DAC beachcroft

# International Data Breach Law

## A Comparative Guide

THE HARMONIE GROUP

CANADIAN LITIGATION COUNSEL

In cooperation with BLD Bach Langheid Dallmayr

BLD
BACH LANGHEID DALLMAYR

# Introduction

In an era where vast quantities of information are stored electronically, individuals and businesses face new challenges in protecting their information and reputation from the risks posed by the loss or theft of data. For individuals there is the threat of viruses, identity theft and cyber stalking. For businesses, there is the fear their systems can come under attack, either externally or by negligent and malicious acts of their employees or third parties, putting vital data and reputations at risk. Cyber risks are commonly regarded as the most significant threat for businesses in the 21st century.

The international nature of modern business means that data is frequently transferred across national boundaries, which creates jurisdictional uncertainty. The advent of cloud computing as a lower cost, efficient, easily accessible solution to data storage and retrieval has introduced a further layer of complexity to an already complex area.

Data protection and privacy laws vary by country and are very complex. With the increase in the number and value of data breach incidents, regulators across Europe and in the USA are continually reviewing how legislation can be used to force organisations to better protect sensitive data. However, what is increasingly clear is that there is not going to be a single, global 'one size fits all' solution. The result is a headache for international companies trying to comply with or anticipate the law, for risk managers trying to advise on best practice and monitor global compliance and for insurers looking to provide the innovative risk transfer solutions required by their clients.

In conjunction with our colleagues from the Harmonie Group and Canadian Litigation Counsel, we have produced this practical guide to the most significant legal issues in the principal North American and European jurisdictions. We hope that you find it informative and interesting. Please do contact the individuals listed at the back of the guide if you would like to further discuss any of the issues.

**Patrick Hill, Hans Allnutt**

# Contents

# 1. How is “data” defined within the jurisdiction?

**Austria**

A distinction is made between “Data” and “Sensitive Data”, the processing of which requires a greater level of elaborateness.

“Data” (”Personal Data”) is defined as information relating to data subjects who are identified or identifiable (e.g. name or mobile number). Data is ”only indirectly personal” for a controller, a processor or recipient of a transmission when the Data relates to the subject in such a manner that the controller, processor or recipient of a transmission cannot establish the identity of the data subject by legal means. “Sensitive Data” (“Data deserving special protection”) is defined as Data relating to natural persons concerning their racial or ethnic origin, political opinion, trade-union membership, religious or philosophical beliefs, and data concerning health or sex life.

Under Austrian law legal persons may also be data subjects, although the regulations with regard to sensitive data do not apply to legal persons.

**Belgium**

A distinction is made between “Personal Data”, “Sensitive Personal Data”, “Health Data” and “Judicial Personal Data”. Whereas processing “Personal Data” is normally allowed, the processing of the other types of data is normally prohibited.

**Czech Republic**

There are two basic categories of personal data, “Personal Data” and “Sensitive Data”. The processing of Sensitive Data requires a greater level of vigilance. “Sensitive Data“ includes personal data revealing nationality, racial or ethnic origin, political attitudes, trade-union membership, religious and philosophical beliefs, conviction of a criminal act, health status and sexual life of the data subject, genetic data of the data subject and a biometric data permitting direct identification or authentication of the data subject.

**England & Wales**

There are two categories of personal data, “Personal Data” and “Sensitive Personal Data”. There are seven categories of “Sensitive Personal Data” which include health data, but not financial data. Processors must comply with extra conditions in order to process Sensitive Personal Data including obtaining “explicit consent” from the data subject.

**France**

“Personal data” is defined very broadly as “any information relating to an individual who is or can be identified, directly or indirectly, by reference to an identification number or to one or more factors specific to him/her”. The legislation distinguishes a category of “sensitive” data, i.e. data which reveal, directly or indirectly, the racial or ethnic origins, the political, philosophical, religious opinions or trade union membership of persons or which concern their health or sexual life. The collection and processing of these data is in principle prohibited (authorization can nevertheless be granted if data are modified to become anonymous). Other types of data are distinguished, such as health personal data, data related to the criminal offences and convictions or security measures, and personal data allowing to assess the personality of an individual.

**Germany**

Pursuant to § 3 p. 1 BDSG (Federal Data Protection Act) personal data relating to individual details concerning personal or factual circumstances of a determined or determinable individual person (affected individual).

Pursuant to § 3 p. 9 BDSG, personal data relating to racial and ethnic origin, political opinions, religious or philosophical conviction, trade union membership, health or sexual activities. C. f. § 42 a) no. 2–4 BDSG.

**Ireland**

There are two categories of personal data, “Personal Data” and “Sensitive Personal Data”. Personal data refers to data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller. Sensitive personal data relates to specific categories of data which are defined as data relating to a person’s racial origin; political opinions or religious or other beliefs; physical or mental health; sexual life; criminal convictions or the alleged commission of an offence; trade union membership.

**Italy**

“Personal Data” which means any information relating to natural persons that are or can be identified, even indirectly, by reference to any other information including a personal identification number. “Identification Data” which means Personal Data allowing a data subject to be directly identified. “Sensitive Data” which means Personal Data allowing the disclosure of racial or ethnic origin, religious, philosophical or other beliefs, political opinions, membership of parties, trade unions, associations or organizations of a religious, philosophical, political or trade-unionist character, as well as personal data disclosing health and sex life.

“Judicial Data” which means Personal Data concerning the criminal record office, the register of offence-related administrative sanctions and the relevant current charges, or the status of being either a defendant or the subject of investigations.

**The Netherlands**

Under the Dutch Data Protection Act (Wet bescherming persoonsgegevens, "DPA") the concept of personal data is defined as any data related to an identified or identifiable natural person. Within the concept of personal data, "sensitive personal data" are a special category of personal data. The categories of sensitive personal data include health data, racial or ethnic data, political opinions, religious or philosophical beliefs, trade-union membership and data on sex life, but not financial data. Furthermore under the DPA there is a special regime for numbers prescribed by law to identify natural persons, such as the social security number and equivalents thereof.

**Poland**

There are two basic categories of personal data, "Personal Data" and "Sensitive Personal Data". "Sensitive Personal Data" includes data concerning racial or ethnic origin, political opinions, religious or philosophical beliefs, membership in a political party or political views, trade-union membership, data concerning health, DNA, addictions or sex life, as well as information on convictions, punishment, imposed fines, as well as decisions rendered in the course of court or administrative proceedings.

**Portugal**

Law 67/98 considers any information of any nature which, with support, renders any single person identified or identifiable. Identifiable means someone that may be identified, directly or indirectly, by any identification number or by reference to one or more specific elements of his physical, physiological, psychological, economic, cultural or social identity. Law 67/98 also deals with video surveillance and other forms of collection and treatment of data as images, voices or sounds.

"Personal Data" and "Sensitive Data" are also defined. The processing of Sensitive Data is only allowed if and when it is: a) necessary for the protection of the data subject or other person, if the data subject is incapacitated; and b) being done, with the data subject's consent, by foundation, association or other non-profit institution for restricted use; or c) being necessary to the exercise or defence during judicial trial.

**Scotland**

As Data Protection in Scotland is within the jurisdiction of the United Kingdom's Information Commissioner please refer to England & Wales. However it is relevant to mention that there is also a Scottish Information Commissioner, whose jurisdiction relates to Freedom of Information demands made against Scottish Public Authorities. Freedom of Information demands against Public Authorities operating in Scotland in relation to non-devolved ("Retained") matters are dealt with by the UK Information Commissioner.

**Spain**

Bearing in mind that any information concerning identified or identifiable natural persons is protected, there are two categories of information concerning identified or identifable persons which should be protected: "personal data" and "data with special protection". "Data with Special Protection" concerns data relating to ideology, religion or beliefs; racial origin, health or sex life; criminal or administrative offences; and health.

Spanish Data Protection Law distinguishes between basic, medium and high-level security measures, depending on the kind of data processed. All files or processing of data shall adopt basic-level security measures. The medium-level security measures shall also be implemented in the case of certain files (e.g. criminal or administrative offences, those controlled by financial institutions for purposes related to the provision of financial services – including insurance – , those controlled by Tax Authorities, etc). The high-level security measures shall be implemented in case of the above mentioned "data with special protection", and also in case of those files containing data collected for security forces or data arising from acts of gender-based violence.

**Sweden**

Generally, "personal data" must be protected which is defined as "all kinds of information that is directly or indirectly referable to a natural person who is alive".

**USA**

There is no single federal law providing a uniform classification of the types of personal information; information is classified by sector. For instance, the Health Insurance Portability and Accountability Act (HIPAA) concerns "protected health information" and "individually identifiable health information." The Gramm-Leach Bliley Act (GLBA) concerns "personally identifiable financial information." The Privacy Act of 1974 protects an "identifying particular assigned to an individual." The Freedom of Information Act (FOIA) protects "personal identifying information," and the Family Educational Rights and Privacy Act (FERPA) protects "personally identifiable information."

Individual states have different definitions of "personal information." Minnesota's notification statute, Minn. Stat. § 325E.61, defines "personal information" as a person's name in combination with a person's Social Security number, driver's license or identification card number, account number or credit or debit card number in combination with any required security code, access code, or password permitting access to an individual's financial account.

**California**

There are laws pertaining to "medical information", "personal information", "health insurance information", and "business records". These definitions vary for different purposes and protections.

**Texas**

Texas has two general classifications of protected data: Personal Identifiable Information (PII) and Sensitive Personal Information (SPI). PII means "information that alone or in conjunction with other information identifies an individual." Sensitive Personal Information is defined to include (a) an individual's first name or first initial and last name in combination with any one or more of (i) social security number; (ii) driver's license number or government-issued identification number; or (iii) account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account; or (b) information that identifies an individual and relates to (i) the physical or mental health or condition of the individual (ii) the provision of health care to the individual; or (iii) payment for the provision of health care to the individual.

**Canada**

The Personal Information Protection and Electronic Documents Act (PIPEDA), the most significant piece of federal legislation addressing data security, provides for two classifications of personal data: (1) "Personal Information"; and, (2) "Personal Health Information".

"Personal Information" is broadly defined in PIPEDA to include any "information about an identifiable individual" with the exception of basic contact information of an employee of an organization. The ambit of "personal information" has been interpreted, by way of jurisprudence and examination of alternate statutory language (e.g. the Freedom of Information and Protection of Privacy Act) to extend to a wide range of categories, including: race; ethnic origin; religion; marital status; level of education; e-mail address and messages; I.P. (internet protocol) address; age; height; weight; medical records; blood type; DNA code; fingerprints; voiceprint; income; purchases; spending habits; banking information; credit/debit card data; loan or credit reports; tax returns; Social Insurance Number (SIN); and, other government issued identification numbers. Alberta, British Columbia, and Quebec have enacted specific legislation defining "personal information", though, with a few minor exceptions, they mirror the provisions set out in PIPEDA (e.g. British Columbia's "Personal Information Protection Act" specifically excludes "work product information" from the definition of "personal information").

"Personal Health Information" is defined more specifically in PIPEDA to include any information with respect to an individual's, living or deceased, mental or physical health; health services provided; donation preferences; test or examination results; and, information collected, directly or incidentally, from the course of health services. Ontario, Alberta, Manitoba, and Saskatchewan have enacted specific legislation addressing "personal health" information that override the provisions provided in PIPEDA. However, none of these respective acts materially deviate from the contours of "Personal Health Information" provided by PIPEDA.

**Mexico**

The Mexican Data Protection Act governs the treatment of personal data to guarantee privacy, and to establish the right of individuals to decide upon the treatment of their personal data. It also establishes the right of individuals to decide what type and which of their personal data they wish the service provider to transfer. The Act introduces a number of standards and principles, the purpose of which is to guarantee the proper use of personal data, these principles including legality, consent, information, quality, purpose, loyalty, proportionality and responsibility, which must be observed at all times, particularly by service providers, in order to guarantee the security of individuals.

"Personal Data" includes a wide range of information including names, addresses, telephone numbers, e-mail addresses, nationality, age, names of relatives, etc. Employment information such as position, place of work, personal and employment references are included.

"Sensitive Personal Data" means information that affects the privacy of an individual, or the improper use of personal data which may lead to discrimination or put the individual at serious risk. This includes racial or ethnic origin, genetic information; religious, philosophical and moral beliefs; union membership; political opinions and sexual preference.

Although all Personal Data is protected, a higher level of protection is established for Sensitive Data. Individuals who handle Sensitive Data must meet higher requirements and face higher penalties for misuse. This is because the improper use of Sensitive Data could possibly harm individuals, legally, physically and/or morally.

