Since January 2020 Elsevier has created a COVID-19 resource centre with free information in English and Mandarin on the novel coronavirus COVID-19. The COVID-19 resource centre is hosted on Elsevier Connect, the company's public news and information website.

Elsevier hereby grants permission to make all its COVID-19-related research that is available on the COVID-19 resource centre - including this research content - immediately available in PubMed Central and other publicly funded repositories, such as the WHO COVID database with rights for unrestricted research re-use and analyses in any form or by any means with acknowledgement of the original source. These permissions are granted for free by Elsevier for as long as the COVID-19 resource centre remains active.
European National News

Nick Pantlin*

Herbert Smith Freehills Exchange House LLP, Primrose St, London EC2A2HS, United Kingdom

ARTICLE INFO

Keywords: Internet, ISP/Internet service provider, Software, Data protection, IT/Information technology, Communications, 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.

Authors

| Country   | Contact Information                                      |
|-----------|----------------------------------------------------------|
| Belgium   | Cédric Lindemann, Associate, cedric.lindemann@stibbe.com and Carol Evrard, Associate, carol.evrard@stibbe.com from Stibbe, Brussels (Tel.: +32 2533 53 51) |
| Denmark   | Arly Carlquist, Partner, ac@bechbruun.com and Jens Grønkjær Sjølander Pihl, Senior Associate, jgp@bechbruun.com from Bech-Bruun, Copenhagen office, Denmark (Tel.: +45 7227 0000) |
| 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) |
| Germany   | Dr. Alexander Molle, LL.M. (Cambridge), Partner, alexander.molle@gleisslutz.com, from the Berlin Office of Gleiss Lutz, Germany (Tel.: +49 30800979210) |
| Italy     | Salvatore Orlando, Partner and Head of JODI (Juridical Observatory on Digital Innovation) from the Rome Office of Ughi e Nunziante (Tel. +39 06 474831) |
| The Netherlands | Joe Jay de Hass, joejay.dehaas@stibbe.com, Amsterdam office of Stibbe (Tel.: +31 20 546 0036) |
| Norway    | Dr. Rolf Riismaa, Partner, rri@wr.no, and Dr. Emily M. Weitenboeck, Senior Lawyer, emw@wr.no, Wikborg Rein Advokatfirma AS, Norway (Tel.: +47 22 82 75 00) |
| Spain     | Albert Agustinoy, Partner, albert.agustinoy@cuatrecasas.com, Jorge Monclús, Senior Associate, jorge.monclus@cuatrecasas.com, and Pedro Méndez de Vigo, Associate, pedro.mendezdevigo@cuatrecasas.com, at Cuatrecasas, Spain (Tel.: +34 93 290 55 85) |
| 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) |
| UK        | Nick Pantlin, Partner, nick.pantlin@hsf.com, Miriam Everett, Partner, mailto:miriam.everett@hsf.com, Hayley Brady, Partner, hayley.brady@hsf.com and Rachel Kane, Associate, rachel.kane@hsf.com from the London Office of Herbert Smith Freehills LLP (Tel.: +44 20 7374 8000) |

* Corresponding author: Nick Pantlin, Herbert Smith Freehills Exchange House LLP, Primrose St, London EC2A2HS, United Kingdom. E-mail address: nick.pantlin@hsf.com

https://doi.org/10.1016/j.clsr.2020.105453
0267-3649
1. Belgium

No contribution for this issue.

2. Denmark

No contribution for this issue.

3. France

No contribution for this issue.

4. Germany

4.1. German Higher Regional Courts decided on treatment of influencer postings

Over recent months, a number of German Higher Regional Courts have ruled on the legality of influencer postings not labelled as advertisements. The Regional Higher Courts in Hamburg, Munich and Braunschweig (the “Courts”) have issued the latest decisions. While the Courts in Hamburg and Munich take the view that the postings in question were legal, the Court in Braunschweig disagrees.

