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, UK

Keywords:
Internet
ISP/Internet service provider
Software
Data protection
IT/Information
Technology
Communications
European law/Europe

A B S T R A C T

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

Cédric Lindenmann, *Associate, cedric.lindenmann@stibbe.com* and **Carol Evrard**, *Associate, carol.evrard@stibbe.com, from Stibbe, Brussels (Tel.: +32 2533 53 51).*

2. Denmark

No contribution for this issue

Arly Carlquist, *Partner, ac@bechbruun.com* and **Henrik Syskind Pedersen**, *Attorney, hsp@bechbruun.com, from the Bech-Bruun, Copenhagen office, Denmark (Tel.: +45 7227 0000).*

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

No contribution for this issue

Dr. Stefan Weidert, *LL.M. (Cornell), Partner stefan.weidert@gleisslutz.com* and **Dr. Martin Hossenfelder**, *Associate martin.hossenfelder@gleisslutz.com, from the Berlin Office of Gleiss Lutz (tel.: +49 30 800 979 0).*

5. Italy

Salvatore Orlando, *Partner s.orlando@macchi-gangemi.com* and **Laura Liberati**, *Associate l.liberati@macchi-gangemi.com, Rome office of Macchi di Cellere Gangemi (Rome Office tel. +39 06 362141).*

5.1. *ECJ Ruling on Safe Harbor – Italian authority's implementation of Safe Harbor declared invalid*

On 6 October 2015, as has been widely reported in the press, the European Court of Justice (**"ECJ"**) declared invalid the long-

For further information, see: www.herbertsmithfreehills.com

* Herbert Smith Freehills, Exchange House, Primrose St, London, EC2A 2HS, UK. Tel.: +44 20 7374 8000.
E-mail address: Nick.Pantlin@hsf.com

http://dx.doi.org/10.1016/j.clsr.2015.12.012

standing EU Commission's Safe Harbor Decision of 26 July 2000 (the **"ECJ Ruling"**). The full effect of the ruling and the impact on data-flows between EU Member States and the US remains to be seen. The initial outcome, however, is that transfers of personal data from EU Member States to the US can no longer rely on the US-EU Safe Harbor framework, which enabled US companies, complying with Safe Harbor principles, to "self-certify" that they grant a sufficient level of data protection with regard the processing of personal data transferred from the EU.

On 22 October 2015, the Italian Data Protection Authority (**"IDPA"**) adopted a provision which declared invalid Resolution No. 36 of 10 October 2001 (**"IDPA Resolution No. 36"**) which had permitted the IDPA to authorise the transfer of personal data to entities established in the US if carried out in compliance with the "Safe Harbor Privacy Principles". The adoption of this provision resulted in the IDPA prohibiting any transfer of personal data to the US carried out on the basis of IDPA Resolution No. 36. Furthermore, the IDPA reserved the right at any time to carry out, if required, the necessary controls on lawfulness and fairness of data transfers and processing operations, and to take any measures provided by the Italian Data Protection Code.

Finally, the IDPA acknowledged the WP29 Statement of 16 October 2015 which confirmed that data transfers to the US can be lawfully carried out on the basis of alternative solutions set forth by EU data protection law, in particular those providing generally feasible solutions. These solutions include standard contractual clauses, binding corporate rules, specific informed consent by the data subject (where applicable) and authorisation by the IDPA issued on the basis of contractual safeguards.

http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/4393308

6. The Netherlands

Friederike van der Jagt (*friederike.vanderjagt@stibbe.com/ +31 20 546 0144*) *and* **Joost van Eymeren** (*joost.vaneymeren@stibbe.com/ +31 20 546 0332*).

6.1. *Dutch Data Protection Authority decides that a parcel distributor may not provide its customers with the name, photo and location of its couriers*

NE Distriservice B.V. (**"NDS"**) delivers parcels within the Benelux countries with customers having the ability to track their parcels via a track and trace system. NDS sends their clients an e-mail with a link to a secure online portal, which enables the customers to see who will deliver the parcel and where the courier is located at a certain moment. In the future, NDS would like to include further information by placing a photo of the courier on the portal.

In response to a complaint, the Dutch Data Protection Authority (**"Dutch DPA"**) started an investigation regarding NDS. The supervision of personal data processing in the employee-employer relationship remains one of the priorities of the Dutch DPA in 2015 as according to the Dutch DPA, employees are in a vulnerable position because they are financially dependent on their employer.

According to NDS, their system would offer a higher sense of safety to their customers as each customer would know exactly which courier would come knocking on their door. For this reason, NDS believes that it has a legitimate interest in providing the above-mentioned personal data of its employees to its customers, in accordance with article 8(f) of the Dutch Data Protection Act (**"DDPA"**). Over the last few years, NDS has been dealing with a declining customer base. With this in mind, NDS must distinguish itself from other parcel distributors in order to find new customers, to retain existing customers and to promote continuity and employment. NDS has tried to achieve this by providing as much information as possible about the delivery of the package. In addition, the system also allows for an optimisation of the logistics process.

NDS has examined whether the same goal could be achieved by using a staff pass. The introduction of a staff pass, however, was not considered to be a good alternative, given that customers are not familiar with their requirements and because such a system does not provide any information on the location of the transmitted parcel. Furthermore, according to NDS, such staff passes are often easy to falsify.

In its analysis, the Dutch DPA first stated that NDS failed to demonstrate why providing the personal data of the couriers is necessary to optimise its logistics processes or for business continuity. The Dutch DPA stated that giving the customer as much information as possible about the delivery time can also be achieved without providing the personal data of employees to the customers, believing that providing information about the date and time of delivery is sufficient for this purpose. This way, the customer knows exactly when to expect an NDS courier at the door. The couriers can also be recognised by NDS and usually drive a NDS company vehicle, which should provide sufficient safety from the customer's point of view. In addition, the Dutch DPA considered that the interests of NDS do not outweigh the invasion of privacy of the couriers. Employees have a reasonable expectation of privacy, which also applies in the workplace. While the information provided allows the customer to constantly track the couriers, it also results in security risks as their whereabouts would be known at all times.

The Dutch DPA subsequently checked whether NDS could rely on the consent of the employees as a basis of authorisation to make the provision of personal data still possible (article 8 (a) DDPA). The couriers themselves even offered to demonstrate their explicit consent through a petition to the Dutch DPA; however, the Dutch DPA ruled in line with previous investigations and legislative history, that since the couriers are financially dependent on NDS and NDS is linking the provision of personal data to the preservation of employment, they are unable to give their consent "freely".

The Dutch DPA also addressed the future plans of NDS to put a photo of the courier on the online portal. One can discern a person's race from a photo and the processing of racial data is prohibited, in principle, unless the DDPA makes provisions for an exception (article 16 in conjunction with articles 18 and 23 DDPA). The question is whether providing a photo leads to the processing of racial data. According to NDS, the photo does not constitute racial data in this context, given that the photo is not intended to distinguish between races. The Dutch DPA took a different view and concluded that the customers of NDS