DATA PROTECTION IN THE INTERNET: A EUROPEAN UNION PERSPECTIVE

Pedro A. DE MIGUEL ASENSIO *

Published in:

Data Protection in the Internet

D. Moura Vicente and
S. de Vasconcelos Casimiro (eds.),

Springer, 2020, pp. 457-477

ISBN: 978-3-030-28048-2

* Catedrático de Derecho internacional privado
Facultad de Derecho
Universidad Complutense de Madrid
E- 28040 MADRID
pdmigue@der.ucm.es

Pedro A. De Miguel Asensio, "Data Protection in the Internet:
A European Union Perspective", *Data Protection in the Internet*, D. Moura Vicente and
S. de Vasconcelos Casimiro (eds.), Springer, 2020, pp. 457-477

DATA PROTECTION IN THE INTERNET: A EUROPEAN UNION PERSPECTIVE

Pedro A. DE MIGUEL ASENSIO*

Contents

Abstract

A general overview of European Union law concerning data protection in the Internet is provided with a view to facilitate comparison with the regulatory framework in other relevant jurisdictions. The entry into force of the new General Data Protection Regulation has brought about significant changes in EU law. The new Regulation has become a particularly influential piece of legislation regarding Internet activities even beyond the EU. It has also triggered an intense debate about the challenges posed by the EU approach to the protection of personal data and its enforcement. Other EU instruments relevant in the field and the case law of the Court of Justice interpreting legislation on data protection law are also discussed.

* Chair Professor, Complutense University of Madrid. Research Project DER 2015-64063 (MINECO/FEDER).

1. General data protection framework

1.1 Regulation (EU) 2016/679

The general framework on Data Protection in the EU is established in 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 or GDPR)[1]. Pursuant to Article 99, the Regulation shall apply from 25 May 2018 and Directive 95/46/EC is repealed with effect from the same date. The GDPR shares the main objectives and principles of Directive 95/46/EC[2] but establishes a more detailed set of rules which are directly applicable in all Member States to prevent fragmentation in the implementation of data protection across the Union and to ensure a uniform high level of protection in all Member States. In contrast with the mere harmonization of national laws under Directive 95/46/EC, the GDPR establishes a one single set of rules for the Union.

The GDPR applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system [art. 2(1)].[3] The GDPR does not apply to personal data of deceased persons are not governed by the GDPR. Moreover, the GDPR does not cover the processing of personal data which concerns legal persons, such as undertakings established as legal persons. However, the fact that information concerning natural persons is provided as part of a professional activity does not mean that it cannot be characterised as personal data.[4]

The GDPR does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity [art. (2)(2)(c)]. This exception covers only activities that are carried out in the context of the private or family life of individuals. The CJEU has held that such an exception does not relate to the processing of personal data consisting in publication on the internet so that those data are made accessible to an

[1] OJ L 119, 4.5.2016, p. 1. For an initial general overview of the GDPR, see De Hert and Papakonstantinou (2016), Härting (2016), Paal and Pauly (2017) and Albrecht and Jotzo (2017).
[2] 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 L 281, 23.11.1995, p. 31).
[3] The free movement of personal data within the EU granted by GDPR is intended to be complemented by a new Regulation on a framework for the free flow of non-personal, see the Proposal of 13 September 2017 by the Commission at COM(2017) 495 final.
[4] *See* Judgments of the CJEU of 16 July 2015, *ClientEarth and PAN Europe v EFSA*, C-615/13 P, EU:C:2015:489, para. 30; and of 9 March 2017, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v Salvatore Manni*, ECLI:EU:C:2017:197, para. 34.

indefinite number of people.[5] Moreover, the CJEU has ruled that door-to-door preaching by members of a religious community is not a purely personal or household activity because the preaching extends beyond the private sphere of a member of a religious community who is a preacher.[6]

The GDPR does not apply to the processing of personal data in the course of activities which fall outside the scope of Union law, such as activities concerning national security, or to the processing of personal data by competent authorities for the purposes of the prevention or prosecution of criminal offences (see this chapter, section 3.4, infra). The GDPR does not apply to matters concerning the processing of personal data in connection with the provision of publicly available electronic communications services in public communication networks in the Union in relation to matters for which they are subject to specific obligations (see this chapter, section 3, infra). Moreover, the processing of personal data by the Union institutions is governed by Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000.[7] This Regulation contains measures with regard to the processing of personal data by the Union institutions and the free movement of such data. It is based on the same principles that the general framework on data protection in EU law.

The Court of Justice of the European Union (CJEU) has developed a significant body of case law regarding the interpretation of the EU instruments in the field of data protection law, founded on the basic idea that the general framework on Data Protection in EU Law seeks to ensure a high level of protection of the fundamental rights and freedoms of natural persons, in particular their right to privacy, with respect to the processing of personal data.[8]

Furthermore, an independent European advisory body on data protection and privacy, composed of a representative of the supervisory authority of each Member State, the European Data Protection Supervisor and a representative of the Commission, has played a very significant. The so-called Working Party on the Protection of Individuals with regard to the Processing of Personal Data set up under Article 29 of Directive 95/46/EC has become particularly influential in the interpretation, application and evolution of EU Data Protection Law by means of the opinions and other documents.[9] As of 25 May 2018 the Article 29 Working Party ceased to exist and was replaced by the European Data

[5] Judgment of the CJEU of 6 November 2003, *Bodil Lindqvist*, C-101/01, ECLI:EU:C:2003:596, para. 47.
[6] Judgment of the CJEU of 10 July 2018, *Jehovan todistajat*, C-25/17, ECLI:EU:C:2018:551, para. 50.
[7] OJ L 8, 12.1.2001, p. 1.
[8] *See, e.g.*, Judgment of the CJEU of 13 May 2014, rendered in case C-131/12, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, ECLI:EU:C:2014:317, para. 66 with further references.
[9] Available at http://ec.europa.eu/justice/article-29/documentation/index_en.htm.

