations of Shanghai Municipality on the Protection of Consumers' Rights and Interests* which prohibits the disclosure of consumer personal information without consent.[293]

It is important to note that the Chinese Government itself admits that these laws are not always applied fairly and systematically.[294]

The right of privacy is not listed under the General Principles of Civil Law but privacy protection is recognized in the form of traditional right against defamation or right to reputation.

The 7th Amendment to the Criminal Law, in force since February 28, 2008, provides that it is a criminal offence to sell or illegally provide to third parties the personal information obtained in the course of performing their duties. If the nature of such violation is serious, the guilty person is subject to a fine or even a jail term up to three years.

c) Drafting of a comprehensive data protection law

China is in the process of drafting a comprehensive law on data protection. So far, the draft legislation is closely aligned on Directive 95/46. However the registration requirement will not be introduced.[295]

---

289 *Employment Service and Employment Management Regulations* (2008), p. 2: unavailable in French or English, but a summary is provided at www.bmhk.com/PRC/2007-534.pdf.

290 *Municipal Interim Measures on Administration of the Collection of Personal Credits:* unavailable in French or English.

291 *Interim Measures on Administration on Personal Credit Information Fundamental database*: unavailable in French or English.

292 *Insurance Law of the People's Republic of China:* http://english.sohu.com/2004/07/04/79/article220847975.shtml.

293 *Regulations of Shanghai Municipality on the Protection of Consumers' Rights and Interests:* http://www.asianlii.org/cn/legis/sh/laws/rosmotpocrai878/.

294 Privacy International, *PHR2006 – People's Republic of China:* http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-559508.

295 Chris Connolly, "Asia-Pacific Region at the Privacy Crossroads", pp. 25-26, see note 231.

The development of data protection laws is of crucial importance in China. The lack of a strong data protection regime could impair China's economic relations with Western Countries. The growth of the industry of business processing outsourcing ("**BPO**") also calls for an important reform of data protection laws, in order to stay competitive.[296]

2. MALAYSIA

a) Constitutional protection

The *Constitution of Malaysia*[297] does not recognize a right to privacy or to protection of personal data.

b) Final stages of the drafting of the Personal Data Protection Bill

Malaysia is in the final stages of drafting its *Personal Data Protection Bill* (the "**Bill**"), a comprehensive law on data protection. This law is very ambitious, as it aims to be a world class leading edge cyberlaw and promote Malaysia as a top investment centre for the communications and multimedia industry. It is closely aligned with Directive 95/46's principles.[298] The Bill is to be unveiled in October 2009.[299]

c) Protection under sector-specific laws

Meanwhile, some data protection is provided in specific-sector legislation. For example, the *Communications and Multimedia Act*[300] (1988) prohibits the interception and disclosure of communications (s. 234). The *Banking and Financial Institutions Act*[301] (1989) protects the privacy of banking information (Part XIII).

---

296 Steven Robertson, "Privacy and outsourcing to China" (January 2008) Galexia: http://www.galexia.com/public/research/articles/research_articles-art49.html.

297 *Constitution of Malaysia*: http://www.helplinelaw.com/law/constitution/malaysia/malaysia01.php.

298 Ministry of Energy, Communications and Multimedia, "Presentation of Personal Data Protection Bill to Participants of the Asian Personal Data Privacy Forum, 27 March 2001, Hong Kong" (2009), Powerpoint presentation available at: www.pcpd.org.hk/misc/malaysia/Malaysia.ppt.

299 Chua Sue-Ann, "Personal Data Protection bill to be unveiled in October", *The Edge Malaysia* (06/17/2009): http://www.theedgemalaysia.com/political-news/16580-personal-data-protection-bill-to-be-unveiled-in-october.html.

300 *Communications and Multimedia Act*: http://www.commonlii.org/my/legis/consol_act/cama1998289/.

301 *Banking and Financial Institutions Act:* http://www.bnm.gov.my/index.php?ch=14&pg=17&ac=14&full=1.

