Online Privacy Law:
the European Union

June 2012
Updated: May 2014

The Law Library of Congress, Global Legal Research Center
(202) 707-6462 (phone) • (866) 550-0442 (fax) • law@loc.gov • http://www.law.gov

LAW LIBRARY OF CONGRESS

EUROPEAN UNION

ONLINE PRIVACY LAW

Executive Summary

The right to data protection and the right to privacy are two distinct human rights recognized in the Charter of Fundamental Rights of the European Union, the Treaty on the Functioning of the EU (TFEU), and in two legal instruments of the Council of Europe, to which all the EU Member States are parties.

In January 2012, the European Commission proposed a major overhaul of the existing legislative framework on the protection of personal data. The reform was necessitated mainly by three factors: (a) new challenges posed by globalization and Internet developments in the area of online services, which impact the processing of personal data and endanger the privacy of individuals; (b) a new legal basis in the TFEU; and (c) a dramatic increase in Internet users and serious concerns expressed by 70% of individuals in the EU about the possible misuse of their personal data.

Landmark EU Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data on the Free Movement of Such Data, which was adopted in 1995 when the Internet was still in its infancy, met to some extent its twin objectives of safeguarding the personal data of individuals and improving the flow of personal data among EU Member States, but it resulted in diversity of implementation by the twenty-seven EU Members. By contrast, the pending proposal, which is in the form of a draft regulation because of its direct applicability in the legal systems of the Member States of the EU, will bring about greater harmonization of data protection rules, legal certainty, and transparency, and will also remove any obstacles in the flow of personal data within the single market and improve competition.

The draft regulation builds upon the fundamental principles on the processing of personal data established by Directive 95/46/EC. Thus, online processing of personal data is prohibited unless it meets necessary safeguards and is based on one of the required legal grounds, such as consent or the protection of vital interests of data subjects. Special categories of data, such as data concerning race, ethnic origin, political affiliations, religion, genetic data, or criminal convictions (the last two added by the Draft Regulation), are granted extra protection.

The proposal is designed to enhance the rights of data subjects by introducing two distinct rights: the right to portability and the right to be forgotten. The right to be forgotten was upheld by the European Court of Justice in May 2014. http://www.loc.gov/lawweb/servlet/lloc_news?disp3_l205403625_text These rights are in addition to those provided for in Directive 95/46/EC, that is, the right to access, object, correct, and erase. The right of portability allows individuals to obtain a copy of their data from one service provider and transfer it easily to another; the right to be forgotten allows individuals to request the elimination of personal data that are no longer needed or wanted. Additional safeguards include new provisions on profiling, and a requirement that data controllers notify individuals in the event of a security breach in order to avoid identity fraud. The privacy of children and their right to personal data protection is also enhanced, because the draft regulation prohibits the processing of personal data of a child below the age of thirteen without the consent of a parent or guardian.

Companies are obliged to implement the principles of privacy by design and privacy by default early in their business practices. The first principle relates to a company's obligation to include data protection safeguards from the very beginning in the development of products or services, whereas the second requires that privacy-friendly default settings must be the norm.

The draft regulation also strengthens the enforcement powers of data protection authorities, established under Directive 95/46/EC, by granting them the authority to impose a fine of €250,000 (about US$306,500) on individuals and administrative fines of up to 2% of global annual turnover on companies. Another innovation is that companies that employ more than 250 employees are required to appoint an independent data protection officer. Processors of personal data are required to notify data supervisory authorities within twenty-four hours when there is a security breach of personal data.

The scope of territorial applicability of the Regulation is broad. It will apply when a controller or processor is established in the EU and also to those established outside the EU who offer goods and services to data subjects in the EU or are involved in monitoring the behavior of individuals in the EU. Adequacy decisions verifying that a third country meets the EU standards will be further simplified and clarified. For transfers of personal data outside the EU, contractual clauses and simplified binding corporate rules will ensure that data processed outside the EU are adequately handled and protected.

The draft regulation will be further discussed in the Council and the Parliament and will enter into force two years after its publication in the Official Journal of the European Union.

I. Legal Framework

Under European Union (EU) law, the right to privacy and the right to protection of personal data are two distinct fundamental human rights.[1] The Charter of Fundamental Rights of the European Union (CFR), which acquired binding status on December 1, 2009, recognizes the right to privacy in article 7 and the right to the protection of one's personal data in article 8.[2] Furthermore, article 8 reaffirms the principle that personal data must be processed fairly and for specific purposes, based on the consent of the individual concerned or some other legitimate purposes laid down by law. It also recognizes the right of individuals to access the data collected and the right to have it rectified, in case of inaccuracy or incompleteness. Compliance with such rules is entrusted to the control of an independent authority established by EU Member States.[3] In a society, the right to personal data may be restricted by law in order to strike a balance with the freedoms and rights of others and with the general interest, subject to the principle of proportionality, which is established in the EU and legal systems of the Member States.[4]

In addition, the Treaty on the Functioning of the European Union (TFEU), recognizes the right of every individual to his/her personal data.[5] It also introduced a new and specific legal basis for the adoption of rules on data protection and grants the authority to the EU legislative bodies (Parliament and Council) to adopt rules concerning the processing of personal data by EU institutions, bodies, and Member States, and to ensure that compliance with such rules is assigned to the control and review of independent authorities.[6]

II. Current EU Law

A. Directives

Social networking, or "online services" as it is referred to in EU terminology, falls within the scope of the basic framework of Directive 95/46/EC on the Protection of Individuals with

---

[1] The right to privacy is also protected by article 8 of the European Convention of Human Rights and Fundamental Freedoms, to which all the EU Member States are states parties, as members of the Council of Europe. In addition, automatic processing of personal data is protected and governed by the 1981 Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data and Its Protocol. Recently, the Council of Europe began revising the 1981 Convention to bring it in line with contemporary technology and ensure harmonization with EU legal reform.

[2] Charter of Fundamental Rights of the European Union, 2010 O.J. (C 83) 02, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0389:0403:EN:PDF.

[3] *Id*. art. 8.

[4] *Id.* art. 52(1).

[5] Consolidated Version of the Treaty on the Functioning of the European Union [TFEU], art. 16, 2010 O.J. (C 83) 47, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0047:0200:EN:PDF.

[6] *Id.*

Regard to the Processing of Personal Data and on the Free Movement of Such Data[7] (hereafter the Data Protection Directive) because it involves the processing of personal data of users. The Data Protection Directive was designed to achieve two basic objectives: (1) protect the fundamental right to the personal data of data subjects; and (2) ensure the free flow of personal data in the internal market.