Protection Board (EDPB)[10] established under the GDPR. The EDPB is composed of the head of one supervisory authority of each Member State and of the European Data Protection Supervisor [Art. 68(3) GDPR].

1.2. The concept of personal data and data protection as fundamental right

For the purposes of the GDPR, personal data means: "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person" [Art. 4(1)GDPR]. The case-law of the CJEU has confirmed that the concept of personal data encompasses IP addresses[11].

The protection of natural persons in relation to the processing of personal data is considered a fundamental right under EU law.[12] Article 8(1) of the Charter of Fundamental Rights of the European Union ('the Charter') and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her. The CJEU had previously made clear that Union data protection law establish a specific and reinforced system of protection compared with the right to privacy[13] which is laid down in Article 7 of the Charter. Notwithstanding this, both the CJEU and the European Court of Human Rights (EUCtHR) tend to treat data protection as closely related to the right to privacy. It is noteworthy that the European Convention on Human Rights (ECHR) has no corresponding provision to Article 8 of the Charter which addresses specifically the fundamental right to data protection and provides that personal data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or on some other legitimate basis laid down by law. In the absence of a similar provision, the ECtHR has derived the right of data protection from Article 8 of the ECHR on the

[10] https://edpb.europa.eu/.

[11] *See* Judgment of the CJEU of 19 October 2016, case C-581/14, *Patrick Breyer v Bundesrepublik Deutschland*, ECLI:EU:C:2016:779, establishing that Article 2(a) of Directive 95/46/EC "must be interpreted as meaning that a dynamic IP address registered by an online media services provider when a person accesses a website that the provider makes accessible to the public constitutes personal data within the meaning of that provision, in relation to that provider, where the latter has the legal means which enable it to identify the data subject with additional data which the internet service provider has about that person". Furthermore, *see* Judgments of the CJEU of 8 April 2014, *Digital Rights Ireland and Seitlinger*, Joined Cases C-293/12 and C-594/12, ECLI:EU:C:2014:238, para. 26; and of 21 December 2016, *Tele2 Sverige AB and Secretary of State for the Home Department*, Joined Cases C-203/15 and C-698/15, ECLI:EU:C:2016:970, para 98. See also Judgment of the ECtHR of 24 April 2018, *Benedik v. Slovenia*, (app. no. 62357/14) regarding dynamic IP addresses.

[12] See on this matter González Fuster (2014).

[13] Judgment of the CJEU of 29 June 2010, *Comisión/Bavarian Lager*, C-28/08 P, ECLI:EU:C:2010:378.

right to privacy.[14] From the perspective of EU law, it can be considered that both rights are closely linked and overlap to a significant extent but differences in their respective scopes may also be identified. For instance, EU legislation on data protection is limited to information relating to natural persons but the right to privacy encompasses legal persons.[15]

The CJEU has constantly held that EU Data Protection Law, in so far as it governs the processing of personal data liable to infringe fundamental freedoms, must necessarily be interpreted in the light of the fundamental rights guaranteed by the Charter[16] (and the case-law cited). Given the position of data protection law as a fundamental right the case-law of the CJEU on the balancing of the fundamental right to data protection with others, such as the protection of intellectual property, the fundamental freedom to conduct a business enjoyed by Internet intermediaries[17], has become particularly significant.

1.3. Special categories of personal data

The GDPR subjects the processing of special categories of personal data, which are particularly sensitive and create significant risks, to reinforced protection in addition to the general rules of the Regulation for lawful processing. Pursuant to Article 9 of the GDPR, such special categories encompass: "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership" as well as "genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation". Article 4 of the GDPR provides definitions of the terms 'genetic data', 'biometric data' and 'data concerning health' relevant for these purposes.

The processing of the special categories of data listed in Article 9(1) is prohibited unless one of the exceptions laid down in Article 9(2) applies: express consent by the data subject to the extent that the prohibition may be lifted; processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law; processing is necessary to protect the vital interests of the data subject; processing is

[14] See Judgments of the ECtHR of 16 February 2000, *Amann v Switzerland*, App. no. 27798/95, para. 65; and 4 May 2000, *Rotaru v Romania*, App. No. 28341/95, para. 43, available at http://hudoc.echr.coe.int.
[15] J. Kokott and C. Sobotta, «The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR», *International Data Privacy Law* (*IDPL)*, vol. 3(4), 2013, pp. 222-228, p. 225.
[16] *See* Judgment of the CJEU of 6 October 2015, C-362/14, *Schrems v. Data Protection Commissioner*, ECLI:EU:C:2015:6506, para. 38, with further references.
[17] See, e.g., Judgments of the CJEU of 24 November 2011, *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, C-70/10, ECLI:EU:C:2011:771; of 16 February 2012, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV*, C-360/10, ECLI:EU:C:2012:85; and 19 April 2012, *Bonnier Audio and Others v Perfect Communication Sweden AB*,, C-461/10, ECLI:EU:C:2012:219.

carried out in the course of its legitimate activities with appropriate safeguards by a foundation or any other not-for-profit body with a political, philosophical, religious or trade union aim; processing relates to personal data which are manifestly made public by the data subject; processing is necessary for the establishment, exercise or defence of legal claims; processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law… Furthermore, the GDPR allows Member States to maintain or introduce further conditions with regard to the processing of genetic data, biometric data or data concerning health.