3. THE PHILIPPINES

a) Constitutional protection

The right to privacy is protected under a few sections of the *Bill of Rights*, Article III of The *1987 Constitution of the Republic of the Philippines*.[302] The relevant sections are:

> **Section 2.** The right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures of whatever nature and for any purpose shall be inviolable, and no search warrant or warrant of arrest shall issue except upon probable cause to be determined personally by the judge after examination under oath or affirmation of the complainant and the witnesses he may produce, and particularly describing the place to be searched and the persons or things to be seized.
>
> **Section 3.** (1) The privacy of communication and correspondence shall be inviolable except upon lawful order of the court, or when public safety or order requires otherwise, as prescribed by law.
>
> (2) Any evidence obtained in violation of this or the preceding section shall be inadmissible for any purpose in any proceeding.
>
> **Section 4.** No law shall be passed abridging the freedom of speech, of expression, or of the press, or the right of the people peaceably to assemble and petition the government for redress of grievances.
>
> **Section 7.** The right of the people to information on matters of public concern shall be recognized. Access to official records, and to documents and papers pertaining to official acts, transactions, or decisions, as well as to government research data used as basis for policy development, shall be afforded the citizen, subject to such limitations as may be provided by law.

b) Drafting of a comprehensive law on data protection

The Philippines are in the process of drafting a comprehensive law on data protection, the *Act to Establish Fair Practices in the Processing of Information Relating or Personal to Individuals Creating for the Purpose a Personal Data Protection Commission, and for Other Purposes*.[303]

---

302 *Bill of Rights, Article III of The 1987 Constitution of the Republic of the Philippines:* http://www.chanrobles.com/article3.htm.

303 *Act to Establish Fair Practices in the Processing of Information Relating or Personal to Individuals Creating for the Purpose a Personal Data Protection Commission, and for Other Purposes*: for the current version of the draft, see http://www.senate.gov.ph/lisdata/54754855!.pdf.

The early drafts of the Act are directly inspired by the structure and language of Directive 95/46 and the UK *Data Protection Act*. However, the Philippines will very likely not introduce the registration requirements found in Directive 95/46.[304]

4. THAILAND

a) Constitutional protection

The right to privacy is protected under the Constitution of the Kingdom of Thailand:[305]

> **Section 35.** A person's family rights, dignity, reputation and the right of privacy shall be protected.
> The assertion or circulation of a statement or picture in any manner whatsoever to the public, which violates or affects a person's family rights, dignity, reputation or the right of privacy, shall not be made except for the case which is beneficial to the public.
> Personal data of a person shall be protected from the seeking of unlawful benefit as provided by the law.

b) Drafting of a comprehensive law on data protection

Thailand is in the final stages of drafting a comprehensive privacy law. This draft law on data protection is founded on eight principles, closely aligned on the European data protection principles: consent, notice, purpose specification, use limitation, accuracy, access, security and enforcement.[306]

Businesses urge Thailand to enact privacy laws, in order to stimulate business transactions and commerce, especially outsourcing opportunities.[307]

c) Protection under sector-specific laws

Meanwhile, specific legislation impacts data protection in Thailand. Namely, the *Official Information Act* 1997[308] provides guidelines for government agencies that handle personal data. The *Computer Crime Act*,[309] which came into force on June 10, 2007, imposes penalties for

---

304 Chris Connolly, "Asia-Pacific Region at the Privacy Crossroads", p.33, see note 231.

305 *Constitution of the Kingdom of Thailand*: http://www.asianlii.org/th/legis/const/2007/1.html#C01.

306 Chris Connolly, "Asia-Pacific Region at the Privacy Crossroads", p. 33, see note 231.

307 Don Sambandaraksa, "We need data privacy act to attract BPO" Bangkok Post (02/07/2007) http://www.bangkokpost.net/20th_database/07Feb2007_data52.php.

308 *Official Information Act* 1997: http://www.oic.go.th/content_eng/act.htm.

309 *Computer Crime Act*: http://www.prachatai.com/english/node/117.

identity fraud, the interception of confidential data, and misuse or abuse of information on others' computers. This law has been severely criticized by human rights organizations for imposing penalties that are too harsh, and for giving too much power to officials when handling personal data.[310]

D. COUNTRIES THAT ONLY HAVE PRIVACY PROVISIONS IN SECTOR-SPECIFIC LAWS

These countries have not adopted comprehensive privacy legislation, but some sector-specific laws contain privacy commitments. These provisions could serve as a foundation for the development of more extensive privacy legislation.