The Data Protection Directive was transposed by the twenty-seven EU Member States[8] and the three European Economic Area States: Iceland, Liechtenstein, and Norway.[9] Switzerland has also implemented the Directive in the areas related to the Schengen Agreement[10]. The Commission's 2002 report on the transposition of Directive 95/46/EC and its subsequent Communication in 2007[11] concluded that the Data Protection Directive had partially achieved its twin objectives of safeguarding the right to personal data and facilitating the flow of such data within the EU.[12] The Commission noted that the Directive "did not manage to fully achieve its internal market policy objective," or to remove obstacles in implementation across the EU. Existing divergences among EU Members relate to the interpretation of such key terms as "controller," "personal data," and "in enforcement."[13]

In addition to the Data Protection Directive, online services are also governed by the following Directives:

---

[7] 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, 1995 O.J. (L 281) 31, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1995:281:0031:0050:EN:PDF.

[8] The European Commission initiated legal action against Luxembourg before the European Court of Justice (ECJ) for failing to transpose the Data Protection Directive within the prescribed period (by October 24, 1998). The ECJ issued its decision in 2001, found against Luxembourg, and ordered it to pay the costs. Case C-450/00, Judgment of the Court (Grand Chamber), European Commission v. Grand Duchy of Luxembourg, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62000CJ0450:EN:PDF.

[9] Decision of the European Economic Area Joint Committee No. 83/1999 Amending Protocol 37 and Annex XI (Telecommunications Services) to the EEA Agreement, 2000 O.J. (L 296) 41, http://eur-lex.europa.eu/Result.do?aaaa=2000&mm=&jj=&type=l&nnn=296&pppp=41&RechType=RECH_reference_pub&Submit=Search.

[10] Annex B (Article 2(2)), Agreement Between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's Association with the Implementation, Application and Development of the Schengen Acquis, 2008 O.J. (L 53) 52, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:053:0052:0079:EN:PDF.

[11] *Communication from the Commission to the European Parliament and the Council on the Follow-up of the Work Programme for the Better Implementation of the Data Protection Directive*, COM (2007) 87 final (Mar. 7, 2007), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0087:FIN:EN:PDF.

[12] Report from the Commission: First Report on the Implementation of the Data Protection Directive (95/46/EC) COM (2003) 265 final (May 15, 2003), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52003DC0265:EN:NOT.

[13] For an in-depth analysis of transposition of Directive 95/46/EC by EU Member States, *see* DOUWE KORFF, EC STUDY ON IMPLEMENTATION OF DATA PROTECTION DIRECTIVE: COMPARATIVE SUMMARY OF NATIONAL LAWS (Sept. 2002), *available at* http://www.garanteprivacy.it/garante/document?ID=455584. *See also* Annex 2 to the Impact Assessment Evaluation on the Implementation of the Data Protection Directive, http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_annexes_en.pdf (last visited June 30, 2012).

- Directive 2002/58/EC Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications)[14]
- Directive 2006/24/EC on the Retention of Data Generated in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks and Amending Directive 2002/58/EC[15]
- Directive 2009/136/EC Amending Directive 2002/58/EC on Universal Service and Users' Rights Relating to Electronic Communications Networks and Services[16]

B. Regulation

EU institutions are also bound to protect the fundamental rights and freedoms of individuals, in particular their right to privacy and personal data protection, by virtue of Regulation (EC) No. 45/2001 on the Protection of Individuals with Regard to the Processing of Personal Data by the Community Institutions and Bodies and on the Free Movement of Such Data.[17]

C. Definitions

The Data Protection Directive introduced some key concepts that have been used in subsequent EU legislation on personal data protection. It defines "personal data" as "any information relating to an identified or identifiable natural person ('data subject')."[18] The broad definition has resulted in differences of interpretation among EU Members. The Commission has noted that IP addresses, which identify computers on networks; digital pictures; geo-location data; and telephone numbers are considered to be personal data by some EU Members, while

---

[14] 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), 2002 O.J. (L 201) 37, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:EN:PDF.

[15] 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, 2006 O.J. (L 105) 54, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF.

[16] Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 Amending Directive 2002/22/EC on Universal Service and Users' Rights Relating to Electronic Communications Networks and Services, Directive 2002/58/EC Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector and Regulation (EC) No 2006/2004 on Cooperation Between National Authorities Responsible for the Enforcement of Consumer Protection Laws, 2009 O.J. (L 377) 11, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:EN:PDF.

[17] Regulation (EC) No. 45/2001 of the European Parliament and of the Council of 18 December 2000 on the Protection of Individuals with Regard to the Processing of Personal Data by the Community Institutions and Bodies and on the Free Movement of Such Data, 2001 O.J. (L 8) 1, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:008:0001:0022:EN:PDF.

[18] Directive 95/46/EC, *supra* note 7, art. 2(a).

others define them as such only under certain conditions.[19] An "identifiable person" is a natural person who can be identified either by an identifiable number or on the basis of some elements, including his/her physical, physiological, mental, economic, cultural, or social identity.[20] "Processing of personal data" means "any operation or set of operations which is performed upon personal data, whether or not by automatic means."[21]

The Data Protection Directive provides a nonexhaustive list of what constitutes processing. Thus, "processing" is a very broad term and includes the following: collection, recording, storage, organization, alteration or adaptation, use, disclosure, retrieval, alignment, combination, blocking, erasure, or dissemination or otherwise making data available.[22]

The Data Protection Directive also differentiates between "controller" and "processor." The term "controller" means any natural or legal person, public authority, agency, or any other body that jointly with others or alone determines the purposes and means of processing of personal data. "Processor" is defined as a natural or legal person or public authority, agency, or other body that "processes personal data on behalf of the controller."[23] In many instances, the roles of the controller and processor are not easily distinguishable. Whether an organization is a controller or a processor and the applicable criteria for each designation were clarified by the Article 29 Working Party, which was established by the Data Protection Directive in Opinion 1/2010 on the Concepts of "Controller" and Processor."[24]

D. Fundamental Principles Governing Personal Data Processing

Under the Data Protection Directive, all processing of personal data must (subject to some exceptions provided in article 13) comply with the principles related to data quality prescribed in article 6 and with one of the six grounds for making data processing legitimate, as contained in article 7. Article 7 contains an exhaustive and restrictive list of grounds.

Specifically, in compliance with article 6 of the Data Protection Directive, controllers of online services who deal with personal data must ensure that personal data are

- processed fairly and lawfully;
- gathered for specific, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes (processing for historical, statistical, or

---

[19] Annexes to the Impact Assessment, European Commission, Annex I Current EU Legal Instruments for the Protection of Personal Data, http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_annexes_en.pdf (last visited June 30, 2012).

[20] Directive 95/46/EC, *supra* note 7, art. 2(a).

[21] *Id*. art. 2(b).

