Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

European national news

Nick Pantlin[*]

Herbert Smith Freehills LLP, London, United Kingdom

Keywords:
Internet
ISP/internet service provider
Software
Data protection
IT/information technology
Communications
European law/Europe

ABSTRACT

The regular article tracking developments at the national level in key European countries in the area of IT and communications – co-ordinated by Herbert Smith Freehills LLP and contributed to by firms across Europe. This column provides a concise alerting service of important national developments in key European countries. Part of its purpose is to complement the Journal's feature articles and briefing notes by keeping readers abreast of what is currently happening "on the ground" at a national level in implementing EU level legislation and international conventions and treaties. Where an item of European National News is of particular significance, CLSR may also cover it in more detail in the current or a subsequent edition.

1. Belgium

No contribution for this issue.

Nicolas Roland, *Senior Associate, nicolas.roland@stibbe.com* and **Cédric Lindenmann**, *Junior Associate, cedric.lindenmann@stibbe.com from Stibbe, Brussels (Tel.: +32 2533 53 51).*

2. Denmark

2.1. *New legislation proposed on net and information security in Denmark*

New legislation is in the pipeline, which will increase the powers granted to the Danish Centre for Cyber Security ("**CFCS**"). The telecommunications industry has criticised the proposal for being too broad and granting the CFCS too sweeping powers.

The CFCS, a national security authority under the Department of Defence, will, according to the draft legislation, receive a broad mandate to introduce new regulations and enforce new measures to secure the integrity of public networks. This mandate, which has been criticised for being too sweeping may result in increased costs for the affected companies, providers of public telecommunication networks and services. Additionally, the CFCS will assume all authority concerning net and information security in the telecommunications sector, which has previously been handled by the Danish Business Authority.

According to one particular power granted to the CFCS, the CFCS will be able to demand that supply agreements relating to significant parts of a telecommunication operators service or network shall be disclosed to the CFCS. The CFCS may prior to the execution of such agreements demand a 10-day standstill period in the negotiations, during which the CFCS reviews the agreement, and examines its network security implications. This is in part motivated by fears that it may compromise national security if companies with a close relationship with a foreign country operate critical parts of the network.

The CFCS will be expanding and will open new departments, one of which will specialise in advising companies on their SCADA-systems (supervisory control and data

* Herbert Smith Freehills Exchange House, Primrose St, London EC2A 2EG, United Kingdom. Tel.: +44 20 7374 8000.
E-mail address: Nick.Pantlin@hsf.com.
URL: http://www.herbertsmithfreehills.com

http://dx.doi.org/10.1016/j.clsr.2015.05.016
0267-3649/

acquisition-systems) as these are often not originally designed to handle security risks and can be considered a security risk themselves.

The proposed legislation is expected to take effect on 1 December 2015.

Lau Normann Jørgensen, *partner, LNJ@kromannreumert.com and* **Alexander Philip Dam Rasmussen**, *Assistant Attorney, apr@kromannreumert.com* from *Kromann Reumert, Copenhagen office, Denmark (Tel.: +45 70 12 12 11).*

3. France

No contribution for this issue.

Alexandra Neri, *Partner, alexandra.neri@hsf.com and* **Jean-Baptiste Thomas-Sertillanges**, *Avocat, Jean-Baptiste.Thomas-Sertillanges@hsf.com from the Paris Office of Herbert Smith Freehills LLP (Tel.: +33 1 53 57 78 57).*

4. Germany

4.1. *Publication of photographs and videos of employees on the company website requires employees' explicit written consent*

This February, the German Federal Labour Court (Bundesarbeitsgericht) ruled in a landmark case that in order to post photographs and videos of employees on the company website, the employer needs to obtain the employees' prior written consent. If such consent is provided for an indefinite period of time, it will not automatically terminate together with the employment relationship.

In the case at hand, a former employee had sued his employer, demanding that it cease and desist from using certain parts of a video in which the employee appeared in order to demonstrate certain production steps on the company website and that it pay compensation for related personal suffering. The German Federal Labour Court dismissed this claim.

The court first clarified that the employer could use the video showing the employee on the company website only with the employee's explicit written consent and that a mere oral or tacit consent would not be sufficient. Furthermore, the court stressed that the employer must ensure that withholding such consent will not have a negative impact on the employment relationship, meaning, for example, that the consent must be obtained separately from the employment agreement. In the case at hand, this did not help the employee, as the employer was able to prove that it had properly obtained the employee's written consent.

Secondly, the court held that a consent given by an employee for an indefinite period of time will not automatically terminate once the employment relationship comes to an end, at least not if the photograph or video involved is used only for illustrative purposes and does not convey a particular content related to the specific employee. In that case, a revocation of the consent would only be possible if the employee could show reasonable grounds to substantiate his/her demand that the employer cease using the photograph or video in the future.

With its decision, the German Federal Labour Court strengthens the employers' position regarding the use of photographs and videos of its employees on the company website.

Dr. Alexander Molle, *LL.M. (Cambridge), Counsel, alexander.molle@gleisslutz.com from the Berlin Office of Gleiss Lutz, Germany (Tel.: +49 30 800979210).*

5. Italy

5.1. *Online profiling: new guidelines issued by the Italian Data Protection Authority*

On 19 March 2015, the Italian Data Protection Authority ("**IDPA**") issued new guidelines concerning the processing of personal data for purposes of online profiling which were subsequently published on 6 May 2015 in the Italian Official Gazette (the "**Guidelines**"). The Guidelines are addressed to providers of online services accessible to the public through communications networks (i.e. information society services providers) and are intended to protect both authenticated users (i.e. those who access services through an account, e.g. e-mail) and non-authenticated users (i.e. those surfing on the internet). The rationale for the Guidelines is to provide rules in connection with the ability of the providers to collect a large quantity of information and data (through the various features offered on the internet, such as social networks, e-mail service, online shops etc.) that is then used to track individual behaviour across websites, to create profiles based on that behaviour and to analyse data and infer interests, for targeted advertising purposes.

The main data protection compliance obligations provided by the Guidelines are as follows:

Informative Note: information on the processing of data must be clear, complete, exhaustive and made visible from the home page of the website; it shall specify the purposes and mechanisms of the processing of users' data, including profiling. Informative notes should be structured on several levels: a first level immediately accessible with just one click on the web page, including the most important information (e.g. purposes of the processing and kind of data processed); and a second level, accessible from the first, with additional information about the services offered.

Consent: providers shall always obtain the users' prior informed specific consent for profiling and behavioural advertising. In particular, the consent requirement applies to both profiling carried out by means of data collected through the use of the offered service (e.g. e-mail), and profiling based on the crossing of personal data collected in connection with the use of more features by users (e.g. e-mail and web browsing, participation in social networks and use of maps or display of audio–visual content, etc.), and, finally, profiling based on the use of cookies and other similar identification tools (such as fingerprinting). Data subjects shall also be able to exercise their right to object to the processing of their data for profiling purposes. Consent shall be documented by the providers.

Data retention: a specific data retention period shall be established by providers in compliance with the Italian Data Protection Code.