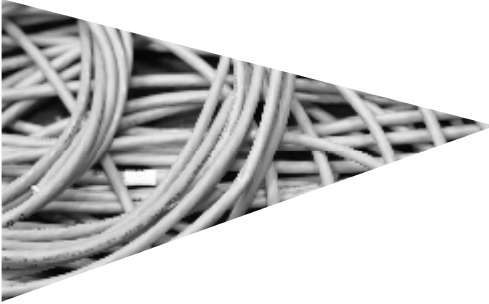


Update IP/ICT legal practice



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 a 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

■ Standard contractual clauses to be updated

Companies and Data Protection Authorities have been working for several years on the standard contractual clauses for the transfer of personal data to processors which have been established in third countries under Directive n°95/46/EC adopted by the European Commission on December 27, 2001 (n°2002/16/CE).

However, these standard contractual clauses need to be updated and this update is motivated by global outsourcing. Indeed, several companies transfer their data to processors and to sub-processors, and sometimes also to “sub-sub processors.”

However, decision n°2002/16/CE does not take into account the case of complex onward transfers to “sub-sub processors”.

For this reason, the European Commission recently issued a draft proposal in order to find and provide a legal solution allowing the transfer of 1) personal data to data processors established in third countries and notably 2) sub-sub processing to processors established in third countries.

The opinion of the Working Party stresses that the draft Commission decision does not provide recommendations concerning the international transfer of personal data by a sub-processor established in the European Union. Indeed, the Working Party considers that a legal solution should be provided in order to facilitate the international transfer of personal data.

At this stage, the Working Party set up under Article 29 of Directive n°95/46/EC, adopted a favorable opinion on the proposed draft decision of the European Commission.

■ The 31st International Data Protection Conference

On November 4, 5 and 6 November 2009, the 31st International Data Protection Conference will be organized in Madrid by the Spanish Data Protection Authority.

The main objective of this next International Data Protection Conference is to obtain the approval of a joint proposal regarding “International standards of Data Protection requirements” which will enable the development of a legal, worldwide and mandatory mechanism (see below, the opinion of the President of the CNIL).

France

■ HADOPI Law

The HADOPI bill on the dissemination and protection of works on the Internet in order to enforce compliance with copyright law (“Projet de loi favorisant la diffusion et la protection de la création sur Internet”), has recently been adopted. This text aims to organize a fight against infringement of Intellectual Property Rights on the Internet.

In March 2008, the French Government consulted the French Data Protection Authority (CNIL) regarding the HADOPI bill. The bill implies the Data Processing - by the HADOPI Authority and the Internet Service Providers - of Personal Data on the individuals whom Internet connection is interrupted because of piracy.

On April 29, 2008, the CNIL rendered a critical opinion^[1] on the HADOPI Bill mainly regarding the lack of proportionality between the protection of the right of the copyright holders and the respect of individual. Despite the opinion of the CNIL, the Bill has been adopted.

The constitutionality of the HADOPI law has also been contested by elected members of the French National Assembly.

The Constitutional Council decision n°2009-580 dated June 10, 2009, provides that the HADOPI Authority shall not be entrusted with the possibility to limit or interrupt Internet access in cases of piracy. The Constitutional Council decided that these provisions were not compliant with the French Constitution and such powers may only be applied by a judge.

[1] The CNIL's opinion is not available to the public

■ Major figures on the French Data Protection Authority's (CNIL) activities in 2008

In 2008, the French Data Protection Authority (CNIL):

- ▶ Recorded 4,244 claims related to non compliance with the French Data Protection Law. These claims concern the following fields: commercial (25%), banks (25%), labour (15%), telecom operators (15%), education (10%) and other (10%);
- ▶ Received 2,516 requests for access to the Personal Data Processing of the French police force;
- ▶ Received 71,990 notifications of Personal Data Processing. Since 1978, CNIL registered 1,288,394 Personal Data Processing;
- ▶ Numbered 989 Data Protection Correspondents;
- ▶ Adopted 586 deliberations;
- ▶ Sent 126 formal notices;
- ▶ Carried out 218 investigations;
- ▶ Issued 1 warning;
- ▶ Ordered 9 financial sanctions (e.g., a fine of 30,000€ for lack of notification and information and breach in data retention requirements applied to an entity of the retail sector; a fine of 7,000€ for non-respect of the right of access and partial response to the CNIL applied to an entity in the telecom sector; a fine of 5,000€ for non-respect of the right of access and lack of information applied to an entity in the business sector.