# 2. What are the requirements with respect to data breaches in the jurisdiction?

**Austria**

Federal Act concerning the Protection of Personal Data (DSG 2000) governs the protection of personal data and their processing and establishing the terms and conditions under which personal data can be processed. Under Section 24 para 2a DSG 2000 there is an obligation to notify the data subjects, who are affected by a systematic and significant unlawful usage of data, provided that such breach may cause damage to the affected data subjects. The notification has to be provided immediately and in an 'adequate form' – it is disputed what this means, especially if the controller is not aware of the data subject's addresses; certain commentators argue that public announcement would be required then. There is an exemption of the notification duty if the threatening damage is only minor and the costs of information are disproportional.

Noncompliance may trigger: administrative fines up to EUR 10,000; civil law claims by any affected data subjects, which may also include immaterial damage; inspections by authorities; and, bad publicity.

**Belgium**

Act of 8 December 1992 on the protection of privacy in relation to the processing of personal data ("PPDA"). The PPDA as the Internal Regulation does not hold any provisions regarding a term for notification, nor does it provide for any sanctions or penalties in case of failure of notification.

Any individual with a sufficient interest can file a complaint with the Privacy Commission ("PC") regarding a data breach. The PC will mediate between the individual and the data controller and refer the to the Courts of First Instance if necessary.

**Czech Republic**

Act 127/2005 (the Electronic Communications Act) requires each provider of a public electronic communication service to notify the Office for Personal Data Protection without delay in the case of a personal data breach. Where the circumstances of the data breaches are likely to adversely affect the personal data of a customer or where the provider did not take appropriate measures to remedy the situation then the service provider is obliged to also notify the customer. A fine up to EUR 800 may be imposed on the service provider for a breach of these obligations.

Under the National Data Protection Law (PDPA), a Processor who discovers that the Controller breaches the obligations provided by the PDPA must notify the Data Controller of this fact without delay and terminate the respective personal data processing.

**England & Wales**

From 26 May 2011, the Privacy and Electronic Communications (EC Directive) (Amendment) Regulation ("PECR") required "service providers" to notify the ICO "without undue delay" in the case of a personal data breach. A service provider is in essence any provider of an electronic communication service that is provided so as to be available for use by the members of the public. The PECR is aimed at but not limited to telecommunications and internet service providers. Where the circumstances of the data breaches are likely to "adversely affect" the personal data of a customer then service providers are obliged to notify the customer.

Failures by service providers to comply with these provisions may attract fines of up to £500,000.

**France**

The CNIL is an independent administrative body who has powers to investigate possible infringements, and, if they are established, may order administrative penalties. Public prosecution may occur in parallel. Indeed, breaches of the protections provided in the French Data Protection Act are also reprimanded under articles 226–16 to 226–24 of the Criminal Code by up to a 5 year imprisonment sentence and a fine up to € 300,000 (up to €1.5 million if the offender is a legal entity). Hindering the action of the CNIL is punished by a one year imprisonment sentence and a fine of up to € 15,000. Pursuant to Article 34 bis of the French Data Protection Act, the provider of electronic communication services accessible by the public must notify the CNIL of any infringement of personal data (unless the CNIL is satisfied that appropriate protection measures were carried out by the provider in order to render data incomprehensible to all non-authorised persons who can access them). Regarding the right to privacy and secrecy of personal correspondence, Article 226–15 of the Criminal Code reprimands all actions likely to deprive the addressee, even momentarily, of the correspondence addressed to him/her.

**Germany**

If particular kinds of personal data (e.g. health records etc; data that are covered by professional secrecy) are unlawfully transmitted to third persons and if there is the risk of severe impairments, the competent supervisory authority as well as the affected person must be notified. Notice must be given immediately, i. e without undue delay.

A failure to notify is punishable by a fine and also possibly enforced by penalties. C. f. § 42 a) BDSG (Federal Data Protection Act), § 43 p. 2 no. 7 BDSG, § 44 BDSG.

**Ireland**

Where an incident gives rise to a risk of "unauthorised disclosure, loss, destruction or alteration of personal data, in manual or electronic form," the data controller must give immediate consideration to informing those affected. In addition, all incidents of loss of control of personal data in manual or electronic form by a data processor must be reported to the relevant data controller as soon as the data processor becomes aware of the incident.

In situations where personal data has been put at risk, all incidents should be reported to the Office of the Data Protection Commissioner as soon as the data controller becomes aware of the incident, except when the full extent and consequences of the incident has been reported without delay directly to the affected data subject(s) and it affects no more than 100 data subjects and it does not include sensitive personal data or personal data of a financial nature.

In appropriate cases, data controllers should also notify organisations that may be in a position to assist in protecting data subjects including, where relevant, the police, financial institutions etc.

Affected individuals may bring civil claims for damage against the data controller or data processor. They may also seek remedies under the existing law for defamation, breach of confidentiality, negligence etc. Criminal proceedings may be brought and prosecuted by the Data Protection Commissioner with fines of up to €100,000.

**Italy**

The Data Protection Code does not include an obligation to notify a data breach.

However, according to section 141 of the Data Protection Code, data subjects may apply to the Garante (the Italian Data Protection Authority): (a) to lodge a circumstantial claim pursuant to Section 142, to point out an infringement of the relevant provisions on the processing of personal data; (b) to lodge a report, if absence of a call upon the Garante to check up on the aforementioned provisions; c) to lodge a complaint with a view to establishing specific rights established by Section 7 (Right to Access Personal Data and Other Rights). The rights as per Section 7 may also be enforced either by filing a lawsuit (or by lodging a complaint with the Garante) – Section 152 Data Protection Code.

In discharging its tasks, the Garante may also request the data controller, the data processor, the data subject or a third party to provide information and produce documents (section 153); failure to do so may result in a fine of between €10,000 and €60,000.

**The Netherlands**

Clause 11.3a of the Dutch Telecommunications Act requires providers of public telecommunication services to immediately notify the Independent Post and Telecommunications Authority (OPTA) of any security breach which adversely affects the protection of personal data processed in relation to the public telecommunication services. If aforementioned breach is also likely to adversely affect the private life of the data subject, the provider must additionally immediately inform the data subject. Breach of this obligation is subject to a penalty of up to EUR 450,000.

There is now a bill in consultation to introduce a general obligation to notify data breaches under the Dutch Data Protection Act, for all data controllers. The proposed bill will amend the Dutch Data Protection Act.

It may also be argued that the general requirement under the Dutch Data Protection Act to process personal data are processed with due care (fairly), under certain circumstances already requires data controllers to report data breaches to the relevant data subjects. In the financial sector, a notification duty may exist depending on the severity of the security breach.

**Poland**

In Autumn 2012, the Polish Parliament is expected to enact an amendment to the Telecommunications Law Act of 16 July 2004 which will impose certain obligations on providers of publicly available telecommunications services. Any personal data breach must be reported to the Polish data protection regulator, GIODO, within three days of discovery. Further, if a data breach may have a negative effect on the rights of a subscriber or end-user (i.e. a breach which, in particular, may result in unauthorized use of personal data, loss in property, defamation, or disclosure of information, which under legal provisions should be maintained confidential), who is an individual (not a corporate entity), the provider shall also notify the subscriber or end-user within three days of breach discovery. GIODO may impose such an obligation on a provider, even when there is no obligation to report a data breach.

**Portugal**

Those dealing in Personal Data are under a duty to make a prior notification to the CNPD but there is not legal obligation to notify in the event of a data breach. Law 67/98 imposes duties on the security data and infringements are sanctioned (including criminal sanctions). Therefore, whilst there is no obligation to notify data breaches there is a real exposure to risk for entities in charge of the data.

**Scotland**

As Data Protection in Scotland is within the jurisdiction of the United Kingdom's Information Commissioner please refer to England & Wales. We are currently running the first Scottish appeal against a monetary penalty (£250,000) and these appeals are determined by the Information Tribunal not the courts. Monetary Penalties were introduced in April 2011 and there are as yet no decided appeals.

The Information Commissioner has stated at a conference in Edinburgh in February 2011 that he expects the UK to move to a system requiring organisations to disclose details of personal data loss. However one of the points we are taking in the monetary penalty appeal referred to above (and which has also been taken in one of the other appeals) is that no credit whatsoever seems to be given for voluntary disclosure at present – the penalties that have been imposed to date give no hint of any discount on this basis which we would say is contrary to the spirit of the penalties scheme which was supposed to encourage voluntary disclosure.

**Spain**

The Data Protection Laws do not include an obligation to notify a data breach. However, any individual can file a complaint with the Spanish Data Protection Agency regarding a data breach.

The Spanish regulation includes some obligations to notify and, sometimes, to obtain a prior authorisation, but not refer to a data breach. For example, according to Section 25 of Organic Law 15/1999, natural persons or companies intending to create files of personal data shall first notify it to the Data Protection Agency. Minor infringements could be punished with a fine up to € 40,000. Serious infringements could be punished with a fine up to € 300,000.

**Sweden**

The Personal Data Protection Act provides that the controller shall compensate the registered person for damage and violation of personal integrity caused by the processing of personal data in contravention of the Act unless the error was not caused by the controller. Intentional or grossly negligent contraventions of the applicable laws may result in a fine or imprisonment of six months (or two years for grave offences). The same applies to a person who, when processing personal data in unstructured material, violates the personal integrity of the registered person by processing sensitive personal data or information on violations of the law, etc or by transferring personal data to a third country which does not have an adequate level of protection of personal data.

**USA**

There is no comprehensive federal law on data breach notification. The HITECH Act requires notice to individuals when it is reasonably believed that a breach of unsecured personal health information has occurred. Notice must be given without unreasonable delay, but no later than 60 days after discovery of the breach. If a breach affects more than 500 residents of a state, notice must also be given to prominent media outlets in the state. Notice must also be given to the Secretary of the US Department of Health and Human Services.

The GLBA does not have express notification provisions, but its security guidelines recommend implementing a risk-based response program, which have been interpreted as including customer notification where misuse of information has occurred or is reasonably possible.

The majority of states (46) have legislation requiring notification of security breaches involving personal information. Only Alabama, Kentucky, New Mexico, and South Dakota lack such legislation. Obligations vary from state to state. Minnesota statutes (Minn. Stat. § 325E.61) require that any person or entity doing business or that owns or licenses data including "personal information" must disclose any discovery of a breach of the security system by notifying Minnesota residents "in the most expedient time possible" that unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person. And notification must be made to the owner or licensee of the information. The Minnesota Attorney General enforces the statute. If notification of more than 500 persons is required, notice must be given within 48 hours to all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis.

**California**

Under the Information Practices Act of 1977 any person or business that conducts business in California that owns or licenses computerized data that includes personal information, must disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. Notification must be done expediently and without unreasonable delay, with consideration of other factors. The Attorney General must be notified where more than 500 California residents are affected.

In certain circumstances, customers may institute a civil action to recover damages and costs. They may also be entitled to recover a civil penalty of up to $500 per violation, or three thousand dollars ($3,000) per violation for a wilful, intentional, or reckless violation.

There are various other rights and remedies granted to injured individuals under the Cal Civ Code and Cal Fin Code.

**Texas**

Identity Theft Enforcement and Protection Act (Texas Business & Commerce Code, Chapter 521) Any person or business that conducts business in Texas and owns or licenses electronic PII or SPI must disclose any breach of system security to any Texas resident whose PII or SPI was, or is reasonably believed to have been, acquired by an unauthorized person. A person that maintains computerized data that the person does not own must notify the owner or license holder of the data.

The notification must be given "as quickly as possible" subject to certain caveats. Notification may be given in writing or in some instances by electronic means. When the number of affected persons of the security system breach exceeds 10,000 persons, notice must also be given to each consumer reporting agency. Depending on the circumstances, the notice must be given to Texas residents and persons outside Texas.

The failure to comply with the statute can result in civil penalties of at least $2,000 but not more than $50,000 for each violation. The attorney general may bring an action to recover the civil penalty. Failure to notify could result in a civil penalty of not more than $100 for each individual per day that notice is not given, limited to $250,000 for a single breach.

The Texas Attorney General may also grant injunctions against violations of this statute.

**Canada**

PIPEDA does not prescribe mandatory notification requirements for data breaches. Instead, individual provincial laws make up a defacto, albeit piecemeal, legislative scheme. In provinces where notification requirements do exist, specific to personal health information or otherwise, they have adopted an ombudsman based model.

Alberta is the only province that imposes a statutory obligation on private-sector organizations to disclose privacy-related data breaches. The Personal Information Protection Act requires that an organization having suffered a data breach must provide notice to the Commissioner who may further require notification to individuals with potential exposure (37.1(1)). Failure to comply with Alberta's privacy legislation may result a fine of up to $10,000 CAD for individual persons and up to $100,000 CAD for organizations.