The GDPR imposes similar obligations with regard to the processing of personal data on public actors and private parties. However, public authorities to which personal data are disclosed in accordance with a legal obligation for the exercise of their official mission are not regarded as recipients if they receive personal data which are necessary to carry out a particular inquiry in the general interest, in accordance with Union or Member State law [Article 4(9) GDPR].

1.4 Supervisory authorities

Under the GDPR, the establishment of supervisory authorities in Member States, empowered to perform their tasks and exercise their powers with complete independence, is an essential component of the protection of natural persons with regard to the processing of their personal data. Member States are able to establish more than one supervisory authority to reflect their constitutional and organisational structure (art. 51 GDPR). Each supervisory authority is competent on the territory of its own Member State. Unlike the previous regime[18], the provisions of the Regulation on its territorial scope (Art. 3 GDPR) do not determine the competent national supervisory authority. The Regulation includes specific provisions on the distribution of competences between the supervisory authorities of the Member States with regard to cross-border situations. The GDPR introduces the so-called one-stop-shop mechanism that ensure that one national data protection authority (DPA) is responsible for the supervision of cross-border data operations carried out by a controller or processor in the EU. The GDPR establishes a consistency mechanism for cooperation between the national supervisory authorities.

With a view to guarantee consistent enforcement of the GDPR throughout the Union, the supervisory authorities have in each Member State the same powers. The tasks of the DPAs are listed in Article 57 of the GDPR and the powers are dealt with in Article 58. The tasks include to monitor and enforce the application of the Regulation; promote

[18] CJEU Judgment of 1 October 2015 in case C-230/14, *Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság*, ECLI:EU:C:2015:639 and CJEU Judgment of 5 June 2018 in case C-210/16, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH*, ECLI:EU:C:2018:388.

public awareness on data protection issues; perform advisory functions; handle complaints lodged by a data subject; conduct investigations on the application of the Regulation… The powers of the supervisory authorities are classified in Article 58 in three main groups: investigative powers (such as request and obtain access to information an premises, carry out data protection audits, notify alleged infringements); corrective powers (including to issue warnings and reprimands, order to comply with a data subject's request, to impose a limitation including a ban on processing or to impose an administrative fine); and authorisation and advisory powers (such as to issue opinions, to issue certifications or to adopt certain authorisations). Supervisory authorities are empowered to bring infringements of the GDPR to the attention of the judicial authorities and engage in legal proceedings. The exercise of the powers conferred on the supervisory authority are subject to effective judicial remedy and due process.

2. Personal data processed by electronic means

2.1. Main principles

The general legislative framework established in the GDPR applies also to the protection of personal data in the context of services provided at a distance, by electronic means. It covers the processing of personal data wholly or partly by automated means [Arts. 2(1)], including the collection, recording, structuring, storage, alteration, retrieval, consultation, use, disclosure and making available of such data [Art. 4(2)]. Therefore, the GDPR applies to the protection of personal data in social networks.[19] As regards Internet intermediaries, it is noteworthy that pursuant to article 2(4) the GDPR is without prejudice to the application of Directive 2000/31/EC on electronic commerce[20], in particular of the rules on the limitation of liability of intermediary service providers laid down in Articles 12 to 15 of that Directive. However, the latter provisions do not establish rules on the protection of personal data.[21]

The processing of personal data is only deemed lawful on the basis of at least one of the grounds listed in Article 6 GDPR: (a) the data subject has given consent to the processing of his or her personal data for specific purposes; (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; (c) processing is necessary for

[19] See, e.g., Article 29 Working Party on Data Protection, Opinion 5/2009 on online social networking, WP 163, adopted on 12 June 2009.
[20] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') (OJ L 178, 17.7.2000, p. 1).
[21] De Miguel Asensio (2015) pp. 218-383.

compliance with a legal obligation to which the controller is subject; (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person; (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority; (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights of the data subject.

Where processing is based on the data subject's consent, the controller has to be able to demonstrate that consent has been given [Art. 7(1) GDPR]. Consent is not be regarded as freely given if the data subject is unable to refuse consent without detriment. Consent requires a clear affirmative act by the data subject establishing a freely given, specific, informed and unambiguous indication of his or her agreement to the processing of personal data. Therefore, Recital 32 to the GDPR acknowledges that consent may be given by electronic means, such as by ticking a box when visiting an internet website or choosing technical settings for information society services. However, pre-ticked boxes or inactivity are not regarded as appropriate since they do not clearly indicate the data subject's acceptance.

The principles of transparency and fair processing require that the data subject be informed of the purposes of the processing. Under the GDPR the specific purposes for which personal data are processed have to be explicit and determined at the time of the collection of the personal data. Otherwise consent by the data subject can not be regarded as informed. Consent is to be given for all purposes in those situations where processing has multiples purposes. The processing has to be restricted to personal data which are adequate and relevant and limited to what is necessary for the purposes for which they are processed. Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means.

2.2. Minors

Article 8 of the GDPR provides for special conditions regarding child's consent in relation to information society services. As noted in the Preamble, such specific protection applies, in particular, to the use of personal data for the purposes of marketing or creating personality or user profiles of children and the collection of personal data when using services offered directly to a child (Recital 38). Where processing is based on the consent given by the data subject, the processing of data of children below the age of 16 years is only deemed lawful to the extent that consent is given or authorised by the holder of parental responsibility over the child. Member States are granted certain discretion in this regard, since they may provide by law for a lower age provided that it is not below 13 years. Furthermore, in those situations controllers are under a "reasonable efforts"

obligation to verify that consent is given by the holder of parental responsibility over the child, taking into consideration available technology.

