

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 damage the organisation's reputation, brand or business relationships. These may result in legal liabilities or regulatory sanctions, lawsuits for deceptive business practices and loss of customers' and employee's confidence. Apart from the potential for legal sanctions, negative publicity remains the key driver for organization to ensure data protection law compliance.

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

France

■ Data processings related to struggle against money laundering and data protection requirements

Under the new French legislation implementing the European directive 2005/60/CE relating to anti-money laundering, financial institutions must collect more detailed information about all customers, even occasional customers.

In accordance with the money laundering legislation, Banks now collect information on employment, economic and financial status (proof of address, current professional activity, income and other resources...). Occasionally, the customers are requested to provide the bank with the amount, nature or economic justification for a specific operation, on the source or destination of funds or property.

The CNIL (French Data Protection Authority) has received several claims from customers of different banks who have been requested to provide a copy of their ID and/or were addressed a detailed questionnaire on their family or financial situation.

Even if the collection of certain data is necessary to ensure the compliance with legal provisions, the CNIL stresses that the French Data Protection requirements still apply.

The purpose of the data collection must be strictly respected. For instance, the data collected to fight against money laundering should not be used for marketing purposes, without informing the people concerned and giving them the opportunity to exercise their right of opposition. Forms or questionnaires addressed to customers must specify the purpose and recipients of data and the means to exercise their rights (right of access and correction).

The CNIL will pay specific attention to the compliance of banks with these rules and is currently working on the update of the single authorization AU-003 on data processing implemented by financial institutions in the fight against money laundering and terrorist financing.

■ Public warning against ACADOMIA

On April 22, 2010, the CNIL decided to issue a public warning against the company AIS 2 (ACADOMIA).

ACADOMIA, specialized in academic support, has been inspected by the CNIL in November 2009. Among other breaches of the French Data Protection Law, it appeared that the company's files contained thousands of excessive and abusive comments concerning teachers, parents or students (for instance "big jerk", "bastard child", "Lung cancer as deserved").

The investigation also revealed detailed information on the health of students, parents and teachers,

such as "admitted in ER for a cancerous brain tumor", "anorexic and bulimic". The CNIL considered that such data collection was not possible without the prior consent of the people concerned even if the data collection may be justified by organizational purposes.

In addition, it appeared that ACADOMIA collected data concerning potential crimes and offences (for instance "student returned to jail", "stole bags and money with a friend", "the father had been in prison"). The CNIL considered that the company must not processed unverified data which could lead to the creation of a prohibited file of offenses.

In consideration of the number and seriousness of the Data Privacy breaches, the CNIL has issued a public warning against ACADOMIA and has referred the case to the public prosecutor.

■ Labellisation

The CNIL will exercise its labellisation prerogatives next Y 2011 focusing at first on labellisation of data protection law assessment/audit and training programs. A limited list of major stakeholders (including Ernst & Young, société d'avocats) have been selected by the CNIL to participate in a hearing on best practices in labellisation (scheduled on June 22 & 23, 2010)

■ Car tracking tools

On April 8, 2010, the CNIL adopted a recommendation concerning the implementation of car tracking tools by insurance companies and car manufacturers.

Germany

■ Pay As You Drive devices

The “Pay As You Drive” devices tracking are proposed by insurers in order to adapt the insurance premiums to the specific criteria such as the lengths of driving period.

The CNIL recommendation specifies that these tools must not lead to the creation of prohibited files of offenses. In addition, as the people concerned may not inactivate the tools, the insurers must obtain their prior consent and provide them with a clear notice.

Moreover, the CNIL recommends that the tracking data will be stored in the cars in order to limit the data transfers. Otherwise, the data shall be stored by the external provider who will periodically send the data to the insurer. The data retention period must be limited to the time necessary to calculate the premium and data transfers between the provider and insurer must be limited.

■ Emergency tools

These tools will enable, for instance, to contact and provide the nearest emergency center with the localization of the car involved in an accident.

The CNIL points out that:

- i) The data must only be used to bring emergency aid;
- ii) The localization data must be deleted after use;
- iii) The data subject must be provided with a prior and clear notice;
- iv) The access to such data has to be limited.

