

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

1. The 30th International Data Protection Conference

On October 17, 2008 the 30th International Data Protection Conference was organised by the CNIL and the German Data Protection Authority to celebrate the anniversary of the said institutions. Around 600 persons participated at this event held by the French Presidency Sarkozy. The Conference stresses that while self regulation may be an important tool to ensure the rights of data subjects, national laws are necessary to edict data protection principles in order to face the challenges of a borderless world.

The Conference also permitted to stress out the importance of increased cooperation between the data protection community and the business sector. Personal data need to be processed under strict conditions including for instance personal data of customers and consumers. However, the data protection regulation must not be considered as an obstacle by the companies. The Conference also supported the proposal to set up a working group party in order to submit a report related to the realization of an International data protection award, at the 31st International Data Protection Conference, which will be held in Madrid, next year.

Website of the 30th International Conference of data protection and privacy commissioners
<http://www.privacyconference2008.org/index.php>

2. GOOGLE, for a better consideration for data protection

On April 4, 2008 the Article 29 Working Party published an opinion concerning personal data collected by search engines and recommended a maximum retention period of 6 months. Five months later and in reaction to the opinion of the Article 29 Working Party on search engines, Google announced on September, 8, 2008 that it will reduce its retention period from 18 to 9 months. In this context, IP addresses collected by Google would be anonymised after 9 months. This is the second reduction realized by Google in the past two years. Indeed, the initial period of retention has been reduced from an indefinite period of retention to 18 months.

However, Google still does not meet the recommendations of the European data protection law which requires from search engines to delete or anonymise personal data after a period of retention of 6 months.

Alex Türk, Chairman of the Article 29 Working Party, appreciates the collaboration of Google to ensure the protection of personal data, but he still stresses out the non compliance of Google with the provisions of the European data protection law.

The company's global privacy lawyer of Google argued that "*loss of security, quality and innovation may result from having less data*". Google provides that the period of retention of 9 months would be justified by the "*quality of service*" of the search engine.

Read the full opinion of Article 29 Data Protection Working Party
http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm

Finland

3. "Lex Nokia"- a disputed amendment

On March 4, 2009 the Finnish Parliament passed a bill for the amendment of the Act on the Protection of Privacy in Electronic Communications and some other related acts (HE 48/2008). In Finland the bill is widely known as "Lex Nokia" due to unconfirmed allegations that Nokia acted as initiator and strong advocator of the amendments. The Act increases significantly the rights of employers and other organizations providing users with communications networks to process identification information for the purpose of investigating unauthorized use of communications networks as well as unauthorized disclosure of business secrets. Amongst others the amendment allows employers to monitor traffic data based on automatic search criteria and to process and track identification data of employees' emails manually, in case the employer has sufficient reason to suspect that an essential business secret has been revealed by its employee via electronic communication. The amendment does, however, not entitle the employer to read the contents of the e-mail message.

In the view of many academics the amendment is unconstitutional as it interferes with the confidentiality of communications, a fundamental right guaranteed by the Finnish Constitution. Nevertheless the amendment was handled by Parliament in the legislative procedure applied for ordinary

laws in accordance with the statement of the Finnish Parliament's Constitutional Law Committee.

The use of the processing and monitoring rights under "Lex Nokia" is subject to the fulfillment of specific conditions and procedures that have to be complied with prior to starting the processing of the identification data. An employer would, amongst others, need to have in use all other available means to prevent unauthorized use of communications networks and disclosure of business secrets, provide written instructions and conduct with its employees a cooperation procedure. The processing requires also a prior notification of the Data Protection Ombudsman.

France

4. Major figures on the French Data Protection Authority's activities in 2007

Since 2004, the French Data Protection Authority ("CNIL") has increased its staff. Indeed, 10 new jobs were created on 2007 and 15 more on 2008. However, France with approximately 120 civil servants employed by the CNIL is still behind British, German or Spanish peers. The budgeting efforts allocated by the French government have been significant, but nowadays the CNIL would recommend an inter-regional decentralisation in order to bring the CNIL closer to the realities of business activities.

In 2007, CNIL:

- ▶ recorded **56,404** new personal data files processed;

- ▶ numbered **685** Data Protection Correspondents;
- ▶ received **4,455** complaints;
- ▶ adopted **393** decisions;
- ▶ conducted **164** investigations;
- ▶ sent **101** notices to comply;
- ▶ issued **5** warnings;
- ▶ ordered **9** financial sanctions;
- ▶ referred **5** reports to the Courts.

2008 figures shall be made public in mid 2009.