1. INDONESIA

a) Constitutional protection

The *1945 Constitution of the Republic of Indonesia* does not protect the right to privacy.[311]

b) Protection under sector-specific law

The *Law on Information and Electronic Transactions*[312] is an omnibus law that regulates e-government, electronic contracting, privacy, cybercrime, digital copyright and other cyberlaw issues. One provision addresses privacy:

> **Article 26**
>
> (1) The utilization of any information by means of electronic media relating to data about private right of anyone shall be carried out with the approval of the person concerned unless otherwise stipulated by the statutory regulation.
>
> (2) Any person whose rights are violated in the manner detailed in paragraph (1) is entitled to compensation for any loss as explained within this legislation.

Statutory legislation may waive the requirement for consent in specific circumstances.[313]

---

310 Asian Human Rights Commission, *THAILAND: Unintelligible Computer "Law" Passed Under Junta's Watch*: http://www.ahrchk.net/statements/mainfile.php/2007statements/1133.

311 *1945 Constitution of the Republic of Indonesia*, http://asnic.utexas.edu/asnic/countries/indonesia/ConstIndonesia.html.

312 *Law on Information and Electronic Transactions*, unavailable in French or English, as cited by Chris Connolly, "Asia-Pacific Region at the Privacy Crossroads", see note 231.

313 Chris Connolly, "Asia-Pacific Region at the Privacy Crossroads", p. 27, see note 228.

2. SINGAPORE

a) Constitutional protection

The *Constitution of the Republic of Singapore*[314] does not protect the right to privacy.

b) Self-Regulation: Model Data Protection Code

Singapore is the only country in the Asia-Pacific region to have adopted a policy of industry-based voluntary self-regulation rather than legislation. The *Model Data Protection Code*[315] ("**Model Code**"), based on the OECD Guidelines, provides a flexible framework applicable by a wide range of organizations in the private sector. It assists them in developing and implementing personal data protection policies and procedures (s. 1.1 of the Model Code).[316]

The Model Code is meant to be an interim measure towards the enactment of privacy legislation. There is no stated timeframe to do so.[317]

c) Protection under sector-specific laws and at common law

Privacy protection is currently based on the common law (duty of confidentiality and tort of breach of confidence)[318], contract law, and sector-specific laws, such as the *Banking Act* (Third Schedule)[319] or the *Electronic Transactions Act.*[320]

---

314 *Constitution of the Republic of Singapore*, http://statutes.agc.gov.sg/non_version/cgi-bin/cgi_retrieve.pl?&actno=Reved-CONST&date=latest&method=part.

315 *Model Data Protection Code*: http://www.trustsg.com.sg/downloads/Data_Protection_Code_v1.3.pdf.

316 Chris Connolly, "Asia-Pacific Region at the Privacy Crossroads", p. 34, see note 228.

317 Idem.

318 Gabriela Kennedy, Sarah Doyle, Brenda Lui and Contributors, "Data Protection in the Asia-Pacific region", p. 64. see note 228.

319 *Banking Act* (Third Schedule): http://agcvldb4.agc.gov.sg/non_version/cgi-bin/cgi_retrieve.pl?actno=REVED-19&doctitle=BANKING%20ACT%0A&date=latest&method=part.

320 *Electronic Transactions Act*: http://agcvldb4.agc.gov.sg/non_version/cgi-bin/cgi_retrieve.pl?actno=REVED-88&doctitle=ELECTRONIC%20TRANSACTIONS%20ACT%0a&date=latest&method=part&sl=1.

3. VANUATU

Vanuatu is the only small Pacific Island with specific privacy legislation. It has adopted the *Electronic Transactions Act* in 2000.[321] Part 5 addresses encryption and data protection.

4. VIETNAM

Even though Vietnam has no comprehensive privacy legislation, privacy and data protection is covered in several pieces of legislation.

There is currently no time-frame for the adoption of a comprehensive privacy legislation in Vietnam.[322]

a) Constitutional protection

The Constitution of Vietnam[323] protects the right of privacy to a certain extent:

> **Article 50 [Human Rights]**
>
> In the Socialist Republic of Vietnam human rights in the political, civic, economic, cultural and social fields are respected. They are embodied in the citizen's rights and are determined by the Constitution and the law.
>
> **Article 73 [Inviolability of Domicile, Secrecy of Correspondence]**
>
> (1) The citizen is entitled to the inviolability of his domicile.
>
> (2) No one is allowed to enter the domicile of another person without his consent, except in cases authorised by the law.
>
> (3) Safety and secrecy are guaranteed to the citizen correspondence, telephone conversations and telegrams.
>
> (4) Domiciliary searches and the opening, control, and confiscation of a citizen's correspondence and telegrams can only be done by a competent authority in accordance with the provisions of the law.

b) Protection under the Civil Code

---

321 *Electronic Transactions Act* (2000): http://www.vanuatu.usp.ac.fj/pacific%20law%20materials/Vanuatu_legislation/English/2000/Vanuatu_Electronic_Transactions.html

322 Gabriela Kennedy, Sarah Doyle, Brenda Lui and Contributors, "Data Protection in the Asia-Pacific region", p.65, see note 228.

