IADC International Law Committee Survey of Electronic Discovery and Data Privacy Law

Edited by James M. Sullivan

THE INTRODUCTION of computers and email into the workplace and everyday life has dramatically increased the information available to employers, regulators and litigants. Often this information is confidential or of a personal nature. This puts into conflict the obligation to disclose information and the obligation to keep private information confidential.

It is interesting to see how different jurisdictions have chosen to resolve this conflict. The European Union has produced a **Data Protection Directive**[1] that has been implemented, in varying degrees, in its member states. The EU Directive broadly defines "personal data" to mean "any information relating to an identified or identifiable person". Each member state has considered how best to integrate and implement that directive in their nation. The survey of French data privacy laws, in particular, provides an example of the pitfalls that United States corporations may face in complying with United States law in the face of the EU Directive.

Common law counties such as Canada and New Zealand have also had to deal with the conflict between broad obligations of disclosure and personal and private confidentiality concerns. In Canada, there are ongoing changes to disclosure rules in many of the provinces

[1] Directive 95/46/EC of October 24, 1995 (hereinafter, "EU Directive").

James Sullivan is the editor of this survey and was responsible for compiling and introducing the work of the many IADC contributors identified below. Mr. Sullivan is a litigation partner at Blake, Cassels & Graydon's Vancouver office and the firm's lead environmental litigation counsel. This survey is a project of the 2009-2010 IADC International Law Committee, chaired by Pamela McGovern, with Gord McKee serving as Vice-Chair of Publications. Authors and contributors include: Ellen S. Hong and James M. Sullivan, Blake, Cassels & Graydon (Canada); Robert Gapes, Simpson Grierson (New Zealand); Ariel Ye, King and Wood (China); Godelieve Alkemade, Royal Dutch Shell (Netherlands); Emmanuele Lutfalla, SPC Soulie & Coste-Foret (France); Dr. Henning Moelle, Taylor Wessing, Peter Klappich and Juergen Hartung, Linklaters LLP, Christina Speer-Reinsch, Pant Legal (Germany); GianBattista Origoni, Gianni, Origoni and Grippo & Partners (Italy); Dr. Jodok Wikki and Adrian Zogg, CMS von Erlach Henrici AG (Switzerland); Michal Nulicek, Lovells (Czech Republic); Krystyna Szczepanowska, Lovells (Poland); Takis Kommatas, T.G. Kommatas & Associates (Greece); Gonzalo Gallego, Lovells (Spain); Caroline Bush, Clayton Utz (Australia).

the goal of which is limiting the traditionally broad disclosure obligations. Further, statutes have been enacted such as the **Personal Information Protection and Electronic Documents Act**,[2] to provide guidelines for the production of confidential information.

Similarly, New Zealand has enacted the **Privacy Act 1993** to establish the parameters for the collection, handling and use of personal information. In both Canada and New Zealand, there is the development of the common law concept of a tort of invasion of privacy.

It is fascinating to compare how the various jurisdictions have handled this complex and sensitive issue. I thank each of the contributors for their thoughtful and useful essays.

Canada

Canada is a federal country and as a result has a patchwork of privacy and data protection laws governing the collection, use, and disclosure of personal information. However, most legislation defers to the court process. Recent changes to rules of civil procedure which limit the scope of discovery, including e-discovery show a trend away from the broad disclosure law obligations for disclosure to a proportional principle of discovery.[3] The current privacy laws in Canada generally exempt disclosure in a legal proceeding, including electronic documents, from statutory restrictions.[4]

Under the **Personal Information Protection and Electronic Documents Act**, information may be collected and used without consent in investigating a breach of an agreement or a contravention of law.[5] Section 7(3)(c) allows information to be disclosed without consent if the disclosure is required to comply with rules of court relating to the production of records or a court order.[6] Under Section 8(8), if the organization has the personal information that is being requested, it must retain the information for as long as necessary to allow the individual to exhaust any recourse that they may have to obtain the information.[7] The **Personal Information Protection Act**[8] includes a broad exemption for litigation discovery. Section 3(4) expressly states that it "does not limit the

---

[2] S.S.C. 2000, c. 5.

[3] The Sedona Conference Working Group 7, "The Sedona Canada Principles: Addressing Electronic Discovery", (January 2008) at 34 ["Sedona Canada Principles"]; Andrew F. Wilkinson, *Recent Developments in Electronic Discovery in Canada: Effects of the Sedona Canada Principles and the New Rules of Civil Procedure on the Discovery Process in Insurance Litigation*, in Insurance Law Conference – 2009 (September 2009) at 5.1.1.

[4] Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5 ["PIPEDA"]; Privacy Act, R.S.C. 1985, c. P-21; Freedom of Information and Protection of Privacy Act, R.S.B.C. 1996, c. 165; Personal Information Protection Act, S.B.C. 2003, c. 63 ["PIPA"]. *See also* Julius Melnitzer, *Balancing Privacy with E-discovery*, 17 L. TIMES No. 26 9 (August 2006); Alex Cameron & Julie DesBrisay, *Existing and Emerging Privacy-based Limits in Litigation and Electronic Discovery*, 4 CAN. PRIVACY L. REV. 125, 127 (Sept. 2007).

[5] *PIPEDA*, s. 7(1)(b), 7(2)(a).

[6] Cameron & DesBrisay, *supra* note 4 at 126 [reference added]; *PIPEDA*, s. 7(3)(c).

[7] *PIPEDA*, s. 8(8).

[8] S.B.C. 2003, c. 63.

information available by law to a party to a proceeding."

The courts have upheld Sections 7(3)(c) and 8(8) of *PIPEDA* as to third-party internet service providers in *BMG v. Doe*, stating that "... ISPs are not entitled to 'voluntarily' disclose personal information such as the identities requested except with the customer's consent or pursuant to a court order."[9] Practically speaking, a third-party organization who is requested to hand over personal information would probably request a court order before doing so.

PIPEDA's approach to litigation differs slightly from similar legislation in British Columbia, Alberta, and Quebec. Section 7(3)(c) in particular leaves open the question whether, in oral examinations for discovery, certain personal information must be disclosed. For this reason, *PIPEDA* has been criticized as being too narrow and impeding litigation and may be amended similar to the wording of the British Columbia and Alberta laws.[10]

In addition to legislation, courts and working groups have issued guidelines to assist parties when dealing with e-discovery issues. "The Sedona Canada Principles Addressing Electronic Discovery" and the Supreme Court of British Columbia "Practice Direction re: Electronic Evidence" provide guidelines dealing with e-discovery. These tools are helpful in determining how data protection and privacy laws affect the discovery process.

In 2006, the Supreme Court of British Columbia published a practice direction addressing procedures when dealing with large volumes of electronic documents. The procedures in the practice direction should be applied when: (a) a substantial portion of the potentially discoverable documents consist of electronic material; (b) the total number of potentially discoverable documents exceeds 1,000 documents; or (c) there are more than three parties to the proceeding.[11] If the parties agree, the plaintiff or petitioner must inform the court of that fact and the terms of the agreement.[12] Provision is also made for parties to apply to the court for an order that the proceeding be conducted in accordance with the provisions of the Practice Direction.[13] The impracticality of broad disclosure of electronic documentation, as currently required under the *Peruvian Guano* rule,[14] was a motivating factor for the reform of the rule requiring any document relating to any matter in question in the action.[15]

The new Supreme Court Rules incorporate the Sedona Canada Principles, twelve principles addressing e-discovery issues particular to Canadian law.[16] In particular, the new rules adopt the principle of proportionality espoused by the second Sedona Canada Principle.

