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. *Danish bookkeeping material may soon be stored abroad*

On 22 January 2015, a bill was passed in the Danish Parliament amending the Danish Bookkeeping Act so that Danish companies will be allowed to store bookkeeping material abroad in an electronic format. Under the former regime, such storage abroad required a dispensation from the Danish Business Authority.

The former Danish Bookkeeping Act (the "**Former Act**") was adopted at a time where bookkeeping material was predominantly paper based. The new bill was introduced with the purpose of bringing legislation up to date with technological developments, which have seen an increased use of cloud-based solutions to store company data on foreign servers. The storage of bookkeeping material in such cloud-solutions would, under the Former Act, be considered storage abroad, and would thus require a specific dispensation.

The amended Bookkeeping Act (the "**New Act**") will allow for bookkeeping material to be stored abroad if the following conditions are met:

A. the company ensures that the bookkeeping material is stored in a prudent manner, and that all material can be accessed online from a Danish address at all times;
B. any system specifications and passwords needed to access the material must be stored in Denmark, in order to allow for efficient audit by the Danish authorities; and

* 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.2015.01.013

C. if the bookkeeping material is paper-based rather than electronic, the material cannot, as a general rule, be stored outside of Scandinavia.

If the above mentioned requirements are met, companies may store bookkeeping materials abroad, i.e. on cloud-based solutions, without prior filing or approval from the authorities.

The New Act will enter into force on 1 March 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. *Patient rights vs. their physicians' data privacy rights*

This January, the German Federal Court of Justice (Bundesgerichtshof) ruled in a landmark case that patients do not have a right to request their physicians' private addresses from the hospital where they were treated.

In the case at hand, the plaintiff argued that he needed the address to serve his claim against the physician. A court of lower instance decided that the hospital had to disclose the private address to the patient, arguing that the physician's anonymity is not compatible with the patient-to-doctor relationship.

The Federal Court of Justice has overruled the decision, principally on the basis of two arguments:

Firstly, the court argued that data privacy regulations prevent the hospital from disclosing the physician's private address. Although an employer is allowed to process employee data, such processing is only permissible to the extent necessary for the performance of the employment contract or with the consent of the employee. According to the court, the disclosure of the private address to the patient as a third party is not necessary for such purposes. The patient-to-doctor relationship does not constitute an exception to the general privacy of personal data.

Secondly, the court has confirmed prior case law according to which an action against a physician who is employed at a hospital can be served under the address of the hospital if the name and the function of the physician are indicated in the action. Since the hospital is obliged to grant the patient with the name of the physicians who treated him/her, there is no further necessity to disclose the private address of the physician.

With its decision the Federal Court of Justice strengthens employees' data privacy rights. Employers should therefore carefully assess the legal situation before they disclose employees' personal data to third parties, e.g. customers.

*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. *The Italian Data Protection Authority establishes requirements for the launching of Google- Street View Special Collections in Italy*

On 4 December 2014 the Italian Data Protection Authority ("**IDPA**"), following a request by Google Inc. ("**Google**"), established the requirements Google must comply with for the launch of its Street View Special Collections service (the "Special Collections") in Italy. Special Collections is a Street View feature aimed at capturing 360-degree images of cultural, natural and tourist locations, (both public and private), such as museums, beaches and parks. Due to the peculiarities of the locations, the images cannot be collected by operators shooting images from cars and can only be collected through special trekker devices carried by Google's operators on foot, or placed on boats and/or trains. Following their collection, the images are intended to be transferred by Google to the US for processing, and those which identify individuals, (e.g. faces, license plates of vehicles), will be automatically obscured through the use of certain technologies.

Among other things, the IDPA established that Google must:

A. in the case of images relating to delimited or restricted access locations (e.g. rooms, villas, museums, gardens etc.), inform the persons present of their right not to be photographed and allow them to exercise the same right;
B. provide potential data subjects with prior information relating to the planned images' collection by means of:
   i. publication on Google's web site, namely www.google.it, as well as on all web pages available in Italian in any way related to Google, during the three days prior to the programmed images' collection;
   ii. publication on web sites, newsletters or other informative publications of Google's partners (which are authorized by Google to collect the images) and/or entities that own/manage the locations concerned, during the seven days prior to the planned images' collection (for web sites), or on the last issue of the relevant publication in all other cases;
   iii. publication of warnings or signs placed at the entrance in case of enclosed areas or places open to the public; and
C. provide stickers, signs or other distinguishing marks clearly visible on equipment through which photographic images are captured and on clothing of operators, so as to unequivocally indicate that Google is acquiring photographic image snapshots that will be published online through the service of Google Special Collections as part of Street View on Google Maps.