[22] *Id*.

[23] *Id*. art. 2(d)–(e).

[24] Article 29 Data Protection Working Party, *Opinion 1/2010 on the Concepts of "Controller" and "Processor"*, 00264/10/EN, WP 169 (Feb. 16, 2010), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf.

scientific purposes shall not be deemed in violation of the directive, if the EU Members provide further safeguards);

- adequate, relevant, and not excessive to the purpose the data were initially collected;
- accurate and current, where possible (inaccurate data must be either corrected or deleted; and
- kept in a form that allows identification of the data subject for no longer than is necessary for the purposes for which the data were gathered or for which they are further processed.[25]

E. Grounds for Processing of Personal Data

As stated above, processing—that is, collection, storage, and use of personal data—by online media or services is prohibited. The Data Protection Directive provides six legal grounds for processing. Consequently, processing is lawful in the following instances:

- Where the data subject has granted its unambiguous consent
- To perform a contract in which one of the parties is the data subject
- To enable the controller to comply with a legal obligation
- To protect the vital interests of the data subject
- To perform a task for the public interest or in the exercise of an official authority vested in the controller
- To pursue legitimate interests by the controller or third parties who have become privy to such data, unless the protected interests of the data subject override those of the controller or third parties[26]

The last ground requires a balancing act between the interests of the data subject and those of the controller or third parties to whom the data have been disclosed. The Commission's First Report on Implementation of the General Directive has clarified that the factors to be taken under consideration in such a case include the nature of the data, the nature of processing, and whether the action is carried out by the private or public sector. The Commission also indicates that implementation of this test differs among EU Members.[27] Several EU Member States adopt a strict interpretation of this ground and decide in favor of the data subject or limit its application to certain categories of data.[28]

---

[25] Directive 95/46/EC, *supra* note 7, art. 6.

[26] *Id*. art. 7.

[27] European Commission, First Report on the Implementation of the Data Protection Directive (95/46/EC), COM (2003) 265 final,http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2003:0265:FIN:EN:PDF. *See also Analysis and Impact Study on the Implementation of Directive 95/46/EC in Member States*, http://ec.europa.eu/justice/policies/privacy/docs/lawreport/consultation/technical-annex_en.pdf.

[28] *Id.*

F. Processing of Special Categories of Data

Online services are not permitted to process certain data because of their sensitive nature. These data relate to one's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data related to one's health or sex life.[29] However, the Data Protection Directive allows the processing of such data, inter alia, where

- the data subject has granted explicit consent;
- processing is necessary so that the controller can carry out obligations and rights in the field of employment, and is authorized by national law;
- processing is necessary to protect the vital interests of the data subject;
- processing is carried out in the course of legitimate activities by a foundation or association that has political, philosophical, religious, or trade-union objectives, with appropriate guarantees and with the condition that such processing relates to the entity's members or those having regular contact with the entity; or
- processing relates to data made public by the data subject or is necessary in connection with a legal claim.[30]

In case of offenses or criminal convictions or security measures, data can be processed only by an official authority[31]

G. Exemptions

The Data Protection Directive permits EU Member States to adopt legislation to restrict the rights of data subjects for the following reasons, including

- national security, public security, and defense;
- prevention, investigation, detection, and prosecution of criminal offenses or violations related to codes of ethics of regulated professions;
- important economic or financial interests of the EU or a Member State; and
- the protection of data subjects or the rights and freedoms of others.[32]

In addition, the Privacy and Electronic Communications Directive allows the adoption of legislative measures by the EU Members to retain personal data for a limited period and for the purposes stated above.[33]

---

[29] Directive 95/46/EC, *supra* note 7, art. 8.

[30] *Id*. art. 8(2)(a)–(e).

[31] *Id*.

[32] *Id*. art. 13.

[33] Directive 2002/58/EC, *supra* note 14, art. 15.

H. Consent

The Data Protection Directive defines "the data subject's consent" as "any freely given specific and informed indication" of the data subject's wishes that signifies his or her agreement to the processing of personal data.[34] Thus, consent must meet the requirements of being (a) freely given, (b) specific, and (c) informed. In Opinion 15/2011 on the Definition of Consent, the Article 29 Working Party emphasized the significance of consent in the processing of personal data.[35] It clarified that in many instances, consent cannot be granted freely—for instance, due to the relationship between the data subject and the controller or in cases of personal data provided to public authorities. Under those circumstances the word "freely" means that it must be given free of intimidation or deception. On the other hand, "informed" consent means the data subject understands well the context and substance of what it means to his or her personal data.[36] The Directive on Privacy and Electronic Communications builds upon these principles and clarifies in recital 17 that "[c]onsent may be given by any appropriate method enabling a freely given specific and informed indication of the user's wishes, including by ticking a box when visiting an Internet website."[37]

I. Rights of Data Subjects

1. Right of Access

One of the basic rights of data subjects is the right to access their personal data. The right to access involves the right to receive, free of charge, notification as to whether data are being processed and information on the purpose of processing, categories of data being processed, and individuals or organizations to whom the data are disclosed.[38]

Data subjects also have the right to rectify, erase, or block the processing of data that are incompatible with the provisions of the Data Protection Directive, or of data that are incomplete and inaccurate.[39] Furthermore, they have the right to request that the controller notify third parties who are recipients of personal data about the correction.[40]

---

[34] Directive 95/46/EC, *supra* note 7, art. 2(h).

[35] Article 29 Data Protection Working Party, *Opinion 15/2011 on the Definition of Consent*, 01197/11/EN WP187 (July 13, 2011), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf.

[36] *Id*. at 12.

[37] Directive 2002/58/EC, *supra* note 14, recital 17.

[38] Directive 95/46/EC, *supra* note 7, art. 12.

[39] *Id.*

[40] *Id.*

2. Right to Object

Data subjects have the right to object

- at any time on "compelling legitimate grounds" regarding the processing of their personal data carried out for the performance of a task for public interest reasons, in the exercise of official authority exercised by the controller, or when processing is necessary for the legitimate interests of the controller; and
- where processing is for the purpose of direct marketing.[41]

J. Installation of Technical and Organizational Security Measures

The Personal Data Protection Directive introduced the general requirement that the controller must put in place "appropriate technical and organizational measures" designed to safeguard personal data against unlawful destruction, accidental loss, alteration, unauthorized access, or disclosure, especially where the processing entails the transmission of data over a network.[42] The measures must be appropriate to the risk involved and to the nature of data processed, taking into account the state of the art available and the cost of implementing such measures.[43]

In addition, when processing is performed by a processor on behalf of a controller, the processor must also provide guarantees that the processing will be done in compliance with technical and organizational measures.[44] In such a case, the working relationship between the controller and processor must be dealt with through a contract specifying that the processor must only act based on instructions by the processor.[45]

The Privacy and Electronic Communications Directive contains the same language, requiring providers of publicly available electronic communications services to adopt organizational and technical measures in order to provide security for its services.[46] Directive 2009/136/EC, which amended the E-Privacy Directive, added the following additional requirements that the adopted security measures must meet:

- Ensure that only authorized people can access personal data for lawful purposes
- Protect personal data that are stored or transmitted against accidental loss or unlawful destruction

---

[41] *Id.* art. 14.