In 2009, the CNIL notably aims to develop its claims service in order to facilitate access to data subjects.

■ The 10 key points of the annual reports issued by the French Data Protection Authority (CNIL)

In 2008, the annual report of the CNIL revealed that:

- ▶ CNIL has increased its investigations and financial sanctions;

- ▶ CNIL has accrued its vigilance on direct marketing. In this context, the report also mentions that search engines have accepted to reduce the retention period of the Personal Data collected;

- ▶ CNIL has received several notifications related to Personal Data Processing concerning biometry and video surveillance ;

- ▶ CNIL has consulted the main online social networks (as Facebook, Twitter...) in order to verify their compliance with Data Protection requirements;

- ▶ CNIL proposed that Data Protection become a constitutional right;

- ▶ CNIL aims to be more implicated in the development of information technologies;

- ▶ CNIL aims to establish a new way of financing in order to guaranty its independence[2];

- ▶ CNIL aims to develop a labelling system;

- ▶ CNIL aims to develop an extranet to Data Protection Correspondents.

■ Intervention of the President of the CNIL (Alex Türk) during the 5th Conference of the Data Protection Correspondent dated June 10, 2009 in Paris

The main points of information provided by the President of the CNIL during this speech are as follows:

- ▶ The CNIL will increase/develop its action of control over the entire French territory;

- ▶ Alex Türk stressed that he is in favor of the implementation of « International Data Protection requirements » but also pointed out the necessity to ensure their opposability (for instance via the adoption of an international convention on this matter);

- ▶ The budget allocated to the CNIL will increase next year;

- ▶ The Report[3] of the French Senate dated May 27, 2009, recommends that the Data Protection Correspondent become mandatory in France for legal entities having more than 50 employees. The President of the CNIL indicates that he is in favor of this recommendation.

[2] However, during the 5th Conference of the Data Protection Correspondent, the President of the CNIL indicated that the French government was not in favour of the implementation of this new financing which included new corporate costs

[3] See the report: <http://www.senat.fr/noticerap/2008/r08-441-notice.html>

Finland

■ Privacy in electronic communications - additional guidance

The Data Protection Ombudsman has issued guidelines on the processing of identification data under the Act on the Protection of Privacy in Electronic Communications ("Asiaa tietosuojasta" 1/2009, Yhteisötilaajan oikeus käsitellä tunnistamistietoja väärinkäytöstapauksissa).

In the guidelines, the Data Protection Ombudsman provides for a more detailed description of the conditions that need to be fulfilled by a company that intends to use the monitoring and processing rights set out in an amendment to the Privacy in Electronic Communications Act that entered into force in June 2009.

According to this amendment, a company is entitled to monitor and process electronic identification data, subject to certain conditions, in order to prevent or investigate unauthorized use of communication networks or in order to prevent or investigate disclosure of business secrets by employees via electronic communication networks.

A decree implementing the above Act and setting forth the surveillance fees was adopted by the Ministry of Justice on 28.05.2009. In connection with the adoption of this decree, the Ministry of Justice made clear that - according to its interpretation of the amendment - the Data Protection Ombudsman was entitled to make inspections within the companies in order to fulfill surveillance tasks under the Privacy in Electronic Communications Act. The scope and existence of this inspection right had been disputed earlier by the Confederation of Finnish Industries (EK).

■ Mystery Shopping must to pay attention to data protection

In a recent statement the Data Protection Ombudsman commented on so-called Mystery Shopping systems, where an external quality controller performed, on behalf of the employer, controls regarding the quality of, for example, sales and customer service and the expertise of the sales personnel.

The Data Protection Ombudsman noted in its statement that, in cases where personal data is processed, the data protection rules and in particular the Act on the Protection of Privacy in Working Life needed to be taken into account.

According to this Act, an employer is only entitled to process personal data that is directly necessary for the employment relationship. In addition, the employer has to comply, amongst other regulations, with its obligation to inform the employee beforehand of the data collection and the period when the external controller will make its visits. Furthermore, the employer needs to take care that the data be stored and secured in accordance with the provisions of the Personal Data Act.

The Data Protection Ombudsman therefore held that it would not be in accordance with the Personal Data Act, in cases where the assessment form was published at the work place in a way that personal data was disclosed and that access to this data was not restricted and controlled.

