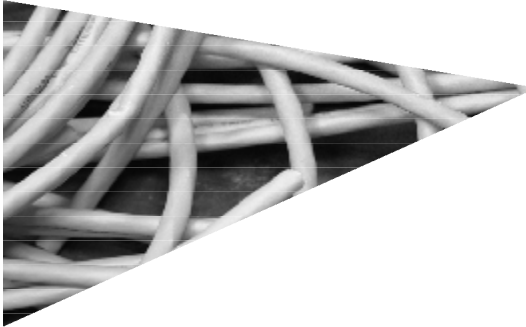


**Update IP/ICT
Law Practice**



Privacy and data protection law

European Developments

Privacy as a key business issue

Data privacy has become a growing concern for individuals as well as for organisations. Nowadays, legal compliance with European data privacy rules has become an essential business practice for European and non-European organisations that wish to develop trusted relationships with their customers, suppliers and employees. Compliant privacy practices are a key element of corporate governance and accountability.

Failures regarding privacy compliance may result in damages to the organisation's reputation, brand or business relationships as well as legal liability or regulatory sanctions, lawsuits for deceptive business and loss of customers' and employee's confidence. Apart from the sanctioning regime negative publicity is a key driver for organisations' efforts to ensure data protection compliance.

This publication is intended to quarterly **highlight issues** and to mention **recent developments** with respect to privacy and data protection laws in Europe.

European Union

1 EU 'Cookie directive'

On 24 November 2009 European Parliament approved Directive 2009/136 EC which finalized the so-called "Telecom Reform Package". The Directive 2009/136/EC contains amendments for the Directives 2002/22/EC (Universal Service Directive) and 2002/58/EC (Directive on privacy and electronic communications and also Regulation (EC) 2006/2004 (the Regulation on consumer protection cooperation). The amendments of the Directive on privacy and electronic communications (also referred to as "the ePrivacy Directive") aim to enhance the protection of individual privacy and personal data and introduce new regulation regarding security breaches, spyware, cookies and spam. The revised Directives must be implemented by the Member States within 18 months.

Finland

2 Statement of the Finnish Data Protection Ombudsman regarding the disclosure of personal data in connection with mergers and acquisitions

In connection with mergers and acquisition the acquirer or new employer is in general interested in obtaining information regarding the company's employees including names, salaries and performance assessments. Such information might to some extent be part of the due diligence material provided to the prospective purchaser. The question therefore arises at what point of time in what form and on what basis such data may be provided to the prospective purchaser.

The Finnish Data Protection Ombudsman recently made a statement regarding the issue of disclosure of personal data in connection with mergers and acquisitions. He found that employees' data form one or more personal data files that had been created for the purpose of personnel administration. These personal files might in their entirety only be transferred to the new employer, when the transaction had been actually consummated e.g. by means of a binding agreement. In this respect the provisions of Chapter 1 Section 10 of the Employment Contracts Act apply. According to this provision rights and obligations and employment benefits related to the employment relationships valid at the time of the assignment of the business devolve to the new owner or proprietor upon assignment of the business.

The Finnish Data Protection Ombudsman found that prior to the consummation of a merger or acquisition the transfer of personal data that was not sensitive, was permitted, if the purpose for which the data was disclosed to the purchaser was not incompatible with the purpose of the processing and if it could be assumed that the employee was aware of such disclosure. The Data Protection Ombudsman took the view that the disclosure of the names of employees including salary information and performance assessment was not compatible with the purpose of the processing. He therefore recommended that e.g. salary data was presented on an aggregate basis for instance on the basis of the costs/business unit, so that individual employees could not be identified. In respect of key personnel the disclosure of more detailed data on the basis of a letter of intent, might be permitted, provided that such disclosure fulfilled the specific necessity requirement.