[42] *Id.* art. 17.

[43] *Id*.

[44] *Id*. art. 17, para. 2.

[45] *Id*. art. 17, para. 3.

[46] Directive 2002/58/EC, *supra* note 14, art. 4.

- Ensure the implementation of security policy[47]

In case of a breach of personal data, the provider of publicly available electronic communications services must notify (a) the competent national authority, and (b) the subscriber or individual if the breach is likely to adversely affect his or her personal data or privacy.[48]

The Data Retention Directive (discussed below) also requires the adoption of appropriate technical and organizational measures in order to safeguard data that have been retained against accidental loss; accidental destruction; or unauthorized storage, processing, access, or disclosure. These measures must also ensure that such data can only be accessed by authorized personnel.[49]

K. Data Collection by Smartphone Applications

The relevant legal framework on data collection by smartphone applications is the Personal Data Protection Directive. In Opinion 13/2011 on Geolocation Services on Smart Mobile Devices the Article 29 Working Party expressed the view that the Personal Data Protection Directive applies in all cases where personal data are being processed as the result of the processing of location data.[50]

The Privacy and Electronic Communications Directive, as revised by Directive 2009/136/EC, only applies to the processing of base station data by telework operators. Telework operators process base station data within the framework of offering public electronic communications services. Article 2(c) of Directive 2009/136 defines "location data" as "any data processed in an electronic communications network or by an electronic communications service, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service."[51] Consequently, because location data derived from base stations relate to an identified or identifiable natural person, they are subject to the Data Protection Directive.

Users have the right to receive from different controllers access to location data collected from their smart mobile devices as well as information on the purpose of processing including recipients to whom the data are disclosed.[52] The E-Privacy Directive introduced a mandatory notification requirement where personal data is breached.[53]

---

[47] Directive 2009/136/EC, *supra* note 16, art. 4(b).

[48] *Id.* art. 4(c)(3).

[49] Directive 2006/24/EC, *supra* note 15, art. 7(b), (c).

[50] Article 29 Data Protection Working Party, *Opinion 13/2011 on Geolocation Services on Smart Mobile Devices* 19, 881/11/EN, WP 185 (May 16, 2011), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp185_en.pdf.

[51] Directive 2009/136/EC, *supra* note 16, at 29, *amending* Directive 2002/58/EC, *supra* note 14, art. 2(c).

[52] Article 29 Data Protection Working Party, *Opinion 13/2011*, *supra* note 50.

[53] Directive 2002/58/EC, *supra* note 14, art. 4(c)(3), *as amended by* Directive 2009/136/EC, *supra* note 16.

L. Limits on Geodata

The processing of location data from smart mobile devices is not allowed unless the data subject has granted his or her prior informed consent. The consent must also meet the requirements of being specific to the type of purposes for which the data are processed, and the subject must be given the option of withdrawing consent. The data subject must also have the same rights provided by the Data Protection Directive—i.e., the right to access, rectify, or erase any profiles created based on the collection and processing of location data.[54] When location data other than the traffic data of users of publicly available electronic communications services are processed, such data may only be processed if they are made anonymous or with the consent of the users, to the extent and for the duration necessary to provide value-added service.[55]

Moreover, the service provider is responsible for notifying users, prior to obtaining their consent, of the type of location data (other than traffic data), the purposes and duration of the processing, and whether their location data will be forwarded to a third party. Users must be given the option to withdraw their consent at any time.[56]

M. Protection of Minors

Although the privacy right of children is enshrined in several international legal instruments,[57] there are no specific rules pertaining to the personal data of children in either the Data Protection Directive or the Privacy and Electronic Communications Directive. Because the scope of both Directives extends to the data of "every natural person," however, the built-in safeguards arguably apply to both children and adults. Consequently, the general principles on data quality contained in the Personal Data Protection Directive, such as fairness, proportionality, and relevance, apply to children. In addition, the general obligations that only adequate, relevant, and nonexcessive data can be collected and processed govern the processing of the personal data of children. In general, controllers must take into account the circumstances of a child and his/her best interests. Moreover, the personal data of children must be accurate and current; inaccurate or incomplete data must either be erased or corrected. The Data Protection Directive's article 7 on the legality of processing and article 9 on the processing of personal categories of data are also applicable to children. As far as the right of access, it can be exercised either by the child based on his/her maturity level, or by the child's representative. Children's data cannot be used for purposes other than those for which they were collected.

The Article 29 Data Protection Working Party has issued a number of opinions on the protection of personal data of children, including an opinion addressed to school authorities,

---

[54] For an analysis on the applicable law and limitations on processing of location data collected through smart mobile devices, *see* Article 29 Data Protection Working Party, *Opinion 13/2011*, *supra* note 50.

[55] Directive 2002/58/EC, *supra* note 14, art. 9.

[56] *Id*.

[57] For example, article 16 of the Convention on the Rights of the Child provides that no child shall be subject to arbitrary or unlawful interference with his or her privacy, family, home, or correspondence, nor to unlawful attacks on his or her honor and reputation. Convention on the Rights of the Child, *entered into force* Sept. 2, 1990, U.N. Doc. A/44/49 (1989), http://www2.ohchr.org/english/law/crc.htm.

Opinion 2/2009 on the Protection of Children's Personal Data (General Guidelines and the Special Case of Schools).[58]

N. Retention of Data

Directive 2006/24/EC 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[59] (hereafter, the Data Retention Directive) requires EU Members to adopt legislation ensuring that operators of publicly available electronic communications services or networks retain traffic and location data generated from fixed and mobile telephony, Internet access, and Internet email and telephony for a period of six months and up to two years to investigate, detect, and prosecute serious crime.[60]

Article 5 of the Date Retention Directive specifies that the following categories of data must be retained, with specific data types depending on whether it is fixed network or mobile telephony, or Internet email and Internet telephony:

- Data necessary to trace and indentify the source of a communication
- Data necessary to identify the destination of a communication

EU Members were obliged to transpose Directive 2006/24/EC by September 15, 2007, with the option of postponing certain obligations related to Internet access, email, and telephony by a March 15, 2009, deadline. In April 2011, the Commission published its evaluation report on implementation of the Data Retention Directive.[61] EU Members responded that data retention is "very valuable and in some cases indispensable, for preventing and combating crime, for protecting victims and for the acquittal of the innocent in criminal cases."[62] The Commission also noted that requests to access stored data by law enforcement authorities is constantly increasing and that the number of requests varies considerably among the EU Member States.[63]

As of April 2011, twenty-five EU Members had notified the Commission of their transposition of the Data Retention Directive; however, in Romania, Germany, and the Czech Republic, the transposition laws have been annulled by the respective constitutional courts.[64] On May 31, 2012, the Commission referred Germany to the European Court of Justice for not

---

[58] Article 29 Data Protection Working Party, *Opinion 2/2009 on the Protection of Children's Personal Data (General Guidelines and the Special Case of Schools)*, 398/09/EN, WP 160 (Feb. 11, 2009), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp160_en.pdf.