The three Courts had to decide on remarkably similar cases. In each instance, the post in dispute displayed a product and contained a link to the website of the company making that product. The influencers had no advertising contract with the companies and as a result received no compensation. Therefore, none of the influencers labelled the post as an advertisement.

The Courts in Hamburg and Braunschweig ruled that even if an influencer does not receive compensation for a post itself, the post serves to promote both the influencer’s own company and other companies’ business. It is therefore a so-called business act, which means that competition law is applicable. The Braunschweig Court (2 U 78/19) further considers that not labelling the post as advertising is misleading. Mixing private and commercial content makes it difficult for users to recognise that they are on a commercially operated profile. The Higher Regional Court in Hamburg (15 U 142/19) takes a different view. Mixing private and commercial content is a well-known method for promoting sales. Furthermore, print magazines do not have to show comparable articles separately as advertising. Therefore, in the opinion of the Court it is obvious that every post on an influencer’s profile is an advertisement, and labelling it as such is unnecessary.

The Munich Higher Regional Court (4 HK O 14,312/18) takes yet another line of argument. In its opinion, such a post is not even a business act. Therefore, only one thing is certain: the final decision will be taken in Karlsruhe by Germany’s Federal Court of Justice.

5. Italy

5.1. Green light to the COVID-19 alerting App “Immuni” by the Italian data protection authority

With authorisation No. 95 of 1 June 2020 (the “Authorisation”), the Italian Data Protection Authority (the “Authority”) authorised the Italian Ministry of Health (the “Ministry”) to commence the data processing operations related to the COVID-19 alert system (the “Alert System”) operated via an app for mobile devices called ‘Immuni’ (the “App” or “Immuni”).

The Alert System is an exposure notification system which aims to alert the App’s users (the “Users”) when they have been exposed to other Users who possess symptoms of Coronavirus. The download and use of the App are not mandatory. When two Users come sufficiently close to each other for long enough, as established by an algorithm, their devices record each other’s rolling proximity identifier in local memory. Rolling proximity identifiers are generated from temporary exposure keys and change multiple times each hour. Temporary exposure keys are generated randomly and change once per day. The Users who have tested positive for the virus can decide to upload the cryptographic keys associated with their device to the App’s server, to enable the App to make the alert notification. To ensure that only Users who have actually tested positive for the virus may upload their cryptographic keys, the assistance of an authorised healthcare operator is required to perform the upload. The App uses a Bluetooth Low Energy technology, in order to avoid the gathering of data on the identity or the location of the users. The system uses no geolocation data, including GPS data. In particular, the App leverages the Apple and Google Exposure Notification framework made available to mobile devices using iOS and Android systems, which includes application programming interface and technologies designed to enable the tracing of the contacts without the geolocation of the Users’ devices.

Besides the temporary exposure keys, the App also sends to the server some analytics data for the purposes of helping the Italian National Healthcare Service and for improving the performance of the Alert System. Immuni has been developed by the Italian Extraordinary Commissioner for the COVID-19 pandemic, in collaboration with the Ministry and the Ministry for Innovation Technology and Digitalisation.

The Authorisation follows a favourable opinion issued by the Authority on 29 April 2020, on the basis of which the Italian Government adopted on 30 April 2020 a number of urgent provisions aimed at establishing the Alert System via the App (Law Decree No. 28 of 30 April 2020: the “Decree”).

The Ministry and the Authority followed the data protection impact assessment procedure and the prior consultation procedure as per Articles 35 and 36 of the EU Regulation 2016/679 (the “GDPR”). In particular, on 28 May 2020 the Ministry sent to the Authority the impact assessment report to obtain a prior authorisation by the Ministry pursuant to Article 36 paragraph 5 of the GDPR. The Ministry, in turn, issued the Authorisation declaring that the processing of personal data
within the framework of the Alert System can be considered to be proportionate and that measures have been put in place by the Ministry to adequately safeguard the rights and freedoms of the data subjects by mitigating the risks resulting from the processing.