2.3. Right to erasure and right to object

Article 17 of the GDPR is devoted to the right to erasure, also known as the 'right to be forgotten', which was admitted under Directive 95/46/EC by the CJEU in its landmark judgment in the *Google Spain* case.[22] Data subjects are granted the right to obtain from the controller the erasure of personal data concerning him or her without undue delay where one of the following grounds applies: data are no longer necessary in relation to the purposes for which they were collected or processed; the data subject withdraws consent on which the processing is based and there is no other legal ground for the processing; the data subject objects to the processing of the data and there are no overriding legitimate grounds for the processing; the data have been unlawfully processed; the data have to be erased for compliance with a legal obligation to which the controller is subject; the data have been collected in relation to the offer of information society services directly to a child.

However, the obligation of the controller to erase the personal data does not apply to the extent that processing is necessary for any of the grounds listed in Article 17 GDPR. Such grounds include: exercising the right of freedom of expression and information; for compliance with a legal obligation or for the performance of a task carried out in the public interest or in the exercise of official authority; for reasons of public interest in the area of public health; for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes; or for the establishment, exercise or defence of legal claims. The CJEU has held that the right to be forgotten cannot be generally applied to a company register.[23]

Article 21 of the GDPR grants data subject the right to object at any time to processing of personal data concerning him or her for direct marketing purposes, which includes profiling to the extent that it is related to such direct marketing. Moreover, the legislation on the protection of personal data in electronic communications regulates the conditions under which under which unsolicited communications for direct marketing may be conducted. The proposed new ePrivacy Regulation (see this chapter, section 3.1, *infra*) applies to persons who use electronic communications services to send direct marketing

[22] CJEU Judgment of 13 May 2014, case C-131/12, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, ECLI:EU:C:2014:317. See Article 29 Working Party on Data Protection, «Guidelines on the Implementation of the CJEU Judgment on "Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" C-131/12», 26 November 2014.

[23] CJEU Judgment of 9 March 2017, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v Salvatore Manni*, ECLI:EU:C:2017:197, paras 55-56.

commercial communications, including advertising messages sent by political parties and non-profit organisations. The safeguards provided for by the ePrivacy Regulation to protect end-users against unsolicited communications for direct marketing purposes are to be found in Article 16 of the Proposal.

The ePrivacy Regulation is based on an opt-in approach. Commercial electronic communications for direct marketing purposes may only be sent to end-users who are natural persons that have given their consent. As an exception, the use of e-mail contact details within the context of an existing customer relationship is allowed for the offering of similar products or services, provided that customers are clearly given the opportunity to object. Moreover, end-users that have provided their consent to receiving unsolicited communications for direct marketing purposes are enabled to withdraw their consent at any time in an easy manner. To facilitate effective enforcement of the rules on unsolicited messages for direct marketing, the masking of the identity and the use of false identities and the use of false return addresses are prohibited. Unsolicited marketing communications are required to be clearly recognizable as such. They have to indicate the identity of the person transmitting the communication or on behalf of whom the communication is transmitted and provide the necessary information for recipients to exercise their right to oppose to receiving further marketing messages. A link or an email address has to be provided to end-users so that they can easily withdraw their consent.

2.4. Processing of personal data in the context of employment

The ePrivacy Regulation does not include specific provisions on the processing of personal data of employees through electronic means. The general data protection framework applies to the processing of personal data in the context of employment with some additional provisions laid down in Article 88 of the GDPR. Processing personal data in the field of employment law is one of the grounds that allow derogating from the prohibition on processing special categories of personal data (see this chapter, section 1.3, supra).

According to Article 88 of the GDPR, Member State law or collective agreements may provide for specific rules on the processing of employees' personal data in the employment context, in particular for the conditions under which personal data in the employment context may be processed. Those rules shall include suitable and specific measures to safeguard the data subject's human dignity, legitimate interests and fundamental rights.

2.5. Data security and data breach

The basic storage limitation in the GDPR is applicable to data conveyed and stored through electronic means. Pursuant to Article 5(1)(e) of the GDPR a basic principle relating to the processing of personal data is that such data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. At the time when personal data are obtained, the controller is obliged to provide the data subject information regarding the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period. Moreover, pursuant to Article 25 of the GDPR the controller is under an obligation to implement measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed, including the period of their storage. Furthermore, pursuant to Article 32, the controller and the processor are obliged to implement technical and organisational measures, such as encryption, to ensure a level of security appropriate to the risks inherent in the processing. Such risks include accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted or stored.

The GDPR establishes specific obligations on controllers to notify a personal data breach to the supervisory authority (art. 33) and to the data subject (art. 34). A definition of 'personal data breach' is provided for in Article 4(12) of the GDPR. It means a "breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed".

An obligation is imposed on the controller to notify the personal data breach to the supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the controller is able to demonstrate that the breach is unlikely to result in a risk to the rights and freedoms of natural persons. Such notification shall include information on the nature of the breach including where possible, the categories and approximate number of data subjects and personal data records concerned; the likely consequences of the breach; and the measures taken or proposed to be taken by the controller. The obligation of the controller to communicate the personal data breach to the data subject without undue delay applies to the situations where the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

2.6. Codes of conduct

The drawing up and approval of codes of conduct in the field of data protection and certification mechanisms in this area are regulated in detail in Article 40 to 43 of the GDPR. Associations and bodies representing controllers or processors are encouraged to

draw up codes of conduct in order to facilitate the effective application of the Regulation. The main goal of such codes of conduct is to specifying the application of the data protection legislation on issues such as fair and transparent processing; the interests pursued by controllers in specific contexts; the collection of personal data; the information provided to data subjects; the exercise of the rights of data subjects; the international transfer of personal data; or alternative dispute resolution procedures for resolving disputes between controllers and data subjects with regard to processing. Draft codes of conducted submitted by associations and other bodies may be approved by the competent supervisory authority if it finds that it provides sufficient appropriate safeguards. Such codes are registered and published by the competent supervisory authority. The Commission may decide that an approved code of conduct which relates to processing activities in several Member States has general validity within the Union. The monitoring of compliance with a code of conduct may be carried out by a body which is accredited for that purpose by the competent supervisory authority.