[59] Directive 2006/24/EC, *supra* note 15.

[60] *Id*. arts. 1, 6.

[61] Frequently Asked Questions: Evaluation Report of the Data Retention Directive, Memo/11/251 (Apr. 18, 2011), http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/11/251&format=HTML&aged=0&language=EN&guiLanguage=en.

[62] *Id*. at 2 (PDF version).

[63] *Id*. at 3.

[64] *Id*.

complying with its obligation to transpose the Data Retention Directive after the initial transposition law adopted by Germany was annulled by the German Federal Constitutional Court in 2010. The Commission suggested that the ECJ impose a daily penalty payment of €315,036.54 (about US$396,260).[65] In addition, the Commission announced its intention to discontinue its proceedings against Austria based on Austria's notification of measures that fully transpose the Data Retention Directive into national law, and to partially withdraw charges against Sweden.[66]

On April 8, 2014, the Court of Justice of the European Union (ECJ) issued a much-anticipated judgment concerning the legality of Directive No. 2006/24/EC. The Directive was challenged on the grounds of infringement of the right to private life and of the right to protection of the personal data of individuals, as enshrined in the Charter of Fundamental Rights of the European Union. The ECJ declared the Data Retention Directive invalid. Consequently, telecommunications companies and Internet service providers are no longer obliged to retain traffic and location data belonging to individuals or to legal entities for the prevention of crime.
http://www.loc.gov/lawweb/servlet/lloc_news?disp3_l205403625_text

O. Remedies and Sanctions

EU Members are required to provide means of redress to data subjects whose personal data have been infringed. Thus, the Personal Data Protection Directive provides data subjects with the following rights:

- Administrative remedies before the national supervisory authority[67]
- Judicial remedies for any breach of rights guaranteed by national law[68]
- Compensation by the controller for the damage suffered for any processing in violation of the rules; a controller may avoid liability in whole or in part, however, by proving that he/she is not responsible for the violation[69]

When implementing EU law, Member States are also obliged to make provisions in their national legislation for sanctions to be imposed in case of infringement.[70]

Users of online services whose personal data are unlawfully processed also have the same remedies on the basis of the Privacy and Electronic Communications Directives.[71] Moreover, data subjects whose personal data have been retained in violation of the Data Retention Directive enjoy the same remedies as those provided to data subjects based on the Personal Data Protection Directive.[72]

P. Transfer of Personal Data to Third Countries Outside the EU

The Data Protection Directive has extraterritorial application and prohibits the transfer of personal data that are undergoing processing, or will be processed after the transfer, to third

---

[65] *Id.*

[66] Press Release, European Commission, Data Retention: Commission Takes Germany to Court Requesting That Fines Be Imposed (May 31, 2012), http://www.statewatch.org/news/2012/jun/eu-com-germany-mand-ret.pdf.

[67] Directive 95/46/EC, *supra* note 7, art. 28, para. 4.

[68] *Id*. art. 22.

[69] *Id*. arts. 22–23.

[70] *Id*. art. 24.

[71] Directive 2002/58/EC, *supra* note 14, art. 15, para. 2.

[72] Directive 2006/24/EC, *supra* note 15, art. 13(1).

countries (outside the EU) that do not meet the standard of "an adequate level of protection."[73] In the case of transfers, the preliminary question that must be examined is what constitutes a transfer, within and outside the EU. The Data Protection Directive does not provide a definition of "transfer," but the concept of international transfer was clarified in the *Bodil Lindqvist* case heard before the European Court of Justice. The ECJ held that the mere publication of data on the Internet is not a transfer of data to a third country outside the EU, even though the data is accessible to Internet users in other countries.[74] The ECJ reasoned that the data were not sent automatically from the server to other Internet users, but users instead had to access the data on their own, and that there was no direct transfer of personal data between the person who loaded the information and the persons accessing it on the Internet.[75] Thus, the criterion is whether data have actually been received in a third country. It is not sufficient that the data were available on the Internet.[76]

The adequacy standard is assessed based on a number of factors related to the transfer, including the nature of the data, the purpose and duration of processing of the data, the country of origin and country of final destination, and the existing general or sectoral rules of law in the third country or international commitments assumed by the third country.[77] EU Members are required to notify each other and the Commission if a country does not meet the adequacy criterion.[78] If the Commission finds that the third country does not meet the criterion, the EU Members are required to prohibit any transfer. The Directive empowered the Commission to enter into negotiations with a third country to remedy the situation, however.[79]

The Article 29 Working Party established a functional test to review the adequacy criterion. In its 1998 Opinion on transfers, it developed a number of substantive and procedural criteria to reach a conclusion that a particular country meets the adequacy standard, including

- purpose limitation;
- data quality and proportionality;
- transparency and security;
- rights to access, rectify, and object; and

---

[73] Directive 95/46/EC, *supra* note 7, art. 25(1).

[74] Case C-101/01, Judgment of the Court of 6 November 2003, Criminal Proceedings Against Bodil Lindqvist, http://curia.europa.eu/juris/showPdf.jsf?text=&docid=48382&pageIndex=0&doclang=en&mode=doc&dir=&occ=first&part=1&cid=42578.

[75] *Id*.

[76] CHRISTOPHER KUNER, EUROPEAN DATA PROTECTION LAW: CORPORATE COMPLIANCE AND REGULATION 186 (2007).

[77] Directive 95/46/EC, *supra* note 7, art. 25(2).

[78] *Id*. art. 25(3).

[79] *Id*.