323 *Constitution of Vietnam*: http://www.servat.unibe.ch/icl/vm00000_.html.

The right to privacy is protected in the Civil Code of Vietnam:[324]

> **Article 34.- The right to personal secrets**
>
> 1. An individual's rights to personal secrets are respected and protected by law.
>
> 2. The collection and publication of information and materials regarding the private life of an individual must have the consent of that person or his/her relatives if that person has died or lost the capacity for civil acts, except in circumstances where the collection and publication of information and materials are made by decision of a competent State authority but must be done in accordance with law.
>
> 3. No one may take the liberty to open, seize or destroy the letters and telegrams, or tap the telephone or commit other acts for the purpose of preventing or hindering the communication lines of an individual.
>
> The inspection of an individual's letters, telephones or telegrams may be performed only in circumstances stipulated by law and it is done on order from a competent State authority.

c) Protection under sector-specific laws

Sector-specific laws protect personal data. For example, the *Law on E-Transactions* protects the confidentiality of the information disclosed in online transactions:[325]

> **Article 46**
>
> 1. Agencies, organizations and individuals shall have the right to select security measures in accordance with the provisions of the law when conducting e-transactions.
>
> 2. Agencies, organizations and individuals must not use, provide or disclose information on private and personal affairs or information of other agencies, organizations and/or individuals which is accessible by them or under their control in e-transactions without the latter's consents, unless otherwise provided for by law.

The *Law on Information Technology* provides that more detailed legislation could be enacted in the future to regulate the protection of personal information.[326]

---

324 *Civil Code of Vietnam*: http://www.worldlii.org/vn/legis/cc73/index.html.

325 *Law on E-Transactions*: unavailable in French or English, but a copy of s. 46 may be found at Chris Connolly, "Asia-Pacific Region at the Privacy Crossroads", p. 36, see note 228.

326 Chris Connolly, "Asia-Pacific Region at the Privacy Crossroads", see note 228.

Decree no. 55/2001/nd-cp of August 23, 2001 on the management, provision and use of internet services[327] provides that the confidentiality of the private information of organizations and individuals on the Internet must be ensured pursuant to the Constitution and laws (s. 8).

d) Sanctions

Vietnam law also provides civil and criminal sanctions for violations of privacy laws. For example, article 226 of the Penal Code[328] makes it an offence to illegally use information in computer networks:

> **Article 226.- Illegally using information in computer networks**
>
> 1. Those who illegally use information in computer networks and computers as well as put information into computer networks in contravention of law provisions, causing serious consequences, who have already been disciplined, administratively sanctioned but continue to commit it, shall be subject to a fine of between five million dong and fifty million dong, non-custodial reform for up to three years or a prison term of between six months and three years.
>
> 2. Committing the crime in one of the following circumstances, the offenders shall be sentenced to between two and five years of imprisonment:
> a) In an organized manner;
> b) Causing very serious or particularly serious consequences.
>
> 3. The offenders may also be subject to a fine of between three million dong and thirty million dong, a ban from holding certain posts, practicing certain occupations or doing certain jobs for one to five years.

E. COUNTRIES THAT DO NOT HAVE PRIVACY LEGISLATION

Still, many Asian-Pacific countries seem not to have privacy legislation: Brunei, Cambodia, Laos, Myanmar and the majority of the small Pacific Island countries. However, some of them are committed to the development of harmonized data protection legislation by 2015, as ASEAN members.

Some initiatives were taken by the Pacific Islands Forum[329] with regard to data protection. For example, they project to implement harmonized cyberlaw in the future.[330]

---

327 *Decree no. 55/2001/nd-cp of August 23, 2001 on the management, provision and use of internet services*, http://www.business.gov.vn/assets/fbbc1d48c42d4f36a161a8a3d8749744.pdf.

328 *Penal Code*, article 226: http://www.worldlii.org/vn/legis/pc66/s246.html.