---

[9] [2005] F.C.J. No. 858 (QL) at para. 37.
[10] Cameron, *supra* note 4 at 126.

[11] The Supreme Court of British Columbia, "Practice Direction Re: Electronic Evidence" (July 2006), s. 2.3.
[12] *Id.* at s. 2.4.
[13] *Id.* at s. 2.5.
[14] The Compagnie Financiere et. Commerciale du Pacifique v. The Peruvian Guano Company (1882), 11 Q.B.D. 55 (C.A.).
[15] Wilkinson, *supra* note 3 at 5.1.5 – 5.1.6.
[16] *Id.* at 5.1.2.

While the new rules will not include an exclusive rule regarding e-discovery,[17] they will affect discovery of electronic documents by addressing the substantive aspects of information and limiting the scope of discoverable information in general.

Common Law

The common law relating to privacy in e-discovery continues to develop. Melnitzer notes that courts dealing with privacy issues generally apply common law principles to e-discovery issues[18] Privacy protections are built into discovery with the implied undertaking of confidentiality prohibiting parties from using or disclosing information obtained during discovery for purposes other than the litigation.[19]

The courts of British Columbia and Alberta have adopted the proportionality principle in several judgments dealing with privacy in e-discovery, while courts in Ontario follow the principle of broad disclosure. Most cases in this regard deal with a request for direct access to hard drives and other electronic resources for the purpose of discovery. In British Columbia, a string of cases dating back to 1996 denied access to the other party's hard drive for the purpose of discovery, citing a lack of proportionality.[20] The Alberta Court of Appeal recently followed the British Columbia line of cases, denying access to a hard drive for the purpose of discovery.[21] In Ontario, requests for access to the other party's hard drive for the purpose of discovery have been granted several times.[22]

Invasion of Privacy

Generally, there is no universally recognized common law tort of "invasion of privacy" in Canada. However, there is some movement in Ontario jurisprudence toward recognizing such a legal right under common law. Several Ontario lower court decisions have suggested that individuals can be compensated for violation of privacy, while some have taken the position that such a tort does in fact exist under common law. In *Somwar v. McDonald's Restaurants of Canada Ltd.*, Stinson J. remarked that "[t]he traditional torts such as nuisance, trespass, and harassment may not provide adequate protection against infringement of an individual's privacy interests. Protection of those privacy interests by

---

[17] *Id.* at 5.1.3.

[18] Melnitzer, *supra* note 4 at 9.

[19] Jouman v. Doucette, 2008 SCC 8.

[20] *See* Northwest Mettech Corp. v. Metcon Services Ltd., [1996] B.C.J. No. 1915 (S.C.) (QL); Park v. Mullin, 2005 BCSC 1813; Baldwin Janzen Insurance Services (2004) Ltd. (c.o.b.) Baldwin Insurance Brokers) v. Janzen, 2006 BCSC 554; Desgagne v. Yuen, 2006 BCSC 955; Bishop (Litigation guardian of) v. Minichiello, 2009 BCSC 358.

[21] Innovative Health Group Inc. v. Calgary Health Region, 2008 ABCA 219.

[22] In CIBC World Markets Inc. v. Genuity Capital Markets, [2005] O.J. No. 614 (Sup. Ct. J.) (QL), the court allowed the motion. In Catalyst Fund Partner I Inc. v. Hollinger Inc., [2004] O.J. No. 5160 (Sup. Ct. J.) (QL) and [2005] O.J. No. 4231 (Sup. Ct. J.) (QL), the court also allowed the motion, citing that the individual inspecting the hard drives was a non-party. A more recent decision is Vector Transportation Services Inc. v. Traffic Tech Inc. (2008), 58 C.P.C. (6th) 364 (Ont. Sup. Ct. J.).

providing a common law remedy for their violation [of tort of invasion of privacy] would be consistent with Charter values and an "incremental revision" and logical extension of the existing jurisprudence."[23]

New Zealand

Privacy law in New Zealand (other than the emerging tort of invasion of privacy) is governed by the **Privacy Act 1993**. The Privacy Act identifies a number of Information Privacy Principles that establish norms of conduct in relation to the collection, handling and use of personal information. By contrast, disclosure of official information is governed by the **Official Information Act 1982** (for central government agencies) and the **Local Government Official Information and Meetings Act 1987** (for local government).

The Privacy Act applies to personal information, that is, information about an "identifiable individual". An identifiable individual must be a living natural person. The Privacy Act does not apply to information about a deceased person or corporate persons. The New Zealand Court of Appeal decision in *Harder v. Proceedings Commissioner*[24] discussed the concept of personal information under the Privacy Act. Although not making any definitive finding on this point, the Court of Appeal commented that the concept of personal information needs to be balanced with concepts of human rights and social interests in the free flow of information. These concepts are relevant to the scope of the definition of personal information. The *Harder* case indicates that the concept of personal information under the Privacy Act is not unqualified.

The Privacy Act applies to "agencies" including all governmental agencies covered by official information legislation, private sector organizations and, in some instances, individuals. "Information" is not defined by the Privacy Act. Electronically stored documents fall within the definition of "document", which includes: "any information recorded or stored by means of any tape-recorder, computer, or other device; and any material subsequently derived from information so recorded or stored." Reports from the Ombudsman have clarified that email correspondence falls within the definition of a document. However, where an email has been deleted and no hard copy exists it may be argued that the information is no longer held by the agency or is not readily retrievable. Information can also include unrecorded information held in a person's memory. This may be of relevance when conducting proceedings where the disclosure of information may occur through the giving of evidence before a tribunal or court. The concept of information held in a person's memory was discussed by the New Zealand Court of Appeal in *Commissioner of Police v Ombudsman*.[25]

Information Privacy Principles

The Privacy Act contains twelve Information Privacy Principles. Among

[23] (2006), 79 O.R. (3d) 172 (Sup. Ct. J.) at para. 29.
[24] [2000] 3 NZLR 80.
[25] [1988] 1 NZLR 385.

the most significant principles limiting day to day use and disclosure of personal information are:

Principle 1 – Personal information shall not be collected by any agency unless the information is collected for a lawful purpose connected with a function or activity of the agency, and the collection of that information is necessary for that purpose.

Principle 10 – Information collected for one purpose shall not be used for any other purpose. There are a number of exceptions where the use of information for another purpose may be allowed, for example where the individual has authorized the use or the information is publicly available. In addition, information may be used for the conduct of proceedings before a court.

Principle 11 – Personal information shall not be disclosed to another person, body or agency. The same types of exceptions as apply to Principle 10 also apply here, including the disclosure of information for the conduct of proceedings before a court.

The Information Privacy Principles do not confer legal rights enforceable in New Zealand Courts, with the exception of an individual's right of access to personal information held by an agency under Principle 6. If an individual believes there has been a breach of the Information Privacy Principles, a complaint can be made to a statutory officer-holder, the Privacy Commissioner, who will conduct an investigation and try to secure settlement between the parties. If settlement is not reached, proceedings can be brought before the Complaints Review Tribunal. For the Privacy Commissioner or Complaints Review Tribunal to find that there has been interference with an individual's privacy, there must have been a breach of an Information Privacy Principle *and* loss or damage (which may include an adverse effect on the individual's rights or obligations, significant humiliation, loss of dignity or injury to feelings).

Potential Pitfalls

There is very little judicial comment in New Zealand on the application of Principles 10 and 11, in particular in terms of data protection and discovery. For practitioners unaware of the New Zealand privacy landscape, it will be important to review the Information Privacy Principles and determine the purpose for which the information was collected. If information is to be used for another purpose or disclosed through discovery, the practitioner should ensure the use or disclosure is reasonably necessary for the conduct of the court proceedings.