Germany

■ Burst of data protection scandals in Germany

Recently, data protection has featured highly in the German media. The latest "data protection scandals" concern some of the biggest German companies in key industries such as transportation, finance, automotive, retail and healthcare. The main topics are:

- ▶ screening of the workforce for corruption and automatic filtering, deletion and control of private E-Mails of employees;
- ▶ spying on employees by compliance teams;
- ▶ illegal storage and transfer of medical constitution data of employees;
- ▶ granting all employees unlimited access to patient files.

All of these scandals reflect a national and international phenomenon: the mishandling of personal data. The attention given to data protection breaches by the media has sparked a public interest in data protection issues. Politicians as well as consumers and trade unions are demanding the tightening of data protection laws. Although there are strong arguments that existing data protection laws are sufficient, the German legislator plans to take specific steps to amend the law.

■ Credit reference agencies and scoring

In May 2009, the German Federal Parliament confirmed a legislative initiative to amend the Federal Data Protection Act in respect of credit reference agencies and scoring.

The bill concerns the introduction of requirements regarding the transmission of both positive and negative data to credit reference agencies as well as the calculation and use of (credit) scores for decisions regarding the initiation, realization or termination of a contractual relationship.

Such scores shall display the trust- and creditworthiness of an individual in a particular situation. The score calculation is based on an analysis of the individual's personal data (e.g. credit report information) in combination with relevant statistical data.

The amendment of the Federal Data Protection Act strengthens the position of the individual by granting further information and disclosure rights. For example: The scoring shall not be based solely on address data and the person concerned has to be informed in advance, if this kind of data is being used additionally. If the facts/data transmitted to the credit reference agencies have changed subsequently, the transmitting company is obliged to inform the credit reference agency about this matter. Otherwise a monetary fine may be imposed. The credit reference agency on the other hand has to inform the company about the deletion.

■ Further reform proposals

Further reform proposals to tighten data protection regulations are in the pipeline, however it remains unclear if these efforts may pass legislative procedures before the upcoming election in September.

A key provision in a draft is, for instance, to weaken the so called "list privilege" (it states that companies can access certain personal data consolidated in lists - such as name, address, occupation or type of business, date of birth and a further characteristic - for advertising or market research without the consent of the data subject). Moreover the draft legislation creates a duty to inform for companies if certain personal data, which is classified to be particularly worthy of protection, unlawfully becomes known to third parties and the affected party is threatened with serious harm. Simultaneously the maximum fine in case of offences will be increased to € 300,000.00, and for the first time the confiscation of profits is also provided for.

Italy

■ The Main Areas of Activity in 2008 of the Italian Data Protection Authority

The Italian DPA focused also in the past year on the most at-risk areas for citizens – on improving the efficiency of public administrative agencies and services; enhancing the security of major public and private databases; supervising the processing of data in the telecom, judicial and security sectors.

Italian DPA monitored the activities of media carefully and also tackled issues arising from the use of modern technologies. Finally, Italian DPA started up a wide-ranging exercise of simplification for the benefit of businesses and public administrative agencies.

▶ Simplification

The simplification initiatives were aimed, in particular, at sparing companies and the business sector cumbersome red-tape requirements and costs – without lowering the protection level for citizens and consumers alike.

Notification requirements and security measures were simplified to make them less cumbersome and more effective without exposing customers and suppliers to whatever risks.

To facilitate cross-border data flows to third countries, Italian DPA started authorizing the adoption of binding corporate rules. The latter are a tool to make data protection both more effective and accountable at international level, whilst bringing Italy into line with other major European countries.

Corporate mergers and split-ups were facilitated to expedite the restructuring of Italy's production system.

▶ Protecting Citizens as Consumers

Unrelenting attention was paid to strike the right balance between business needs and protection of users and customers.

A decision was issued to set forth clear-cut, binding rules that apply to profiling activities performed by telephone operators with a view to monitoring customers' consumptions, habits, and even wage brackets – whilst consumers are often unaware of such activities.

Further to the balancing of interests principle, Italian DPA allowed a company running public transportation services to geo-locate their fleet continuously, in compliance with employees' rights and with their consent, as well as to monitor the drivers' driving pattern to better safeguard users. This was the first case in which the Italian DPA addressed the use of new traffic monitoring technologies – an area that is currently the focus of specific initiatives by the European Commission and calls increasingly for the attention of all DPAs.

▶ Unsolicited Calls, Unsolicited Services, and Anti-Spam Measures

Italian DPA continued its efforts to protect citizens against unsolicited calls and services also in the past year. Italian DPA re-affirmed that email addresses may not be used without any limitations merely because they can be found on the Net; indeed, the user's consent is always necessary.