F. OUTSIDE THE ASIA-PACIFIC REGION : THE CASE OF INDIA

1. Constitutional protection

Even though no right of privacy is expressly recognized in the *Constitution of India*,[331] the Supreme Court of India has implied it from article 21:

> **Article 21 Protection of life and personal liberty**
>
> No person shall be deprived of his life or personal liberty except according to procedure established by law.

However, this right is not absolute and can be restricted under procedures established by law or if a superior interest commands it. There is no general right to the protection of personal data.[332]

2. Main piece of legislation: the Personal Data Protection Bill

(1) General remarks

In 2006, the *Personal Data Protection Bill* (the "**Bill**") was introduced in the Rajya Sabha (Council of State).[333] The Bill is to be tabled at the next Dewan Rakyat (House of Representatives) sitting. Details of the Bill should be made public in October.[334]

(2) Definition of "personal data"

---

329 The Pacific Islands Forum is a regional organization formed by Australia, the Cook Islands, Micronesia, Fiji, Kiribati, the Marshall Islands, Nauru, New Zealand, Niue, Palau, Papua New Guinea, Samoa, the Solomon Islands, Tonga, Tuvalu, and Vanuatu (New Caledonia and French Polynesia are associate members. Tokelau and East Timor are only observers).

330 Pacific Islands Forum, *Pacific Plan For Strengthening Regional Cooperation and Integration: Pacific Regional Digital Strategy*; available at http://www.forumsec.org.fj/UserFiles/File/Regional_Digital_Strategy.pdf.

331 *Constitution of India*: http://www.servat.unibe.ch/icl/in00000_.html.

332 CRID – University of Namur, "First Analysis of the Personal Data Protection Law in India, Final Report" (2005), p. 70: http://ec.europa.eu/justice_home/fsj/privacy/docs/studies/final_report_india_en.pdf.

333 *Personal Data Protection Bill*: rajyasabha.nic.in/bills-ls-rs/2006/XCI_2006.pdf. Please note that The only version of the Bill that is available is the one as introduced in the Rajya Sabha on December 8, 2006. The Bill may have changed since then.

334 "Personal Data Protection Bill To Be Tabled In Dewan Rakyat" *Bernama.com* (07/16/2009) http://www.bernama.com/bernama/v5/newsgeneral.php?id=425714.

Under the Bill, "personal data" means "information or data which relates to a living individual who can be identified from that information or data whether collected by any Government or any private organization agency" (s. 2(c)).

(3) Highlights of the Bill

The final version of the Bill has not yet been adopted. Based on the version as introduced in the Rajya Sabha on December 8, 2006, the highlights of the Bill are the following:

- The Bill introduces **principles that are very similar to the EU principles**, such as the purpose limitation principle with regard to the collection of data (s. 3), the non disclosure of personal data for commercial purposes or for direct marketing purposes (s. 4), and the right to compensation under the Bill (s. 5),

- Personal data may not be processed without obtaining the **prior consent** of the individual concerned. Consent is not required in some instances, for instance when the data is publicly available, or when the data is processed for the prevention of crime, the prosecution of offenders or for a tax assessment. (s. 3).

- The Government shall appoint **Data controllers** to overview complaints relating to the processing and disclosing of personal data and claims for compensation (s. 6).

    - There is an obligation for organizations or persons engaged in the commercial transaction and collection of personal data to **report** to the Data controller (s. 7(i)).

- The Bill sets out **sanctions** for whoever contravenes, attempts to contravene or aids in the contravention of the provisions of the Bill. The possible sanctions are imprisonment for up to three years, or a fine of up to ten lakh rupees (s. 9).

3. Protection under sector-specific laws

The *Information Technology Act*[335] as amended by the *Information Technology (Amendment) Act*[336] in 2008 addresses data protection through s. 43A (compensation for failure to protect data) and s. 72A (Punishment for Disclosure of information in breach of lawful contract).

The *Credit Information Companies (Regulation) Act*[337] ensures the complete protection of credit information, but is very limited in scope. It does not grant data subjects a comprehensive right to information, nor does it designate a specific authority to ensure compliance with the act.

---

335 *Information Technology Act*: http://www.mit.gov.in/default.aspx?id=192.

336 *Information Technology (Amendment) Act*: Available for download at: http://www.mit.gov.in/default.ASPX?id=191.

337 *Credit Information Companies (Regulation) Act*: www.ebc-india.com/downloads/credit_information.pdf.

