Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

EU update

Kit Burden *

DLA Piper UK LLP, UK

Keywords:
EU law
Intellectual property
Information technology law
Telecommunications law

A B S T R A C T

This is the latest edition of the DLA Piper column on developments in EU law relating to IP, IT and telecommunications. This news article summarizes 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 websites are included where possible. No responsibility is assumed for the accuracy of information contained in these links.

1. Data privacy

Mari Martin, *Trainee, and* **Wiebke Jakob**, *Associate, DLA Piper Munich*

1.1. *New U.S.-EU privacy shield details released*

On February 29, 2016, the European Commission and U.S. Department of Commerce released the highly anticipated details of the new U.S.-EU Privacy Shield programme. According to the materials released, the new programme includes an expanded set of privacy principles, details for increased operational vetting to be conducted by the Commerce Department's International Trade Administration, assurances of enforcement from the Federal Trade Commission (FTC) and the Department of Transportation (DOT), as well details on a new arbitration model.

1.1.1. *EC adequacy determination*

The EU Commission has adopted an implementing decision regarding the adequacy of protection provided by the EU-U.S. Privacy Shield. In its draft decision adopted on February 29, 2016 ("Draft Adequacy Decision"), the EU Commission concluded that for the purposes of Article 25(2) of Directive 95/46/EC, the United States ensures an adequate level of protection for personal data transferred under the EU-U.S. Privacy Shield from the European Union to self-certified organizations in the United States. Such self-certified organizations will be included in the so-called "Privacy Shield List," which will be maintained and made publicly available by the U.S. Department of Commerce.

The new EU Privacy Shield is intended to reflect requirements set out by the European Court of Justice (ECJ) in its ruling in the *Schrems* case on October 6, 2015, which invalidated the existing Safe Harbor Agreement. The ECJ's rejection of Safe Harbor was largely based on potential U.S. government surveillance practices. The Draft Adequacy Decision addresses concerns regarding the use of personal data by U.S. public authorities in Section 3, as follows:

- Clear Limitations on U.S. Public Authorities' Access and Use of Personal Data: The Draft Adequacy Decision states explicitly that the U.S. has given the EU written assurances that the access of public authorities for law enforcement and national security will be subject to clear limitations, safeguards and oversight mechanisms. Specifically, the U.S. government has given the European Commission explicit assurance that the U.S. Intelligence Community "does not engage in indiscriminate mass surveillance of anyone, including ordinary European citizens."

For further information, see: http://www.dlapiper.com/.

* DLA Piper UK LLP, 3 Noble Street, London EC2V 7EE, UK. Tel.: +44 0 8700 111 111; fax: +44 0 20 7796 6666.
E-mail address: kit.burden@dlapiper.com

http://dx.doi.org/10.1016/j.clsr.2016.04.001

- Annual Joint Review: To regularly monitor the functioning of the arrangement, there will be an annual joint review by the European Commission and the U.S. Department of Commerce, which will address the issue of national security access. This meeting will be open for EU DPAs and representatives of the Article 29 Working Party.
- Individual Redress: Any EU data subject concerned that his data has been misused under the new arrangement will have several redress possibilities. Companies must reply to complaints within given deadlines. European DPAs can refer complaints to the Department of Commerce and the Federal Trade Commission. In addition, Alternative Dispute resolution will be free of charge. Further, the Foreign Intelligence Surveillance Act would allow non-U.S. citizens to bring a civil cause of action for money damages against the United States, sue U.S. government officials in their personal capacity for money damages, and challenge the legality of surveillance in the event the U.S. government intends to use or disclose any information obtained or derived from electronic surveillance against the individual in judicial or administrative proceedings in the United States.
- Privacy Shield Ombudsperson: In order to provide for an additional avenue accessible for all EU data subjects, the U.S. government has decided to create a new mechanism, the Privacy Shield Ombudsperson. According to the Draft Adequacy Decision, in particular, according to the binding commitments from the U.S. government, the Privacy Shield Ombudsperson will guarantee that individual complaints are investigated and individuals receive independent confirmation that U.S. laws have been complied with or, in case of a violation of such laws, the non-compliance has been remedied.