▶ Securing Data in IT Systems

As for the security measures applying to the IT sector, Italian DPA issues a new decision on system administrators – which ranks among the most important ones in the past few years.

System administrators have been basically overlooked so far, whilst they are actually indispensable to ensure the operation of networked systems – indeed, they can access any data in the system at any time and can potentially change, delete or add whatever data.

Italian DPA decision sets forth rules to assess their technical skills, ensure that their accesses are logged, and enable users (in particular, employees) to be appropriately informed on their doings.

Another decision to be mentioned is referred to the rules that should apply to the so-called "recycling" of e-waste, i.e. the re-use of computers and other electronic or electrical equipment to be disposed of, which often contains a considerable amount of personal data. The decision of the Italian DPA is addressed to users and consumers as well as – more importantly – to major entities that decide to re-use old/obsolete equipment for different purposes and/or in other locations when revamping their technological outfits.

► **Media and New Technologies**
Italian DPA had to tackle issues related to media and the use of new technologies on several occasions.

Italian DPA repeatedly witnessed the publication of pictures showing victims of accidents and/or violent crimes that had been taken from Facebook without whatsoever controls and without the persons' consent – indeed, those pictures showed other individuals that had nothing to do with the events. This raises the issue of how dangerous it can be to exploit the new opportunities provided by the Internet naively and/or inattentively – which is all the more serious given that media people are involved.

For this reason Italian DPA banned publication of the pictures and reported the cases to the National Board of Journalists and the National Publishers' Federation, requesting that our recommendations be adequately circulated.

► **Data Protection in the Judicial Sector**

The world of justice was the focus of considerable attention by Italian DPA.

Italian DPA issued a pilot decision with regard to the Court of Rome in order to secure their archives and data processing operations so as to ensure that the minimum conditions would be fulfilled to respect citizens' rights in administering justice.

Another important achievement was the adoption of the new Code of Practice for lawyers and private detectives, which also applies to investigational and party-driven activities that had not been regulated specifically yet.

To be recorded the many cases in which the Italian DPA stepped in to secure the telephone traffic data held and used for judicial purposes.

The Netherlands

■ **Sending people annoying mail (SPAM)**

Sending uncalled-for and undesired information – spam - is regarded as an infringement on the right of privacy. Therefore, spamming is prohibited under Dutch law unless certain conditions are met. While the spamming prohibition currently applies to natural persons only, these rules will apply to legal entities as well as from 1 July 2009.

This prohibition will have several consequences. A first positive consequence of this new legislation will be a decrease in the amount of spam a company receives. However, as the prohibition merely applies to senders located in the Netherlands, the decrease in spam will be limited. A second consequence implies that companies are obliged to acquire the receiver's consent prior to sending the information. They have to be able to prove the acquisition if necessary. Because the consent needs to be explicit it cannot be obtained through general terms and conditions. As an exemption to this rule information can be sent to specially designed addresses such as mailing@....nl. A third consequence entails that companies need to mention the identity of the sender in their communication. Furthermore, it is necessary that every communication offers the possibility to unsubscribe from the mailing list. Another consequence of the spamming prohibition is that businesses can no longer use their existing databases in the same manner as they are used to. They can only send information if it offers the company's own and similar products and if the information is sent in accordance with the purposes for which the receiver has provided the data.

The spamming prohibition does not apply in the event that the receiver lives outside the European Economic Area and the relevant regulations concerning spam in that country are applicable.

■ **Electronic health record – a continuing story**

To improve information facilities in the area of healthcare the Dutch government is going to introduce a national Electronic Health Record (EHR). This national EHR is expected to solve problems concerning inadequate exchange of information and it is expected to reduce medical errors. However, the introduction of the national EHR has been delayed because research has shown that security systems with regard to the records do not meet the legal requirements.

Meanwhile, regional EHRs are set up by private initiatives for the same reason. These regional EHRs cause some difficulties regarding the violation of privacy. The following aspects need to be taken into consideration when using a regional EHR. Firstly, patients need to be informed if their data is recorded in an EHR so they can use their right to oppose to the recording. Secondly, Dutch privacy legislation as well as article 8 ECHR require an active behavior regarding the protection of medical records. Therefore, measures need to be taken to guarantee that only the attending physician can attain access to the record. Merely logging the consultations of an EHR is an insufficient measure. The logs need to be structurally monitored to make sure that no unauthorized doctor has accessed the EHR.

