

Available online at www.sciencedirect.com

ScienceDirect

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

**Computer Law
&
Security Review**

EU update

Kit Burden*

DLA Piper UK LLP, United Kingdom

ARTICLE INFO

Article history:

Keywords:

EU law

Intellectual property

Information technology law

Telecommunications law

ABSTRACT

This is the latest edition of the DLA Piper column on developments in EU law relating to IP, IT and telecommunications. This news article summarises recent developments that are considered important for practitioners, students and academics in a wide range of information technology, e-commerce, telecommunications and intellectual property areas. It cannot be exhaustive but intends to address the important points. This is a hard copy reference guide, but links to outside web sites are included where possible. No responsibility is assumed for the accuracy of information contained in these links.

© 2018 Kit Burden. Published by Elsevier Ltd. All rights reserved.

1. EU& Japan: Free flow of personal data from EU to Japan soon possible

Patrick Van Eecke, *Partner* and Anne-Gabrielle Haie, *Associate*
DLA Piper Brussels

On 17 July 2018 the European Union and Japan agreed to recognise each other's data protection systems as 'equivalent' and to adopt reciprocal adequacy decisions.

1.1. What is an adequacy decision?

An adequacy decision is a decision establishing that a third country provides a comparable level of protection of personal data to that in the European Union. As a result, personal data can flow from the European Economic Area (EEA) (the 28 EU Member States as well Norway, Liechtenstein and Iceland) to that third country without being subject to any further safeguards or authorisations.

Adequacy decision is one of the tools provided for under the General Data Protection Regulation to transfer personal data from the EU to third countries.

1.2. What does it mean for business?

When the EU declares that a third country offers an adequate level of protection, businesses can transfer data to another company in that third country without the data exporter being required to provide further safeguards or being subject to additional conditions. That means that the requirements of Article 46 of GDPR imposing additional measures to be taken providing a legal ground and appropriate safeguards for such data transfer (such as the use of a Data Transfer Agreement, the conclusion of Binding Corporate Rules or the use of the European Commission's standard data protection clauses) will cease to apply to data transfers between the EU and Japanese companies. The transfer of data between EU and Japan will be comparable to a transmission of data within the EU.

* Corresponding author: Kit Burden, DLA Piper UK LLP 3 Noble Street London EC2V 7EE United Kingdom T: +44 (0) 8700 111 111 F: +44 (0) 20 7796 6666 For further information see: <http://www.dlapiper.com/>.

E-mail address: kit.burden@dlapiper.com

However, please note that such an adequacy decision will only apply to the transfer of data between the EU and Japan, which means that global companies might still need to implement an Intra-Group Data Transfer Agreement (IGDTA) in order to cover the transfer of data to countries other than EU Member States and Japan. Moreover, it does not remove the obligation for a company to conclude a data processing agreement with its processor(s) as prescribed by Article 28 of GDPR.

1.3. What will be the scope of the future adequacy decisions?

The future adequacy decisions will cover personal data exchanged for commercial purposes as well as personal data exchanged for law enforcement purposes between EU and Japanese authorities. In particular, the EU's adequacy decision will concern the protections provided under the Japanese Act on the Protection of Personal Information (APPI) and will thus apply to all transfers of personal data to business operators in Japan.

To align with European standards, Japan has committed to implementing the following additional safeguards to protect EU citizens' personal data, before the Commission formally adopts its adequacy decision:

- A set of rules providing individuals in the EU whose personal data are transferred to Japan, with additional safeguards that will bridge several differences between the two data protection systems. These additional safeguards will strengthen, for example, the protection of sensitive data; the conditions under which EU data can be further transferred from Japan to another third country; and the exercise of individual rights to access and rectification. These rules will be binding for Japanese companies importing data from the EU, and enforceable by the Japanese independent data protection authority (PPC) and courts.
- A complaint-handling mechanism to investigate and resolve complaints from Europeans regarding access to their data by Japanese public authorities. This new mechanism will be administered and supervised by the Japanese independent data protection authority (PPC).

1.4. When will the adequacy decision become applicable?

The European Commission will shortly launch the process leading to the adoption of the adequacy decision under the General Data Protection Regulation. This includes obtaining an opinion from the European Data Protection Board, which brings together all of the national data protection authorities, and the green light from a committee comprised of representatives of the EU Member States. Once this procedure has been completed, the Commission will adopt the adequacy decision. The adequacy decision is therefore expected to be adopted in the last quarter of 2018 and should be applicable shortly after its adoption.

Japan will also launch its relevant internal procedure for the adoption of its adequacy decision.

2. ECJ and responsibility for personal data processing on Facebook fan pages

Tanislav Bednar and Jan Metelka, DLA Piper Prague

In June 2018 the European Court of Justice's Grand Chamber¹ decided on a long awaited case² regarding the responsibility of the administrators of Facebook fan pages, relating to the personal data of visitors to fan pages. The original dispute started in 2011, discussing whether there is any liability of a private organization running a fan page on Facebook. The case itself was in the regime of Directive 95/46/ES³ (the "original directive"), however, as the definitions of data controller and data processor are identical in both the original directive and EU General Data Protection Regulation (GDPR)⁴ the conclusions are fully applicable in the current GDPR regime as well.

In the present case, the German Wirtschaftsakademie collected the data of the fan page visitors, using special tools provided by Facebook itself. The administrator of the fan page (i.e. Wirtschaftsakademie) defined the parameters of the fan page via content targeted specifically to its visitors. The special tools from Facebook equip the fan page administrator with demographic data of the visitors (in anonymized form) and therefore the administrator processes such data concerning the target audience, including age, sex, relationship and occupation, information of lifestyle and geographical data. Based on this data, the administrator may make special offers or organize events, which are better targeted to the "right" audience. Just the mere fact, that the tools are provided by Facebook, does not exempt the administrator of the fan page from his responsibility.

The General Advocate Bot issued a related opinion in October 2017⁵, which stated that the fan page administrator and Facebook were joint controllers. The final decision was even more specific in this respect by stating that amount of the responsibility of both joint controllers is different.

The result of this final June decision is that the fan page administrator is a joint controller responsible for that pro-

¹ See case C-210/16 Request for a preliminary ruling under Article 267 TFEU from the Bundesverwaltungsgericht (Federal Administrative Court, Germany), made by decision of 25 February 2016, received at the Court on 14 April 2016, in the proceedings *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein V Wirtschaftsakademie Schleswig-Holstein GmbH*, interveners: Facebook Ireland Ltd, Vertreter des Bundesinteresses beim Bundesverwaltungsgericht,

² <http://curia.europa.eu/juris/document/document.jsf?text=&docid=202543&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=336916>.

³ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31).

⁴ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, OJ 2016 L 119, p. 1).

⁵ <http://curia.europa.eu/juris/document/document.jsf?text=&docid=195902&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=336916>.

Download English Version:

<https://daneshyari.com/en/article/10225867>

Download Persian Version:

<https://daneshyari.com/article/10225867>

[Daneshyari.com](https://daneshyari.com)