People's Republic of China

Articles 38 and 40 of the **Constitution of People's Republic of China** establish general protections for a PRC citizen's rights relating to privacy, such as the right of dignity of the person, prohibitions against insult, defamation, false accusation or false information directed against Chinese citizens and a right of freedom and secrecy of correspondence. Corresponding provisions of the **General Principles of Civil Law** of the People's Republic of China recognize the right to identity and the right to protection of reputation of

individuals and legal persons. However, the People's Supreme Court has not treated privacy as a separate right—it treats a claim to privacy violation akin to that of violation of one's reputation under its relevant judicial interpretations. This means that under the current law, an action for privacy violation can be considered by a court only if the plaintiff's reputation has also been violated or affected.

Provisions of computer-related, internet-related and database-related laws, such as the **Regulation on Management of the Administration of Internet Electronic Messaging Services** (hereinafter "RMAIEMS"), require that the contents of particular databases be kept confidential, be protected by security measures and procedures and not be breached, altered or distributed. Article 12 of RMAIEMS requires particular consents to be obtained before personal information may be collected in certain circumstances. The **Postal Law** of the PRC provides protection on citizen correspondence, "Freedom and privacy of correspondence of citizens are protected by law." The **Practicing Physician Law** requires that doctors not reveal health information obtained during treatment and those who violate this law face criminal penalties.

Discovery in the PRC

There is no *inter-partes* discovery in PRC civil procedure. The people's courts have the right to conduct investigation and collect evidence from legal persons or individuals, who may not refuse to provide information and evidence.

When a foreign enterprise is a party to foreign litigation which requires the investigation or the gathering of evidence from its subsidiaries in the PRC, the applicable foreign court may not conduct the investigation, issue and/or enforce a discovery request against the PRC entities on its own motion, as such action may constitute a violation of judicial sovereignty contrary to Articles 260, 265 or 266 of the PRC Civil Procedure Law. The proper course, if it is necessary for a discovery request or order to be made directly against the PRC entity, is for an application to be made by the foreign court or by a party to the foreign litigation to the people's court or to the PRC ministry of justice pursuant to international treaties or reciprocal arrangements.

For example, in *Suqian Wahaha Beverage Co. Ltd. et. al. v. KPMG Guangzhou*,[26] the plaintiff successfully sued the defendant for investigating its affairs pursuant to a disclosure order issued by a foreign court. Staff of the defendant company, an accounting firm, had been appointed by the High Court in the British Virgin Islands to gather evidence and seek disclosure of the claimant's affairs in the PRC. Accordingly, they sent letters to banks, government bodies, accounting firms and to the plaintiff's trade counterparts in the PRC, requesting cooperation with their investigation and attaching a court order to their letters which included the legend "It is a contempt of court for any person notified of this order to assist in or permit a breach of this order. Any person doing so may be imprisoned, fined or have their

[26] (2008) Su Zhong Min Er Chu Zi 0040.

assets seized." In litigation before the people's court in the PRC, the plaintiff successfully proved that the letters had infringed its right of reputation under Article 101 of the General Principles of Civil Law. In addition, the people's court held that an accounting firm is not authorized under the PRC Accounting Law to gather evidence or to conduct investigations and that by doing so at the instance of a foreign court, the defendant accounting firm had exceeded its lawful business scope and offended the judicial sovereignty of the PRC courts in violation of the PRC Civil Procedure Law.

When faced with a discovery request or foreign court order directed against the foreign parent company of a PRC entity, the foreign parent company may comply by requiring the PRC entity to voluntarily produce the documents in its possession or custody to it. There are no laws or regulations which prevent or prohibit such voluntary disclosure to a shareholder. Such requests by shareholders may be considered as the exercise of the shareholder's "right to know" which is a right enshrined in Articles 34 and 98 of the **PRC Company Law**. Note that while giving shareholders a "right to know", these provisions also limit the scope of requests for information or documents which shareholders may make such that even some of those Company Law requests may only be enforced by having recourse to the people's courts.

Exceptions also arise where compliance with a lawful request for production would result in a violation of the abovementioned privacy protections afforded under PRC laws, i.e., requiring the production of protected medical records, and private correspondence. Note that in relation to private correspondence, it is inherently unlikely that a PRC entity would have possession of correspondence that may be deemed "private". Under PRC law, information including any employee correspondence stored on an entity's computer systems is typically considered company intellectual property rather than private correspondence.

China currently has no major e-discovery or data protection laws. The requirement, under Article 67 of the PRC Civil Procedure Law that all documentary evidence used in PRC civil proceedings be notarized to a certain extent restricts the development of e-discovery in PRC civil litigation. As a result, the need to make new laws regulating this area of litigation practice has not arisen.

France

The CNIL (*Commission nationale de l'informatique et des libertés*) is the entity dedicated to data protection and supervises the implementation of the **Data Protection Act of January 6, 1978**, as amended by the August 6, 2004 Act relating to "information technology, files and liberties" called *"loi informatique et libertés"*. This French Act was one of the principal inspiration of the European Directive adopted on October 24, 1995.

The principles of data protection are given by the act n°78-17 of January 6, 1978 on data processing, data files and individual liberties and the decree n° 2005-1309 of October 20, 2005 enacted for the application of Act n° 78-17 of January 6, 1978 on Data Processing, Files and Individual Liberties (Amended by

Decree n° 2007-451 of March 25, 2007) consolidated on the 25th of March 2007.

Personal data must be loyally collected with a lawful end purpose with the prior knowledge of the individual. According to the law, personal data means any information relating to an identified or identifiable individual; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number (e.g. social security number) or one or more factors specific to his physical, physiological, mental, economic, cultural or social identity (e.g. name and first name, date of birth, biometrics data, fingerprints, DNA). To define personal data, account must be taken of all the means available to the "data controller" to determine whether a person is identifiable. Personal data are any anonymous data that can be double checked to identify a specific individual (e.g. fingerprints, DNA, or information such as "the son of the doctor living at 11 Belleville St. in Montpellier does not perform well at school"). All fraudulent, unfair or illegal collection of data is prohibited.[27]

Pursuant to the Law, computer processing must be done according to an explicit end purpose, and it is with regard to this end purpose that one can appreciate the relevant, adequate and non-excessive nature of the data recorded, the categories of persons or organisations who may receive these data, and the duration for which the collected data may be stored.[28]

Persons whose personal data are collected must be informed of:

- the compulsory or optional nature of the responses,
- the consequences of failing to give an answer,
- the categories of persons or organisations who could eventually have knowledge of the data, and
- the place where the right of access and rectification may be exercised.[29]

Any information which shows, directly or indirectly, racial origins, political, philosophical or religious opinions, trade union membership, or moral principles of the person can only be collected and recorded with the express (written) agreement of the person concerned. Such data may, for reasons of public interest, be collected on the authorization of a decree by the Council of State issued on the recommendation of the CNIL (this may be the case for certain police files). No decision concerning an individual may be taken based only on a processing whose original purpose is to evaluate the "profile" or presumed personality of the person by statistics.[30]

---

[27] *See* Article 226-18 of the Criminal Code (5 years' imprisonment, 300 000 € fine).

[28] *See* Articles 226-21 and 226-20 of the Criminal Code (using personal data for purposes other than those that justified their collection, or storing them beyond a date justified by the purpose of the processing is punished, respectively, by 5 years' imprisonment and a 300 000 € fine and 3 years' imprisonment and a 45 000 € fine).

[29] Decree of December 23, 1981, Article 2.

[30] Act n°78-17 of January 6, 1978, Article 2.

