

**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 organizations. Nowadays, legal compliance with European data privacy rules has become an essential business practice for European and non-European organizations 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 damage to the organization's reputation, brand or business relationships as well as a legal liability or regulatory sanctions, lawsuits for deceptive business practices and loss of customers' and employees' confidence. Apart from the sanctioning regime, negative publicity is a key driver for organizations' efforts to ensure data protection compliance.

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

## EU

In a press release (18 October 2010), the European Data Protection Authorities, assembled in the Article 29 Working Party, announced that they are awaiting publication of the review of the Data Protection Regulatory Framework. In the next few months, the Article 29 WP will issue several opinions including on applicable law and on consent.

The Article 29 WP and the WP on Police and Justice have expressed their strong views regarding the data protection standards in the Terrorist Finance Tracking Program (TFTP) II Agreement ('SWIFT agreement') in a joint letter to the European Parliament.

## Germany

### Government approves draft law regarding employee data protection

The German government has recently approved a draft law concerning special rules for employee data protection. This draft law would amend the German Federal Data Protection Act (BDSG) by adding provisions that specifically address data protection in the employment context.

The draft law covers the following key subject areas:

#### **Employer Internet searches:**

Employers may use public information found through web searches, but may only use information from social networks if the networking platform is intended to present professional qualifications.

#### **Medical examinations:**

Medical tests are permitted provided that they are necessary to assess the employees' ability to perform the essential functions for their position.

#### **Automated data scanning:**

Allowed in anonymized or pseudonymized form to detect criminal activity or other serious violations. If unauthorized activity is suspected, data may be associated with specific individuals. Employers must document the circumstances of the screening, and inform the relevant employee after the screening.

#### **Video surveillance:**

Covert monitoring is prohibited. Video surveillance may be used only if employees receive proper notice, and only in particular areas or for certain reasons (e.g., quality control, security of facilities or entrance). The monitoring of locker rooms or similar locations is prohibited.

#### **Tracking of employees:**

Collection of employee data via tracking systems (e.g., GPS) is only allowed during working hours, and only if the positioning helps to ensure employee safety or is used to coordinate the work force (e.g., logistics company). Covert tracking of employees is prohibited.

#### **Biometric data:**

Such data may be collected, processed or used for authorization and authentication purposes only, provided there are no prevailing employee interests. Photographs of employees may be used for other purposes subject to the employee's consent.

#### **Telephone, Internet and email monitoring:**

The draft law only allows traffic and content data from business email and Internet use to be collected, processed, and used, where necessary to (1) ensure the orderly functioning of the telecommunications network and services, (2) promote data security, (3) facilitate billing, and (4) occasionally monitor performance and behaviour, but only if there is no overriding employee privacy interest. Telephone calls may be monitored only where there is a legitimate employer interest, and if the employee and the other party to the communication have been informed about, and have consented to the monitoring.

#### **Notification in case of security breach:**

Employers must notify affected employees if it is determined that employee data has been unlawfully disclosed to a third party. In the event of a serious threat to the rights or protected interests of an employee, the employer must also notify the competent data protection authority.

It remains unclear, though, to what extent the draft law will be changed and amended in discussions before the German Parliament or if it will pass without any corrections. The first reading is expected in November 2010, leaving open the possibility that the law may be passed this year.

## France

### National security

The bill entitled '*Projet de loi d'orientation et de programmation pour la performance de la sécurité intérieure*' (referred to as the 'Bill') is currently under discussion in the French Parliament.

The purpose of the Bill is to increase the level of national security in France by extending, for instance, the possibility of public authorities to collect and process personal data in case of police investigations. The main provisions of the Bill are the following:

- ▶ the criminalization of online identity theft;
- ▶ the possibility for public authorities to intercept computer data in case of organized crimes;
- ▶ the installation of body scanners in airports for a three year period;
- ▶ the expansion of the use of video surveillance in public areas.

As many provisions of the Bill have an impact on data protection, the French Ministry of the Interior has requested the CNIL to review 7 articles of the Bill related to, for instance, the interception of computer data, the identification of people by their DNA, judicial records, sexual offence data processing (FIJAIS) and the consultation of police data for administrative enquiry purposes.