1.1.2. *Next steps in the EU*

It is unclear whether EU authorities will agree with the Commission's draft Adequacy Decision. The Commission will now obtain advice from the Article 29 Data Protection Working Party and representative DPAs of Member States, several of which have expressed concerns regarding adequacy of the proposed EU-U.S.-Privacy Shield in the past. It is certain, however, that the Draft Adequacy Decision will be analyzed carefully in any such advice submitted to the Commission.

2. Internet

2.1. *The applicability of EU data protection laws to non-EU businesses*

Carol A.F. Umhoefer, *Partner, and* **Caroline Chancé**, *Associate, DLA Piper France*

On December 16, 2015, the Article 29 Data Protection Working Party ("WP29") updated their Opinion 8/2010[1] on applicable law in light of the landmark decision *Costeja v. Google*[2] rendered by the Court of Justice of the European Union ("ECJ") on 13 May 2014.

In a context where local data protection authorities are increasingly scrutinizing cross-border data processing operations, companies worldwide need to identify whether and which EU data protection law(s) apply to processing of personal data taking place wholly or partially outside the EU.

Yet the extent of the territorial scope of the Directive has always raised many questions. In 2010, the WP29 concluded in their Opinion 8/2010 that Article 4(1)(a) of the Data Protection Directive 94/46/EC[3] ("Directive"), which provides that a Member State's data protection law shall apply to data processing "*carried out in the context of the activities of an establishment of the controller on the territory of the Member State*", suggests a very broad scope of application.

The exact extent of application remained rather unclear despite the WP29's guidelines until four years later when the question of whether EU data protection laws should apply to a business based and processing personal data outside the EU came up before the ECJ in the so-called "right to be forgotten" case, *Costeja v. Google*. In its judgment, the ECJ held that Spanish law applied to the personal data processing performed by the search engine operated by Google Inc., a US-based controller, on the ground that it was "*inextricably linked to*", and therefore was carried out "*in the context of the activities of*" Google Spain, whose advertising and commercial activities constituted the "*means of rendering the search engine at issue economically profitable*".

The WP29 have recently updated their 2010 opinion to take into account *Costeja*. According to the WP29, the implications of the judgment are very broad and should certainly not be limited to the question of determining applicable law in relation to the operation of the Google search engine in Spain. And indeed, *Costeja* confirms the broad territorial application of Article 4(1)(a) of the Directive that was espoused by the W29 in 2010. In this respect, the WP29 recall that the notion of establishment in itself must be interpreted broadly, in line with recital 19 of the Directive, which provides that the notion of "*establishment (. . .) implies the effective and real exercise of activity through stable arrangements*",[4] such as subsidiaries or branches for example. In *Costeja*, there was no doubt that Google Spain, the Google Inc. subsidiary responsible for promoting in Spain the sale of advertising space generated on the website google.com, fell under that definition. However, it was disputed whether the data processing in question, carried out exclusively by Google Inc. by operation of Google Search without any intervention on the part of Google Spain, was nevertheless carried out "*in the context of the activities of*" Google Spain.

The ECJ then introduced a new criterion: the "*inextricable link*" between the activities of a local establishment and the data processing activities of a non-EU data controller. As underlined by the WP29, the key point is that even if the local establishment is not involved in any direct way in the data processing, the activities of that establishment might still trigger

[1] WP29, Opinion 8/2010 on applicable law, December 16, 2010.

[2] Case C-121/12, Google Spain and Google Inc. v. Agencia Espanola de Protección de Datos (AEPD) and Mario Costeja Gonzalez, May 13, 2014.

[3] Directive 95/46/EC of the European Parliament and of the Council of October 24, 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[4] Recital 19 of the Directive.