Spain

■ **The personal data leak on the internet - Risk for the companies.**

The Spanish Data Protection fines are now one of biggest threats for companies based in Spain. Many sanctions pronounced by the Spanish Data Protection Agency are related to Peer to Peer ("P2P") Records Exchange Programs. These Networks are used frequently to share files that contain video, audio, text, software and, in general, any type of personal data in digital format.

From the beginning of 2007, the number of sanctions pronounced by the Spanish Data Protection Agency (hereinafter "AEPD") in connection with the diffusion on the Internet of personal data via the utilization of records exchange programs, has dramatically increased.

In 2007 the AEPD opened 21 proceedings for disclosure of personal data on the Internet including files containing personal information on members of a religious community ; on members of Trade Unions; on clients' databases; on medical records or employees' files. Moreover, in 2008, 3 Public Administrations and 14 private controllers were fined on similar grounds.

The following sanctions are good illustrations of AEPD priorities:

► A data controller who had not taken adequate security measures to prevent unauthorized access by third parties was also fined. Sanctions taken by the AEPD in connection with the extraction of a file containing more than 40 000 records by an employee for sharing purpose on eMule, were reduced from 60,000 euros to 12,000 euros because the company has a security policy available on the intranet and has properly defined internal data protection policy.

Although the company management prohibits filesharing of any personal data, the file in question found its way to the Internet via a computer company which was repairing the ASG computer.

► A sanction of 6 000 euros was imposed by the AEPD on the sport Club "CLUB DEPORTIVO S.C.S.A.A", because of the publication of the records of 220 employees on the Internet.

► Frequently, heavier sanctions have been imposed by the AEPD. A fine of 150,000 € was imposed on a medical center, for failure to protect medical secrecy" and allowing the medical records of 11,300 patients including under going undergoing voluntary termination of pregnancy to be spread on the Internet.

Although the infractions made by employees may be voluntary or involuntary in nature, they are symptomatic of a general need for companies to improve security measures. It is for these reasons that the head of AEPD has made a general appeal so that every "Every company, hospitals, banks, nursery schools, schools...check their systems. We must stimulate an active training policy, information and awareness. The information society has certain risks that must be controlled and with these cases the limitations of many citizens show up even when they correctly use technological tools." The Lack of control that has been highlighted the AEPD in its Report of year 2008, indicating "the necessity of becoming aware urgently of that security means avoiding the spread of internet files of information contained on the working tools of the employees.

Switzerland

■ Swiss Safe Harbor

The Swiss Safe Harbor framework between the United States of America (US) and Switzerland entered into force on 16 February 2009. This framework agreement enables US domiciled companies to register with the US Department of Commerce and to give a voluntary commitment to respect data protection compliant with Swiss legislation. As a result Swiss companies can transfer data more easily to registered companies in the U.S. while at the same time an improved data protection is achieved.

A recent analysis of the about 1,800 companies registered under both Safe Harbor frameworks (EU and Switzerland) showed that only 44 are classed as global players. It turns out that the Safe Harbor framework is of particular interest to small and medium-sized enterprises which maintain business relations with U.S. companies.

See issue 1 of this IP/IT Update and Legal News May 2009 under section Publications at www.ey.com/ch/legal

■ Data privacy at health insurance companies

Recently, the Swiss Federal Data Protection and Information Officer (FDPIC) released its 16th annual report. Part of this report is the result of the data privacy survey of the health insurance companies. This survey among other things showed that 59% of the health insurance companies, which cover 90% of the population of Switzerland, have a data privacy concept governing the data privacy strategy and organization.

Such data privacy concept is not mandatory according to Swiss law. Contrary to that, only 26% of the health insurance companies, which cover 62% of the population of Switzerland, have regulations governing the processing of personal data, which are mandatory according to Swiss law. In sum the FDPIC states that most health insurance companies are aware of data privacy matters and willing to address such matters.

For more information find the 16th annual report at www.edoeb.admin.ch

IP/ICT Legal practice group

The IP/ICT Legal practice group covers both national and international IP and ICT practice in its broadest sense. 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, transactions and advisory services. Worldwide, our 130.000 people are united by our shared values and unwavering commitment to quality. We make a difference by helping our people, our clients and our wider communities achieve potential.

For more information please visit:

www.ey.com.

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.

www.ey.com

© 2009 Ernst & Young

Disclaimer

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.