Data transfers

When all or part of a file containing personal data is transferred towards a foreign country, the person in charge of the transfer has to make sure that the legislation of the State towards which he sends his data guarantees a level protection of the particular amount to the country of origin. All the countries of the European Union generally give an equal level of protection as the treatments of personal data are supervised by the EU Directive. The CNIL does not have to authorize transfers towards countries granting an adequate protection. The CNIL will however have to be informed about the existence of these transfers within the framework of the preliminary formalities in the implementation of the main treatment from which these transfers arise.

The EU Directive and the French data protection acts regulate the transfers of personal data outside the territory of the European Union. The exporter of data, responsible for the treatment on the European territory, must ensure that the European data will be protected in an adequate way outside the European Union. On principle, transfers outside the European Union are forbidden except when the country or the company addressee insures an adequate level of protection to the transferred data. This adequate protection can be brought by several manners:

- The country addressee of the personal data has a legislation recognized by the European Commission as offering an **adequate level of protection** (Canada, Isle de Man, Switzerland, Argentina, Guernsey, Jersey),
- In a contractual way, by the signature of Typical Contractual Clauses adopted by the European Commission by the exporting entity and that importer of personal data,
- By subscribing to the principles of Safe Harbor, defined by the European Commission and the American Commerce Department, the American company addressee of the information,
- By adopting internal rules of company or "BCR". These rules, applicable to all the entities of the group, contain the key principles allowing supervision of transfers of personal data from the European Union. These internal standards can serve as guide for the employees in management of the data. It insure the customers and the partners that the conditions of transfer of their personal data by the company at the world level.
- By calling upon an exception planned by Article 69 of data protection acts.

According to the general principles of the French law and the community law, these dispensations must be strictly interpreted because they imply a total absence of protection in the country addressee for the concerned person.

United States Pre-trial Discovery

CNIL has found that a growing number of motions are being filed, requiring the disclosure of personal data held, among other, by French subsidiaries of United States corporations subject to pre-trial discovery procedures in US litigation cases. It has become frequent to see companies or their foreign subsidiaries forced to turn over copies of the full contents of the hard disks or e-mail boxes of some employees, or even the entire personnel.

Furthermore, though in a different legal context, a number of United States authorities, such as the Securities and Exchange Commission (SEC) or Federal Trade Commission (FTC), may also issue information injunctions demanding that foreign companies produce documents or evidence, by virtue of their respective powers of investigations. Information injunctions may concern French companies who are subsidiaries of United States corporations listed on United States exchanges, or French-law companies operating in the United States.

As the United States does not offer an adequate level of protection, such disclosure requirements breach the French legal provisions on data protection, and more specifically those applicable to the information and consent of individuals, to the proportionality of the data processing involved and to the conditions of data transfers outside the EU. In addition, these situations give rise to difficulties falling within remits other than just the Data Protection Act, related among other to international judicial cooperation, protection of domestic economic interests, industrial and commercial secrecy, or even to national sovereignty.

The French Law of July 26, 1968 on the disclosure of documents and information of an economic nature prohibits, unless otherwise provided under international covenants, any person from requesting or disclosing any documents or information of an economic, commercial, industrial, financial or technical nature likely to be used to compile evidence intended for use in legal or administrative proceedings or arising from them. Hence, such requests from foreign administrative authorities may be legally allowed only if covered under an international agreement or treaty.

Furthermore, a Mutual Assistance Agreement was signed between different French authorities like the *"Autorité des Marchés Financiers"* (AMF), and the corresponding UN authorities like the US Securities Exchange Commission (SEC). Thus, for example in financial matters, French companies directly requested by the SEC to disclose information must file a prior information request to the AMF in order to protect themselves from any subsequent risk of criminal prosecution.

Germany

In Germany, the EU Directive[31] has been implemented by the **Federal Act.**[32]

[31] Directive 95/46/EC of October 24, 1995 (Eur. Official Journal 95/L281, p. 31); available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML.

[32] *Bundesdatenschutzgesetz* of December 20, 1990 as promulgated on January 14, 2003 (Federal Law Gazette Vol. I, 2003, p. 66), last

Subject to a few minor exceptions, this Act thus provides for the same data privacy standards that apply in all EU member states. It is lawful to process data only if either all affected individuals have provided consent or statutory permissions apply. Obtaining consent often is simply impracticable. Moreover, employees' consent may considered invalid.

If a company has allowed its employees to use its e-mail system for private purposes or has at least tolerated such usage, far-reaching additional restrictions may apply under the **Federal Telecommunications Act**[33] and the **Federal Telemedia Act**[34] in which case specific remedies must be taken to make E-discovery of emails at all feasible.

In accordance with the EU Directive, the Federal Data Protection Act broadly defines "personal data" to mean "any information relating to an identified or identifiable person." Thus, the application of German data privacy laws does not depend on how significant or trivial the information may appear or on the circumstances under which the data was generated or stored. For example, the following information would be protected: the name, position, and email address of an employee; that an employee sent or received a certain email, wrote a certain document or had a certain file stored on his/her computer (each irrespective of the contents of the email or the file); and that he/she attended a certain meeting. It suffices that the data subject (e.g. employee, customer or supplier of the company) is "identifiable". For example, even if minutes of a meeting mention an attendant by its job titles only (e.g. "Head of Finance"), the minutes are protected because the attendant can usually be identified by recourse to other information. In summary, effectively all emails and, as a rule, all electronic documents are thus protected by German privacy laws.

In addition to data privacy laws, German labor law should be considered. In particular, under the **Works Constitution Act**,[35] the Works Council

---

amended by Act of August 14, 2009 (Federal Law Gazette Vol. I, 2009, p. 2814); available at http://www.gesetze-im-internet.de/bundesrecht/bdsg_1990/gesamt.pdf; non-official English version (possibly outdated) available at http://www.bfdi.bund.de/cln_111/EN/DataProtectionActs/DataProtectionActs_node.html.

[33] *Telekommunikationsgesetz* of July 25, 1996, as revised on June 24, 2004 (Federal Law Gazette Vol. I, 2004, p. 1190), last amended by Act of August 14, 2009 (Federal Law Gazette Vol. I, 2009, p. 2821); available at http://www.gesetze-im-internet.de/bunderecht/tkg_2004/gesamt.pdf; non-official English version (possibly out-dated) available at http://www.bfdi.bund.de/cln_111/EN/DataProtectionActs/DataProtectionActs_node.html.

[34] *Telemediengesetz* of February 26, 2007 (Federal Gazette Vol. I, 2007, p. 179), last amended on August 14, 2009 (Federal Gazette Vol. I, 2009, p. 2814); available at http://www.gesetze-im-internet.de/bunderecht/tmg/gesamt.pdf (German version available only).

[35] *Betriebsverfassungsgesetz* of January 15, 1972 in the version promulgated by Act of September 25, 2001 (Federal Law Gazette Vol. I, 2001, p. 2518), last amended by Act of July 29, 2009 (Federal Law Gazette Vol. I, 2009, p. 2424); available at http://www.gesetze-im-internet.de/bunderecht/betrvg/gesamt.pdf; non-official English version (possibly outdated) available at http://besondere-dienste.hessen.verdi.de/download-bereich/data/BetrVG%20Englisch.pdf.

of the company may assert a right to approve or disapprove methodologies for the collection of employee data.

Potential Pitfalls

The scope of "personal data" in the meaning of Data Protection Act is broad and not consistent with the concept of privacy rights. It comprises (i) not only private, but also merely work-related information, and (ii) both information directly relating to an individual (such as names) as well as information otherwise attributable to an individual. Most emails include some personal data. Prior to document production, proper document retention policies should be in place. European Data Protection Authorities demand, before document production, the redaction of materials, data filtering operated in Germany by independent trustees, proper advance notices to data subjects, protective orders, technical and organizational measures, conclusion of data processor agreements and/or EU Model Contracts.