The GDPR encourages associations or other bodies representing categories of controllers or processors to draw up codes of conduct to facilitate the effective application of the Regulation and calibrate the obligations of controllers and processors. Pursuant to Article 40 of the GDPR, the drafting of such codes is deemed of particular interest to take account the specific characteristics of the processing carried out in certain sectors and the specific needs of micro, small and medium enterprises. Relevant stakeholders, including data subjects, should be consulted in the process of adopting a code of conduct. Where a draft code of conduct relates to processing activities in several Member States, it may be submitted to a procedure at European level that can lead to a decision by the Commission establishing that an approved code of conduct has general validity within the Union. The Commission shall ensure appropriate publicity for such codes [Article 40(10) GDPR].

In the previous practice of the Article 29 Working Party, a reference can be made to Opinion 4/2010 on the European code of conduct of FEDMA for the use of personal data in direct marketing[24] and to Opinion 02/2015 on C-SIG Code of Conduct on Cloud Computing[25], concluding that the code provided important guidance to cloud computing providers with regard to applicable data protection and privacy rules in Europe, but could not be formally approved, since it did not always meet the minimal legal requirements, and its added value with respect to Directive 95/46/EC and national legislation was not always clear.

[24] WP 174, adopted on 13 July 2010.
[25] WP 232, adopted on 22 September 2015.

The establishment of certification mechanisms and data protection seals and marks are also encouraged under the GDPR to promote transparency by allowing data subjects to easily assess the level of data protection of products and services.

3. Data protection in the electronic communications sector

3.1. From the ePrivacy Directive to the ePrivacy Regulation

Since the content and metadata of electronic communications may reveal sensitive information about the persons involved, the EU has traditionally adopted special legislation concerning data protection for users of electronic communications services. Previously that special regime was contained in the so-called ePrivacy Directive or Directive 2002/58/EC.[26] In order to ensure consistency with the new GDPR and to adapt the previous regime to the technological and market evolution, Directive 2002/58/EC was intended to be replaced with effect from 25 May 2018 by a the new ePrivacy Regulation. However, pending the final approval of the new Regulation, the current survey is based on the Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) of 10 January 2017 (ePrivacy Regulation)[27].

The e-Privacy Regulation is regarded as *lex specialis* to the GDPR. It particularises and complements the general rules on the protection of personal data laid down in the GDPR as regards electronic communications data that qualify as personal data (Recital 6 of the ePrivacy Regulation). All matters concerning the processing of personal data not specifically addressed by the ePrivacy Regulation are covered by the GDPR as the general legal framework in the field. It is noteworthy that the e-Privacy Regulation applies to both natural and legal persons who are end users of electronic communications.

3.2. Scope of application

The scope of application of the ePrivacy Regulation is very much influenced by its close connection to the EU regulatory framework for electronic communications. The ePrivacy Regulation covers electronic communications data processed in connection with the provision and use of electronic communications services in the Union. It applies to providers of electronic communications services, to providers of publicly available

[26] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37).
[27] COM(2017) 10 final.

directories, to software providers permitting electronic communications, and to persons who use electronic communications services to send direct marketing commercial communications or collect information related to or stored in end-users' terminal equipment.

The ePrivacy Regulation relies on the definition of 'electronic communications services' provided for by the proposal for a Directive establishing the European Electronic Communications Code.[28] Such an approach is intended to ensure an equal protection of end-users when using functionally equivalent services, for instance, traditional text messages (SMS) and electronic mail conveyance services and new messaging services and web-based e-mail services. Therefore, the definition of 'electronic communications services' encompasses not only internet access services –including wireless networks provided to an undefined group of end-users in public and semi-private spaces- and services consisting wholly or partly in the conveyance of signals, but also interpersonal communications services, such as voice over IP, messaging services and web-based e-mail services. The ePrivacy Regulation covers as well interpersonal communications services that are ancillary to another service and have a communication functionality. Moreover, it applies to the transmission of machine-to-machine communications since it is intended to ensure the protection of privacy and confidenciality with regard to the Internet of Things. Electronic communications services which are not publicly available are not included.

Electronic communications data are defined in Article 4 of the ePrivacy Regulation in a broad and technological neutral way. It encompasses any information concerning the content transmitted and the information concerning an end-user processed for the purposes of transmitting, distributing or enabling the exchange of electronic communications content; including data to trace and identify the source and destination of a communication, geographical location and the date, time, duration and the type of communication. Therefore, electronic communications metadata are covered by the Regulation.

3.3. Legal framework

The basic rule is provided for in Article 5 of the ePrivacy Regulation which establishes that electronic communications data shall be confidential and prohibits any interference with electronic communications data, such as by listening, monitoring or any kind of interception or processing of electronic communications data, by persons other than the end-users, except when permitted by the Regulation. Article 6 of the ePrivacy Regulation

[28] Commission proposal for a Directive of the European Parliament and of the Council establishing the European Electronic Communications Code (Recast) (COM/2016/0590 final - 2016/0288 (COD)).

establishes the restrictive conditions under which providers of electronic communications networks and services may process electronic communications data (6.1), electronic communications metadata (6.2) and electronic communications content (6.3). Moreover, pursuant to Article 7 of the ePrivacy Regulation providers of electronic communications services are under strict obligations to erase electronic communications content and metadata or make that data anonymous when it is no longer needed for the purpose of the transmission of a communication or billing.