The Data Protection Ombudsman stressed furthermore the employer's obligations to inform the employees in accordance with the Personal Data Act and to comply with the requirements under the Act on the Cooperation within Undertakings. He pointed also out that prior to the disclosure of the personal data the employer was obliged to review the personal data contained in the personnel files from the point of view of accuracy and necessity and to take care that outdated, unnecessary and inaccurate data was not transferred to the new employer.

3 The Act on Electronic Identification and Electronic Signatures (617/2009) entered into force on 1 September 2009.

The Act on Electronic Identification and Electronic Signatures replaces the Act on Electronic Signatures (14/2003) that incorporated Directive 1999/93/EC of European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

Strong electronic identification is used to identify and verify the authenticity and identity of a person. Under the new act it is defined as an individualization of a person and verification of the authenticity and genuineness of the identifier by means of an electronic method, whereby at least two different factors are used in conjunction to authenticate. An electronic strong identification must therefore be based upon two out of three of the following methods, namely (i) upon a password or something that only the user knows, (ii) upon an electronic smartcard or something that only the user has in his possession or (iii) upon a fingerprint or something that identifies only the user. Strong electronic identification might, for instance, be used in online banking, in electronic commerce or in relation to

other services, where the authentication of the parties involved is necessary. Weak identification that is typically based upon identification by a user name in combination with a password does not fall within the application of the act.

The new Act introduces general rules regarding the offering of strong electronic identification services with the purpose of promoting the provision of services related thereto. Amongst others the rules on strong electronic identification set out the requirements regarding the identification process and the service provider and provide for general obligations of the service provider offering strong identification services. The Act also contains rules relating to the use of the identification device and limitations regarding the liability of the user of the identification device. The Act's provisions regarding electronic signatures and the offering of qualified certification services incorporate mainly the provisions of the previous Act on Electronic Signatures.

The new Act requires that an identification service provider as well as a certification provider providing qualified certificates notifies the Finnish Communications Regulatory Authority (FICORA) prior to starting operations. FICORA is responsible for the surveillance of the providers of identification services and certification services providers that provide qualified certificates and may issue technical regulations on the requirements for the reliability and information security of their operations.

France

4 Data Protection Bill

A bill was presented before the Senate on 6 November 2009 in order to improve the protection of the privacy and the personal data protection of each individual in the technological environment.

This bill aims to give additional safeguards to the privacy/data protection of the individuals taking into account for instance the development of information technologies and the risks of online social networks.

The main provisions of the said bill are as follows:

- ▶ IP addresses are explicitly qualified, in Article 2 al. 2 of the French Data Protection Law (FDPL), as personal data (see Article 2 of the said bill);
- ▶ An entity employing 50 people or more must appoint a Data Protection Officer (see Article 3 of the said bill) (it is optional pursuant to current legislation);
- ▶ The Data Controller is subject to additional obligations as regards the information of the data subject (e.g., mention of the data retention period to the data subject), to the extent the Data Controller has a website, the Data Controller i) must provide the data subject with the possibility to contact him by electronic means concerning his right of access, rectification and deletion and ii) must insert on its website a section dedicated to the data protection information (see Article 6 of the said bill);
- ▶ The Data Controller must notify any security breach concerning the personal data processing to the French Data Protection Authority (CNIL) (see Article 7 of the said bill);

- ▶ The terms « right of deletion » (more explicit) replace the terms « right of opposition » (see Article 8 of the said bill);
- ▶ The Data Controller must indicate the origin of the personal data processed to the data subject who carried out his right of access (Article 9);

The bill also aims to increase the amount of the financial penalties provided for by the CNIL. In case of a first breach, the penalty may not exceed € 300.000 (instead of € 150.000 as of today) and in case of a second breach within 5 years, the penalty may not exceed 600.000€ (instead of 300.000€ as per today) (cf. Article 12 of the said bill). The provisions of this bill will apply only 6 months after the publication of the bill in order to enable the data controller to move to compliance with this bill if passed as an Act.