Italy

In Italy, data processing is ruled by **Legislative Decree no. 196 of 2003**, the so called Privacy Code (the "Code"), which is basically in line with the European Directive on Data Processing-[36] the broad and all-inclusive definition of personal data included.

The most relevant cases where the Code departs from the EU Directive and which should be consequently taken in account as potential pitfalls, include the following:

(i) Data relating to legal entities (and not to individuals only) are subject to the Code;

(ii) The "legitimate interest" exemption from the consent is not based on a self-assessment but requires a specific assessment by the Garante (the Italian Data Processing Authority); and

(iii) Consent for the processing of sensitive data as well as the appointment as processor and/or person in charge of the processing have to be in writing.

An e-discovery plan in compliance with opinion no. 1 of February 11, 2009, issued by Article 29 Data Protection Working Party and concerning pre-trial discovery for cross border civil litigation, is in general terms possible in Italy, provided that the above requirements are met. As far as the data transfer abroad is concerned, it can be dealt with ordinary means, the EU standard clauses or Safe Harbor.

Potential Pitfalls

E-mail and internet monitoring in workplace is governed by a quite detailed Guideline issued by the Garante.[37] Statute 300 of 1970, the so-called **Workers' Statute**, provides for some limitations in relation to the data that employers can collect and the ways whereby such a collection may take place. If the conditions set forth by the Guideline and Workers' Statute have not

[36] *See supra* note 1.

[37] Available at www.garanteprivacy.it/garante/doc.jsp?ID=1408680.

previously been satisfied, the "secondary use" of the data for discovery purposes can be very problematical.

Switzerland

In litigation, parties may request disclosure of specific documents as part of the evidence collection. Provided the requesting party made relevant and specific allegations it its pleadings, the court may direct the other party, but also third parties not involved in the proceedings and government agencies, to disclose relevant documents in their possession relevant to the proceeding. Disclosure may be rejected by the court if it would unjustifiably violate the opposing party's privacy, and additional limitations may also apply. In agency relationships, and related contracts, the principal may request disclosure of specific information from the agent as part of his right for appropriate accounting. No distinction is made between electronic or paper information.

Article 13 of the **Swiss Federal Constitution**[38] provides for the fundamental right to privacy in the private and family life, at home, and in relation to mail and telecommunications and that everyone has the right to be protected against the misuse of his personal data. The data protection is codified in the **Swiss Federal Act on Data Protection** ("FADP")[39] which came into force on July 1, 1993. The appropriate Ordinance[40] governs the details.

Many rules exist in other acts and areas with the purpose to protect the personality. Specifically, Articles 28 - 28l of the **Swiss Civil Code**[41] stipulate how to proceed in case of violation of personality rights. The website of the Swiss Federal Data Protection and Information Commissioner (http://www.edoeb.admin.ch) provides further information (some in English) about data protection and privacy laws.

Based on Article 8 of the FADP, any person may request information from the controller of a data file as to whether data concerning that person is being processed, subject to the limitations set forth in Article 9 et seq. of the FADP. This right is independent of whether the data is stored in paper or electronic form.

The Netherlands

Dutch law does not provide for a general duty to disclose comparable to the English or American discovery rules. In the Netherlands, parties will generally only disclose those documents which assist their case and on which they wish to rely. However, the Dutch law of procedure does contain a limited number of specific regulations which allow the court to order the disclosure of specific documents. Such an order may be disregarded by the parties concerned, but the court may then draw any conclusion it

[38] Available at http://www.admin.ch/ch/e/rs/c101.html.

[39] Available at http://www.admin.ch/ch/e/rs/c235_1.html.

[40] Available at http://www.admin.ch/ch/e/rs/c235_11.html.

[41] Available at http://www.admin/ch/ch/d/sr/c210.html.

deems appropriate from the fact that the parties have refused to disclose the requested documents. In addition, the court may, upon application by a party or ex officio, also order the disclosure of documents upon payment of a fine for every day the ordered party fails to comply with the order.

The **Netherlands Data Protection Act** ("NL Act") is an implementation of the EU Directive.[42] The NL Act addresses the fully or partly automated processing of personal data and the non-automated processing of personal data in a file. Practitioners should be aware that simply collecting or reviewing for example e-mails of an employee (the data subject i.e. the person to whom personal data relate) will be considered to be "processing of personal data." Processing of personal data shall not take place where precluded by an obligation of confidentiality by virtue of office, profession or legal provision. In the Netherlands, 'privilege' doesn't apply to company lawyers. If documents of a Netherlands company lawyer are governed by U.S. or U.K. data protection law, they may remain privileged.

Data may be processed where:

1. the data subject has unambiguously given his consent for the processing;
2. the processing is necessary in order to comply with a legal obligation to which the data controller is subject;
3. the processing is necessary for upholding the legitimate interests of the data controller or of a third party to whom the data are supplied, except where the interests or fundamental rights and freedoms of the data subject, in particular the right to protection of individual privacy, prevail.

Articles 76 and 77 of the NL Act contain additional requirements for the transfer of data to countries outside the EEA which do not provide a so-called "adequate level of data protection," but are permitted if:

1. The data subjects have unambiguously given their consent thereto;
2. The recipient in the U.S. adheres to the so-called Safe Harbor Principles;
3. The recipient signs a so-called EU model agreement on the basis of which the Dutch data controller has received a permit from the Ministry of Justice;
4. The transfer is necessary on account of an important public interest or for the establishment, exercise or defense in law of any right.

The truly safe way to process and transport personal data from the EEA to a recipient that does not offer an adequate level of protection or that otherwise is covered by an exception is to obtain a court order from a Member state that authorizes the production of the result through the use of a letter of request submitted under the Hague Evidence Convention. The Netherlands have signed this convention with the reservation under

[42] *See supra* note 1.

Article 23 with the effect of declaring that (pre-trial) discovery of any information regardless of relevance, would not be allowed if it is sought in relation to foreign legal proceedings.

Potential Pitfalls

Don't forget to comply with the applicable internal company polices. According the Dutch co-determination law, staff councils have to give consent to such policies. Sensitive personal data are data concerning a person's religion or philosophy of life, race, political persuasion, health and sexual life, trade union membership criminal behavior, or unlawful or objectionable conduct connected with a ban imposed with regard to such conduct. These data and the tax and social security numbers have extra legal protection.

Poland

Legislation on the protection of personal data in Poland is intricate. On the one hand, there is a statutory regulation of a general nature, namely the Polish **Act on the Protection of Personal Data of August 29, 1997** (the "Act"). On the other hand, there are detailed regulations defined in the laws governing separate areas of business activities, such as the **Telecommunications Law**, the **Banking Law**, the **Act on Providing Services by Electronic Means** and the **Law on Insurance Activity**. These acts often increase the requirements for the processing of personal data. There are also other minor pieces of legislation covering technical and organizational conditions of data protection. The provisions of the Act apply to entities which process personal data for business or professional activity purposes or for the implementation of statutory objectives, and which have their registered office or reside in the territory of Poland or in a third country, if they are involved in processing personal data by means of technical devices located in the territory of Poland.

The Act recognizes as personal data any information relating to an identified or identifiable natural person. Information which makes a person identifiable directly or indirectly is, in particular, any identification numbers or one or more factors specific to the physical, physiological, mental, economic, cultural or social identity of that person. The objective scope of the Act only includes the personal data of natural persons. The provisions of the Act do not apply to the processing of personal data of other entities, especially legal persons, organizational units which are not legal persons, or personal data of deceased persons.