Providers of electronic communications services are obliged to inform end-users of measures they can take to protect the security of their communications, such as using specific types of software or encryption technologies. Moreover, they are also obliged to take, at their own costs, appropriate and immediate measures to remedy any new, unforeseen security risks and restore the normal security level of the service. Pursuant to article 10 of the ePrivacy Regulation, software placed on the market permitting electronic communications shall offer the option to prevent third parties from storing information on the terminal equipment of an end-user or processing information already stored on that equipment. Upon installation, the software shall inform the end-user about the privacy settings options and, to continue with the installation, require the end-user to consent to a setting. Additionally, specific obligations on the protection of information stored in and related to end-users' terminal equipment are laid down in Article 8. The use of processing and storage capabilities of terminal equipment, the collection of information from end-users' terminal equipment and the collection of information emitted by terminal equipment to enable it to connect are prohibited except on the grounds provided for in Article 8(1) and (2).

The enforcement of the provisions of the ePrivacy Regulation is entrusted to the same authorities competent for the enforcement of the GDPR (see this chapter, section 1.4, supra). The tasks and powers of those supervisory authorities are also basically those established in the GDPR, but they have the additional task of monitoring the application of the ePrivacy Regulation regarding electronic communications data for legal entities. The ePrivacy Regulation confirms expressly the power of each supervisory authority to impose penalties including administrative fees for any infringement of the Regulation and indicates infringements and the upper limit and criteria to be followed by the supervisory authority when setting administrative fines. According to Article 23, infringements of the principle of confidentiality of communications, permitted processing of electronic communications data, time limits for erasure pursuant are subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

3.4. Digital forensics

The ePrivacy Regulation contains provisions on the protection of electronic communications of natural and legal persons and of information stored in their terminal equipment. Such provisions include rules on the confidentiality of electronic communications data, permitted processing of electronic communications data, and storage and erasure of electronic communications data and protection of information stored in and related to end-users' terminal equipment. However, the ePrivacy Regulation does not apply to the activities of competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security [Art. 2(2)(d)].

The ePrivacy Regulation does not include any specific provisions in the field of data retention. In line with Article 23 of the GDPR, Article 11 of the ePrivacy Regulation provide for the possibility for the Union or Member States under specific conditions to restrict by law certain obligations and rights to safeguard specific public interests, including national security, defence, public security and the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security and other important objectives of general public interest, or a monitoring, inspection or regulatory function connected to the exercise of official authority for such interests. In sum, the ePrivacy Regulation does not affect the ability of Member States to create national data retention frameworks and to carry out lawful interception of electronic communications, in accordance with the Charter[29] and the ECHR[30].

[29] *See* Judgment of the CJEU of 8 April 2014, *Digital Rights Ireland and Seitlinger*, Joined Cases C-293/12 and C-594/12, ECLI:EU:C:2014:238, on the invalidity of Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC. Additionally, *see* Judgment of the CJEU of 21 December 2016, joined cases C-203/15 and C-698/15, *Tele2 Sverige AB v Secretary of State for the Home Department*, ECLI:EU:C:2016:970. For instance, the latter considered that the equivalent to Article 11 in the previous version of the ePrivacy Regulation (Art. 15 of Directive 2002/58) read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, precluded national legislation which, for the purpose of fighting crime, provides for general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication. Additionally, the Court established that those provisions precluded national legislation governed access of the national authorities to the retained data, where the objective pursued by that access, in the context of fighting crime, is not restricted solely to fighting serious crime, where access is not subject to prior review by a court or an independent administrative authority, and where there is no requirement that the data concerned should be retained within the European Union.

[30] See Judgment of the ECtHR of 13 September 2018, *Big Brother Watch and Others v. The United Kingdom* (Apps. nos. 58170/13, 62322/14 and 24960/15).

At EU level the basic instrument providing common rules for the processing of the personal data of individuals involved in criminal proceedings is Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA[31]. It entered into force on 5 May 2016 and it has to be transposed into national law by Member States by 6 May 2018.

Directive (EU) 2016/680 is aimed at ensuring a consistent and high level of protection of the personal data of natural persons and facilitating the exchange of personal data between competent authorities of Members States. It focuses in strengthening the rights of data subjects and of the obligations of those who process personal data. A criminal offence within the meaning of Directive (EU) 2016/680 is an autonomous concept of Union law and it is not limited to crimes committed through electronic means. The Directive applies to the processing of personal data wholly or partly by automated means, and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

EU Data Protection Law and particularly the GDPR, the ePrivacy Regulation and Directive (EU) 2016/680 do not apply to the processing of personal data related to activities which fall outside the scope of Union law, such as those concerning national security and defence. Hence, the processing of personal data by the Member States when carrying activities concerning national security are not covered by those instruments.

4. Remedies and international dimension of EU law

4.1 Remedies and sanctions

EU Data Protection Law grants significant corrective powers to supervisory authorities which are empowered, among others, to issue warnings and reprimands to controllers and processors; to impose a temporary or definitive limitation including a ban on processing; and to impose administrative fines [see, particularly, Article 58(2) of the GDPR]. Data subjects are granted the right to lodge a complaint with a supervisory authority (art. 77 GDPR); to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them (art. 78 GDPR); and the right to an effective judicial remedy where the rights of the subject under the GDPR have been infringed (art. 78 GDPR). The latter is particularly relevant with respect to the right to

[31] OJ L 119, 4.5.2016, p. 89.

receive compensation from the controller or processor for the damage suffered which is granted to any data subject who has suffered material or non-material damage as a result of an infringement of the GDPR (art. 82).