In its decision (decision No. 2009-200 of 16 April 2009), the CNIL expressed its concerns about the above-mentioned Articles of the Bill (e.g., regarding the conditions under which the interception of computer data may be implemented, the data which may be processed in judicial records, the conditions for

updating and deletion of data in judicial records).

Certain recommendations have been implemented in the new version of the Bill:

#### **The judicial records:**

Indeed, following the CNIL's decision, the Bill has been modified regarding issues such as the conditions of the update and deletion of data in judicial records.

#### **Interception of computer data:**

Indeed, in compliance with the CNIL's decision, the interception will be carried out only if this interception is necessary to establish the truth. Moreover, these investigations require the prior motivated decision of the competent French court.

In an additional document, the CNIL also provides certain recommendations concerning video surveillance.

The Bill allows public authorities (subject to prior notification of the mayor) to delegate the video surveillance system management to public or private operators.

The CNIL argued that such a delegation to private operators may undermine the reliability and security of the system used.

In addition, Article 18 of the Bill provides the possibility to use body scanners for a three-year period in order to carry out body searches in airport areas.

Although the Bill provides several safeguards in consideration of the use of body scanners (e.g., there will be no data storage), the CNIL recommends security improvements to the legal framework.

Accordingly, the CNIL recommends the passing of a decree to define the conditions under which the body scanner data may be accessed by authorized persons, the security means to be implemented, etc.

The debate has been postponed to the beginning of November.

#### **Personal consumer data**

At the end of 2008, the French National Consumer Council (*Conseil National de la Consommation* - hereinafter referred to as the 'CNC') received a request from the French Secretary of State in charge of consumption to work on the topic of consumer data protection. The CNC set up a task force for this topic that has since also collaborated with the CNIL.

The objectives of this task force include:

- ▶ to set up a legal, economic and practical assessment regarding the collection of consumer data;
- ▶ to identify/study means in order to improve the protection of consumer data.

This task force, consisting of consumers and professionals, presented a report about the consumer data protection topic containing many principles and recommendations including the following aims:

- ▶ to raise awareness and to educate consumers about the risks involved in disclosing their personal data and about their rights provided by the French Data Protection Law (right of access, right to object, right to correct, etc.);
- ▶ to set up training courses for entities and their employees concerning the legally applicable rules (obligation to inform consumers, ensure data security, limited storage of data, etc.);
- ▶ to implement certification systems or labels enabling people to identify those entities that are committed to ensuring transparency and to guaranteeing the rights of consumers in consideration of the use of their data;
- ▶ to ensure the creation of a website for entities in the near future, providing an unambiguous electronic procedure for consumers enabling them to exercise their rights;
- ▶ to encourage the appointment by the entities of data protection officers;
- ▶ to provide additional means to the CNIL in consideration of the increase of its tasks and at a level commensurate with that of other European data protection authorities;
- ▶ to support the fight against spam by developing spam notification platforms. The report furthermore recommends that the scope of the consent given by consumers be clearly defined (e.g., which entities or categories of entities will be authorized to use their data).

In the first half of 2012, the CNC (in collaboration with the CNIL) will carry out an assessment of the implementation of its advice.

### **International data transfers**

Since several years, the CNIL (French Data Protection Authority) has published a guide on its websites relating to international data transfers including principles and practical advice to companies about Binding Corporate Rules (BCR), Standard Contractual Clauses, Safe Harbour and exceptions to the prohibition of international data transfers.

In consideration of the increase of international data transfers (due to, for instance, business globalization and the rising use of IT), the CNIL decided to develop a new 'framework' entirely dedicated to international data transfers and provided with specific sections regarding:

- ▶ BCR;
- ▶ Safe Harbour;
- ▶ Standard Contractual Clauses;
- ▶ Exceptions to prohibition.

The purpose of the CNIL is to help companies to comply with the requirements regarding international data transfers.

For instance, in the BCR section, the CNIL provides reference to the Article 29 WP documentation (including, for instance, the Working Document to set up a framework for the structure of BCR), the application form of the BCR and information concerning the mutual recognition procedure.