The Act determines the principles of personal data processing and the rights of natural persons whose personal data is processed. The Act applies to the processing of personal data in data filing systems, as well as to data processing in computer systems, and defines processing as any operation which is performed on personal data, including data collection, recording, storage, organization, alteration, disclosure and erasure. As a consequence of such a broad definition of data processing, any operation on personal data does in fact fall within the scope of the Act. The basic principle with which the processing of personal

data must comply is to demonstrate the legal basis for the processing of personal data. Generally speaking, the basis for the processing of personal data can be divided into conditions requiring the consent of the individual whose data is processed, and conditions not requiring such consent, e.g. processing is necessary for the purpose of exercising rights and duties resulting from a legal provision or the performance of a contract to which the data subject is party, or is necessary for the performance of tasks provided for by law and carried out in the public interest.

Polish legislation also introduced the obligation to report a data filing system for registration by the Inspector General for Personal Data Protection ("GIODO"). The data filing system as such is subject to notification and registration. The data controller is required to carry out the registration before the start of personal data processing. The Act states that, in certain circumstances, data controllers are not obliged to submit a data filing system for registration. Exemption from registration does not, however, mean exemption from the application of other provisions on the protection of personal data. The data controller is obliged to inform the GIODO about any changes affecting the information notified for registration within 30 days following the date of the change. The GIODO issues a certificate of registration of the data filing system to the data controller immediately after the registration.

The Act also provides a closed list of data recognized as sensitive data, i.e. data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, religious, party or trade-union membership, as well as data concerning health, genetic code, addictions or sex life and data relating to convictions, decisions on penalties, fines and other decisions issued in court or administrative proceedings. The Polish legislature has provided a full transposition of the EU Directive in this field and consequently, as a general rule, the processing of this data is prohibited except for the conditions clearly stated in the Act.

Polish provisions establish technical and organizational measures designed to protect the personal data being processed, appropriate to the risks and category of data being protected, and in particular to protect data against its unauthorized disclosure, its takeover by an unauthorized person, processing in breach of the Act, and any change, loss, damage or destruction.

As the Act does not enumerate any criteria that should be taken into consideration while estimating the level of personal data protection in force in a third country, the evaluation of the level of protection is on each occasion within the competence of the data controller, and the GIODO does not issue any certificate in this matter. The transfer of personal data to a third country which does not ensure at least the same level of personal data protection as that in force in the territory of Poland may take place subject to the prior consent of the GIODO, provided that the data controller ensures adequate safeguards with respect to the protection of privacy, rights and freedoms of the data subject.

Potential Pitfalls

In the Polish legal system, a breach of the provisions on the protection of personal data may result in legal consequences of an administrative, civil and even criminal nature. As regards administrative sanctions, the GIODO may, by means of an administrative decision, order the data controller to restore the proper legal state. However, certain acts concerning the processing of personal data are subject to criminal liability. Criminal sanctions (a fine, a partial restriction of freedom or even a prison sentence of up to three years) can only be imposed on natural persons at the data controller who are responsible for the processing of personal data.

Since 2008, a legislative process in the Polish parliament aimed at introducing administrative sanctions to the Act has been in progress. The GIODO will be authorized to impose a financial penalty of between € 1,000 and € 100,000 on a data controller who does not comply with the GIODO's previous decision, ordering the proper legal state to be restored. The GIODO will also be authorized to impose (by means of an administrative decision) a financial penalty of up to 300 percent of the monthly revenues on the manager of the entity being inspected or a person acting on his authorization, if they prevent or hinder the performance of inspection activities.

Czech Republic

The primary source of data protection law in the Czech Republic is **Act No. 101/2000 Coll., the Data Protection Act** (the "DTA"). In addition, "sector-specific" provisions apply to data protection in areas such as archiving, tax proceedings, electronic communication, surveillance systems, unsolicited commercial communications, police procedure, labor relations and employment, personal documents, radio and television fees, and healthcare.

The DTA and other laws dealing with the data protection protect "personal data", that is, any information relating to an identified or identifiable data subject (i.e. a natural person) to which the personal data relates. The definition is broad and includes very basic information such as a person's name, address and profession, whether contained in emails, personnel files or business correspondence. It is sometimes possible to identify the subject from a single piece of data (e.g. a photograph), but this is unusual. Czech data protection legislation does not protect the data of legal entities.

The data subject must give a valid consent to the collection, processing and use of personal data. There are several exceptions set out in Sec. 5 para. 2 of the DTA, including:

(a) compliance with the controller's legal obligations;
(b) performance of a contract to which the data subject is a contractual party;
(c) to protect the vital interests of the data subject, in that case the controller must obtain the consent without undue delay. If consent is not given, the processor must immediately stop the processing and discard the data;

(d) in accordance with special legislation;
(e) to protect the rights and legally protected interests of the data processor;
(f) if the data subject is a publicly-employed person, officer or employee of a public administration, and the data reveals the public or official details of the data subject's career or job assignment; or
(g) solely for archival purposes under a special law.

The data subject must consent to the data processing knowingly and of his/her own free will, and must be informed of the details of the data to be processed, the purpose for which it is to be processed, the identity of the data controller and the extent of the processing period. The data controller must be able to demonstrate that the data subject's consent extended to the entire period of processing.

Specific rules exist with respect to certain categories of data. As a principle, sensitive data, (i.e. personal data revealing national, racial or ethnic origin, political attitudes, trade union membership, religious and philosophical beliefs, criminal convictions, health and sexual data, genetic information and biometric data which allows the direct identification or authentication of the data subject) can only be processed with the data subject's explicit consent. Moreover, the data subject must be made aware of the details of the data to be processed, the purpose for which it is to be processed, the identity of the data controller and the extent of the processing period.

Personal data may only be transferred from the Czech Republic to a country outside the European Union or European Economic Area on the basis of an international treaty dealing with the free transfer of personal data or on the basis of a decision of the EU (such as Safe Harbor). If these conditions are not fulfilled, the transfer may only be carried out under special circumstances (Sec. 27 para. 3 DTA). In such cases, the controller must obtain an authorization from the Office for Personal Data Protection (the "Office") prior to the transfer of personal data to third countries pursuant to Sec. 27 para. 3 DTA.

Transfer of data to the U.S. for discovery including e-discovery purposes

The transfer of documents including personal data to the U.S. for discovery purposes is problematic under Czech and EU data protection law. One of the main difficulties with cross-border litigation is the control of use, for litigation purposes, of personal data which has already been legitimately transferred to the U.S. for other reasons. Another problem is that EU data controllers have no legal grounds for storing personal data for an unlimited period of time because of the possibility of litigation in the U.S., however remote this may be.

In order for the pre-trial discovery procedure to take place lawfully, the processing of personal data must be legitimate and must satisfy one of the three grounds listed above, i.e. the data subject must consent, or the data processing must be necessary to comply with a legal obligation, or the data must

be processed to fulfill a legitimate interest of the controller or a third party to whom the data is disclosed. In practice, none of these grounds seem to be fulfilled.

As stated above, consent must be informed and freely given. However, if a company has chosen to do business in the U.S. or involving U.S. counterparts, the data subjects (e.g. the customers and employees of a company) are usually not given a choice or are not involved in the decision to do business in or with the U.S., or are not properly informed. Therefore, data controllers might in practice have problems with obtaining clear evidence of the data subject's informed and free consent. Regarding the second ground, it must be noted that an obligation imposed by a foreign legal statute or regulation may not qualify as a legal obligation which would permit data processing in the EU. Therefore, fulfillment of the obligations imposed by U.S. laws will not constitute a legal ground for transfer of data. The third ground can only apply in cases where such legitimate interests are not overridden by the data subject's fundamental rights and freedoms. This balance of interest test should take into account issues of proportionality, the relevance of the personal data to the litigation and the consequences for the data subject. A possible alternative solution is to make the data anonymous or use pseudonyms.