- existing enforcement mechanisms.[80]

The Data Protection Directive contains a number of derogations to the general prohibition on transfers to a third country. Thus, national law may provide that a transfer of personal data to a third country that does not meet the adequacy criterion is possible on several grounds, including, inter alia, the following:

- Where the individual has granted his unambiguous consent to the proposed transfer
- Where the transfer is necessary for the performance of a contract between the individual and the controller
- Where the transfer is necessary for the protection of the vital interests of the individual
- Where the transfer is necessary or is required by law based on significant public interest grounds[81]

Q. EU Members' Authorization

EU Members may also authorize a transfer of personal data to a third country that does not meet the adequacy criterion if the controller adopts one of two options to ensure that personal data are protected: (a) contractual clauses, or (b) corporate binding rules.[82] A controller who intends to use contractual clauses may avail him or herself of standard contractual clauses adopted by the Commission or other customized clauses. No prior authorization is needed for a transfer of data if standard contractual clauses are used. Corporate binding rules are designed to be used by multinational corporations that transfer tremendous amounts of data within a group of companies when some are outside the EU.[83] EU Members must notify the Commission and other EU Members of authorizations granted.

R. Safe Harbor Agreement

The US Department of Commerce and the European Commission have concluded a Safe Harbor Agreement to ensure that personal data transfers from the EU to the US meet the required adequacy criterion. US corporations that are or will be engaged in the processing of EU data are

---

[80] Working Document, Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection Directive, DG XV D/5025/98, WP 12 (July 24, 1998), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1998/wp12_en.pdf.

[81] Directive 95/46/EC, *supra* note 7, art. 26, para. 1.

[82] *Id.* art. 26, para. 2.

[83] The Article 29 Working Party has published three papers on the procedure for approval of Binding Corporate Rules (BCRs): (a) Working Document: Binding Corporate Rules (2003); (b) Model Checklist: Application for Approval of Binding Corporate Rules (2004); and (c) Working Document Setting Forth a Cooperation Procedure for Issuing Common Opinion on Adequate Safeguards Resulting from "Binding Corporate Rules" (2005). *See* list of documents prepared by the Working Party, http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/index_en.htm (last visited June 30, 2012).

legally obliged to adhere to the standards, as contained in the Directive. The Safe Harbor Agreement contains the Safe Harbor Principles[84] and a set of "Frequently Asked Questions."[85] The European Commission has issued decisions on the adequacy of the protection of personal data in third countries with regard to the domestic law of the following countries and the listed arrangements: Andorra, Argentina, Australia, Canada, Switzerland, the Faeroe Islands, Guernsey, the State of Israel, the Isle of Man, Jersey, the US Department of Commerce's Safe Harbor Privacy Principles, and the transfer of Air Passenger Name Record Data to US Customs and Border Protection.[86]

III. European Court of Justice Decisions

A. Limitations on the Right to Personal Data

In general, the right to privacy and right to protection of personal data are subject to limitations imposed by the principle of proportionality and the case law of the European Court of Justice (ECJ). Most of the legal issues on data protection that reach the ECJ are in the form of requests for a preliminary ruling forwarded by the national courts.

The European Court of Justice (ECJ) held in the case of *Volker und Markus Schecke v. Land Hessen* that the right to protection of personal data is not an absolute right, but must be viewed in relation to its function in society and be balanced against any other fundamental human rights based on the principle of proportionately.[87] Proportionality, a well-established principle in the legal order of the EU Members and the case law of the ECJ, allows limitations on the exercise of fundamental rights as long as they are provided by law and respect the core of such rights. Article 52(1) of the Charter of Fundamental Rights provides that "subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet the objectives of general interest recognized by the Union or the need to protect the rights and freedoms of others."[88] In the *Schecke* judgment, the ECJ held that the pursuit of the objectives of the EU must be balanced with the fundamental rights of article 7 and 8 of the Charter, dealing with privacy and personal data protection. Specifically, the ECJ held that the Council and Commission must balance the European Union's interest in increasing security by

---

[84] *Safe Harbor Privacy Principles*, US DEPARTMENT OF COMMERCE (July 21, 2000), http://export.gov/safeharbor/eu/eg_main_018475.asp.

[85] *Frequently Asked Questions*, US DEPARTMENT OF COMMERCE http://export.gov/faq/index.asp (last updated Mar. 21, 2012). *See also* Commission Decision (EC) 2000/520 of 26 July 2000 Pursuant to Directive (EC) 95/46 On the Adequacy of the Protection Provided by the Safe Harbor Privacy Principles and Related Frequently Asked Questions Issued by the US Department of Commerce, 2000 O.J. (L 215) 7, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:215:0007:0047:EN:PDF.

[86] *Commission Decisions on the Adequacy of the Protection of Personal Data in Third Countries*, EUROPEAN COMMISSION, http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm (last updated Oct. 4, 2012).

[87] Joint Cases C-92/09 and C-93/09, Volker und Markus Schecke GbR, Hartmut Eifert v. Land Hessen, Judgment of the Court (Grand Chamber) (Nov. 9, 2010), http://curia.europa.eu/juris/liste.jsf?language=en&jur=C,T,F&num=C-92/09&td=ALL.

[88] Article 52(1) of the Charter of Fundamental Rights of the EU, *supra* note 2, provides for limitations only when they are provided by law and observe the essence of those rights and freedoms.

fighting crime against "the interference with the right of the beneficiaries concerned to respect for their private life in general and to the protection of their personal data in particular."[89]

B. Downloading Songs Illegally

On February 16, 2012, the ECJ rendered an important judgment on the illegal downloading of songs by Internet users. The ECJ held that online social networking sites cannot be forced to take measures, such as installing filtering systems, in order to prevent users from downloading songs illegally.[90] The case arose in 2009 when Sabam, a Belgian national music royalty collecting society, sought an injunction from the Court of First Instance in Belgium to require Netlog—a social networking site similar to Twitter and Facebook—to take measures in order to prevent users from downloading songs illegally or pay a penalty of €1,000 daily in the case of noncompliance. The Belgian Court asked for a preliminary ruling on whether European Union law precludes a national court from issuing an injunction against an Internet service hosting provider that obliges it to install a filtering system at its own expense and for an unlimited period, which would apply indiscriminately to all of its users.

The ECJ first confirmed that Netlog meets the requirements of a hosting service provider, that the filtering system would enable Netlog to identify all the files stored on its servers by the service users, and that those files may contain works that belong to copyright holders. Consequently, the ECJ reasoned, hosting service providers such as Netlog would have to ascertain which of these stored files contain works that are unavailable to the users unlawfully and would have to prevent such files through filtering systems.[91]

The ECJ noted that national authorities, in protecting the rights of copyright holders, must balance the rights of such holders against the fundamental rights of users, such as the right to their personal data and the right to receive and impart information, which would likely be impacted by such measures. The ECJ affirmed that the e-Commerce Directive prohibits the "general monitoring of the information stored on its servers." The ECJ held that

> in adopting an injunction requiring the hosting service provider to install such a filtering system, the national court would not be respecting the requirement that a fair balance be struck between the right to intellectual property, on the one hand, and the freedom to conduct business, the right to protection of personal data and the freedom to receive or impart information, on the other.[92]

---

[89] Volker und Markus Schecke GbR, Hartmut Eifert v. Land Hessen, ¶¶ 76, 77.