Taking into account the complexity of the Alert System and the number of individuals potentially involved, the Authority considered it necessary to set out a number of measures and requirements in order to enhance security of the data related to the Users, including the following:

- Users shall be informed adequately about the functioning of the algorithm used to assess the exposure risk;
- Users shall be made aware that the system might generate exposure alerts that do not reflect in all cases an actual risk situation;
- Users shall be able to temporarily deactivate the App through an easily accessible function on the home page of the App;
- the data collected via the Alert System may not be used for purposes other than those specified in the legislation regulating the App;
- transparency of the data processing for statistical and epidemiological purposes will have to be ensured and appropriate safeguards for the processing will have to be laid down. To that end, any matching with identifiable individuals will have to be prevented and adequate security measures and anonymisation techniques must be put in place. Measures shall be adopted to enable the tracing of any operations performed by system administrators on the operating systems, the network and the databases;
- the IP addresses of mobile phones of the Users will have to be stored for a period commensurate to what is strictly necessary to detect malfunctioning or attacks;
- technical and organisational measures will have to be implemented to mitigate the risks related to false positives; and
- special care will have to be taken in drafting the information notices and alert messages, given that the Alert System may also be used by minors aged above 14 years.

Finally, the Authority emphasised that processing by unauthorised entities of the personal data collected via the App may constitute a criminal offence.

6. The Netherlands

No contribution for this issue.

7. Norway

No contribution for this issue.

8. Spain

8.1. Data Protection Authority focuses on cookies

The Spanish Data Protection Authority (the “SDPA”) has been targeting infringements regarding cookies. In June 2020, the SPDA issued five different infringement proceedings that ended with sanctions up to 30,000 Euro.

Most of the infringements are related to cookies that are automatically stored in the web browser as well as with cookie policies that do not offer the possibility of managing cookies on a granular level.

In the past year, the SDPA updated its guidelines on cookies. The latest update focused precisely on the two points that are the subject of most of the infringements. It recommended informing users about cookies using a two ledger system. The first information ledger (pop-up or similar) should allow users to know about the existence of the different cookies that could be stored when browsing through the website and if such cookies belong to the owner of the website or to third parties, as well as the possibility to accept such cookies or manage them. The second information ledger should inform users about the specific cookies and give data subjects the option to manage the storage or rejection on a granular basis.

The SDPA also suggested that consent could be given in a valid way if the data subject continued browsing through the website without accepting or managing the storage of cookies.

However, on May 2020, the European Data Protection Board also updated its guidelines on consent to address issues such as the requirements for valid consent to store cookies and rejected the approach of the SDPA regarding the possibility to consent to cookies by browsing through a website. Therefore, following this recent update, and considering the approach adopted by the SDPA in its decisions, it is not advisable anymore to consider a continued browsing through a website as a strong enough affirmative action to understand that consent to the storage of cookies has been given in a valid way.

9. Sweden

No contribution for this issue.

10. UK

10.1. Airbnb, TripAdvisor, Booking.com and Expedia strike data sharing deal with the EU

5 March 2020 saw the European Commission (the “EC”) announce an unprecedented agreement with short-stay accommodation titans Airbnb, Booking.com, Expedia and TripAdvisor to share and publish data (on the number of nights booked
and the number of guests staying) with the EC via Eurostat (the EU’s statistical office) (press release here). Eurostat will then aggregate the data by municipality and publish that data on a Member State and individual region level.

This collaborative venture represents an initial step by the EC in tackling the absence of regular and reliable data in this area, and recognises the need to balance:

• the opportunities for micro-entrepreneurs using these growing platforms; and
• adverse societal effect on local communities of landlords using their properties for short term lets, e.g. increasing property prices.

While this agreement has been universally welcomed, it is noted that there are other categories of information that could also be useful from a policy-making perspective, such as the number of listings, hosts, beds and types of accommodation.