Pursuant to Personal Health Information Act, Ontario requires, in the context of personal health information, that an organization "without unreasonable delay, provide notice to the Commissioner" of a data breach (34.1(1)). Ontario does not explicitly provide penalties or sanctions for failure to notify the Commissioner of a breach.

**Mexico**

The Federal Act for the Protection of Personal Data in the Possession of Private Individuals does not include an obligation to notify a data breach. However, any individual can file a complaint with the IFAI regarding a data breach. The Act establishes a procedure to provide protection against the supervisory authority designated in the Act: the Federal Access to Information and Data Protection Institute (currently known as Federal Access to Public Information Institute). The Institute must also ensure that data is protected and persons responsible act in a manner stipulated in the Act. To this end, the Institute shall have access to all information and documents it considers as necessary. However, the procedure, terms and conditions for doing so shall be established in the Regulations of the Act, which do not yet exist.

The Act also authorizes the Institute to impose penalties for transgressions which range from the failure to apply for exercising ARCO rights up to obstructing the inspections of the authority, including the illegal and unauthorized transfer of data and obtaining data deceitfully or fraudulently. Penalties range from a simple warning up to a fine of 320,000 days of the Mexico City minimum wage (and doubled if the transgression involves sensitive personal data. As with the procedure for protecting rights, inspection procedures and administrative fines shall be established in the Regulations of the Act, which do not yet exist.

# 3. Who must comply with the data breach law within the jurisdiction?

**Austria**

Section 4 DSG 2000 distinguishes between Controllers and Processors. A Controller is defined as a natural or legal person, group of persons or organ of a territorial corporate body or the offices of these organs, if they decide alone or jointly with others to use data, without regard to whether they use the data themselves or have it done by a service provider. They are also deemed to be controllers when the service provider instructed to carry out an order, decides to use data for another purpose and thus against its contractual obligation. A Processor is defined as natural or legal person, group of persons or organ of a federal, state and local authority or the offices of these organs, if they use data only for a commissioned work.

The DSG 2000 applies to all controllers or processors, regardless of their size/turnover. Organizations are not classified by size/turnover in this regard.

"Third Parties" who do not directly receive the data from the data subject fall within the scope of the DSG 2000. They may be classified as Controller (if they receive the data for their own purposes) or as Processor (if they receive the data for the purposes of a controller, with whom they entered into a controller-to-processor contract).

**Belgium**

The PPDA only applies to data which is processed by "data controllers" regardless of their size or turnover. A data controller means every person or entity which determines the goal and means for processing personal data. The PPDA does not apply to data processors or third parties.

**Czech Republic**

The PDPA applies to both a data controller and a data processor subject to some express exclusions.

A Data Controller means anyone who determines the purpose and means of personal data processing; performs such data processing; and is responsible for such data processing. A data processor is anyone who is separate from the data controller and processes personal data in accordance with the PDPA based on an authorisation by a Data Controller or under a special act.

There is no classification by size or turnover.

Third parties who do not receive data directly from the data subject are subject to the PDPA only if they are processing the data as a Data Controller or Data Processor.

**England & Wales**

Data Controllers are subject to the DPA. No provisions of the DPA apply to Data Processors. There is no classification by size or turnover. Third parties who receive data other than from the data subject are subject to the DPA if they are processing the data as a Data Controller.

Data Controller means "a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed".

**France**

The scope of the French Data Protection Act is very broad as it concerns all automated personal data processing as well as non-automated personal data processing save from data processing for activities exclusively personal. It applies to all persons responsible for data processing (i) who is established in France (exercising an activity in France no matter the legal status), and i(ii) who, without being established in France or in any other member State of the European Union, uses means for data processing located in France, except when they are only used to transit through these territories). It does not apply to data processing implemented in relation to exclusively personal activities. It distinguishes between a data controller (who controls or owns the personal data) and a data processor (who provides services to data controllers).

**Germany**

There are public and private bodies, § 2 BDSG. This classification is decisive for the issue of the applicability of specific law.

Within applicable data protection law is to be decided between responsible bodies (i.e. the data processors), affected individuals (persons, whose data has been stored) and third persons. Furthermore, there are even commissioned data processing services, i.e. persons or organizations who act on commission of a responsible body. Insofar as those fulfill legal requirements, they are treated as if they were part of the responsible body, i.e. they are neither third persons nor a responsible body themselves.

**Ireland**

Both data controllers and data processors are subject to the DPA. A "data controller" refers to a person who, either alone or with others, controls the contents and use of personal data. A "data processor" means a person who processes personal data on behalf of a data controller but does not include an employee of a data controller who processes such data in the course of his employment.

There is no classification by size or turnover.

Third parties who receive data other than from the data subject are subject to the DPA if they are processing the data as a controller or data processor.

**Italy**

The Code applies to the processing of personal data: (a) where the processing is performed by any entity established either in the State's territory or in a place that is under the State's sovereignty; and, (b) that is performed by an entity, established outside the EU, that makes use in connection with the processing of equipment, whether electronic or otherwise, situated in the State's territory, unless such equipment is used only for purposes of transit through the territory of the European Union. The Code also applies to natural persons who process personal data for exclusively personal purposes where the data is intended for systematic communication or dissemination (Section 5).

There is no classification by size or turnover.

A Data Controller means any natural or legal person, public administration, body, association or other entity that is competent, also jointly with another data controller, to determine purposes and methods of the processing of personal data and the relevant means, including security matters. A Data Processor means any natural or legal person, public administration, body, association or other agency that processes personal data on the controller's behalf. "Persons in charge of the processing" means natural persons who have been authorized by the data controller or processor to carry out processing operations. If a third party joins in the processing, it will fall within the scope of the Code.

**The Netherlands**

In accordance with the Data Protection Directive 95/46 the Dutch Data Protection Act makes a distinction between the concepts of data controller and data processor. The obligations under the Dutch Data Protection Act are imposed upon the data controllers. Only limited obligations (with regard to security measures) under the Dutch Data Protection Act apply to data processors. There is no classification by size or turnover. Third parties who receive data other than from the data subject are also subject to the Dutch Data Protection Act (but also third parties that receive personal data from the data subject). Only providers of public telecommunication services are subject to the notification duty of data breaches under the Dutch Telecommunications Act. Financial Institutions, like banks and insurance companies are also bound by a sector specific Code of Conduct on the processing of personal data.

**Poland**

The PDPA applies to data controllers and data processors because the latter under the PDPA are those to whom data controllers entrust data processing. There is no specific classification by size or turnover.

Third parties who do not receive data directly from data subjects also fall within the scope of the PDPA if they act as data controllers.

**Scotland**

As Data Protection in Scotland is within the jurisdiction of the United Kingdom's Information Commissioner please see England & Wales. However it is relevant to mention that there is also a Scottish Information Commissioner, whose jurisdiction relates to Freedom of Information demands made against Scottish Public Authorities. Freedom of Information demands against Public Authorities operating in Scotland in relation to non-devolved ("Retained") matters are dealt with by the UK Information Commissioner.

Third parties who receive data other than from the data subject are subject to the DPA if they are processing the data as a Data Controller. It is a legal requirement that a contract between Data Processor and Data Controller be in writing, contains prescribed obligations and the Data Controller is seemingly expected to monitor compliance.

**Spain**

Spanish Law distinguishes between "Data Controller" and "Data Processor". "Data controller" is the natural or legal person (public or private), or government body that determines the purpose, content and use of the processing. "Data processor" is the natural or legal person public authority, agency or any other body that processes personal data on behalf of the controller.

Data Protection Laws apply to personal data recorded on any support susceptible to processing, as well as to the subsequent use of such data. Certain files, however, fall out of scope. For example, files kept by natural persons in connection with solely personal or domestic activities and files created to investigate terrorism and organised crime.

Spanish Law does not classify organisations by size/turnover, but distinguishes between public and private organisations.

The scope of Spanish Law is determined by various factors including: whether the data controlling establishment is in Spanish territory and if not, is subject to Spanish Law pursuant to the norms of Public International Law; and, when the data controller is not established in European Union territory and uses means located on Spanish territory for the processing of data.

Third parties who do not receive data directly from the data subjects fall within the scope of the Laws. In these instances, the data controller must inform the data subject (Organic Law 15/1999) within three months of: (i) the content of the processing; (ii) the source of the data, and, (iii) the purpose of collecting the data, the recipients of the information and the possibility of exercising rights of access, rectification, erasure and objection.

**Sweden**

The Personal Data Act applies to data controllers established in Sweden. Swedish law also applies to controllers established outside the EU and EEA but using equipment situated in Sweden for the processing of personal data. In such cases, an agent must appoint an agent who is established in Sweden who will be deemed a controller under the Personal Data Act.

Data controller (controller) means a person who alone or together with others decides why and how personal data shall be processed. Personal data assistant (assistant) means a person (who may be an independent service provider) who processes personal data on behalf of the controller.

**USA**

Federal statutes and regulations apply to persons and entities meeting the statutory definitions, which are not based on size. The GLBA Safeguards Rule, however, requires companies to develop a security plan that is appropriate to the company's size and complexity.

Federal statutes and regulations do not refer to data "controllers" and "processors," but they require subject entities to pass on legal obligations to any entity accessing or receiving regulated personal information. For instance, the GLBA Safeguards Rule requires a financial institution to "oversee service providers" by contracting with them to have appropriate safeguards. The HIPAA Security Rule allows an entity to work with a "business associate" to create, receive, maintain or transmit protected health information if the business associate contractually agrees to implement and maintain safeguards. Companies must also ensure that any third party to whom they give personal information is using it in a manner consistent with published privacy notices, otherwise they may be subject a lawsuit by the Federal Trade Commission for an unfair or deceptive trade practice. Third parties are subject to federal laws if they meet the statutory definitions or are in contractual agreements with defined entities.

**California**

Virtually everyone falls within the scope of the Information Practices Act of 1977, however it does not apply to those businesses regulated under the Confidentiality of Medical Information Act, California Financial Information Privacy Act, the medical privacy and security rules issued by the federal Department of Health and Human Services, or some other minor exceptions.

The Confidentiality of Medical Information Act applies to every provider of health care, health care service plans, pharmaceutical companies, or contractors who create, maintain, preserve, store, abandon, destroy, or dispose of medical information. It also applies to employers who receive medical information.

The California Financial Information Privacy Act applies to any institution the business of which is engaging in financial activities doing business in California. An institution that is not significantly engaged in financial activities is not a financial institution. The term does not include any institution that is primarily engaged in providing hardware, software, or interactive services, provided that it does not act as a debt collector or engage in activities for which the institution is required to acquire a charter, license, or registration from a state or federal governmental banking, insurance, or securities agency. There are other specific exceptions as well.

The California Public Records Act applies to governmental agencies and elected state or local officers, including any state or local appointees, employees, or consultants.

**Texas**

Any person or business that conducts business in Texas and owns or licenses electronic PII or SPI falls within jurisdiction of the Identify Theft Enforcement and Protection Act. Additionally, any person that maintains computerized data that the person does not own must comply with the Act. (It should be noted that the scope of the Identity Theft Enforcement and Protection Act includes private health data and therefore, medical professionals also falls within the scope of the act as well as the Texas Health Privacy Act and HIPAA.)

**Canada**

Federal and provincial legislation apply to organizations engaged in commercial activities and, therefore, encompass the gambit of private enterprises irrespective of size or turnover.

Similarly, Canadian data protection legislation does not explicitly distinguish or address "data controllers" or "data processors". However, PIPEDA does provide that an organization is responsible for personal information in either its possession or custody, including information that been transferred to a third party for processing. In this instance, the organization bears the obligation of assuring comparable levels of protection, by contractual or other means, while the information is in the possession of the third party.

**Mexico**

The Data Protection Controller is the corporate or natural person, that sole or jointly, processes personal data on account of the Responsible. The appointment of this position can be granted to a natural person or to an administrative department within or external to the organization. Transferring personal data to a third party (other than for processing on behalf of the data controller) will typically require an agreement that the transferee will assume the same obligations as found in the privacy notice provided by the transferor. A data transfer requires the consent of the individual except in certain circumstances.

# 4. What changes to data breach legislation are anticipated in the jurisdiction within the next 12 months?

**Austria**

There is a draft amendment to the DSG 2000 published for evaluation, but not yet voted on in Parliament. The draft legislation does not deal with data security or breach notification.

**Belgium**

None in the next 12 months. Belgium will have to comply with the expected General Data Protection Regulation although it is largely in line with existing Belgian legislation. The Regulation will only imply minor legislative changes to Belgian legislation.

**Czech Republic**

No legislative changes are expected in the next 12 months.