Potential Pitfalls

Compliance with data protection laws is supervised and enforced by the Office. Inspectors from the Office carry out and supervise inspections, and produce data protection protocols, including remedial measures. They may also conduct administrative proceedings to impose penalties, and proceedings for offences arising from the facts set out in the data protection protocols. Non-compliance with data protection laws constitutes an offence punishable by administrative fines of up to 10,000,000 CZK (approx. 393 000 €) per breach. Unauthorized personal data usage can also constitute a criminal offence under Sec. 180 of the Act No. 40/2009 Coll., the Criminal Code, punishable by up to 8 years' imprisonment. According to Sec. 367 of the Criminal Code, a person who does not prevent the commission of such a crime can be imprisoned for up to 3 years.

Spain

The primary source of data protection law in Spain is the **Data Protection Act 15/1999**, of December 13, 1999 ("LOPD") and its regulation passed by the **Royal Decree 1720/2007**, of December 21, 2007. In addition, there are "sector specific" provisions on data protection, e.g., in the **E-Commerce Act 34/2002**, of July 11, 2002; the **Telecommunications Act 32/2003**, of November 3, 2003 and its regulation passed by the **Royal Decree 424/2005**, of April, 15 2005. Compliance with data protection laws in the private business sector is supervised and enforced by the Spanish Data Protection Agency ("AEPD") (www.agpd.es).

Personal data means information which relates to a living individual and from which he or she can be identified, whether or not in conjunction with any

other information, provided that the identification does not require a disproportionate effort. Data of companies (legal entities) is not protected under Spanish data protection legislation. Common examples of personal data include: name, contact details, CVs, performance reviews, ID card/ passport, pictures/ video, fingerprints/ voice, health data, and trade union membership. However, the AEPD tends to apply the concept of personal data very widely. There are cases where the AEPD has considered that certain information was personal data although it was very difficult to link the information with an individual (for example, license plate number).

In general terms, processing of personal data requires the consent of the data subjects. Under the LOPD, the data subject's consent is valid only when data subjects from whom personal data is requested have been previously provided with specific information set forth therein. There are some exceptions to the consent requirement, which are applied by the AEPD on a restrictive basis, including:

(a) when a law requires the processing of the data;
(b) when the personal data relate to the parties to a contract or preliminary contract for a business, employment or administrative relationship, and is necessary for its maintenance or fulfillment; and
(c) when the data is contained in sources accessible to the public (as regulated in the LOPD) and its processing is necessary to satisfy the legitimate interest pursued by the controller or assignee of the data, unless the fundamental rights and freedoms of the data subject are jeopardized.

International transfers of personal data to public or private entities or individuals located in the territory of a country which is not a member of the EEA and which the EU Commission has not declared that they provide an adequate level of protection are not allowed except with the prior authorization of the Director of the AEPD. Such authorization is obtained on a case-by-case basis. However, there are a number of exemptions which allow carrying out international transfers without the previous authorization of the AEPD. The most relevant are as follows:

(a) when the transfer is necessary or legally required to safeguard a public interest (e.g., a transfer requested by a tax or customs authority for the performance of its task shall be considered as meeting this condition);
(b) when the data subject has given his/her unambiguous consent to the international transfer.
In these cases, in order the consent for the international transfer to be valid, data subject must be provided with information regarding the fact that the transfer is to "X" country not providing an adequate level of protection according to the Spanish and EU data protection

regulations and the purposes of the transfer;

(c) when the transfer is necessary for the performance of a contract between the data subject and the data controller or the adoption of pre-contractual measures taken at the data subject's request; and

(d) when the transfer is necessary for the execution or performance of a contract executed, or to be executed, in the interest of the data subject, between the data controller and a third party.

Note that these exceptions are applied on a very restrictive basis by the AEPD. This is particularly relevant in the last two cases. The "need" identified for the purpose of the exceptions must be a genuine need.

A transfer of documents containing personal data, e.g., business correspondence, to the U.S. for discovery purposes faces difficulties under Spanish data protection law. Obligations under U.S. law to provide certain information to a court or authority do not constitute statutory provisions that allow the processing of personal data under Spanish law. Regarding the described special categories of data, a justification is even more difficult.

Potential Pitfalls

Spain has not implemented the "legitimate interest" or "balance of interest" justification for the processing of data, in the same terms provided for in EU Directive. Generally speaking, "legitimate interest" is only applicable for the processing of data collected from public sources or where the "legitimate interest" is provided for in a Spanish Law or Community provision. This is a relevant difference between the Spanish data protection system and that of most of the Member States and must be taken into consideration when implementing multijurisdictional data protection compliance programs. Thus, different from other Member States, it is not possible to rely on the "legitimate interest" or "balance of interest" exception in order to transfer the data to the U.S. authorities. Under certain circumstances, a solution may be to make the data anonymous. Anonymous data is that which does not allow the identification of the individual, in any way nor by any person (not even by the person who anonymised the data). Another solution could be to obtain the data subjects' valid consents to the data transfers as explained above.

Prior to the creation of a personal data file, data controllers must notify the AEPD of the creation of the data file. In general terms, the notification must contain details of the data controller's corporate identity, security measures implemented (indicating whether they are basic, medium or high level measures), the type of data processed, the purposes of the processing, details of foreseeable disclosures and international transfers of personal data and information about the existence of data processors. The notifications of personal data files must be kept updated. Thus, the data controllers are required to notify to the AEPD any modifications in the personal data.

Greece

Data protection and privacy matters are in generally governed by **Greek Law No. 2472/1997**, which incorporated the respective provisions of the EU data protection directive. The above legislation is interpreted by the regulations and decisions of the Hellenic Data Protection Authority, the regulatory authority being competent for the application of the data protection legislation in Greece. Moreover, **Greek Law No. 3471/2006** contains provisions for the protection of privacy in the field of electronic communication. The provisions of this law apply mostly to the companies engaged in the provision of electronic communication services and therefore, reference will not be made to its provisions herein.

The main distinction in data protection in Greece refers to personal data and sensitive personal data. As personal data[43] is defined, any information referring to the data subject, while sensitive personal data[44] are deemed any data relating to racial or national origin, political beliefs, religious or philosophical beliefs, participation in a union, health, social security and sex life, as well as any data relating with criminal accusations or convictions and participation to any associations relating to all the above. Processing of personal data (including disclosure to third parties) in Greece is subject to either the data subject's prior consent, which has to be in writing in the case of sensitive personal data and is permitted without the data subject's prior consent solely exceptionally, if conditions[45] for sensitive personal data (in which case the permission of the Hellenic Data Protection Authority is also required) are met.

Electronically stored data is not ruled separately by Greek data protection legislation. However, the Hellenic Data Protection Authority has issued decision No. 61/2004 establishing general guidelines on the processing of personal data of the computers of the employees. Under these guidelines, the use of a software enabling the employer to have access to the stored area of each employee's computer has to be announced to the employees in a precise and understandable to everyone way, stating the purpose of the establishment and use of such software by the employer as well. The use of such software has to take place exclusively for the purpose of provision of supporting services and has to be supervised by the employee concerned. The employees are entitled to the use of an area in their computer not accessible by any third party, while the employers have to ensure that all required technical and organizational security measures for the protection of any personal data transmitted through the network and/or stored in the computers of the employees apply.