■ Amended Requirements for Agreements with Data Processors

On 1 September 2009, the amended German Federal Data Protection Act has become effective. The amended regulations include extended and specified legal requirements for data processing agreements. According to the new regulation, data processing agreements need to provide for provisions on subcontracting, breach notifications, audit rights and a couple of other aspects.

Which agreements are affected from the new regulation?

Any collection, processing, or use of personal data on behalf of others must comply with the new regulations, even if the relationship was already in place prior to 1 September 2009. A controller-processor relationship exists when a third party is collecting, processing or using personal data on behalf of another party. Personal data in this context means any information concerning the personal or material circumstances of a natural person.

The Federal Data Protection Act does not provide for a group privilege. As a consequence, the new regulations also need to be applied to intra-group agreements, e.g. where data processing functions are centralized within a group.

What are the detail requirements?

Each controller - processor agreement needs to be concluded in written form. The following catalogue contains the minimum requirements to be set forth in a controller-processor agreement:

- the subject and duration of the work to be carried out;
- the extent, type and purpose of the intended collection, processing or use of data, the type of data and category of data subjects;
- the technical and organizational measures to be taken under Section 9 of the Federal Data Protection Act;
- the rectification, erasure and blocking of data;
- the processors’ obligations;
- any right to issue subcontracts;
- the controller’s rights to monitor and the processor’s corresponding obligations to accept and cooperate;
- violations by the processor or its employees of provisions to protect personal data or of the terms specified by the controller which are subjects to the obligation to notify;
- the extent of the controller’s authority to issue instructions to the processor; and
- the return of data storage media and the erasure of data recorded by the processor after the work has been carried out.

–

The Netherlands

The controller is fully responsible for the compliance with these mandatory contractual provisions and other statutory data protection provisions by the processor. Moreover the controller must diligently select and regularly audit its processors. The results of such audits have to be recorded.

What are the consequences of non-compliance?

Data protection authorities can impose fines of up to € 50.000 in each case on companies having insufficient controller-processor agreements.

To ensure compliance with German Data Protection Law existing controller - processor relationships should be identified, existing documentation reviewed and compliance with new regulations should be procured by amending these agreements, if necessary.

■ Call on Privacy by Design

International data protection authorities from ten different countries, in a unique collaborative effort, call on online companies such as Google to provide - from now on - all products and services with guarantees to properly protect and secure personal data, as early as in the design phase. In a joint letter, they demand a number of specific measures such as providing clearly visible and easy to use privacy settings.

"International data protection authorities make a firm stand for the protection of personal data, also as regards innovative products and services", according to the chairman of the Dutch Data Protection Authority (DDPA) and the Article 29 Working Party (WP 29). "Companies have to deploy their 'experts' to develop services and products in such a way that do not violate, or to a much lesser extent, the privacy of individuals," said Kohnstamm, again emphasising the importance of 'privacy by design'.

■ Financial and Pharma Codes of Conduct

The DDPA has on 13 April 2010 formally declared the Code of conduct for the processing of personal data by financial institutions (Gedragscode Verwerking Persoonsgegevens Financiële Instellingen) to be in line with the DDPA.

The code was jointly drafted by the Dutch Association of Banks (Nederlandse vereniging van banken) and the Association of Insurers (verbond van verzekeraars).

<http://www.verzekeraars.nl/UserFiles/File/download/code-for-conduct.pdf>

On 6 May 2010 the DDPA approved a code of conduct for processing of personal data from the Dutch Association of research orientated pharmaceutical Industries (Nefarma). <http://www.nefarma.nl/cms/publish/content/showpage.asp?pageid=1655>

The DDPA declarations are valid for a period of five years.

■ Care for outsourcing in health care

In a letter to the Dutch Ministry of Public Health, Well-being and Sport the DDPA expresses its concerns with regard to the risks of outsourcing of data processing in health care. Specifically when this entails the outsourcing of sensitive data, such as patient data.