CASES IN THE NEWS AND OTHER CASES OF INTEREST

I. CANADA

A. FACEBOOK CONTRAVENES PIPEDA

In a report made public on July 16, 2009, Canada's Privacy Commissioner concluded that Facebook contravened PIPEDA in many regards. For example, Facebook was non-compliant in respect of the manner of disclosing certain user information, adequate limitation on what information could be disclose to third parties such as application developers and target marketers and adequate notice to users that their information could be used for memorialization purposes after death. The Privacy Commissioner made recommendations to the social network in order for it to better comply with Canada's legislation on privacy.[338]

So far, Facebook has not complied with all the recommendations and it remains to be seen if the matter will be referred to the Federal Court by the Privacy Commissioner.

B. LOSS OF A FILE CONTAINING CUSTOMER INFORMATION OF TALVEST MUTUAL FUNDS (CIBC SUBSIDIARY)

On January 17 2007, the PCC initiated a complaint against CIBC after a backup computer file disappeared while in transit between two offices. The file contained information on more than 400,000 customers of Talvest Mutual Funds. The PCC found that CIBC had violated PIPEDA by not ensuring sufficient safeguards. However, the CIBC took adequate remedial measures after the incident occurred.[339]

---

338 For more information, see: Office of the Privacy Commissioner of Canada, "News Release: Facebook needs to improve privacy practices, investigation finds" (07/16/2009) http://www.priv.gc.ca/media/nr-c/2009/nr-c_090716_e.cfm; PIPEDA Case Summary #2009-008: Report of Findings into the Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc. Under the Personal Information Protection and Electronic Documents Act by Elizabeth Denham Assistant Privacy Commissioner of Canada http://www.priv.gc.ca/cf-dc/2009/2009_008_0716_e.cfm.

339 For more information, see: PIPEDA Case Summary #2008-395: Commissioner initiates safeguards complaint against CIBC http://www.priv.gc.ca/cf-dc/2008/395_20080925_e.cfm.

C. LARGE SCALE CREDIT CARD FRAUD AT TJX COMPANIES INC., OPERATOR OF WINNERS MERCHANT INTERNATIONAL L.P.

On January 17, 2007, the Privacy Commissioners of Canada and Alberta were notified that TJX had suffered a network computer intrusion. This intrusion affected the personal information of approximately 45,000,000 credit cards in Canada, the US, Puerto Rico, the UK and Ireland. After investigation, the PCC found that TJX had retained unnecessary personal information and had not provided sufficient safeguards, in violation of PIPEDA. [340]

II. INTERNATIONAL

A. GOOGLE STREET VIEW RAISES PRIVACY CONCERNS

Google Street View has raised important privacy concerns around the world since its launch was announced. Street View offers a 360-degree view of major cities in the world, based on detailed street-level images. It sometimes show license plates, individuals, and private houses. In response to the main privacy concerns, Google has adopted a policy of automatically blurring the faces of individuals and license plates. Users may also ask to have pictures of themselves, their children, their cars or their houses completely removed from the product, even when the images have already been blurred. Objectionable images may be removed on request. However, the photographs stay part of the company's internal database. In Germany, Google's privacy policy is stricter than in other countries. Google has agreed to erase identifiable raw data depicting people, property or cars from its internal database before their publication if asked. This was done in response to demands by Hamburg's Data Protection Office.[341]

---

340 For more information, see: Office Of The Privacy Commissioner Of Canada And Office Of The Information And Privacy Commissioner Of Alberta, "Report of an Investigation into the Security, Collection and Retention of Personal Information, TJX Companies Inc. /Winners Merchant International L.P." (September 25, 2007): http://www.priv.gc.ca/cf-dc/2007/TJX_rep_070925_e.cfm.