A number of cities including Paris, Barcelona, Berlin and Amsterdam have previously sought to place restrictions on the use of short-stay accommodation platforms, but this has not always been successful. For example, on 19 December 2019, the Court of Justice of the European Union (the EU’s most senior court) ruled that Airbnb did not have to meet particular regulatory requirements as it was correctly classified as an intermediation service rather than an estate agent (a stark contrast to their ruling on Uber with respect to the transportation services space). This new data sharing agreement does not tackle the limited regulatory restrictions that can be placed on online platforms. However, the EC hopes that this data collaboration will allow for more informed and balance policymaking.

With a 2019 survey showing that 21% of EU citizens use a website or app to arrange accommodation, there have been numerous calls for a digital regulator to better police this space. It is thought that the much anticipated EU Digital Services Act will make some progress on this front, but the slow development of this legislation may struggle to match the evolving issues face by online platforms. That said, this remains an interesting example of big tech companies collaborating with supranational bodies on regulation, as well as regulators seeking to become better informed on the nature and effect of new technology platforms to ensure informed decision making in this space.

This information on short-stay accommodation is anticipated to be publicly available as soon as Q3 2020.

10.2. **UK government responds to DCMS select committee report on immersive and addictive technologies**

The UK government has published a formal response to the Department for Digital, Culture, Media and Sport (the “DCMS”) Select Committee’s report on Immersive and Addictive Technologies. The government’s response is likely to be broadly welcomed by the video games industry as the government has proposed to take a cautious, industry-led approach to the Committee’s key recommendations, including the potential regulation of loot boxes under gambling legislation.

Loot boxes (or “gacha” mechanisms as they are known in Japan where many of the games featuring this type of functionality originate), are an in-game mechanic whereby players receive a randomised selection of virtual items or “loot” in return for real or virtual (in-game) currency. Loot boxes are an increasingly common feature in many games and can be lucrative for gaming companies due to their ability to generate revenue after the initial purchase or release of a game.

The DCMS Select Committee, whose report was published in September 2019 following a lengthy and detailed inquiry, recommended that loot boxes should not be sold to children playing games and should be regulated as a ‘game of chance’ under the Gambling Act 2005 (the “Act”). If loot boxes were to be brought within the scope of the Act by future regulation, operators would need to obtain licences from the Gambling Commission and then face an ongoing compliance burden with risk of fines for breach.

The government has responded to this recommendation by announcing a further call for evidence on loot boxes which will take place later in 2020 (no specific date is given). The government also confirmed that any legislative change will take place as part of its wider review of the Act (which was announced in the December 2019 Queen’s Speech). It is therefore unlikely that any legislative changes will be enacted until 2021.

In its response, the government commends a number of recent self-regulating steps taken by the video games industry and relies on these examples as evidence that some of the Committee’s concerns are (at least in part) being addressed on a voluntary basis by industry players. Examples of those steps include:

• the joint announcement by Sony Interactive Entertainment, Microsoft and Nintendo that all future titles across their PlayStation, Xbox and Switch consoles will be required to disclose the relative probability of receiving the randomised virtual items in loot boxes (a similar initiative has been endorsed by the Association for UK Interactive Entertainment (the “UKIE”)); and
• moves by Pan-European Game Information (“PEGI”) to increase the age rating on simulated gambling games and to inform consumers when games contain ‘paid random items’.

There have also been responses to the Committee’s other recommendations regarding online age ratings and the future online harms regulator.

Regarding online age ratings, the government confirmed that it will soon assess the level of voluntary compliance by the video games industry in implementing PEGI age ratings for online games. If it considers that insufficient progress has been made, it will take legislative action. Regarding the future online harms regulator, following a consultation response
published in February 2020 (see our updates here and here), the government will publish a full response and policy details in relation to the regulation of online harms later this year. New rules are likely to require companies to use a range of proportionate tools to verify age and prevent children from accessing age-inappropriate content online. Ofcom is likely to be given regulatory responsibility, although timelines remain unclear.