Many hospitals and care institutions keep their database of patient data on the server of an external service provider and disclose the patient data remotely via the Internet. The outsourcing of processing of patient data without the patients' permission is sought, has expanded considerably. The practice is not standardized to the extent to which outsourcing and

attention to the protection of personal data needs to be set so that to the view of DDPA further regulation or self-legislation is necessary. For security of patient confidentiality high standards should be applied to the outsourced data. Strong safeguards must be provided for a safe and discrete handling of the data concerned. Not only technical, but also organizational and through enforceable legal agreements.

Russia

■ Regulation on Methods and Means of Protection of Information in Personal Data Information Systems

On 5 February 2010 the Russian Federal Service for Technical and Export Control (FSTEC) approved the Regulation on Methods and Means of Protection of Information in Personal Data Information Systems (the "Regulation"). The Regulation marks a new stage in the development of the Russian legislation related to security of personal data in personal data information systems. The Regulation is based on (1) Article 19 of the Russian Personal Data Law (No. 152-FZ of 27 July 2006) stating that an operator must ensure organizational and technical measures to protect personal data against unauthorized or accidental use; and (2) Government Resolution No. 781 of 17 November 2007 clarifying that the specific methods and means of protection are to be established by Russian Federal Service for Technical and Export Control.

The Regulation entered into effect on 16 March 2010. It applies to all personal data operators (state and municipal bodies, legal entities and individuals), as well as to persons that are processing personal data on the basis of an agreement with the operator.

The choice of specific methods and means of protection of information in personal data information systems depends on the class of information system, which is determined according to the joint Order of FSTEC, Russian Federal Security Service and Russian ministry for Information Technology and Communication No. 55/86/20 of 13 February 2008. Classes range from class 1 (requiring maximum protection) to class 4 (requiring minimum protection), depending on the type(s) of personal data processed and the number of subjects whose personal data is included in the system.

Methods and means of protection of information are divided into two major groups:

Group 1: Methods and means of protection against unauthorized access, including:

- limitation of access to premises with relevant technical devices;
- diversified access to information by users and servicing staff;
- recording of the users' and serving staff's actions;

- accountability of portable data media;
- creation of back-up copies;
- use of information means that have duly passed the conformity evaluation procedure;
- use of secured communication channels; etc.

The list of methods and means is substantially more detailed in cases where the personal data information system interacts with a public network.

Group 2: Methods and means of Protection against leakage through technical channels. Such methods and means should be implemented in cases where there is a threat of information leakage through side electromagnetic radiation channels.

Spain

■ Complaints for violating the Data Protection Regulation in Spain

In 2009, the Spanish Data Protection Agency (AEPD) carried out 709 penalty proceedings (total fine of 24.8 million euros (an increase of 13% compared to 2008)).

In Spain, the claims sent to the AEPD for Data Protection Regulation breaches grew more than 75 percent in 2009 (mostly linked to the Internet, video surveillance and misuse of personal data). The study drafted by the AEPD in 2009 provides that the most highly investigated sectors were the financial and telecommunications sectors. This study also reflects that last year there were 2,000 requests of the data subjects concerning the protection of their rights (i.e., right of access, rectification, deletion or opposition (58% more than in 2008)). Mr. Rallo (AEPD Director) said that this "most remarkable" increase demonstrates that the people are "in a higher degree of awareness" about the need to protect their rights.

AEPD has also highlighted the existence of 31 claims concerning Twitter or Facebook users, especially for disseminating pictures without consent (in 2008 there were no claims).

Act,

In 2010, the AEPD imposes inter-alia the following fines:

- fine of 100,000€ imposed on Vodafone Spain for showing customer data. A "serious" penalty" for displaying customer data. The data included the subscribers' name, ID number, passport number, sex, date of birth, nationality, mobile and fixed phone number, mail and email address.

- fine of 420.000€ imposed on Telefónica for a serious infringement of Article 11.1 of the Spanish Data Protection (breach of the said regulation concerning the provision or transfer of a personal data).

- a fine of 60,101.21€ imposed on a Mobile phone company, Orange (France Telecom) for illegally registering an user in Spain as being in default. In addition, it seems that Orange reported data on the user to the file without even making the mandatory prepayment requirement for inclusion in a record of solvency.