Article 83 GDPR establishes the general conditions under which the supervisory authorities of the Member States shall impose administrative fines in respect of infringements of the Regulation, including the general data protection rules, activities in the context of services provided by electronic means, the electronic processing of personal data of employees, the security of personal data processed by electronic means. Concerning the protection of personal data in the context of electronic communications for marketing purposes, it is to be noted that the ePrivacy Regulation establishes that in principle the relevant provisions of the GDPR are also applicable to infringements of the ePrivacy Regulation and includes specific provisions with similarities regarding the right to compensation and liability (Article 22); and the general conditions for imposing administrative fines (Article 23).

Article 83 GDPR envisages the imposition of administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher. Such fines may be imposed, for example, in case of infringement of: the basic principles for processing, including conditions for consent; the data subjects' rights; or transfer of personal data to third countries. The maximum limit of fines is the same in Article 23 of the ePrivacy Regulation and applies to infringements of the principle of confidentiality of communications, permitted processing of electronic communications data and certain time limits for erasure.

EU Law does not provide for criminal sanctions but it establishes that Member States shall lay down the rules on other penalties applicable to infringements of data protection law, particularly for infringements which are not subject to administrative fines [see Article 84 GDPR, Article 24 ePrivacy Regulation; and Article 57 Directive (EU) 2016/680].

4.2. Territorial reach of EU data protection law

The territorial scope of the GDPR is governed by Article 3.[32] First, the GDPR applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not [Article 3(1)]. The GDPR maintains a broad concept of establishment in line with the case law of the CJEU regarding the previous

[32] De Miguel Asensio (2017) pp. 78-86. On some concerns raised by the territorial reach of EU Data Protection Law, see Svantesson (2013) pp. 89-111.

regime.[33] Establishment implies the effective and real exercise of activity through stable arrangements regardless of the legal form (branch, subsidiary…) of such arrangements (Recital 22). According to the guidance provided by the CJEU in its *Google Spain* judgment, the processing of personal data can be regarded as carried out "in the context of the activities of an establishment" where the activities of a processor not established in the Union, such as a provider of a search engine or social network service, are inextricably linked those of its establishment situated in the Member State concerned.[34]

Second, the GDPR applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behaviour as far as their behaviour takes place within the Union. [Article 3(2)]. Recital 23 of the GDPR clarifies that in order to determine whether goods or services are being offered to data subjects who are in the Union, it should be ascertained whether it is apparent that the controller or processor envisages offering services to data subjects in one or more Member States in the Union. The mere accessibility of a website in the Union or the use of a language generally used in the third country where the controller is established is not regarded as sufficient to ascertain such intention, but factors such as the use of a language or a currency generally used in one Member State or the mentioning of customers who are in the Union, may be significant to conclude that the controller envisages offering goods or services to data subjects in the Union. The factors provided by the CJEU in its *Pammer and Hotel Alpenhof* Judgment concerning the application of the special jurisdiction provisions protecting consumers to persons that direct their commercial activities to the Member State of the consumer's domicile may also be relevant in this context.[35] Furthermore, pursuant to Recital 24 of the GDPR, in order to determine whether a processing activity can be considered to monitor the behaviour of data subjects, it should be ascertained whether persons are

[33] CJEU Judgment of 1 October 2015 in case C-230/14, *Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság*, ECLI:EU:C:2015:639, and CJEU Judgment of 28 July 2016, C-191/15, *Verein für Konsumenteninformation v Amazon EU Sàrl*, ECLI:EU:C:2016:612, para. 31, and paras 73-81.
[34] CJEU Judgment of 13 May 2014, rendered in case C-131/12, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, ECLI:EU:C:2014:317, paras 55 and 56. See also Article 29 Working Party on Data Protection, «Update of Opinion 8/2010 on applicable law in light of the CJEU judgment in Google Spain», 16 December 2015, Annex II; Kuner (2015), Oro Martínez (2015) and Van Alsenoy and Koekkoek (2015).
[35] Judgment of the CJEU of 7 December 2010, *Peter Pammer v Reederei Karl Schlüter GmbH & Co KG (C-585/08) and Hotel Alpenhof GesmbH v Oliver Heller* (C-144/09), ECLI:EU:C:2010:740, paras. 77-78.

tracked on the internet including potential subsequent use of profiling a natural person for behavioural advertising practices.[36]

Finally, the third group of situations where the GDPR applies is the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law, such as in a Member State's diplomatic mission or consular post.

4.3. International data transfers

A basic goal of the development of common rules on the protection of personal data within the EU is to ensure the free flow of data. Therefore, Article 1(3) of the GDPR makes clear that the free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data. However, in order to ensure that when the personal data of Europeans are transferred abroad, the protection level is not undermined, transfers of personal data to third countries or international organisations are only allowed if the conditions laid down in Chapter V of the GDPR are complied with by the controller and processor. These provisions are based on the significant enforcement experience in this area developed by the EU in previous years.[37]

Transfers to a non-EU country may take place without further safeguards or a specific authorisation on the basis of a Commission "adequacy decision" establishing that a third country –or a particular territory of a third country or a specific sector or industry within a third country- provides a level of data protection that is essentially equivalent to that in the EU.[38] Article 45(2) GDPR contains a catalogue of elements that the Commission must take into account when adopting decisions on adequacy, which include: the rule of law, respect for human rights and relevant legislation, as well as the implementation of such legislation; the existence and effective functioning of independent supervisory authorities; and the international commitments the third country or international organisation concerned has entered into. The EU-US Privacy Shield is a self-certification mechanism for US based companies which has been recognized by the Commission as providing an adequate level of protection for personal data transferred from an EU entity to US based companies. It is in full effect since 1August 2016.