- ▶ Sanctions of the CNIL cancelled by the Conseil d'Etat (French Administrative jurisdiction)

Pursuant to the FDPL, the CNIL may access the premises in which the data processing is carried out in order to verify its compliance with the FDPL. In 2009, the CNIL carried out 270 verification visits.

On 14 December 2006, the CNIL pronounced sanctions against two French entities which propose business services by contacting the data subject by phone. The CNIL considered that the data subjects were not in a position to refuse the phone calls of these companies and fined both companies.

On 6 November 2009, the Conseil d'Etat decided to cancel these CNIL's sanctions because before carrying out these verifications, the CNIL had not informed the Data Controllers concerned that they may refuse the verification visit (see Article 44 of the FDPL). In this context, the CNIL decided to take into account this decision in order to modify its verification procedures.

Germany

5 Germany Introduces Stricter Data Protection Law – Serious Impact on Business Compliance (Part 1)

On 1 September 2009 a comprehensively revised Data Protection Law entered into force in Germany. The new amendments to the Federal Data Protection Act (BDSG) cover a range of data protection related issues, including marketing, security breach notification, protections for employee data and **commissioned data processing**. They also include new powers for data protection authorities and provide for increased fines for violations of data protection law provisions.

I. Use of Customer Data for Marketing Purposes

As a basic rule the processing and use of personal data for the purposes of selling addresses and using contact details for marketing is permitted only if the individual has expressly consented to such use. There are, however, certain exceptions to this basic rule that allow the data controller to use specific customer data to advertise own products or services and those of a third party. This applies to lists of data or other summaries of data from members of a category of persons defined only in terms of the data subject's membership of this category, his or her occupation, name, title, academic degree(s), address and year of birth. As a requirement this data has to be collected and stored for the purpose of a legal or quasi-legal contractual obligation with the customer. In case personal data shall be collected outside a quasi-legal contractual obligation the consent of the data subject has to be obtained. Moreover data collected from public directories

may be used for advertisement purposes without consent.

II. Introduction of Security Breach Notification Requirement

Data controllers will be subject to comprehensive breach notification requirements. The notification rules will apply to the following categories of data:

- ▶ Sensitive data (any information concerning an individual's race, ethnic origin, political opinions, religious or philosophical beliefs, membership in a trade union, health, or sex life);
- ▶ Personal data subject to professional or official confidentiality obligations (e.g., data held by lawyers and doctors);
- ▶ Data concerning criminal acts or administrative offenses;
- ▶ Personal data regarding bank or credit card accounts.

Notification is required in the event of an unlawful data transfer or unauthorized access by third parties if the data loss is likely to have a serious impact on the rights or protected interests of the individuals concerned.

Where notification is required, the data controller must notify the appropriate data protection authority ("DPA") and the affected individuals without delay. The law also specifies certain minimum content requirements for the notification. In cases where individual notification of an incident that affects a large number of data subjects is too burdensome, notice must be made via at least a half-page advertisement in at least two daily national newspapers or by other means that would provide similar exposure. Organizations will need to prepare incident response procedures and appoint an incident response team in order to ensure that any breach event is dealt with effectively, efficiently and in accordance with the legal notification requirements.

Update IP/ICT Law Practice - February 2010

III. Additional Protections Regarding Employee Data

Any processing of employee data is permissible only if the processing is necessary for the administration (*i.e.*, establishment, maintenance, or termination, of the employment relationship).

For the purposes of investigating employee offenses, employee data can be collected only where (1) the data substantiates the suspicion that the employee has committed an offense in the context of employment, (2) the collection, processing, and use of the data is necessary for the investigation, and (3) the type and scope of the collection, processing, and use of the data is proportional to the employee's protected rights and the circumstances of the investigation. Because the new rules limit the activities companies may engage in when investigating employees, they will have a significant impact on any internal investigations or employee screening efforts.

