COMPUTER LAW & SECURITY REVIEW 000 (2018) 1–4

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/CLSR

Computer Law & Security Review

European national news

*Nick Pantlin**

Herbert Smith Freehills LLP, London, United Kingdom

ARTICLE INFO

Article history:
Available online xxx

Keywords:
Internet
ISP/Internet Service provider
Software
Data Protection
IT/Information Technology
Communications
and European law/Europe

ABSTRACT

This article tracks developments at the national level in key European countries in the area of IT and communications and provides a concise alerting service of important national developments. It is 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

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

No contribution for this issue

2. Denmark

Arly Carlquist, *Partner, ac@bechbruun.com* and **Niclas Jensen**, *Junior Associate, nic@bechbruun.com from Bech-Bruun, Copenhagen office, Denmark (Tel.: +45 7227 0000).*

No contribution for this issue

3. France

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).*

No contribution for this issue

4. Germany

Dr. Matthias Schilde, *matthias.schilde@gleisslutz.com, from the Berlin Office of Gleiss Lutz, Germany (Tel.: +49 30800979210).*

No contribution for this issue

5. Italy

Salvatore Orlando, *Partner, s.orlando@macchi-gangemi.com* and **Laura Liberati**, *Senior Associate, l.liberati@macchi-gangemi.com, from the Rome office of Macchi di Cellere Gangemi* (Tel.: +39 06362141).

* Corresponding author: Nick Pantlin, Herbert Smith Freehills Exchange House, Primrose St, London EC2A 2HS (Tel.: +44 20 7374 8000). For further information see: www.herbertsmithfreehills.com
E-mail address: nick.pantlin@hsf.com

https://doi.org/10.1016/j.clsr.2018.08.002
0267-3649/

Please cite this article as: N. Pantlin, European national news, Computer Law & Security Review: The International Journal of Technology Law and Practice (2018), https://doi.org/10.1016/j.clsr.2018.08.002

5.1. *The Italian Data Protection Authority authorizes body cam on trains for security purposes*

By means of a decision dated 22 May 2018 (the "**Decision**") the Italian Data Protection Authority ("**IDPA**") – upon a request for preliminary check filed pursuant to article 17 of the Italian Data Protection Code ("**IDPC**") – authorised a railway transportation company (the "**Company**") to carry out the processing of personal data connected to a system consisting of wearable devices (i.e. body cams), which allows the collection and transmission of images taken on board trains in real time to a computer located at the Company's premises. The body cams are provided to the security staff and the personnel responsible for checking tickets and the purposes of the system is to improve security and prevent theft, attacks and vandalism.

The IDPA established certain measures that the Company must implement in order to protect the rights of the individuals involved (e.g. employees and travellers), among which:

- the cams shall be activated by the Company's staff only in case of real danger (i.e. they shall not always be on) and a red LED shall show such activation;
- only authorised persons shall view and delete the images and the relevant activities shall be registered;
- the Company shall adopt an internal policy to regulate and provide, among others, appropriate information to employees about the modalities of use and the specific conditions that allow the activation of the body cams;
- specific precautions shall be implemented where the video filming involves individuals belonging to "weak" categories (e.g. witnesses, victims of crimes, minors etc.);
- information shall be given on board to alert people of the mobile video surveillance system and its features;
- the Company shall comply with labour legislation;
- the Company shall retain data for up to 7 days, unless it is held in case of events that give rise to liability for damages, in which case data can be kept for up to two years (as per the statute of limitation period), after which data shall be deleted; and
- video recordings shall be kept in encrypted form.

It is worth noting that, as also stated by the IDPA, this authorisation only concerns the processing bearing the features described in the request filed the Company. Accordingly, since the entering into force of the Regulation (EU) 2016/679 ("**GDPR**") the preliminary check provided by article 17 of the IDPC will no longer be applicable. In case of changes to the system's features, the Company – in accordance with the principle of accountability – shall autonomously assess the compliance of the processing/system with the GDPR. This includes the need to carry out an impact assessment pursuant to article 35 of the GDPR and apply, possibly, for a prior consultation pursuant to article 36 of the GDPR.

6. The Netherlands

Joe Jay de Hass, *JoeJay.deHaas@stibbe.com, Amsterdam office of Stibbe (Tel.: +31 20 546 0036).*

No contribution for this issue

7. Norway

Dr. Rolf Riisnæs, *Partner, rri@wr.no,* **Dr. Emily M. Weitzenboeck,** *Senior Associate, emw@wr.no, Wikborg Rein Advokatfirma AS (as from 1.1.2017), Norway (Tel. +47 22 82 75 00).*

No contribution for this issue

8. Spain

Albert Agustinoy, *Partner, albert.agustinoy@cuatrecasas.com,* **Jorge Monclús,** *Senior Associate, jorge.monclus@cuatrecasas.com and* **Esther Ballesteros**, *Intern, esther.ballesteros@cuatrecasas.com from Cuatrecasas, Spain (Tel.: +34 93 290 55 85).*

8.1. *Urgent Data Protection Measures Come Into Force*

While waiting for the new Spanish Data Protection Act, still in parliamentary process, the Spanish government has passed urgent measures through Royal Decree-Law 5/2018 ("**RDL 5/2018**"), to adapt Spanish Law to the General Data Protection Regulation ("**GDPR**"), particularly in terms of inspection and sanctioning procedures.

The RDL 5/2018 came into force on 31 July, the day after its publication in the Official Gazette of the Spanish State.

The RDL 5/2018 establishes that processing agreements signed before 25 May 2018 will still be valid until their expiration date and, in cases of indefinite duration, until 25 May 2022.

It also identifies the individuals that can be liable for GDPR infringements: data controllers and data processors, data controllers and data processors not established in the European Union, certification authorities and supervisory authorities of codes of conduct. The RDL 5/2018 clarifies that the sanctioning system will not apply to data protection officers.

The new piece of regulation expressly states that the Spanish Data Protection Agency ("**SDPA**") cannot admit abusive claims or those lacking rational grounds supporting the existence of infringement. Also, the SDPA can decide not to admit claims when the controller or the processor, which had already received a warning from the SDPA, has taken the proper measures to correct the infringement, as long as (i) it has not caused damage to the affected individuals, or (ii) the affected individuals' rights are fully protected with those measures.

The approval of this new regulation provides the SDPA with legal coverage to launch investigation and sanctioning procedures derived from infringements of the GDPR while waiting until the new Spanish Data Protection Act is enacted.

9. Sweden

Agne Lindberg, *Partner, agne.lindberg@delphi.se, and* **Erika Hammar**, *Associate, erika.hammar@delphi.se from the Stockholm Office of Advokatfirman Delphi (Tel.: +46 8 677 54 00).*

No contribution for this issue

Please cite this article as: N. Pantlin, European national news, Computer Law & Security Review: The International Journal of Technology Law and Practice (2018), https://doi.org/10.1016/j.clsr.2018.08.002