**England & Wales**

None in the next 12 months. However a draft General Data Protection Regulation is expected to come into effect in 2016. It is expected to introduce the following provisions:

- A compulsory breach notification regime for all organisations (currently drafted as 24 hours for notification to the regulator and "without undue delay" to data subjects);
- A "right to be forgotten" regime where a data subject may demand that an organisation delete all data relating to that subject; and,
- Fines up to €1 million or 2% of global annual turnover.

**France**

A revision of the 1995 European Directive on data protection is awaited, in particular since the communication from the European Commission of 4 November 2010. If this reform takes place, French Law should be modified accordingly.

**Germany**

Contrary to the past years, in which many changes in data protection law have occurred, in the next 12 months no fundamental changes are to be expected. Fundamental changes may arise by as a result of the General Data Protection Regulation.

**Ireland**

No legislative changes are expected in the next 12 months. However, please see reference to the UK above re proposed EU changes.

**Italy**

The "Disegno di legge" Simplifications, approved on October 16 by the Government, excludes those acting in a business capacity, even personal, from the application of the Code. The Garante has already stated that if the proposed Simplifications come into force, they would contradict the EU Directive.

**The Netherlands**

None in the next 12 months. A draft EU General Data Protection Regulation is expected to come into effect within the next two or three years.

Furthermore a bill is under consultation to introduce a general obligation under the Dutch Data Protection Act for all data controllers to notify data breaches (see also above).

**Poland**

Currently, the Polish Parliament is working on an amendment of the Telecommunications Law Act of 16 July 2004 in order to implement a 2009 block of amendments to the telecoms directives. This amendment is expected to be enacted in autumn 2012. Please see also answer no. 3.

At the EU level a regulation on the protection of individuals with regard to processing of personal data and on the free movement of such data (General Data Protection Regulation) is being discussed.

**Portugal**

No material changes are expected other than those arising from the proposed EU General Data Protection Regulation.

**Scotland**

As Data Protection in Scotland is within the jurisdiction of the United Kingdom's Information Commissioner please refer to England & Wales.

Aside from the Draft Communications Data Act, none in the next 12 months. However a draft General Data Protection Regulation is expected to come into effect in 2016.

**Sweden**

There is nothing expected to take place within the next 12 months. Sweden will be required to comply with the proposed General Data Protection Regulation although the current Personal Data Protection Act is already largely in accordance with the proposed requirements. Therefore, the General Data Protection Regulation will only bring minor changes to the Swedish legislation.

**USA**

There is a new rule proposed to amend the Code of Federal Regulations for federal government contractors that would require all federal contracts over $100,000 to include a clause requiring the contractor to have basic data security protections for non-public data. The FTC issued a report in March 2012—*Protecting Consumer Privacy in an Era of Rapid Change*—calling upon Congress to pass baseline privacy legislation extending to all commercial entities using consumer data, and provides best practices for entities in handling consumer private information. Also, the White House issued a Consumer Privacy Bill of Rights in February 2012, stating support for a uniform federal notification law, and calling for Congress to pass legislation that applies the Consumer Privacy Bill of Rights to commercial sectors not currently subject to federal data privacy laws. It also requested that interested stakeholders (companies, privacy advocates, consumer groups, technology experts) convene to develop industry-specific codes of conduct enforceable by the Federal Trade Commission. A number of bills concerning privacy have been introduced in Congress during the current term, but they are unlikely to be enacted. There are no anticipated legislative changes in Minnesota in the next 12 months regarding data security and breach notification.

**California**

We do not believe there will be any legislative changes in the next 12 months.

**Texas**

There are no anticipated legislative additions or changes within the next 12 months.

**Canada**

Bill C1–12, introduced to Parliament on September 29, 2011, would add several new definitions to PIPEDA. It preserves the existing definition of "personal information" as "information about an identifiable individual," but removes the wording excluding the names and coordinates of employees, and creates a new definition for business contact information (clauses 2(1) and 2(3)). It also specifies that PIPEDA's provisions on personal information do not apply to business contact information (clause 4). The bill also clarifies that individuals' consent to collection, use or disclosure of their personal information is valid only if "it is reasonable to expect that the individual understands the nature, purpose and consequences of the collection, use or disclosure to which they are consenting".

Perhaps most importantly, Bill C–12 introduces requirements to notify individuals when there has been a data breach thereby exposing their personal information. In particular, a new section 10.1 requires organizations to notify the Commissioner when there has been a "material breach" of the security surrounding their holdings of personal information. A new section 10.2 additionally requires the organization to notify the individuals involved if it is "reasonable" in the circumstances to "believe that the breach creates a real risk of significant harm to the individual". "Significant Harm" in this context is defined as including "bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property".

As yet, Bill C–12 remains tabled and it is unclear whether it is likely to be made good law in the next 12 months. There are no other anticipated legislative changes expected to be passed in the next 12 months addressing personal data security.

**Mexico**

No legislative changes are expected in the next 12 months that we are aware of at the present moment.

# 5. Is it possible to indemnify against data breach fines and penalties with an appropriate insurance product in the jurisdiction?

**Austria**

No – it is not allowed to indemnify against penalties under Austrian law. Only legal costs occurring in this regard may be indemnified.

**Belgium**

Insurance coverage of criminal fines is prohibited under Belgian law (contrary to the coverage of administrative fines). As data breaches are mostly criminally sanctioned, it is for the moment not possible to seek indemnification, by way of an insurance, against data breach penalties

**Czech Republic**

This issue is not regulated by Czech law. There is no explicit ban on such indemnification, however enforcement of such claims before Czech courts could be problematic.

**England & Wales**

There is no express ban on indemnifying against ICO penalties although it is not clear whether the Courts of England & Wales would enforce an insurance indemnity if contested. It is expressly forbidden for regulated firms to indemnify themselves against an FSA fine.

**France**

The French Data Protection Act provides for administrative and criminal penalties. In the French legal system, criminal penalties are, by nature, uninsurable. This prohibition comes from the principle under which the insurer cannot pay the fine at the place of the offender, which would be contrary to the principle of "the personality of offences" specified in Article 121–1 of the Criminal Code. By assimilation, administrative penalties are also not likely to be covered by insurance. Like criminal penalties, their aim is to reprimand a behaviour which has disturbed public order, so the principle of "personality of offences" should also apply. On the other hand, losses resulting from civil liability may be covered under an insurance contract. Therefore, any losses arising out of a data breach can be insured under a professional liability insurance contract and shall be indemnified unless intentional breach or fraud.

**Germany**

It is controversial under German law in how far it is possible to insure against fines and penalties. There is no explicit law that prohibits it, but many authors see such insuring agreement as null, because they would breach general principles of the law.

**Ireland**

There is no express ban on indemnifying against data protection penalties although it is not clear whether the Irish Courts would enforce such an insurance indemnity if contested.

**Italy**

Article no. 12 of the Insurance Code prohibits insurance which indemnifies administrative penalties. If the Article is breached, the contract shall be void.

Having said this, there aren't any appropriate insurance products to indemnify against data breach penalties.

**The Netherlands**

There is no express (statutory) ban on indemnifying against penalties related to data breaches. In general, the prevailing opinion in the Netherlands has always been that an insurance contract cannot seek to cover fines for public policy reasons. However, an increasing number of insurers now offers cover for fines, often adding "to the extent insurable". These insurers argue that one can differentiate between fines by looking at the facts and circumstances of each case. No case law is available as yet.

**Poland**

Under Polish law property insurance may cover any property interest that can be assessed in monetary terms and which is not unlawful. However, in some cases it is doubtful whether insuring risks related to criminal or administrative penalties is in accordance with the law. Generally, insurance covering risks related to penalties based on criminal law is prohibited. There is some uncertainty as to whether risks related to administrative proceedings can be covered by insurance. However, insurance covering administrative fines is offered on the Polish market and its legality has not yet been challenged in courts.

**Portugal**

Liability Insurance may indemnify third parties for damages arising from any data breach if provided by the policy. Indemnification of administrative or criminal fines is prohibited.

Law 67/98 expressly provides (article 34) that anyone suffering damages caused by illegal data treatment or other violations of data protection has the right to be indemnified unless the responsible entity can demonstrate that there is no grounds for entitlement.

**Scotland**

As Data Protection in Scotland is within the jurisdiction of the United Kingdom's Information Commissioner please refer to England & Wales. There is no express ban on indemnifying against ICO penalties. We have no reason to suppose that the Courts of Scotland would decline to enforce an insurance indemnity if contested. It is expressly forbidden for regulated firms to indemnify themselves against an FSA fine.

**Spain**

Cover for administrative fines under an insurance policy is not prohibited under the Spanish law. Having said this, in a non-binding response to a question posed by an insurance company, the Spanish General Directorate of Insurance indicated that cover of fines was not legal but actually the Authority has not taken any step against such covers. The recent Insurance Contract Bill bans the coverage of criminal and administrative fines only in case of intentional acts.

**USA**

There is no express ban preventing coverage for personal data breach penalties, but consideration must be given to the public policy of individual states regarding insurability of penalties due to intentional and/or criminal conduct, and penalties involving restitution or constituting punitive damages.

**California**

There is nothing to preclude indemnifying against data breach under California law with the exception of breaches that are intentional or result from gross negligence.

**Texas**

Texas law does not preclude insuring (indemnifying) against breaches of data security.

**Canada**

There is no explicit ban on indemnification for statutory data breach penalties in this jurisdiction. However, unlike indemnification for civil liability resulting from data breach, criminal penalties may be uninsurable on public policy grounds.

**Mexico**

Indemnification of administrative fines under an insurance policy is not prohibited under the Mexican law. Premiums on policies issued by admitted insurers may be subject to taxes. Essentially, buying insurance with a foreign insurance company that is not locally admitted could constitute a crime under Mexican law. In the absence of a policy specifically segregating a premium to a company incorporated in the states (USA), there are no local premium tax consequences.

# 6. Are there any legal obligations to delete legacy data, i.e., a "right to be forgotten" rule?

**Austria**

There is no explicit right to be forgotten under Austrian law. However, according to Section 6 DSG 2000, data may only be stored for the period of time necessary for the purposes for which the data was being processed. Further, data shall only be used fairly and lawfully and be collected for specific, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. So in practice this means that data may only be stored during a contractual relationship and during an additional period in which such data may be necessary to defend a claim or make a notification to the customer. Thereafter data has to be deleted.

Non-compliance may trigger: administrative fines up to EUR 10,000; civil law claims by any affected data subject, which may also include immaterial damage; inspections by authorities, and bad publicity.

**Belgium**

Article 4, 5 PPDA states that personal data is stored no longer than actually required, given the initial purpose for processing the data. Furthermore, article 4, 4 PPDA provides that all reasonable measures need to be taken, in order to alter or delete processed data, if they are deemed inaccurate or incomplete. The individuals to whom the data is related, are granted a right through article 12, § 1 PPDA to obtain the removal of the data at hand, if they are processed in a way that is irrelevant, incomplete, prohibited or if the storage period has expired. The former individuals hereby can file a written request with the data controller or the data processor, upon which the latter forwards the request to the former. Subsequently, the data controller has a month to reply to this request. If necessary, article 13 PPDA states that individuals can turn to the Privacy Commission in order to have their rights upheld. In turn, the Privacy Commission can submit the dispute to the Courts of First Instance.

**Czech Republic**

According to the PDPA, a Data Controller is entitled to hold personal data only for the period of time necessary for the purposes for which the data was being processed.

In addition the Data Controller or, on the basis of its instructions, the Processor is obligated to carry out liquidation of personal data as soon as the purpose for which personal data were processed ceases to exist or on the basis of a request by the Data Subject (made due to the fact that his/her personal data were processed in breach of law).

The penalties for "not destroying/not deleting" legacy data may amount up to EUR 200,000 or even EUR 400,000 in case of sensitive data or in case large amount of data subjects is concerned.

**England & Wales**

Principle 5 of the DPA obliges a data controller not to keep data longer than necessary. Section 14 of the DPA gives the right for an individual under certain circumstances to request a court order that their personal data is rectified or destroyed by a data controller.

**France**

The French Data Protection Act establishes a "right to be forgotten" for the benefit of individuals. It sets the rule that collected data is "kept in a format allowing the identification of the concerned persons during a period which does not exceed the period of time necessary for the purposes for which the data are collected and processed". Thus, except if data are processed for historical, statistical or scientific purposes, they must be deleted after a well proportioned period of time.

**Germany**

There is no "right to be forgotten" rule. Yet, the possibility exists to revoke one's consent etc. In case of unauthorized data collection, there are above all penalties but also criminal sanctions.

**Italy**

A data subject shall have the right to obtain erasure, anonymization or blocking of data that has been processed unlawfully, including data whose retention is unnecessary for the purposes for which they have been collected or subsequently processed. The rights as per Section 7 may be enforced either by filing a lawsuit or by lodging a complaint with the Garante. The Court or the Garante may grant an order that the data controller abstain from the unlawful conduct and, in particular the Garante, shall also specify the remedies to enforce the data subject's rights and set a term for their implementation.