The recording of the websites the employees visit is prohibited, but the restriction of the websites the employee is allowed to visit is permitted. Moreover, the collection and processing of personal data referring to calls and generally the

[43] Greek Law No. 2472/1997, Article 2, para. (a).
[44] *Id.* at Article 2, para (b).
[45] *Id.* at Article 5 para. 2 and Article 7, para. 2.

communication (including e-mail) in the field of employment, is advisable to take place only if this is absolutely necessary for the organization and control of the execution and fulfillment of the specific employment and particularly for the expenses' audit. The communication data recorded have to be limited to the absolutely necessary and appropriate ones for the accomplishment of such purposes. In no case whatsoever the recording or processing of the whole number or all communication data or their content is permitted, which must not be processed save upon permission of the Judicial Authorities, if imposed for national security purposes or for the proof of particular serious crimes. Therefore, the access and recording of data of electronic communication, such as the recipients and the content of the electronic communication of the employees is not lawful, while said data may not be used for the control of the employees' behavior.

Destruction of the electronic stored data has to take place according to the provisions and the procedure set forth in the Regulation of the Hellenic Data Protection Authority No. 1/2005 on the safe destruction of the data records after the end of their processing period. The way of destruction recommended by the above Regulation refers to destruction through overwriting of the relevant records with the use of specific programs such as file erasers, file shredders, or file pulverizers. Alternatively, in case of daily destruction, the format of the hardware is proposed, while the destruction of the hardware may be also used as a way of destruction. Destruction includes all backups as well, while a relevant destruction protocol has to be drawn by the data controller.

Australia

Because Australia is a federation, there is some fragmentation of privacy regulation between federal, state and territory legislation. There is further fragmentation due to content specific privacy legislation, such as health information legislation.

At a national level, the handling of personal information is regulated by the **Privacy Act 1988 (Cth)** ("Act"). The Act establishes 11 Information Privacy Principles ("IPPs")[46] which apply to Federal Government agencies,[47] and 10 National Privacy Principles ("NPPs"), which apply, in effect, to the private sector.[48] The IPPs require that Federal Government agencies have a lawful purpose for collecting personal information and require that agencies seek an individual's consent (which may be implied in some cases) to use or disclose information for a purpose that is not directly related to the purpose for which that information was collected. The NPPs require that organizations collect personal information by lawful and fair means and only when necessary

[46] The Information Privacy Principles are similar, but not identical, to OECD Guidelines.

[47] IPPs also apply to Australian Capital Territory agencies. 'Agency' is defined to include ministers, departments, federal courts and other bodies established for a public purpose.

[48] 'Organization' is defined as an individual, a body corporate, a partnership, any other unincorporated association or a trust.

for the organization's functions or activities. Organizations may use and disclose personal information only for the purpose for which it was lawfully collected and are required to have an individual's consent (which may be implied in some cases) to disclose otherwise.

The IPPs and NPPs provide exceptions which permit disclosure of personal information in some limited situation including where it is required or authorized by law.[49] Only a few cases in Australia have considered what is meant by 'law' for the purposes of the 'required or authorized' exception. It has been held that 'law' in the context of the exception includes a Federal Act[50] and court rules.[51] The meaning of 'law' in relation to similar exceptions under state and territory privacy laws have been held to include an order for pre-trial discovery[52] and a subpoena to disclose information to a court.[53] Care should always be taken when disclosing personal information in any court proceeding to ensure that a relevant exemption applies to the disclosure in that particular case. Where documents including personal information are disclosed in the context of discovery, a second layer of privacy protection arises by virtue of an implied undertaking made by each party to the proceedings not to use any document for any purpose, otherwise than in relation to the litigation in which it is disclosed.[54]

In 2006, the Australian Law Reform Commission ("ALRC") was charged with reviewing privacy legislation. Their report[55] was handed down in May 2008. The government is releasing its response to the report in two stages. [56] The first stage focuses on replacing the IPPs and NPPs with a single set of uniform privacy principles to apply to government agencies and private sector organizations. Many of the exceptions in the IPPs and NPPs are intended to be retained but the government will look at exemptions in more detail in the second stage of its response. Importantly however, the government has accepted the ALRC recommendation that there be an exemption allowing personal information to be disclosed when it is necessary for the purpose of a confidential alternative dispute resolution process.[57]

The second stage of the reform process will consider, among other issues for reform, the creation of a cause of action for breach of privacy. The ALRC report recommended that a statutory cause of action be created at the federal level (which would, in effect, specify the

[49] Privacy Act 1988 (Cth) s 14, IPPs 5.2, 6, 10.1(c), 11.1(d); sch 3, NPPs 2.1(g), 6.1(h) and 10.2(b)(i).

[50] Re VBN and Australian Prudential Regulation Authority (2006) 92 ALD 475, [39].

[51] Re An Application by the NSW Bar Association [2004] FMCA 52, [5]–[6].

[52] Grant v Marshall [2003] FCA 1161, [4].

[53] HW v Commissioner of Police [2003] NSWADT 214, [63]–[64].

[54] Esso Australia Ltd v Plowman (1995) 183 CLR 10.

[55] Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice (ALRC 108)* (2009) available at http://www.alrc.gov.au/inquiries/title/alrc108/index.html (hereinafter "ALRC Report").

[56] The ALRC Report made 295 recommendations. We only refer to the most significant expected changes.

[57] *Id.* at recommendation 44-1.

required elements of an actionable invasion of privacy as well as relevant defenses). It is anticipated that the cause of action would incorporate a balancing test, designed to weigh the rights of individuals to personal privacy and the public's right to the free flow of information on matters of public concern. Some Australian courts have also indicated a willingness to take steps towards the evolution of a cause of action for breach of privacy. Such common law developments have been underway for sometime in the United Kingdom, where the action of breach of confidence has become a vehicle for privacy-style claims. The foundations of such an action have recently been developed in a decision of the Victorian Court of Appeal (a state court) in *Giller v Procopets*.[58] In that case, the Court of Appeal resolved that it was unnecessary for it to decide the existence of a tortious action for breach of privacy in Australia in light of its findings in relation to the plaintiff's successful action for breach of confidence. Ashley JA noted that a generalized tort of unjustified invasion of privacy has not been recognized by any superior court in Australia.

In declining to consider whether a tort of invasion of privacy should be recognized in Australian law, Neave JA illustrated the two approaches that have developed in response to claims the law should recognize a cause of action of invasions of privacy. The first approach, epitomized by *Australian Broadcasting Commission v Lenah Game Meats Pty Ltd*,[59] has been to develop existing causes of action to provide greater legal protection for privacy interests. The findings of the Victorian Court of Appeal reflect this first approach.

The second approach, seen for example in the New Zealand Court of Appeal's decision in *Hosking v Runting*,[60] has been to recognize a new tort of invasion of privacy. In that case, the Court (by majority) held a tort was committed by the publication of facts about the private life of a person, where the giving of publicity to such facts would be considered "highly offensive to an objective reasonable person". The Australian decisions of *Grosse v Purvis*[61] and *Jane Doe v ABC*[62] reflect this second approach.

It will be interesting to see which of these approaches ultimately holds sway in Australia. The ALRC position, as made apparent from its Report, holds that a statutory cause of action should be created for invasion of privacy and that Federal legislation should provide that any action at common law for invasion of a person's privacy should be abolished.

[58] [2008] VSCA 236.
[59] [2001] 208 CLR 199.
[60] [2005] 1 NZLR 1.
[61] [2003] QDC 151.
[62] [2007] VCC 281.