■ Whistleblowing

As of today many companies are implementing processes in order to ensure that their internal politics and code of ethics will be effective and dully fulfilled by all of their members. This means that the application of those systems is not limited only to their employees, it also could affect their suppliers and clients.

The most common system used is the implementation of whistleblowing policies which consists on adopting a mechanism by which every member of the company would be able to report the incidents or misconducts regarding the content of said internal rules and/or code of ethics.

However, applying a whistleblowing policy in Spain raises Data Protection concerns because there are no specific rules regarding that issue.

In order to avoid the above-mentioned issues, the AEPD provided several recommendations which should be applied by each company which would like to implement a whistleblowing policy in compliance with the applicable legislation.

According to those recommendations, the company would have to inform its members about the existence and the purpose of the system, how it works and the consequences in case of false complaints.

Finland

The company can inform its members through massive informative reports or insert the information in an annex or a clause within the agreement concluded by the company with the members.

Additionally, the company would also have to include a standard Data Protection clause in order to ensure that personal data collected through those mechanisms would be processed in compliance with the Spanish Data Protection Legislation.

Finally, the whistleblowing systems may raise another issue in practice: anonymous complaints are not allowed in Spain.

The AEPD suggests that the company should explicitly inform its members that the information provided and the identity of the informer would be processed in a confidential and anonymous manner, but only until legal proceedings take place as a consequence of the internal investigations that have been previously conducted.

■ The commission initiates infringement proceedings against Finland regarding protection of personal tax data

On 3 June 2010 the European Commission has issued a warning to Finland that Finnish legislation on personal data may not fulfill the requirements of EU Law, because it does not protect personal tax information published in the media. The warning was given in the form of a so-called letter of formal notice, which is the first stage in the infringement process. (Source: Press Release of the Commission IP/10/673).

In Finland data of individual taxpayers are public information and publicly accessible in order to ensure transparency as regards incomes. Media publish this information amongst others the income of the taxpayers as well as the taxes paid. Businesses collect this information and sell it in the form of special publications, CD and text messages.

The Commission warned Finland that the Finnish legislation on personal data does not fulfill the requirements of the 1995 Data Protection Directive ([Directive 95/46/EC](#)) - because it does not protect personal tax data published in the media.

According to Chapter 1 Section 2 of the Finnish Personal Data Act (1999/523) implementing the EU Data Protection Directive the Personal Data Act does not apply to personal data files containing, solely and in unaltered form, data that have been published by the media.

In the Commission's view the EU Data Protection Directive allows national laws to have some exemptions, eg for security reasons (Article 9 of the Directive) or for journalistic purposes (Article 13 of the Directive). The Commission noted, however, that the European Court of Justice (C-73/07) as well as the Finnish Supreme Administrative Court (KHO:2009:82) have found that the exemption provided for in the Finnish Personal Data Act does not conform with the exemptions allowed under EU rules. On 16 December 2008 the European Court of Justice ruled that the collection and sale of personal tax data did not constitute a journalistic purpose and was therefore not covered by the derogation in Article 9 of the EU Data Protection Directive.

According to the Commission Finland has not yet informed the Commission, how it will amend this legislation to comply with the EU Data Protection Directive.

The Finnish Government proposed on 3 June 2010, that in the future the publicly available data will not contain data regarding the person's home municipality, but the information regarding the province, where the respective taxpayer is resident, would be public information along with information regarding the name, the year of birth, the earned income and income from capital and taxes paid.

■ Processing of identification data - data protection ombudsman issues new guidelines

The Office of the Data Protection Ombudsman has issued additional guidelines on the processing of identification data under the Act on the Protection of Privacy in Electronic Communications. (*Asia tietosuojasta: Tunnistamistietojen käsittely väärinkäytöstapauksissa - ohje toiminnan suunnittelemiseksi*).

Under Finnish law an employer may not process identification data, i.e. data arising from its employees' e-mail correspondence or web-surfing, in order to prevent or investigate unauthorized use of communications networks or disclosure of business secrets by employees, unless the employer has fulfilled certain specific legal requirements and made a notification to the Data Protection Ombudsman. The legal requirements for processing data for the purpose of preventing misuse have been specified in an amendment to the Act on Electronic Communications that has entered into force in June 2009.