[90] Press Release, Court of Justice of the European Union, The Owner of an Online Social Network Cannot be Obliged to Install a General Filtering System, Covering All Its Users, in Order to Prevent the Unlawful Use of Musical and Audio-Visual Work (Feb. 16, 2012), http://curia.europa.eu/jcms/upload/docs/application/pdf/2012-02/cp120011en.pdf.

[91] *Id.*

[92] Case C360/10, Judgment of the ECJ (Third Chamber), Feb. 16, 2012, Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v. Netlog, NV, para. 52, http://curia.europa.eu/juris/document/document.jsf?text=&docid=119512&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=44646.

C. Annulment of the US-EU Passenger Name Record Agreement

On May 30, 2006, the ECJ annulled the Commission's Decision of the adequacy finding and the Council Decision related to the conclusion of a Passenger Name Record Agreement between the US and the EU.[93] On December 11, 2011, the Council of the EU adopted a decision on the Conclusion of the Agreement between the United States of America and the European Union on the Use and Transfer of Passenger Name Records to the United States Department of Homeland and Security.[94]

IV. Public and Scholarly Opinion

A public consultation was initiated by the Commission following the publication of its 2010 Communication, "A Comprehensive Approach on Personal Data Protection in the European Union," with a deadline of January 2011.[95] The Commission received a total of 305 responses—54 from citizens, 31 from public authorities and 220 from business associations, and nongovernmental organizations. The respondents provided opinions on issues identified as critical by the Commission. On improving individuals' rights, the majority of stakeholders felt that "the current lack of harmonization is detrimental to economic activity within the EU."[96] Big companies were keen on having a uniform framework. On increasing transparency of the processing of personal data, even though this principle is embedded in the Personal Data Directive, some respondents called for improvement of the current status. The protection of children from online activities was of paramount importance to citizens. Many respondents urged the adoption of a cut-off age and specific requirements for the processing of children's data, while others called for no specific and detailed provisions on children based on differing rules for the definition of a child among EU Members and the divergence in maturity levels in children. In particular, the issue of data protection authorities was among other issues that drew concern, including data minimization, the right to be forgotten, data portability, and ensuring informed and free consent. Data protection authorities, public institutions and the European Data Protection Supervisor (EDPS) endorsed the initiative of introducing data protection officers, albeit with some skepticism due to the financial and administrative burdens associated with them.[97]

---

[93] Cases C-317/04 & C-318/04, European Parliament v. Council of the European Union and Commission of the European Communities, 2006 E.C.R. I-04721, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62004CJ0317:EN:PDF.

[94] Council of the European Union, Agreement Between the United States of America and the European Union on the Use and Transfer of Passenger Name Records to the United States Department of Homeland Security, 17434/11 (Dec. 8, 2011), http://register.consilium.europa.eu/pdf/en/11/st17/st17434.en11.pdf.

[95] *Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, A Comprehensive Approach on Personal Data Protection in the European Union*, COM (2010) 609 final (Nov. 4, 2010), http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf.

[96] Annex 4, Summary of Replies to the Public Consultation on the Commission's Communication on a Comprehensive Approach on Personal Data Protection in the European Union, at 54, http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_annexes_en.pdf.

[97] *Id*. at 64.

Eurobarometer, the Commission's public opinion analysis section, conducted a large-scale survey of attitudes of European citizens toward the processing of personal data protection and privacy issues.[98] Some notable highlights include the following:

- Six out of ten Internet users usually read privacy statements and 70% of those modify their decisions accordingly[99]
- 62% of Europeans provide the minimum data required
- 70% of Europeans believe that their personal data held by companies could be used for other purposes than those originally collected[100]
- 74% of Europeans view the disclosure of personal data as part of technological developments and globalization
- The majority of Europeans feel uncomfortable about internet profiling [101]
- 98% of the participants in Greece and Cyprus; 97% in the Czech Republic; and 96% in Ireland, Malta, and Slovakia responded that specific consent is required prior to processing[102]

During a conference in Luxembourg in May 2012, the European Union Data Protection Commissioners (130 commissioners from thirty-eight European countries) adopted a Resolution on the pending EU and Council of Europe reforms. The Resolution endorsed the following proposals from the EU proposed legislative package:

- Codification of the principle of data minimization
- More options for redress granted to data subjects whose data are violated
- Specific provisions on children, the right to be forgotten, and the right of portability
- Strengthening the right of access and the right to object[103]

---

[98] EUROPEAN COMMISSION, SPECIAL EUROBAROMETER 359: ATTITUDES ON DATA PROTECTION AND ELECTRONIC IDENTITY IN THE EUROPEAN UNION (June 2011), http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf.

[99] *Id*. at 115.

[100] *Id*. at 146.

[101] *Id*. at 74.

[102] *Id*. at 149.

[103] Spring Conference 2012 of the European Data Protection Commissioners, Resolution on the European Data Protection Reform (Luxembourg, May 3–4, 2012), http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Cooperation/Conference_EU/12-05-04_Spring_conference_Resolution_EN.pdf.

V. Pending Reforms

Since 1995, when the EU put in place fundamental rules on personal data protection, technology and globalization have drastically affected the processing of personal data. Social networks altered the methods of sharing information and the advent of cloud computing, by which more data is stored on remote servers rather than personal computers, poses new challenges.[104] At the same time, the 1995 Data Protection Directive did not achieve the anticipated level of harmonization of data protection rules in the EU. Meanwhile, according to estimates, 250 million people are daily users of the Internet in Europe,[105] and European citizens are becoming increasingly aware of risks to their privacy and personal data posed by online activities. The Commission's 2010 Communication, A Comprehensive Approach on Personal Data Protection in the European Union, emphasized that the EU "needs a more comprehensive and coherent policy on the fundamental right to personal data protection."[106] The Commission's efforts have garnered support from the Parliament[107] and the Justice and Home Affairs Council of the EU. The latter, in its February 2011 conclusions, agreed with a number of the proposed changes.[108]

On January 25, 2012, the European Commission published its proposal for the reform of EU legislation on data protection. The twin objectives of the proposal remain the same as that of the Data Protection Directive. The pending reform is designed to meet the challenges posed by contemporary Internet developments and to safeguard personal data irrespective of future changes in technology and the digital environment.