The remaining changes (including contractual requirements for commissioned data processing, greater recognition for DPOs, new powers for DPAs and stricter punishments) will be discussed in the upcoming newsletter.

The Netherlands

6 National Information database Debts (NID)

The Dutch Data Protection Authority (DDPA) has ruled that the initiative to come to an NID and draft NID is not in line with the Dutch Data Protection Act (DPA). The NID aims at preventing problematic debt situations of consumers by registering non payments. According to the DDPA the NID is thus a negative registration system with a stigmatized character.

The consumer will not only be confronted with a negative image but will also be confronted with organizations that refuse to make supplies. As a result the DDPA wishes to impose a system that is proportional and data which is secure. The draft system does not meet these criteria (yet) according to the DDPA.

Opinion:

The above ruling of the DDPA is called an 'opinion' of the DDPA. Responsible parties or a group of responsible parties may ask the DDPA for their opinion about unresolved questions or explanation of the DPA. Three cumulative criteria must be met for the DDPA to entertain a request:

- ▶ New legal question involving new technology or other developments that cannot be answered based on existing laws and regulations, case law or opinions of the article 29 workgroup
- ▶ Major social or economic importance, which is decided on the basis of 5 factors, e.g. the extent and importance of the risks involved with personal data processing; nature and sensitivity of data, nature of the service, extent to which the citizens' interests are at stake
- ▶ The request must be made in writing.

7 Data protection in the health care sector

As of 1 January 2010 hospitals in the Netherlands are obliged to have a security protocol in place in line with the so-called NEN 7510 standard. The NEN 7510 is an industry standard based on the ISO Code of Information security designed for organizations in the health care sector. Following its implementation in hospitals, the standard will become mandatory for other care institutions. The question

is under debate whether or not this standard can be made mandatory by law and how the (correct) implementation and compliance should be monitored by external audit organisations. The Dutch Hospital Association is said to propose a format for external auditing in the spring of 2010.

Spain

8 Madrid Protocol

On 5 November 2009, the 31st International Conference of Data Protection and Privacy Commissioners was held in Madrid, where a Joint Proposal of International Standards on the Protection of Privacy with regard to the processing of Personal Data was drafted seeking an integration of legislations on five continents.

As the host of the International Conference the Spanish Data Protection Agency was in charge of coordinating the work of drafting and submitting a Joint Proposal for setting international standards on privacy and personal data protection to its closed session.

The Joint Proposal contains principles, rights, obligations and procedures with the aim of expanding these by adding solutions and specific provisions which could apply irrespective of any differences that may exist between the different existing models of data protection and privacy. International flows of personal data are needed in a globalized world.

The purpose of the Document is to define a set of principles and rights guaranteeing the effective and internationally uniform protection of privacy with regard to the processing of personal data.

The rights of data protection and privacy are considered as

fundamental rights of individuals, irrespective of their nationality or residence, and the persisting data protection and privacy disparities in the world, due to the fact that many states have not yet passed adequate laws, harm the exchange of personal information and the implementation of effective global data protection.

The Joint Proposal for a Draft of International Standards on the Protection of Privacy with regard to the processing of Personal Data is based on principles that are present in different instruments, guidelines or recommendations of an international scope and have received a broad consensus in their respective geographical, economic or legal areas.

This Document in its application is aimed at any processing of personal data, wholly or partly by automatic means, or otherwise in a structured manner, and carried out in the public or the private sector. However, States may supplement the level of protection provided for in this Document with additional measures guaranteeing a better protection of privacy with regard to the processing of personal data.

The Proposal comprises 25 Sections and 6 Parts entitled: General provisions, Basic principles, Legitimacy of proceeding, Rights of the Data Subject, Security and Compliance and Monitoring.