Whoever causes damage to another as a consequence of the processing of personal data shall also be liable to pay damages (section 15 Data Protection Code).

**The Netherlands**

There is no 'right to be forgotten' as such under the DPA. Section 10 of the Dutch Data Protection Act does oblige a data controller not to keep data for longer than necessary to accomplish the purposes for which the data are collected or further processed. A data subject may request a data controller (after having received access to his personal data) to delete personal data processed by the data controller. This request can be made for example when data are excessive and may therefore not be processed. A data subject may enforce this right by requesting a court order based on Section 46 of the DPA.

**Poland**

The PDPA requires that data not be stored longer than necessary to achieve the aim for which it was processed. The data subject can also demand that data be completed, updated, rectified, temporally or permanently suspended or erased if it is incomplete, outdated, untrue or collected in violation of the law, or if it is no longer required for the purpose for which it was collected. GIODO may issue an order to complete, update or erase data as well as enforce relevant actions if data is processed in violation of the law. GIODO may enforce such decisions in the course of administrative enforcement proceedings. Subject to certain exceptions, service providers of electronic services cannot process personal data after the use of an electronic service has been completed.

**Portugal**

The data subject has the right to accede to the information in data, the right to oppose the future collection or treatment of personal data even if consent has been given previously, and the right to ask (and to obtain) the effective destruction of information or data held whether effective or not.

**Scotland**

As Data Protection in Scotland is within the jurisdiction of the United Kingdom's Information Commissioner please refer to England & Wales. However it is relevant to mention that there is also a Scottish Information Commissioner, whose jurisdiction relates to Freedom of Information demands made against Scottish Public Authorities. Freedom of Information demands against Public Authorities operating in Scotland in relation to non-devolved ("Retained") matters are dealt with by the UK Information Commissioner.

**Spain**

Pursuant to section 4.5 of Organic Law 15/1999, personal data shall be erased when they are no longer necessary or relevant for the purpose for which they were obtained or recorded. In addition, Section 16.5 stipulates that personal data shall be kept only for the periods set out in the relevant provisions or, where applicable, in the contractual relations between the controller and the data subject. Data Protection Laws provide with specific rights for data subjects, among them, the right of erasure. The exercise of this right shall entail the deletion of inappropriate or excessive data. Failure to erase data where legally in order could be punished with a fine up to €300,000.

**Sweden**

A Controller is entitled to hold personal data only for the period of time necessary for the purposes for which the data were being processed.

**USA**

The HITECH Act provides that personal health information constituting "data at rest" should be encrypted or destroyed. "Data at rest" consists of personal health information in databases, file systems, and other structured storage methods.

**California**

Under Cal Civ Code § 1798.81 a business must take all reasonable steps to dispose, or arrange for the disposal, of customer personal information when the records are no longer to be retained by the business by (a) shredding, (b) erasing, or (c) otherwise modifying the personal information in those records to make it unreadable or undecipherable through any means. An individual may sue for actual damages and recover attorneys fees.

**Texas**

Pursuant to the Texas Information Disposal Act, Texas Business & Commerce Code, Section 521.052, before disposing of business records containing PII they must be "modif[ied] by shredding, erasing or other means the [PII] to make it unreadable or undecipherable". A business that does not comply with the Act is liable for civil penalties of up to $500 for each record that is not appropriately destroyed. The Texas Attorney General may also bring an action against the business failing to comply with the Act and recover the civil penalty, obtain injunctive relief, and recover legal costs. A business that modifies its documents in good faith is not liable for a civil penalty even if the record is reconstructed, in whole or part, by extraordinary means. A Texas business can delegate the duty of document destruction under the Act and be in compliance with the Act if it contracts with a person engaged in the business of disposing of records for the modification of personal identifying information on behalf of the business.

**Canada**

PIPEDA provides that an organization should develop guidelines and implement procedures with respect to the destruction and retention of personal information. These guidelines should include minimum and maximum retention periods. Personal information that has been used to make a decision about an individual must be retained for a sufficient period to allow the individual access to the information after the decision been communicated. Personal information that is no longer required to fulfill its originally identified purposes should be destroyed, erased, or made anonymous. Organizations shall develop guidelines and implement procedures to govern the destruction of personal information. Provincial data security statutes contain similar requirements.

**Mexico**

The Act guarantees that owners of data may exercise the so-called ARCO (access, rectification, cancellation and opposition) rights with the person responsible and establishes a procedure for the protection of rights with the supervisory authority.

The data subject may, at any time, ask the person responsible for access to, rectification, cancellation and opposition of the data provided. The person responsible must process the request and reply within 20 business days. Further recourse may be taken by the data subject against the supervising authority if a reply is not received or is unsatisfactory. The procedure is outlined in the Act, although its regulation must be complemented by the development Regulations which do not yet exist.

An individual also has the right to request the protection of his/her data, the right to rectify his/her personal information, the right to have his/her personal information deleted and the right to oppose the use of his/her personal information.

# 7. Does the jurisdiction recognise damages for the simple loss of data arising from a data breach or does the data subject need to prove any actual financial loss?

**Austria**

Generally speaking, data subjects have to prove an actual loss. However, prima facie evidence is sufficient to do so. In addition data subjects may claim immaterial damages as per section 33 DSG 2000, which strictly speaking are not provable at all.

**Belgium**

In order to successfully file a claim, one always needs to prove (i) faulty or incautious behaviour, i.e. the loss of data, (ii) damages and (iii) causal link between (i) and (ii). Both personal and financial damage can be indemnified, although financial damage will be easier to prove.

**Czech Republic**

Damage incurred due to data loss/data breach must be proved by the respective data subject.

If the data subject incurs damage other than property damage as a result of wrongful personal data processing, the data subject will also have a right to pecuniary damages. The amount of such pecuniary damages must be specified by the court with regard to intensity and circumstances of the infringement.

**England & Wales**

Damage must be proved. Damages may include distress although the English Courts have traditionally been reluctant to allow such claims.

**France**

The person responsible for data processing and any sub-contractor are equally liable to ensure the safety requirements set out in the French Data Protection Act, in order, "with regard to the nature of the data and risks presented by the processing, to protect the safety of the data and in particular avoid that they be distorted, damaged or that not authorised third party access them". The CNIL may inform the Public Prosecutor of any infringement and order data controllers to respect the data subjects' rights. Administrative penalties can be ordered, in an amount reflecting the seriousness of the breach carried out and the advantages gained by this breach, without exceeding €300,000. In case of a serious and immediate breach of fundamental rights and liberties, the President of the CNIL can ask, in summary court proceedings, any safety measure necessary to preserve these rights and liberties. There is no provision in the French Data Protection Act regarding the compensation for damages for the loss of data. Relief must be sought in accordance with common law rules governing liability, i.e. the claimant suffering a loss arising from a data protection breach must bring evidence of (i) a breach, i(ii) a damage, and ii(iii) a causal link between the breach and the damage. All types of damage can be indemnified subject to these requirements.

**Germany**

The loss/damage has to be proven regarding claims pursuant to general civil regulations (§§ 280 p. 1, 311 p. 2, 823 p. 1 [legal asset: litigious property, business, general personal right], 823 p. 2 BGB together with above mentioned StGB regulations, 826 BGB, also: § 7 BDSG).

**Ireland**

Damages must be proved. This may include damage to his or her reputation, possible financial loss and mental distress.

**Italy**

Section 15 (Damage Caused on Account of the Processing) of the Code establishes: "1. Whoever causes damage to another as a consequence of the processing of personal data shall be liable to pay damages pursuant to Section 2050 of the Civil Code. 2. Compensation for non-pecuniary damage shall be also due upon infringement of Section 11". Pecuniary and non-pecuniary damages related to loss of data are sought on the basis of general civil law.

In order to successfully file a claim, one always needs to prove (i) faulty or incautious behaviour, i.e. the loss of data, (ii) damages and (iii) causal link between (i) and (ii). To avoid liability, the data controller has to prove he took all appropriate measures to prevent damages.

In some situations, loss of data may infringe personal interests, e.g. freedom, dignity, freedom of conscience, or privacy of correspondence. In such cases, an individual may demand that the infringing party cease their actions or remove their effects and claim monetary (non pecuniary) damages.

**The Netherlands**

Damage must be proved. For damages other than financial loss, the data subject has a right to a "fair compensation".

**Poland**

Pecuniary damages related to loss of data are sought on the basis of general civil law. This means that simple loss of data is insufficient to raise a claim, damage must be proven. Additionally, protection of personal interests can also be a basis for liability. Where loss of data infringes personal interests (e.g. freedom, dignity, freedom of conscience, or privacy of correspondence) a person may demand the perpetrator to cease actions and pay monetary compensation.

**Portugal**

Any indemnity will depend on the classic rules of third party liability as in any other continental European country: the effective damage is the damage that the victim would not have suffered but for the violation. Future damages may be indemnified if predictable.

**Scotland**

As Data Protection in Scotland is within the jurisdiction of the United Kingdom's Information Commissioner please refer to England & Wales. However it is relevant to mention that there is also a Scottish Information Commissioner, whose jurisdiction relates to Freedom of Information demands made against Scottish Public Authorities. Freedom of Information demands against Public Authorities operating in Scotland in relation to non-devolved ("Retained") matters are dealt with by the UK Information Commissioner.

**Spain**

The data subject needs to prove any actual financial loss and specifically claim for such damages before the judge. Section 19 of the Spanish Data Protection Law states that data subjects who, as a result of a failure to comply with the provisions of the Law, suffer damage to their possessions or rights, shall have the right to damages.

**Sweden**

The data subject may be compensated for damage and violation of personal integrity proven to have been caused by the processing of personal data in contravention of the Personal Data Protection Act.

**USA**

For the federal statutes that provide for compensation, the data subject must show actual damages or loss resulting from a data breach; simple loss of data is insufficient for recovery. E.g., Privacy Act, 5 U.S.C. § 552a(g)(4)(A); Computer Fraud and Abuse Act, 18 U.S.C. § 1030(e)(11), (g). Courts examining state common law claims such as negligence or breach of contract have held that loss of data or data breach, by itself, does not constitute recoverable damage; mere increased risk of identity theft is insufficient. See, e.g., *Reilly v. Ceridian Corp.*, 664 F.3d 38 (3d Cir. 2011); *Pisciotta v. Old Nat'l Bancorp*, 499 F.3d 629 (7th Cir. 2007) (predicting Indiana law and finding standing, but no legally cognizable damages from mere identity theft exposure where no evidence of actual identity theft; credit monitoring costs based solely on identity theft exposure were not compensable); cf. *Anderson v. Hannaford*, 659 F.3d 151 (1st Cir. 2011) (mitigation damages of identity theft insurance and credit monitoring were recoverable where identity theft had actually occurred and unauthorized charges to credit and debits cards had been made). It is interesting to note that the 9th *Circuit in Krottner v. Starbucks Corp.*, 628 F.3d 1139 (9th Cir. 2010), concluded that the plaintiffs had standing and sufficiently pled an injury-in-fact due to credible threat of real and immediate harm where there was exposure of unencrypted personal information due to stolen laptop, and someone tried to open a bank account with plaintiff's information, but account was closed before financial loss occurred. But in a companion, unpublished opinion, the same 9th Circuit panel held that although the plaintiffs had standing, they failed to allege that they suffered a cognizable injury where they had not alleged any loss related to the stolen laptop, and the court dismissed their negligence claim. *Krottner v. Starbucks Corp.*, 406 Fed App'x 129 (9th Cir. 2010).

**California**

There are provisions for the recovery of actual damages, including mental suffering, and damages must be proved. In addition, there are civil penalties for the disclosure of medical information that increase for knowing and wilful violations. There are also punitive damages under certain circumstances for the dissemination of medical information.

**Texas**

Texas does not presently recognize a private cause of action for the security breach of PII or SPI. Damages for a security breach are limited to civil penalties enforced by the Texas Attorney General.

**Canada**

Pursuant to PIPEDA, the court has extended a significant amount of discretion to award damages for data loss. The Act provides that should data loss occur, the court may "award damages to the complainant, including damages for any humiliation that the complainant has suffered". Demonstrating actual financial loss is not a prerequisite to an award of damages for data breach under the act; however, damages under PIPEDA are typically permitted in only the "most egregious situations" (*Randall v. Nubodys Fitness Centres, 2010 FC 681; Nammo v. TransUnion of Canada Inc., 2010 FC 1284*).

**Mexico**

The data subject needs to prove any actual financial loss and specifically claim for such damages before the judge. The Mexican Data Protection Law states that data subjects, who, as a result of a failure to comply with the provisions of the Law, suffer damage to their possessions or rights, shall have the right to damages.