## The Netherlands

### **Regulatory burden relief**

A legislative proposal has been submitted in close consultation with the Dutch Data Protection Authority (DPA); the Confederation of Netherlands Industry and Employers VNO-NCW; and the Administrative Burden Advisory Board, Actal, that should help to reduce the administrative burden of complying with the Personal Data Protection Act. The recommendations contained within the proposal include relaxation of the rules on direct marketing and data transfer to third countries. In addition, the proposal includes a relief of the rules on submitting black lists to the Dutch DPA. The amendment is expected to enter into force on 1 July 2011.

## Russia

### **Data privacy regulation in Russia**

#### ***Developments of privacy legislation<sup>1</sup> adopted since June 2010***

Since June 2010, Russia has not adopted any significant regulations concerning privacy protection specifically.

The only new Law regarding general information protection is a Federal Law 'on combating unauthorized use of insider information...' (No. 224-FZ), which was adopted on 27 July 2010. This new Law introduces the term 'insider information' to the legislation and establishes a legal regime for its use, defining 'insider

information' as secret (non-disclosed) information the dissemination of which may significantly affect prices on securities or commodities markets as well as currency rates.

The Law furthermore imposes requirements towards fuller disclosure of information affecting prices of financial instruments and goods, and aims to create an effective mechanism that would allow revealing and preventing violations committed with the use of insider information.

Where the dissemination of personal data could lead to consequences as mentioned above, the new Law can be considered part of the Russian privacy legislation.

The Law imposes criminal liability for illegal use of insider information. For violation of the Law, penalties may be imposed to the amount of up to 25,000 euros, or imprisonment (up to 7 years), or professional disqualification (up to 3 years).

The Law also prescribes that all companies possessing insider information should notify state authorities (Federal Service for Financial Markets) of their business transactions performed with the use of such insider information, and that they should implement a set of internal compliance measures (e.g., to appoint a person responsible for transactions performed with the use of insider information, to adopt internal rules on such performance, etc.).

The Law will come into effect starting from 27 January 2011.

### **Current level of privacy regulation in Russia**

Currently, Russian privacy legislation and relevant court practice are under development. Privacy is regulated in Russia by the Federal Law 'on personal data' (No. 152-FZ), which was adopted on 27 July 2006.

The main principles of this Law are as follows:

- ▶ The use or processing of any personal data is allowed in Russia only upon prior written consent of the individual concerned (with a short list of exceptions).
- ▶ Any cross-border transfer of personal data is allowed only if and in so far as the recipient jurisdiction is able to ensure a proper level of personal data protection.
- ▶ Any company engaged in personal data processing should ensure a proper level of protection of its computer system to prevent possible personal data disclosure or malfunctions leading to such disclosures (it is necessary for companies to pass special tests to ensure a proper level of protection of their computer system and to obtain a certificate warranting this level of protection).
- ▶ The Law prescribes that all computer systems created before 2010 should be brought into compliance with the technical requirements to ensure a proper level of personal data protection before 2011.

<sup>1</sup> Privacy legislation is understood to mean the area of law pertaining to the protection of privacy rights (private information) of individuals (not companies).

## **Spain**

### **2009 Memorandum: Internet, CCTV and debtor data are the new players in the spotlight.**

Last year, the Spanish Data Protection Agency (SDPA) published the Annual Memorandum for the year 2009. Encouraging results were achieved once again, reinforcing the reputation of Spain as one of the leading countries where personal data protection is concerned. For the SDPA, 2009 was a great year, especially in the sectors of Internet, CCTV (closed circuit television) and debtor data.

The memorandum reports high numbers and continued rapid growth relative to previous years, with complaints concerning violation of personal data growing by 75% and the protection of rights (to access, cancel, oppose or amend) reaching a 58% growth compared to 2008. These days, there is no doubt that personal data protection issues are in vogue, as evidenced particularly by the active participation of Spanish citizens, who made 97,200 calls to customer service centres. Telecommunication still leads the rankings in terms of the largest number of claims and penalties received, but Internet, CCTV and debtor data are the new major players, presenting surprising results.

These upcoming sectors are here to stay and will take over the leading roles.

Internet took a primary participation with 156 investigations initiated regarding the unauthorized disclosure of personal data at sites like Facebook, Tuenti (e.g., unauthorized photos) and YouTube (e.g., videos not allowed).