When the amendment entered into force it was expected that companies would start to take the measures that were required for processing identification data in misuse cases, but so far not a single notification has been made to the Data Protection Ombudsman.

In its new guidelines the Office of the Data Protection Ombudsman describes the measures a company needs to implement prior to starting the processing of identification data for the purpose of preventing or investigating misuse cases. The first part of the guidelines shall provide a support for planning and organizing the processing of identification data in misuse cases. It describes the measures to be taken in order to guarantee a sufficient level of data security, instructions to be provided to employees, corporate governance and policies to be introduced, and notification and information requirements to be complied with.

The second part of the guidelines is addressed to the persons that are in charge of processing identification data and it provides clarifications in respect of the assessments of the measures that need to be taken when irregularities have been discovered in the course of a permitted processing.

The guidelines provide also a question and answer section regarding the relation and limits between the processing of identification data in misuse cases and the processing of identification data for the implementation of data security.

Clarifications regarding the relationship between these two grounds of processing are considered of specific importance as the means and measures used for the processing are similar, and may only be differentiated as regards the purpose pursued. However, processing for the purpose of implementing data security is permitted, whereas processing for the purpose of preventing or investigating misuse is subject to stringent legal requirements.

As some permitted and prohibited processing measures may be similar also companies that do not intend to start processing of identification data in order to prevent or investigate misuse cases need to clarify the internal rules and guidelines that specify whether and under what circumstances processing of identification data is permitted. The above restrictions would also need to be taken into account in case of an outsourcing of certain functions.

RECENT ERNST & YOUNG LAW NETWORK

DATA PROTECTION LAW PROTECTION EVENTS (Illustrations)

FRANCE

- Ernst & Young, société d'avocats member of the AMCHAM data protection taskforce dealing with the governmental consultation on « droit à l'oubli » (May 2010)
- IAPP (International Association of Privacy Professionals) local Paris KnowledgeNet Chair meeting organized by Ernst & Young, société d'avocats & Microsoft EMEA on data protection labellisation /privacy by design (June 3, 2010)
- Hearing of Ernst & Young, société d'avocats by the French Data Protection Regulator, the CNIL, on Labellisation (June 22, 2010)
- Ernst & Young, société d'avocats organizes a conference on the policy of sanction and CNIL's control (June 23, 2010)
- Hearing of Ernst & Young, société d'avocats by the European Commission on the revision of the current legal framework on personal data protection (European Commission targeted private stakeholders' consultation) (July 1st, 2010)

- Ernst & Young, société d'avocats members of the working groups from the AFCDP (association of data protection officers) dealing with « privacy by design », « data protection law and links with the Representative institutions of the staff », and notification of data security breaches (on going)

The NETHERLANDS

Holland Van Gijzen Attorneys at Law in cooperation with EY ITRA is going to take part in a working group installed by the Dutch Association for accreditation of health care organizations.

In the working group will take part specialists in the field of ICT/Data Protection regarding information security from health care institutions, IT Industry, health and privacy authorities and so on.

Goal is to draft workable standards for information security in the health care sector in compliance with EU and Dutch data protection legislation.

SPAIN

- Ernst & Young has hosted a workshop for International Clients based in Spain for discussing with the Spanish Data Protection Agency about the main problems they face when adapting their organization to Spanish Privacy legislation (May, 2010).

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:

Belgium/The Netherlands

E Peter.kits@hollandlaw.nl

T +31 88 407 00 18

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

E peter.katko@de.ey.com

T +49 89 14331 25951

Italy

E Luigi.neirotti@it.ey.com

T +39 02 85 14 828

Poland

E Marek.Gizicki@pl.ey.com

T+ 48 225 57 73 21

Portugal

E Garcia.Pereira@pt.ey.com

T+351 226 002 015

Russia

E Alexey.Markov@ru.ey.com

T+7 (495) 641 2965

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

© 2010 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.