## 8. Are there any notable precedents or examples of data breach litigation in the last 12 months in the jurisdiction?

**Austria**

None

**Belgium**

None

**Czech Republic**

None

**England & Wales**

None

**France**

None

**Germany**

Legitimate interest in credit assessment also without consent (German Federal Court (BGH), NJW 2011, 2204 et seq.) and usability of illegally obtained personal-related data (BGH VersR 2010, 97 et seq.)

**Ireland**

None

**Italy**

There were no significant examples affecting jurisprudence, published on the website of the Garante, that has a specific section about it

**The Netherlands**

None

**Poland**

There were no significant examples affecting jurisprudence. It is worth noting, however, that Polish courts have formulated a uniform approach to employer processing of employee personal data. Namely, in such cases processing of such data must be justified not only by employee consent, but also additional reasons. It is deemed that employees never express their consent in complete freedom, as they are always under certain employer pressure.

**Portugal**

None

**Scotland**

As Data Protection in Scotland is within the jurisdiction of the United Kingdom's Information Commissioner please refer to England & Wales. However it is relevant to mention that there is also a Scottish Information Commissioner, whose jurisdiction relates to Freedom of Information demands made against Scottish Public Authorities. Freedom of Information demands against Public Authorities operating in Scotland in relation to non-devolved ("Retained") matters are dealt with by the UK Information Commissioner.

Scotland has its own court system.

Lyons – v –Stephen House may be of interest

http://www.scotcourts.gov.uk/opinions/2012CSOH45.html [Summary?]

**Spain**

None

**Sweden**

None

**USA**

In the United States, 2011 has been described as the Year of the Breach, resulting in numerous liability and coverage lawsuits. For instance:

*Zurich American Ins. Co. v. Sony Corp. of America*, No. 651982/2011 (N.Y. Sup. Ct. July 2011): Declaratory action filed but no decision. Hackers accessed personal information of more than 100 million users of Sony's online video games, likely including 12.3 million credit card numbers. At least 55 class action lawsuits were filed against Sony. Insurer Zurich American filed a lawsuit seeking a declaration of no coverage under a CGL policy.

*Pardieck v. Sutter Health*, No. 34–2011–00114396 (Cal. Super. Ct. Nov. 2011): Consolidation of 13 class actions against Sutter Health after a password-protected but unencrypted computer was stolen from Sutter Medical Foundation's administrative offices in California. The computer contained data on more than 4 million patients. The consolidated lawsuit seeks $1,000 in statutory damages under California's Confidentiality of Medical Information Act for each patient putting the total demand for relief at over $4 billion.

Other recent litigation:

*Reilly v. Ceridian Corp.*, 664 F.3d 38 (3d Cir. 2011): The Third Circuit held that plaintiffs had not suffered an actual injury when hackers infiltrated a payroll processing company's system, potentially gaining access to personal and financial information belonging to plaintiffs and 27,000 other employees. The court dismissed the claims because "allegations of hypothetical, future injury are insufficient to establish standing" in generalized data theft situations. The court also concluded that the plaintiffs' costs to monitor their financial information to protect against alleged increased risk of identity theft are not enough to show a concrete and particularized or actual or imminent injury for standing.

*Retail Ventures, Inc. v. Nat'l Union Fire Insurance Co. of Pittsburgh*, 691 F.3d 821 (6th Cir. 2012): Hackers used local wireless network at a DSW store to get unauthorized access to a computer system, download credit card and checking account information to 1.4 million customers, and make fraudulent transactions. Plaintiffs incurred expenses for customer communications, public relations, claims and lawsuits, and attorney fees. Under a computer fraud rider to a "Blanket Crime Policy" providing payment for "Loss which the Insured shall sustain resulting directly from … [t]he theft of any Insured property by Computer Fraud," the Sixth Circuit held that a proximate cause standard applied to determine whether the insureds' suffered losses "result[ed] directly from" the computer fraud, and under that standard the insureds sustained losses "resulting directly from" the computer fraud. The insureds did not need to show that the losses resulted "solely" or "immediately" from the theft itself. The court also concluded that an exclusion barring coverage for loss of "proprietary information" did not apply because the data (credit card and checking account information) did not fall within the plain meaning of "proprietary information."

*Stevens v. Amazon.com, Inc. d/b/a Zappos.com*, No. 3:12–cv–00032 (W.D. Ken. Jan. 2012): Hackers gained access to personal information (names, addresses, email addresses, encrypted passwords, and the last four digits of credit card numbers) of over 24 million customers by accessing Zappos.com's internal network. Class action alleging violations of the Fair Credit Reporting Act for failing to maintain adequate protection procedures, negligence, and invasion of privacy.

*In re Science Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litigation*, No. 2360 (US Judicial Panel Multidistrict Litigation June 2012): Backup data tapes were stolen from a car of an SAIC employee in September 2011, constituting a data breach affecting the private health and personal information from 4.9 million active and retired military members and families. The US Judicial Panel on Multidistrict Litigation consolidated 8 civil lawsuits around the country. The consolidated lawsuit seeks $4.9 billion in damages.

*United States v. RockYou*, No. 12–CV–1487 (N.D. Cal. Mar. 26, 2012): Gaming company RockYou settled with the FTC in March 2012, agreeing to pay a $250,000 penalty and implement a data security program after hackers accessed data from RockYou's 32 million users in 2009. RockYou violated the Children's Online Privacy Protection Act Rule by collecting personal information of children, and violating the FTC Act by indicating it did not collect such information when it did.

*In re Myspace LLC*, No. C–4369 (F.T.C. Aug. 13, 2012): Myspace settled with the FTC in September 2012, requiring Myspace to implement a comprehensive privacy program with assessments for the next 20 years, and barring it from future misrepresentations about privacy practices. The FTC charged Myspace with violating its privacy policy by providing advertisers with a unique identifier for users that viewed certain Myspace pages.

**California**

In *Brown v. Mortensen*, 51 Cal. 4th 1052 (Cal. 2011) the California Supreme Court held that an action wherein defendant was asserted to have illegally disclosed confidential patient medical information to various consumer reporting agencies in the course of a dispute over an alleged medical debt was not pre-empted by the federal Fair Credit Reporting Act.

**Texas**

None

**Canada**

*Townsend v. Sun Life Financial*, 2012 FC 550: The Federal Court declined to award damages under PIPEDA where Sun Life Financial, an insurer, erroneously disclosed the Plaintiff's confidential medical information to a third-party insurance advisor. In its decision, the court cited the lack of obvious damage to the Plaintiff and the remedial steps taken by the Defendant insurer to guard against future breaches as dispositive considerations.

Numerous class-action lawsuits are reported to have been commenced in relation to data breaches resulting in the disclosure of personal information (e.g. Honda and Sony).

**Mexico**

None

# 9. What criminal sanctions may be levied within the jurisdiction for hacking or gaining access to electronic systems? What civil/criminal sanctions may be levied against those dealing in personal data without the data subject's consent?

**Austria**

Hacking or gaining access to electronic systems is penalised by Sections 118a, 119, 119a, 126a to 126c, 148a and 278a of the Austrian Criminal Code, provided they are committed with intent. Criminal sanctions are imprisonment of up to 6 month or up to 360 times a cash payment (calculated on the income), under certain circumstances (in the merits: high damage) imprisonment of up to 5 years.

Under civil law the affected data subject may sue for actual and immaterial damages.

**Belgium**

Hacking or gaining access to electronic systems is penalised by the Cybercrime Act 2000 ("CA"). Due to the CA, article 550bis of the Belgian Criminal Code penalises "External" hacking and "Internal" hacking. Internal hacking means someone with limited authority who then exceeds his limited authority and gains access to information or data he/she normally isn't allowed to view. Offences are is punishable by imprisonment (External 1 year, Internal 2 years) and/or fines of up to 25.000,00 EUR.

**Czech Republic**

According to the Act 40/2009, the Criminal Code, it is a crime to gain unauthorised access to computer systems and data carriers data. Criminal sanction of imprisonment, prohibition of activity or forfeiture of property may be imposed. In case of large-scale damages the person may be punished by imprisonment of up to 8 years.

In case a Data Controller or Processor processes the personal data without the required consent of a data subject the Office for Personal Data Protection may issue fines of up to EUR 200,000 or even EUR 400,000 in case of sensitive data or in case a large amount of data subjects is concerned.

**England & Wales**

The ICO may issue fines of up to £500,000 under s.55 DPA if there has been a serious contravention of the DPA by a "data controller" and the contravention was likely to cause substantial damage or substantial distress.

s.55A also makes it a criminal offence for "any person" to obtain or disclose personal data without the consent of the "data controller". The offence is punishable by a £5,000 fine although steps are being taken to increase this fine.

**France**

The repressive provisions in relation to the offence of cyber crime are numerous. We can refer in particular to the following Articles of the Criminal Code:

- Article 323–1: Fraudulently accessing or remaining within all or part of an automated data processing system is punished by two years' imprisonment and a fine of €30,000. Where this behaviour causes the suppression or modification of data contained in that system, or any alteration of the functioning of that system, the sentence is three years' imprisonment and a fine of €45,000.
- Article 323–2: Obstructing or interfering with the functioning of an automated data processing system is punished by five years' imprisonment and a fine of €75,000.
- Article 323–3: The fraudulent introduction of data into an automated data processing system or the fraudulent deletion or modification of the data that it contains is punished by five years' imprisonment and a fine of €75,000.

Additionally, it should be noted that the lack of agreement of the data subject can rely on Article 9 of the French Civil Code, under which *"Everyone has a right to privacy. 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".*

**Germany**

Fines or imprisonment up to one year already upon preparatory measures, § 202 c) StGB; see also §§ 202 a), b) StGB; "handling stolen data" shall be chargeable in future (§§ 202 a), 26, 27 StGB (as the present rules are not sufficient), damages are imaginable, claims would arise e.g. from §§ 280 p. 1, 311 p. 2, 826 BGB (proof of loss may be difficult).

**Ireland**

Summary proceedings for an offence under the Data Protection Act may be brought and prosecuted by the Data Protection Commissioner. Under section 31 of the Acts, the maximum fine on summary conviction of such an offence is set at €3,000. On convictions on indictment, the maximum penalty is a fine of €100,000.

Section 9(1) of the Criminal Justice (Theft and Fraud Offences) Act, 2001 provides that a person who dishonestly, whether within or outside the State, operates or causes to be operated a computer within the State with the intention of making a gain for himself or herself or another, or of causing loss to another, is guilty of an offence.

Section 9(2) states that a person guilty of such an offence under is liable on conviction on indictment to a fine or imprisonment for a term not exceeding 10 years or both.

**Italy**

S.161 of the Code governs Providing No or Inadequate Information to Data Subjects may result in a fine of up to €36,000 which may be tripled depending on the offender's economic status. There are a number of other types of non-compliance under S.162 of the Code which may result in fines of up to €180,000.

S.167 of the Code governs Unlawful Data Processing which, depending on the offence, may be punishable by up to 3 years' imprisonment unless the offence is more serious.

S.168 of the Code governs Untrue Declarations and Notifications Submitted to the Garante which is punishable by imprisonment of up to 3 years unless the offence is more serious.

S.169 of the Code governs Security Measures. Those who fail to adopt the minimum measures may be punished by detention for up to two years. A time limit shall be set either upon detecting the abovementioned offence or, in complex cases, by way of a subsequent provision issued by the Garante, for the offender to comply with the requirements referred to above.

S.170 of the Code governs the Failure to Comply with Provisions Issued by the Garante which is punishable by up to 2 years' imprisonment.

**The Netherlands**

Offences committed under Article 138ab of the Dutch Criminal Code are punishable by a maximum one year prison sentence or a financial penalty of approximately €19,000 for the penetration alone. If the penetrator also records data from the penetrated computer for its own purposes or for another party's purpose, the maximum prison sentence is four years.

There are no specific sanctions for dealing in personal data without the data subject's consent, except for the general enforcement entitlements of the Dutch Data Protection Authority and the possibility for individuals to claim damages.

**Poland**

The following criminal acts are punishable by fines, restriction of freedom or up to eight years imprisonment: illegal access to information that was not intended to a given person, e.g. breach of electronic protection measures including computers; damage to a data base; disruption of a computer system and illegal use of computers and data.

Under the PDPA, any processing of personal data where such processing is forbidden (e.g. without consent or in breach of other data processing conditions) shall be liable to a fine, restriction of freedom or imprisonment up to two years. Illegal processing of sensitive data in a data filing system is subject to a fine, partial restriction of freedom or imprisonment up to three years.

**Portugal**

Infringement of notification and data protection obligations is a crime and may result in up to 1 year's imprisonment.