The processing of personal data in the public and private sector would thus be performed in a more internationally uniform approach implementing the principles of fairly, lawfully and in a proportionate manner processing in relation to specific, explicit and legitimate purposes, accountability and liability, even if the processing operations are carried out by service providers on behalf of the controller, offering more appropriate guarantees where the data are sensitive, ensuring that personal data transferred

internationally benefits from the level of protection provided by this set of standards, ensuring the accuracy, the confidentiality and the security of the data as well as the legitimacy of the processing, and the rights of data subjects to access, rectify and erase data, to object against its processing on the basis of transparent policies, informing adequately the data subjects and without any arbitrary discrimination against them in a new and modern framework of pro-active measures, such as those oriented in particular to prevent and detect breaches and based on the appointment of privacy officers as well as on efficient audits and privacy impact assessments.

As stated in the Joint Proposal for a Draft of International Standards on the Protection of privacy with regard to the processing of Personal Data, the authorities will try to cooperate to achieve a more uniform protection of privacy with regard to the processing of personal data, at both a national and international level. For the purpose of facilitating this cooperation, each State should be able to identify the competent supervisory authorities on its territory as needed.

Switzerland

9 Google Street View

On 11th November 2009 the Federal Data Privacy and Information Commissioner (FDPIC) filed a complaint, taking the online service Google Street View to the Federal Administrative Court. This is an important step in the course of a development that started back in March 2009, when the FDPIC notified Google that the publication of images would only be legally compliant if individuals appearing in them were rendered anonymous.

The FDPIC considers that numerous individuals and vehicle registration numbers had not been rendered

sufficiently anonymous and demanded substantial improvements. Because Google rejected large parts of the recommendation the FDPIC issued, the FDPIC filed the complaint to bring this case to the Federal Administrative Court.

For more information please visit on www.edoeb.admin.ch

10 Data loss at HSBC

On 9 December 2009 the media reported on a data theft at the branch of the British bank HSBC in Geneva. An IT specialist allegedly stole thousands of client related data. Shortly after this news the bank notified that only less than ten client names were affected and that the stolen data was no longer accurate. This was the only information disclosed by the bank for over a week. The media, however, released articles almost every day. The result was that the issue was raised on a political level and the media kept reporting information of HSBC that had hardly been confirmed.

Although the topic of this case is more in the field of data security and banking secrecy, this case showed that whenever reputation is at risk, communication is key and failure to respond is not an option. Since loss of reputation is one of the biggest risks in the area of data privacy as well, we deem it essential to be prepared for such an incident and to have a adequate communication strategy in place.

IP/ICT Law Practice

The IP/ICT Law Practice offers legal services as part of Ernst & Young EMEA Law Services and covers both national and international IP and ICT legal issues in the broadest sense of the word.

For further information please contact:

Finland

E Petra.hietanen-kunwald@fi.ey.com
T +358207280190

France

E Fabrice.naftalski@ey-avocats.com
T +33 1 55 61 10 05

Germany

E Fritjof.boerner@de.ey.com
T+49 6196 996 25758

Italy

E Luigi.neirotti@it.ey.com
T +39 02 85 14 828

Belgium/The Netherlands

E Peter.kits@hollandlaw.nl
T +31 40 2626570

Spain

E Jose.dominguezLeandro@es.ey.com
T +34 915 727 200

Switzerland

E Klaus.krohmann@ch.ey.com
T +41 58 286 4171

Ernst & Young

Assurance | Tax | Transactions | Advisory

About Ernst & Young

Ernst & Young is a global leader in assurance, tax, transaction and advisory services. Worldwide, our 144,000 people are united by our shared values and an unwavering commitment to quality. We make a difference by helping our people, our clients and our wider communities achieve their potential.

Ernst & Young refers to the global organization of member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit www.ey.com

© 2010 Ernst & Young

While every care has been taken in the development of this publication, information may become out of date or incorrect following publication. Ernst & Young cannot therefore be held liable for the consequences of actions taken on the basis of information obtained in this publication. This publication is intended to highlight issues. It is not intended to be comprehensive or to provide legal advice.