However, the biggest area of concern, producing one of the most prominent growth rates (200%), is the so-called 'right of oblivion on the Internet', which refers to the right to obliterate data on the network, especially in search engines such as Google or Yahoo.

CCTV is about to become one of the most 'monitored' sectors of all, as penalties imposed more than quadrupled from 27 in 2008 to 117 in 2009, mostly for lack of public information on camera recording on public roads. This places the CCTV sector second on the list of 'most penalties received', preceding the telecommunications market.

The last big performer is the improper treatment of debtor data (e.g., by violating the duty of confidentiality trying to collect the debt), which shows an exorbitant growth of 225% in reports and complaints and a mind-boggling 570% increase in the protection of rights.

The numbers speak for themselves. These impressive results can be attributed to the effectiveness of the hard work and dedication of the agency and the adoption of Spain's Personal Data Protection Law, which is a big and satisfying reward for the SDPA and the people of Spain.

Now, Switzerland and the US agreed to conclude a separate "US - Swiss Safe Harbour Framework" that also Swiss companies may profit from the benefits of the Safe Harbour framework.

## Switzerland

### **Federal Supreme Court decision regarding covertly probing of IP addresses and their qualification as personal data**

On behalf of copyright owners, a Swiss company gathered IP addresses of users in peer-to-peer networks who are suspected of illegally exchanging copyright-protected content (music or video files). Once in possession of these IP addresses, the copyright owners then initiate criminal proceedings in order to be granted access to files containing the personal details of the users concerned. They then open civil proceedings against them in order to pursue them for damages. The Federal Data Privacy and Information Commissioner (FDPIC) considered this practice to be an abuse of the law, especially given that the processing of personal data is not evident to the user concerned, as required by the Data Protection Act.

On 8 September 2010, the Federal Supreme Court decided that IP addresses are personal data and are thus subject to the Data Protection Act. Furthermore, in a majority decision, the Court considered the covert probing of IP addresses to be unlawful for private companies.

The decision by the Federal Supreme Court stated that there was insufficient justification for such practices.

With immediate effect, the Swiss company is no longer allowed to collect or pass on any further data, i.e., it is required to cease all data processing related to copyright matters.

The decision is not yet available in writing. Some authors already published articles discussing this decision and challenging the conclusion that defending the intellectual property rights of the copyright owners was not to be considered sufficient justification. Therefore, the written reasons for the decision are anticipated with great interest.

## IP/ICT Legal practice group

The IP/ICT Legal practice group is part of Ernst & Young's EMEIA Law Specialty Practice and covers both the national and international IP and ICT practice in its broadest sense.

For further information please contact:

### Belgium/The Netherlands

E [Peter.kits@hollandlaw.nl](mailto:Peter.kits@hollandlaw.nl)

T +31 88 407 00 18

### Finland

E [Petra.hietanen-kunwald@fi.ey.com](mailto:Petra.hietanen-kunwald@fi.ey.com)

T +358207280190

### France

E [Fabrice.naftalski@ey-avocats.com](mailto:Fabrice.naftalski@ey-avocats.com)

T +33 1 55 61 10 05

### Germany

E [Fritjof.boerner@de.ey.com](mailto:Fritjof.boerner@de.ey.com)

T +49 6196 996 25758

E [Peter.katko@de.ey.com](mailto:Peter.katko@de.ey.com)

T +49 89 14331 25951

### Italy

E [Luigi.neirotti@it.ey.com](mailto:Luigi.neirotti@it.ey.com)

T +39 02 85 14 828

### Poland

E [Marek.Gizicki@pl.ey.com](mailto:Marek.Gizicki@pl.ey.com)

T + 48 225 57 73 21

### Portugal

E [Garcia.Pereira@pt.ey.com](mailto:Garcia.Pereira@pt.ey.com)

T +351 226 002 015

### Russia

E [Alexey.Markov@ru.ey.com](mailto:Alexey.Markov@ru.ey.com)

T +7 (495) 641 2965

### Spain

E [jose.dominquezLeandro@es.ey.com](mailto:jose.dominquezLeandro@es.ey.com)

T +34 915 727 200

### Switzerland

E [Klaus.krohmann@ch.ey.com](mailto: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](http://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.