The following are also crimes under the penal code: invasions of privacy by informatics means (article 193); informatics or communications fraud (article 221); racial, religious or sexual discrimination via the internet (article 240). Portugese cybercrime law also specifies the crimes of: informatics falseness, damage to programs or systems, informatics sabotage, illegal access, illegal interception, illegal reproduction of programs (punishable by 5 years' imprisonment).

Legal entities may be subject to criminal sanctions with one month's imprisonment converted to 10 days' fine (of between €100 and €10,000 per day). Portugal has signed the Convention on Cybercrime of the European Counsel (Budapest Convention).

**Scotland**

As Data Protection in Scotland is within the jurisdiction of the United Kingdom's Information Commissioner please see England & Wales.

**Spain**

Hacking or gaining access to electronic systems could involve the commission of different criminal offences (e.g. fraud, phishing, identity theft, etc.). These offences could be penalised with imprisonment or fines. The amount of the fines depends on the gravity of the offence and the resources of the offender.

Civil sanctions for those dealing in personal data without the data subject's consent could consist in a fine from € 40,001 to € 300,000.

**Sweden**

In the wake of several cyber-attacks, some of which targeted Swedish government websites, there has been a new call for a toughening of criminal penalties for hacking and other attacks against computer systems. An on-going parliamentary inquiry into IT-related crimes has been tasked with taking a closer look at the penalties associated with hacking and other forms of cybercrime. Currently, the maximum penalty for anyone convicted of computer hacking in Sweden is two years in prison.

**USA**

Under 18 U.S.C. § 1028, it is a federal crime to knowingly and without authority produce, possess, or transfer an identification document, authentication feature, or false identification document; or use, without authority, identification of another person with the intent to commit or aid or abet unlawful activity under federal law, or that constitutes a felony under state or local law. Conspirators are subject to the same penalties as those who commit an offense. Violations may result in fines and/or imprisonment up to 15, 20, or 30 years.

The Computer Fraud and Abuse Act (CFAA—18 U.S.C. § 1030) makes it a federal crime to, among other things, intentionally access a computer without authorization and obtain information in a financial record of a financial institution or in a consumer reporting agency on a consumer, information from any U.S. department or agency or any protected computer, or knowingly and with intent to defraud, traffick in passwords allowing unauthorized access to computers, engage in computer fraud or computer extortion. The maximum penalty is imprisonment for 20 years. Goods or items obtained through fraud using a protected computer are subject to seizure.

The Electronic Communications Privacy Act (ECPA—18 U.S.C. §§ 2510–2521, 2701–2710) makes it illegal to intercept stored or transmitted electronic communications, or intentionally use or disclose such communications without authorization. Violations may result in imprisonment for up to 5 years and fines of up to $250,000.

The American Recovery and Reinvestment Act (ARRA) applies HIPAA criminal penalties to any person: criminal fines of up to $250,000 and up to 10 years in prison for disclosing or obtaining health information with the intent to sell, transfer, or use it for commercial advantage or malicious harm.

**California**

Under California Penal Code § 502 anyone that knowingly accesses and without permission [accesses], copies, uses, alters, damages, deletes, destroys, or otherwise uses or disrupts the use of any data, computer, computer system, or introduces any computer contaminant into any computer, computer system, or computer network is guilty of a crime. Depending upon the particular violation punishments range from fines from $950 to $10,000, and imprisonment up to three years.

In addition to any other civil remedy available, one who suffers damages as a result of the above activities may bring a civil action against the violator for compensatory damages and injunctive relief or other equitable relief. Compensatory damages include any expenditure reasonably and necessarily to verify that a computer system was not altered, damaged, or deleted by the access. Punitive and exemplary damages may also be recovered. Further, the conduct of an unemancipated minor are imputed to the parent or legal guardian having control or custody of the minor.

**Texas**

Texas penal code, Section 33.02, covers the breach of computer security (hacking) by an unauthorized person, and makes it a crime for someone to knowingly access a computer, computer network, or computer system without the effective consent of the owner. Depending on whether the offender benefitted from the obtained data and the severity of the offense, the offender may be charged with a Class A or B misdemeanour with awards of over $200,000 in damage and a first degree felony (equivalent to murder).

Texas also has two other penal provisions covering the Unauthorized Acquisition or Transfer of Certain Financial Information (Tex. Penal Code Ann. Section 31.17) and Fraudulent Use or Possession of Indentifying Information (identity theft) (Tex. Penal Code Ann. Section 32.51) that provide for criminal sanctions/penalties for utilizing personal data without someone's consent. The classification of the offense ranges from misdemeanour to first degree felony depending on the number of records breached, and enhanced penalties can occur where the offense was committed against an elderly individual.

**Canada**

Section 342.1 of the Criminal Code provides that the fraudulent use of a computer to access unauthorized data is punishable by indictable offense with imprisonment of up to 10 years.

Relatedly, Section 184 of the Criminal Code prohibits the interception of private communications and the illicit storage, modification, or disclosure of personal information, electronically or otherwise, absent statutory exceptions, including law enforcement or to prevent bodily harm. Contravention of Section 184 is punishable by indictable offense with a term of imprisonment of up to 5 years.

**Mexico**

The protection system is complemented by the criminal classification of certain transgressions (violation of security of data for the purpose of illegitimate gain) and deceitfully obtaining personal data for the purpose of illegitimate gain. The question is, how do our legislators expect that the Federal Act for the Protection of Personal Data in the Possession of Private Individuals is complied with if there is no procedure in place to check this information and, even more so, to apply fines and penalties, without there being the essential formality by which the person responsible or the assumed transgressor may defend him or herself as they are entitled to by law. This right is laid down in Article 14 of the Constitution that forms part of citizens' individual rights.

# 10. Are there any notable aspects of data breach law in your jurisdiction for insurance underwriters and claims professionals?

**Austria**

Currently Insurers should be aware of the following issues in addition to the EU Data Protection Directive 95/46: (i) Austria had a base right for privacy since 1980, (ii) Legal persons may be data subjects under Austrian law, (iii) The international transfer of personal data to a country without adequate level of data protection requires approval by the Austrian Data Protection Commission, even if a EU model contract has been entered into, (iv) The Data Protection Commission is heavily understaffed and has not been established in accordance with said Directive (as per a recent ECJ judgement) and (v) There is a general obligation to notify the Data Protection Commission (a subdivision thereof) of each and every data processing, unless listed in a decree with exceptions.

Thereupon at least certain aspects of data management schemes within international groups of companies are to be treated quite different in Austria than in other European countries.

**Belgium**

The vast majority of the provisions of Belgian insurance legislation are mandatory. It is therefore important not to import typical UK or US wording into Belgium without prior compliance screening with the Belgian legislation.

**Czech Republic**

Czech privacy law is and will be in compliance with EU legislation in this area. Thus we recommend the insurers to get acquainted with the relevant EU regulations inclusive of its drafts.

**England & Wales**

Insurers should familiarise themselves with the European draft data protection regulations which aim to harmonise privacy laws across Europe.

**France**

Extension of cover for IT risks can be taken out. Any such cover will have to comply with the mandatory provisions of the Insurance Code. For instance, any exclusion must be precise and drafted in apparent character. Exclusions for failures to comply with the requirements of the French Data Protection Act which are too general will be considered as unlawful.

**Germany**

The cyber issue is and will furthermore become an "European issue". International legislative measures have to be observed.

**Ireland**

Insurers should familiarise themselves with the European draft data protection regulations which aim to harmonise privacy laws across Europe.

**Italy**

Italian insurance law is and will be in compliance with EU legislation in this area. Thus we recommend the insurers to get acquainted with the relevant EU regulations inclusive of its drafts.

Insurers should familiarise themselves with Isvap Regulations and also with "Lettere al mercato" – FAQ published on the Authority website. These aren't legal texts in a strict sense but indicate the guidelines of the Authority on specific topics.

**The Netherlands**

Insurers should keep track of the developments of the legislative bill for a general data breach notification duty. Furthermore they should familiarise themselves with the European draft Data Protection Regulation which aims to harmonise data protection laws across the EU.

**Poland**

As mentioned above, under Polish law property insurance may cover any property interest that can be assessed in monetary terms and which is not unlawful. When preparing insurance products covering risk related to liability for infringement of laws, insurers need to review whether insuring particular risks is allowed.

Additionally, insurers should familiarise themselves with a statutory list of abusive clauses that cannot be employed in insurance products addressed to consumers.

**Portugal**

A large number of mandatory liability insurance (with specific wording fixed by law and by the insurance authority) and a public order principle (making the Portuguese law to prevail) are to consider. Intentional damages may not be excluded from mandatory liability insurances,

**Scotland**

As Data Protection in Scotland is within the jurisdiction of the United Kingdom's Information Commissioner please refer to England & Wales. However it is relevant to mention that there is also a Scottish Information Commissioner, whose jurisdiction relates to Freedom of Information demands made against Scottish Public Authorities. Freedom of Information demands against Public Authorities operating in Scotland in relation to non-devolved ("Retained") matters are dealt with by the UK Information Commissioner.

**Spain**

Most of the provisions of Spanish insurance legislation are mandatory. Usually, UK or US wording fails to comply with local legal requirements, meaning that, in the event of judicial proceedings, Courts will apply the policy but without exclusions.

**Sweden**

Insurers should familiarise themselves with Sweden's existing laws relating to Data Protection and of course be aware that there is a call by many for an increase in the penalties relating to breaches. "Hacking" has been a rather big media issue of later so it will be interesting to see how things develop within the next few months.

**USA**

Regulation of personal information in the United States is multi-layered due to federal and state statutes and regulations, self-regulation (e.g., Payment Card Industry Data Security Standard adopted by organizations handling cardholder information), and state common law.

**California**

Insurers should be aware of the potential defenses to civil actions, including exculpatory provisions and limitation of liability provisions.

**Texas**

Aside from the typical Texas insurance coverage issues, none directly related to cyber breaches. However, it should be emphasized that a recent amendment to the Texas Identity Theft Enforcement and Protection Act (Chapter 521, Texas Business & Commerce Code), effective September 1, 2012, extended the reach of the data notification obligations beyond Texas borders to all affected individuals, whether in Texas or elsewhere. This will clearly increase the costs accompanying notification.

**Canada**

Insurers operating in Canada should familiarize themselves with the interplay between federal and provincial privacy legislation. For example, while PIPEDA may be good law in Nova Scotia, its authority is overcome in full by alternative statutes passed in British Columbia and Alberta, but only in part by Ontario's legislative scheme.

**Mexico**

Filling systems of clients' personal data (including personal data of policyholders, insured and beneficiaries of the insurances). Insurance companies must obtain the owners of personal data's consent so any data compiled is done so lawfully. They may give their consent orally, in writing or in any other irrefutable manner, irrespective of the media used to compile this information. The Act emphasizes that express consent shall be required in order to process financial and property-related information, but consent must be given in writing, by means of an original or electronic signature, for sensitive personal data. The only way to comply with this requirement is with the Privacy Note that shall be signed by the owners of personal data.

# 11. Are there any notable data breach insurance coverage issues that have arisen in your jurisdiction?

**Austria**

Cyber risk policies are relatively new on the Austrian market. Although these risks were previously covered to some extent by other types of insurance policies, nowadays specific cyber risk policies are offered and other policies exclude cyber risk. Nonetheless, these policies have not yet resulted in any relevant insurance coverage litigation.

**Belgium**

For a few years cyber liability insurance policies have become common within the Belgian insurance market. Nonetheless, these policies have not yet resulted in any insurance coverage litigation.

**England & Wales**

There is frequent confusion over the potential overlap between traditional covers such as (e.g.) property and E&O which are not designed to respond to cyber risks, and bespoke cyber policies, which are. Insurers are starting to narrow the scope of cover (e.g. through the use of harsher exclusions for lack of encryption) and clients need to fully understand the scope of the cover provided.

**France**

Attention should be paid to specificities in relation to the use of medical data. Medical data obtained by insurers through a health questionnaire, particularly with regard to credit insurance contracts, are confidential. The use of data in relation to the genetic characteristics of a potential insured is prohibited: Article L. 1141–1 of the Public Health Code expressly prohibits companies and organizations covering disablement or death risks by using data from a person's genetic tests, at the time of the subscription or during the contract.

**Germany**

Generally the question is whether traditional insurance (liability) products are able to insure the client's needs. This is probably not the case, so that the insurance industry started to introduce special forms of cyber liability insurance products in Germany.

**Ireland**

As far as we are aware, no policies have resulted in any insurance coverage litigation.

**Italy**

Specific insurance of cyber risk are becoming more common in Italy but until now no specific litigation has emerged of those policies.