5. No advertising via Bluetooth without prior consent

On November 2008, the CNIL issued an opinion concerning marketing practices of sending advertising on mobile phones via Bluetooth. The CNIL requires that prior consent of the consumer has to be given before sending advertising via Bluetooth. Indeed, the CNIL considers that sending advertising, without prior consent of the owner of the mobile phone, is a new mean of direct marketing. The CNIL also considers that IP address, and the "Bluetooth login" of the mobile phone, are personal data.

For this reason, it is necessary to obtain the consent of the owner of the mobile phone before sending advertising via electronic mail. Moreover, the CNIL considers that sending an email asking to the owner of the mobile phone if he accepts a Bluetooth connexion is not satisfactory because this collection is too late.

The CNIL demonstrates once again its goodwill to conciliate the development of high technologies and liberties of individuals and privacy.

Germany

6. New Soc's? Secret Online Searches

The German Constitutional Court handed down a landmark ruling on the constitutionality of secret online searches of computers by government agencies. The decision states that: "*the individual is depending upon the state respecting justifiable expectations for the integrity and confidentiality of information-technological systems with a view to the unrestricted expression of personality*". Thus, the decision mentions a new, basic right to the confidentiality and integrity of such systems.

Constitutional Court Decision (BVerfG, 1 BvR 370/07 of 27 February 2008) - only in German.

7. 'Under revision'

As a consequence of the most recent cases of data misuse in Germany the existing legislation concerning data protection is planned to be revised.

Major changes include the restriction of excessive address trading which shall be allowed only on the basis of explicit consent. Moreover, civil fines shall be raised and supplemented with the option of skimming illegitimate profits. In case of data loss (e.g. credit card numbers) companies shall be obliged to immediately contact the data protection authority and the person concerned. In addition the position of data protection officers shall be strengthened amongst others by granting protection against dismissal.

Due to heavy criticism of the private sector and the upcoming parliamentary elections, it remains unclear though if the draft bill will be passed during this legislative period.

The same applies to the Act on Data Protection Audits as a basis for the awarding of data protection labels and for the introduction of a mandatory notification of data security breaches.

The Netherlands

8. OPTA and DPA issue joint ruling on "Tell-a-friend" systems

"Tell-a-friend" systems are allowed on websites subject to conditions. Independent Post and Telecommunications Authority of the Netherlands (OPTA) and the Dutch Data Protection Authority (CBP) announced this today in the form of a ruling. "Tell a friend" is a function on a website which allows an internet user to inform an acquaintance about a specific message or new feature on that website. This method of marketing (viral marketing) is used quite extensively on websites and falls within the jurisdiction of both OPTA and the CBP. The regulatory authorities have drawn up a joint ruling to provide clarity about the conditions subject to which "tell-a-friend" systems can be lawfully used.

9. Dutch DPA enlightened

On 22 January 2009 an amendment of the Personal Data Protection Act was proposed, the purpose of which is to reduce the administrative charges and compliance costs involved arising from the Act.

The most significant change is the projected revocation of the obligation to obtain a permit for transferring personal data to third countries that do not have an adequate protection level in place. By virtue of the Act transfer to such countries is prohibited unless the Ministry of Justice has issued a permit or in case one of the exceptions referred to in article 77 subsection 1 occurs (such as unambiguous permission). The permit will only be granted if it is proved that the recipient outside the EC processes the personal data such that the protection level is comparable to that within the EC.

By using approved model contracts a framework is created within which personal data can be transferred between businesses in an EC and non EC country. The European Commission has approved two model contracts.

These model contracts contain safeguards to achieve the protection level required. No permission will be required if these model contracts are used, as is already the case in Germany. This should result in a substantial decrease in (administrative) charges.

In addition, more data processing instances will be exempted from the notification requirement to the Dutch Data Protection Authority. It is expected the Act will enter into force in June 2009.

Switzerland

10. Revision of the Swiss DPA: Registration of data collections

The revised Swiss Data Protection Act (Swiss DPA) entered into force as per 1 January 2008, with a grace period of one year for several actions. For Swiss companies this means that they should now either have their data collections registered with the FDPIIC, have appointed a Data Protection Officer or have obtained a privacy certificate in order to be in compliance with the Swiss DPA.

For more information also regarding other aspects of the revision of the Swiss DPA, read our Legal News of November 2007 (English, German, French).

11. Swiss Safe Harbour

The European Union (EU) has a framework in place to enable and facilitate the transfer of personal data to the United States of America (US). This framework is known as Safe Harbour.

Since Switzerland is not a member of the EU, the Safe Harbour framework is not applicable for data transfers of companies located in Switzerland to their partners in the US. Because of that, a special data transfer agreement between the Swiss company and the partner in the US had to be concluded in order to be compliant with Swiss regulations on cross border data transfers, even if such partner was Safe Harbour certified.

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.

Read the press release of 9 December 2008 [here](#)

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.