In the absence of an adequacy decision, a controller or processor may transfer personal data to a third country or an international organisation only if the controller or

[36] On the data protection implications of those practices, *see* Article 29 Working Party on Data Protection, Opinion 2/2010 on online behavioural advertising, WP 171, adopted on 22 June 2010.
[37] See Kuner (2013), pp. 151-154.
[38] Judgment of the CJEU of 6 October 2015, C-362/14, *Schrems v. Data Protection Commissioner*, ECLI:EU:C:2015:6506, paras. 73-74.

processor provides appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. Instruments to provide adequate safeguards without requiring a specific authorisation from a supervisory authority include: standard contractual clauses establishing obligations between the EU exporter and the third country importer; binding corporate rules adopted by a multinational group of companies a group of enterprises engaged in a joint economic activity to carry out transfers within the group; and approved codes of conduct or certification mechanisms.

Where no adequacy decision is applicable and no appropriate safeguards have been provided pursuant to Article 46 GDPR, transfers of personal data to a third country are only allowed under one of the conditions laid down in Article 49 GDPR. Such derogations for specific situations include: explicit consent by the data subject to the proposed transfer, performance of a contract, important reasons of public interest and protection of the vital interests of the data subject.

Chapter V of Directive (EU) 2016/680 (see number 20, *supra*) contains the common rules on international transfers in the law enforcement sector in order to facilitate cross-border cooperation between police and judicial authorities, both within the EU and with third States. The specific adequacy assessment elements to be made by the Commission when adopting adequacy decisions for the law enforcement sector are listed in Article 36(2) Directive (EU) 2016/680.

4.4. Private enforcement and conflict of laws

EU law does not provide for common conflict-of-laws rules to determine the law applicable to liability for damages caused by the unlawful processing of personal data. The prevailing view is that such claims are excluded from the scope of application of Regulation (EC) No 864/2007 of 11 July 2007 on the law applicable to non-contractual obligations (Rome II) pursuant to Article 1(2)(g). According to this provision, the Regulation does not apply to non-contractual obligations arising out of violations of privacy and rights relating to personality, including defamation.

Although this situation has remained unaffected by the adoption of the GDPR, it is noteworthy that the Regulation includes new special jurisdiction rules concerning private claims by data subjects against a controller or processor as a result of the infringement of the rights granted to them by the Regulation. Such rules, which are intended to supplement those of the Brussels I (Recast) Regulation are of special significance in a context in which private enforcement of data protection law has become

prominent.[39] In particular, that is the case with regard to the enforcement of the right to compensation where a damage results from an infringement of the GDPR. In this respect, Article 79 contains a specific provision on international jurisdiction regarding claims brought by a data subject against a controller or processor where he or she considers that his or her rights under the GDPR have been infringed, including court proceedings for exercising the right to receive compensation.[40] Article 82 of the GDPR provides some common substantive rules on the right of any person who has suffered material or non-material damage as a result of an infringement of the Regulation to receive compensation from the controller or processor for the damage suffered.

References

Albrecht J P and Jotzo F (2017), Das neue Datenschutzrecht der EU, Nomos, Baden-Baden.

Brkan M (2015), Data protection and European private international law: observing a bull in a China shop», International Data Privacy Law, pp. 257-278.

De Hert P and Papakonstantinou V (2016), The new General Data Protection Regulation: Still a sound system for the protection of individuals? 32 Computer Law & Security Review, pp. 179–194.

De Miguel Asensio, P A (2015) Derecho Privado de Internet, 5th edn., Civitas Thomson Reuters, Madrid.

De Miguel Asensio, P A (2017), Competencia y Derecho aplicable en el Reglamento General sobre Protección de Datos de la Unión Europea, 69 (1), Revista española de Derecho internacional, pp. 75-108.

González Fuster G (2014), The Emergence of Personal Data Protection as a Fundamental Right of the EU, Springer, Heidelberg.

Härting, N (2016), *Datenschutz-Grund-verordnung*, Otto Schmidt, Cologne.

Kohler C (2016), Conflict of law issues in the 2016 data protection regulation of the European Union, Rivista di Diritto Internazionale Privato e Processuale, pp. 653-675

Kuner C (2013), Transborder Data Flows and Data Privacy Law, OUP, Oxford.

Kuner C (2015), The Court of Justice of the EU Judgment on Data Protection and Internet Search Engines: Current Issues and Future Challenges, B. Hess and C.M. Mariottini (eds.),Protecting Privacy in Private International and Procedural Law and by Data Protection, Ashgate, Nomos, Baden-Baden, pp. 19-44.

Oro Martínez C (2015) The CJEU Judgment in Google Spain: Notes on Its Causes and Perspectives on Its Consequences, Protecting Privacy in Private International and Procedural Law and by Data Protection, Ashgate, Nomos, Baden-Baden, pp. 45-55.

Paal B P and Pauly D A (2017), Datenschutz-Grundverordnung, C.H.Beck, Munich.

Svantesson D J B (2013), Extraterritoriality in Data Privacy Law, Ex Tuto, Copenhagen, 2013.

Van Alsenoy B and Koekkoek M (2015), Internet and jurisdiction after Google Spain: the extraterritorial reach of the 'right to be delisted', 5.2, International Data Privacy Law, pp. 105-120.

[39] CJEU Judgment of 25 January 2018, C-498/16, Maximilian Schrems v Facebook Ireland Limited, ECLI:EU:C:2018:37.
[40] Brkan (2015), pp. 257-278, Kohler (2016), pp. 653-675 and De Miguel Asensio (2017) pp. 92-106.