**The Netherlands**

More traditional covers such as General Liability Policies and E&O generally do not, or not adequately, provide for cover for cyber risks. A specific policy or schedule covering cyber risks is usually required to cover both 1st party and third party risks and financial loss (not caused by property or personal injury)

**Poland**

Specific insurance of cyber risks is relatively new on Polish market. Although these risks were previously covered, to some extent, by traditional types of insurance, now new types of specific insurance are offered, e.g. Computer Liability Errors & Omissions and specific cyber risks clauses. In consequence, sometimes the scope of these covers may be overlapping or not covering risks crucial for particular clients.

**Portugal**

Until now the liability cover on cyber risks is given within the general liability insurance of Companies and other entities. The data extension cover is becoming more and more detailed.

**Scotland**

There is frequent confusion over the potential overlap between traditional covers such as (e.g.) property and E&O which are not designed to respond to cyber risks, and bespoke cyber policies, which are. Insurers are starting to narrow the scope of cover (e.g. through the use of harsher exclusions for lack of encryption) and clients need to fully understand the scope of the cover provided.

**Spain**

Specific insurance of cyber risk is quite recent in Spain. Until now no specific litigation has emerged of those policies.

**Sweden**

Cyber liability insurance policies are relatively new to Sweden, but with a number of rather high profile breaches / attacks it is anticipated that requests for such coverage will become more frequent.

**USA**

Courts continue to determine the contours of coverage for claims involving cyber risk, electronic or personal data, and privacy issues. In general, traditional insurance (i.e., non-cyber risk coverage) is not a complete answer to cyber risk.

Combined General Liability (CGL) coverage extends to injury to a person or tangible property, data alone is generally not considered tangible property, and newer policies expressly state electronic data is not tangible property. And for personal injury coverage, there must be some publication of material that violates a person's right of privacy.

Professional Liability coverage for cyber risk depends on how the policy defines "professional services."

Commercial Property coverage might apply in limited fashion for loss or damage to data that is destroyed or corrupted by covered cause.

Commercial Crime coverage might provide some coverage, depending on the property at issue and whether losses are direct or indirect.

**CGL:**

ISO's standard forms CG 00 01 10 01 and CG 00 01 12 07 expressly state in the definition of "property damage" that "electronic data is not tangible property." Courts have enforced that provision as unambiguously excluding claims based on electronic data from coverage. *Recall Total Info. Mgmt., Inc. v. Fed. Ins. Co.*, 2012 WL 469988 (Conn. Super. Ct. 2012). Older forms do not have that provision. Courts have generally held that electronic data itself is intangible property, but if taking of a computer, disc or other item containing the electronic data is involved, tangible property is at issue. E.g., *AOL, Inc. v. St. Paul Mercury Ins. Co.*, 347 F.3d 89 (4th Cir. 2003). Allegations of spyware infecting a computer causing the computer (tangible property) to not work properly or at all may trigger property damage coverage. *Eyeblaster, Inc. v. Fed. Ins. Co.*, 613 F.3d 797 (8th Cir. 2010). The exclusion for damage to personal property in the care, custody, or control of the insured might bar coverage, depending on the allegations. *Nationwide Ins. Co. v. Hentz*, 2012 WL 734193 (S.D. Ill. 2012).

Under CGL policy, there was "personal injury" coverage for "making known to any person or organization written or spoken material that violates a person's right to privacy," where software gave a company information about users' online activities, which was disseminated within the company and used for targeted advertising. Publication of the material to third parties was not necessary; in other words, the company's making known information to itself triggered a duty to defend. *Netscape Comm'ns Corp. v. Fed. Ins. Co.*, 343 Fed. App'x 271 (9th Cir. 2009).

In contrast, it has been held that alleged FACTA violations by a merchant printing receipts with more than 5 digits of consumers' credit cards and their expiration dates did not trigger "personal injury" coverage under a CGL policy because printing a receipt and handing it to the card holder did not constitute "publication" of material that violated a person's right of privacy. *Creative Hospitality Ventures, Inc. v. U.S. Liab. Ins. Co.*, 444 Fed. App'x 370 (11th Cir. 2011) (applying Florida law). Similarly, there was no coverage for a transport vendor when a cart with computer tapes of IBM employee data fell out of a van, because there was no publication to a third party. *Recall Total Info. Mgmt., Inc. v. Fed. Ins. Co.*, 2012 WL 469988 (Conn. Super. Ct. 2012).

Breach of privacy claims arising out of a fax blast, violating the Telephone Consumer Protection Act, may trigger personal and advertising injury coverage because it involves written publication of material violating a person's right of privacy. *Penzer v. Transp. Ins. Co.*, 29 So. 3d 1000 (Fla. 2010).

It is possible to have concurrent coverage under a CGL policy and an Information and Network Technology E&O coverage. *Eyeblaster, Inc. v. Fed. Ins. Co.*, 613 F.3d 797 (8th Cir. 2010).

**Property Insurance**

Where hackers took over temporary use of servers, the court concluded temporary loss of use of the servers constituted "loss of" the property. Vonage *Holdings Corp. v. Hartford Fire Ins. Co.*, 2012 WL 1067694 (D.N.J. 2012).

Damage to electronic information after data was corrupted when a system failed constituted "direct, physical loss or damage"; data was intangible but still physical because it can be observed and altered through human action. *Landmark Am. Ins. Co. v. Gulf Coast Analytical Labs., Inc.*, 2012 WL 1094761 (M.D. La. 2012); see also *Am. Guar. & Liab. Ins. v. Ingram Micro, Inc.*, 2000 WL 726789 (D. Ariz. 2000) ("At a time when computer technology dominates our professional as well as personal lives, the Court must side with [the insured's] broader definition of 'physical damage'. The Court finds that 'physical damage' is not restricted to the physical destruction or harm of computer circuitry but includes loss of access, loss of use, and loss of functionality.").

**Crime Policy**

Under a blanket crime policy, the insured only needed to show "loss" sustained "resulting directly from" theft of insured property by computer fraud under proximate cause standard. And an exclusion barring coverage for loss of "proprietary information" did not apply because the data (credit card and checking account information) did not fall within the plain meaning of "proprietary information." *Retail Ventures, Inc. v. Nat'l Union Fire Insurance Co. of Pittsburgh*, 691 F.3d 821 (6th Cir. 2012).

**Coverage Territory**

Another issue to keep in mind regarding cyber risk and claims is how policies define "coverage territory." Under the pre-2001 ISO Form CG 00 01 01 96, "coverage territory" is defined as the United States, Puerto Rico and Canada, as well as:

All parts of the world if:

The injury or damage arises out of:

(a) Goods or products made or sold by you [in the United States, Puerto Rico or Canada]; or

(b) The activities of a person whose home is [in the United States, Puerto Rico or Canada] but is away for a short time on your business; and

(c) The insured's responsibility to pay damages is determined in a "suit" on the merits, in [the United States, Puerto Rico or Canada] or in a settlement we agree to.

An international company or company that subcontracts computer maintenance or other services, particularly those with clients or consumers outside the United States must pay close attention to this aspect of coverage.

Later forms modified the definition of "coverage territory. ISO Form CG 00 01 10 01 includes "[a]ll other parts of the world if the injury or damage arises out of … 'Personal and advertising injury' offenses that take place through the Internet or similar electronic means of communication."

**California**

Coverage issues frequently arise regarding the inability to indemnify for intentional acts and gross negligence, as well as the definition of damages as opposed to penalties and fines.

**Texas**

None so far involving cyber liability policies.

**Canada**

*Zurich American Ins. Co. v. Sony Corp. Of America, No. 651982/2011* (N.Y. Sup. Ct. July 2011), is an action for declaratory judgment in which the insurer, Zurich, seeks a court order denying coverage of a large scale data breach that occurred to its insured (Sony Corp., including Sony Corp. Canada). *Zurich v. Sony* is demonstrative of the increasing divide between the limits of traditional coverage and independent cyber coverage policies. Insureds, particularly in the institutional context, should be cognizant of the emergence of specialized insurance products designed to address data security liability and the variability of their provisions given the lack of standardized coverage in this area.

**Mexico**

Cyber risk insurance is new and recent in Mexico. Only two insurance companies are selling this product. On this basis, we are sure that no specific litigation has arisen out of these policies.

# Contributors

## Europe

**Austria**

Felix Hörlsberger and Marguerita Sedrati-Müller, Dorda Brugger Jordis Rechtsanwälte GmbH

**Belgium**

Hugo Keulers, Lydian

**Czech Republic**

Vít Horáček, Glatzová & Co

**England and Wales:**

Patrick Hill and Hans Allnutt, DAC Beachcroft LLP

**France**

Simon Ndiaye and Sophie Cochery, HMN & Partners

**Germany**

Bastian Finkel, Bach Langheid Dallmayr

**Ireland**

James Colville, DAC Beachcroft Dublin

**Italy**

Claudio Russo, Studio Legale Volpe Putzolu E Russo

**Poland**

Michal Steinhagen, Wardyński & Partners

**Portugal**

Luis Filipe Caldas, Serra Lopes Cortes Martins e Associados

**Scotland**

Paul Motion and Alan Eadie, Brechin Tindal Oatts

**Spain**

Luis Siles and Jesús Iglesias, DAC Beachcroft LLP

**Sweden**

John Daerr, Advokatfirman Vinge KB

**The Netherlands**

Elisabeth Thole and Isabelle Wárlám, Van Doorne N.V.

## North America

**Canada**

Howard Borlack, McCague Borlack LLP

**Mexico**

José Luis Arce Fernández, DAC Beachcroft LLP

**US**

**California**

Anthony Ellrod, Manning & Kass, Ellrod, Ramirez, Trester LLP

**Texas**

Dwayne Hermes and Chris Hansen, Hermes Sargent Bates LLP

**US Overview**

Brad Jones and Anthony Alt, Meagher & Greer LLP

Edited by: Hans Allnutt, Giancarlo Di Santo and Milagros Sanz

# Contact details

## Europe

**Austria**

Dorda Brugger Jordis Rechtsanwälte GmbH
Dr-Karl-Lueger-Ring 10
Vienna, 1010

www.dbj.at

**Belgium**

Lydian
Tour & Taxis
Havenlaan – Avenue du Port 86c b113
1000 Brussels

www.lydian.be

**Czech Republic**

Glatzová & Co.
Husova 5
Prague 1, 110 00

www.glatzova.com

**England & Wales**

DAC Beachcroft LLP
3 Minster Court
Mincing Lane
London EC3R 7DD

www.dacbeachcroft.com

**France**

HMN & Partners
2, Avenue Montaigne
Paris 75008

www.hmn–partners.com

**Germany**

Bach Langheid Dallmayr
Theodor-Heuss-Ring 13–15
50668 Cologne

www.bld.de

**Ireland**

DAC Beachcroft Dublin
Second Floor
Fleming Court
Fleming Place
Dublin, 4

www.dacbeachcroft.com

**Italy**

Studio Legale Volpe Putzolu E Russo
Viale Bruno Buozzi N. 53
Rome, 00197

www.vpr–lex.it

**Poland**

Wardyński & Partners
Aleje Ujazdowskie 10
00–478 Warsaw

www.wardynski.com.pl

**Portugal**

Serra Lopes, Cortes Martins e Associados
N°3 Torre 2 – 12° A E B
Lisboa, 1600–100

www.slcm.pt

**Scotland**

Brechin Tindal Oatts
48 St. Vincent Street
Glasgow G2 5HS

www.bto.co.uk

**Spain**

DAC Beachcroft
Serrano, 37
Madrid, 28001

www.dacbeachcroft.com

**Sweden**

Advokatfirman Vinge KB
Ostergatan 30
Box 4255
Malmo, 201 13

www.vinge.se

**The Netherlands**

Van Doorne N.V.
Jachthavenweg 121
1081 KM Amsterdam
Amsterdam, 1070 AG

www.vandoorne.com

## North America

**Canada**

McCague Borlack
Suite 2700, P.O. Box 136
The Exchange Tower
130 King Street West
Toronto
Ontario
M5X 1C7

http://www.mccagueborlack.com/

**Mexico**

DAC Beachcroft
Monte Pelvoux 210 PB–A,
Colonia Lomas de Chapultepec,
Delegación Miguel Hidalgo,
11000 México, D.F,

www.dacbeachcroft.com

**USA**

**California**

Manning & Kass, Ellrod, Ramirez, Trester LLP
801 S. Figueroa Street
15th Floor
Los Angeles, CA 90017

www.mmker.com

**Texas**

Hermes Sargent Bates LLP
901 Main Street
Suite 5200
Dallas, Texas 75202

www.hsblaw.com

**US overview**

Meagher & Greer LLP
33 S. Sixth Street
Suite 4400
Minneapolis, MN 55402

www.meagher.com