341 For more information, see: Google Maps Street Views' privacy policy, http://www.google.ca/press/streetview/privacy/; Haley A. Lovett, "Google Addresses Street View Privacy Concerns, Removes Images Before Publication" *Finding Dulcinea* (06/24/2009) http://www.findingdulcinea.com/news/technology/2009/June/Google-Addresses-Street-View-Privacy-Concerns--Removes-Images-Before-Publication.html; "Google Bows to German Data Privacy Demands" *Spiegel Online* (06/18/2009), http://www.spiegel.de/international/germany/0,1518,631149,00.html; "Greece puts brakes on Street View" *BBC News* (05/12/2009) http://news.bbc.co.uk/2/hi/technology/8045517.stm; "Japan says 'Ok' to Google's Street View service" *The Hindu* (06/23/2009) http://www.hindu.com/holnus/008200906231780.htm; John C Abell, "Carry On, Google Street View, Britain Rules" *Wired.com* (04/23/2009), http://www.wired.com/epicenter/2009/04/reuters-scraps/; Vito Pilieci, "Google Street View amended to allay privacy concerns, executive tells MPs" *The Ottawa Citizen* (06/18/2009) http://www.ottawacitizen.com/Travel/Google+Street+View+amended+allay+Canadian+privacy+concerns+told/1705995/story.html; Peter Sayer, "Google agrees to delete unblurred German Street View Data" *MacWorld* (06/18/2009) http://www.macworld.com/article/141229/2009/06/google_streetview.html.

B. INDIAN GOVERNMENT DEMANDS RESEARCH IN MOTION TO PROVIDE SECURITY AGENCIES WITH A WAY AROUND THE ENCRYPTION USED BY THE BLACKBERRY NETWORK

The Indian Government pressured Research In Motion ("**RIM**") to provide security agencies with a way around the encryption of the BlackBerry Network. Since the e-mails sent via BlackBerry devices cannot be intercepted or traced, the government feared that they would be used to coordinate terrorist attacks. RIM refused to comply or to set up servers in India. Finally, the government backed off and judged that BlackBerry devices did not pose a security threat.[342]

C. US-EU: SWIFT AND THE TERRORIST TRACKING FINANCE PROGRAMME

In June 2006, the American news revealed the existence of the Terrorist Tracking Finance Programme ("**TTFP**"). The TTFP is an international banking transactions surveillance programme. Its purpose is to fight against the financing of terrorism by identifying persons suspected of being connected to the financing of terrorism. The TTFP allows the CIA and the US Department of Treasury to access millions of items of data transferred by SWIFT (such as the transaction amount, currency, value date, name of the recipient, client who requested the financial transaction and client's financial institution). The program does not only apply to transfers to the United Stated, but to all types of transactions handles by Swift, including in the EU.

The Working Party found that SWIFT did not comply with the EU data protection requirements in several regards. SWIFT later restructured its technical architecture to satisfy Directive 95/46. The Commission and the US government also negotiated guarantees regarding the use of data from the SWIFT database stored by the US Department of Treasury.[343]

***

342 For more information, see: Martin Perez, "India May Crack BlackBerry Encryption" *Information Week* (06/13/2008) http://www.informationweek.com/news/mobility/messaging/showArticle.jhtml?articleID=208403978; Martin Perez, "RIM Questions India's BlackBerry Encryption Worries" *Information Week* (06/02/2008) http://www.informationweek.com/news/security/encryption/showArticle.jhtml?articleID=208401643; Swati Prasad, "India's BlackBerry Case Raises Rrivacy Concerns" *ZDNet Asia* (07/04/2008) http://www.zdnetasia.com/news/business/0,39044229,62043470,00.htm.

343 For more information, see Working Party, *Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)*, WP 128, (11/22/2006) available for download at http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2006_en.htm; *Processing of EU originating Personal Data by United States Treasury Department for Counter Terrorism Purposes — 'SWIFT'*, OJ C 166, (07/20/2007); available for download at: http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm; *Letter from United States Department of the Treasury regarding SWIFT/Terrorist Finance Tracking Programme*, 28 June 2007, OJ C 166, (07/20/2007); available for download at: http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm.

ACC Extras

Supplemental resources available on www.acc.com

European Briefings - June 2008
ACC Docket. May 2008
http://www.acc.com/legalresources/resource.cfm?show=14327

Going Global - Creating an Effective Global Compliance Program with Limited Resources.
ACC Docket. November 2008
http://www.acc.com/legalresources/resource.cfm?show=86641

Employee Data Privacy.
Sample Form & Policy. July 2008
http://www.acc.com/legalresources/resource.cfm?show=12315

Doing Business Internationally.
InfoPak. September 2009
http://www.acc.com/infopaks

Canadian Privacy Law: Making Sense of the Patchwork Quilt.
QuickCounsel. August 2009
http://www.acc.com/legalresources/quickcounsel/cplmsotpq.cfm

Please note, these additional resources are provided by the Association of Corporate Counsel and not by the faculty of this session.