The Commission's reform package contains two legislative pieces: (a) a draft regulation on the Processing of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation),[109] and (b) a Directive on the

---

[104] On July 20, 2012, the European Commission announced that a communication addressing a variety of aspects of cloud computing will be published soon. According to the announcement, the communication will be divided into three sections: personal data protection and security, copyright, and standardization. As far personal data, the communication will address issues such as whether cloud providers should be required to provide a back-up copy, applicable law when the user of a cloud service is a non-EU citizen, and transfers of personal data outside the EU. News Release, EurActiv, Brussels to Unveil EU Cloud Computing Strategy (July 20, 2012), http://www.euractiv.com/infosociety/brussels-unveil-eu-cloud-computi-news-514012.

[105] European Commission, How Does the Data Protection Reform Strengthen Citizen's Rights? http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/2_en.pdf (last visited June 25, 2012).

[106] COM (2010) 609 final, *supra* note 95.

[107] European Parliament: Resolution of July 6, 2011 on a Comprehensive Approach on Personal Data Protection in the European Union (2011/2025(INI)), http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2011-0323+0+DOC+XML+V0//EN.

[108] *Council of the EU, Council Conclusions on the Communication from the Commission to the European Parliament and the Council – A Comprehensive Approach on Personal Data Protection in the EU*, 3071st Justice and Home Affairs Council Meeting, Brussels, 24 and 25 February 2011, http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/119461.pdf.

[109] *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)* [hereinafter Draft Regulation], COM (2012) 11 final (Jan. 15, 2012), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:EN:PDF.

Protection of Individuals with Regard to the Processing of Personal Data by Competent Authorities for Criminal Offenses.[110] The Commission opted for a regulation because of its direct applicability in the legal order of the EU Member States and because, once it is enforced, it will result in greater legal certainty and improve the protection of personal data of individuals. The draft regulation is based on the new legal basis established by article 16 of the TFEU, and once adopted by the Council and the Parliament it will repeal the Data Protection Directive.

In its March 2012 Opinion on the Data Protection Reform Proposals,[111] the Article 29 Data Working Party endorsed certain proposals contained in the draft regulation that are designed to improve data subjects' rights, enhance the responsibility of controllers, and strengthen the position of supervisory authorities at the national and international levels.[112] However, it criticized the introduction of a separate Directive to protect personal data in the area of police and criminal justice because of its potential to result in less consistency and less protection of data subjects.[113] Moreover, it opined that the provisions of the Directive need to be aligned with those of the Regulation, so that personal data are well safeguarded. The Data Protection Working Party expressed its regret that neither instrument deals with the issue of the collection and transfer of data by private parties or non-law enforcement public authorities for law enforcement purposes. It also expressed its reservations regarding the Commission's authority, granted by the draft regulation, to adopt delegated and implementing acts to fully implement the regulation.[114]

A. Definitions and Basic Principles

The draft regulation incorporates the same definitions introduced by the Data Protection Directive, while modifying and improving others. It also defines new terms, such as "genetic data," "biometric data," "data concerning health," "group of undertakings," "binding corporate rules," "child," and "supervisory authority."[115] In general, the draft regulation applies the same principles on data protection as those introduced by article 6 of the Data Protection Directive. The draft regulation adds the principles of transparency, clarifies the data minimization principle, and reinforces a comprehensive scheme of responsibilities and liabilities of the controller. The draft regulation requires controllers and processors to implement a number of policies and technical and organizational measures to ensure data security.[116] A significant innovation is the

---

[110] *Proposal for a Directive of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of Prevention, Investigation, Detection or Prosecution of Criminal Offenses or the Execution of Criminal Parties and the Free Movement of Such Data*, COM (2012) 10 final (Jan. 25, 2012), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0010:FIN:EN:PDF.

[111] Article 29 Data Protection Working Party, *Opinion 01/2012 on the Data Protection Reform Proposals*, 00530/12/EN, WP 191 (Mar. 23, 2012), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp191_en.pdf.

[112] *Id.* at 4.

[113] *Id.* at 5.

[114] *Id.* at 7.

[115] Draft Regulation, *supra* note 109, art. 4.

[116] *Id.* art. 22.

requirement of notification of the supervisory authority within twenty-four hours in case of a personal data breach,[117] and notification of the data subject if the breach will adversely affect the privacy and personal data of individuals.[118] Moreover, it also imposes an obligation on controllers and processors to maintain documentation of all processing operations under their responsibility.[119]

B. Processing of Special Categories of Data

The draft regulation prohibits the processing of personal data that indicate race or ethnic origin, political opinions, religion or beliefs, and trade union membership, and the processing of genetic data or data concerning the subject's health or sex life, criminal convictions, or related security measures.[120] The list of special categories of data is broader than that of the Data Protection Directive because it includes genetic data, criminal convictions, and related security measures.

The Regulation permits the processing of sensitive data under safeguards similar to those provided for in article 8 of the Data Protection Directive.

C. Processing of Health Data

The processing of health data is given added protection by the draft regulation. Thus, processing of such data is permitted on the basis of EU law or Member State law, which must include suitable safeguards to protect the interests of the data subjects, and for the following reasons:

- For preventive or occupational medicine, medical diagnosis, or health care services subject to professional secrecy[121]
- Public interest reasons in the field of public health or in areas such as social protection[122]
- For historical, statistical, or scientific research purposes with the proviso that such purposes cannot otherwise be fulfilled[123]

D. Conditions for Consent

The draft regulation provides a more comprehensive definition of consent than that of the Data Protection Directive through the addition of the word "explicit." This means "any freely

---

[117] *Id*. art. 31, para. 1.

[118] *Id.* art. 32, para. 1.

[119] *Id*. art. 28.

[120] *Id*. art. 9.

[121] *Id.* art. 81.

[122] *Id.*

[123] *Id*. art. 83.

given specific, informed and *explicit* indication" of the data subject's wishes that is either provided in a statement or in a clear affirmative action indicates agreement to personal data being processed.[124] The Regulation places the burden of proof of the data subject's consent on the controller who processes the personal data for specified purposes. Individuals have the right to withdraw their consent at any time. When there is a significant imbalance between the position of the data subject and the controller, mere consent given by an individual will not provide the basis for processing.[125]

E. Data Protection by Design and by Default

An innovation of the draft regulation is the requirement that controllers must incorporate appropriate technical and organizational measures at an early stage when they determine the means of processing and also at the time of processing itself.[126] Moreover, processors will be required to ensure that, by default, only those data are processed "which are necessary for each specific purpose of the processing," and that such data are not retained in larger quantities or for a longer period of time than is necessary.[127]

The privacy by design principle is also espoused by the US Federal Trade Commission, which incorporates this principle as one of its key recommendations to companies in a March 2012 report on protecting consumer privacy.[128]

F. Rights of the Data Subject

The draft regulation introduces a new requirement for controllers to provide transparent, easily accessible, and understandable information on personal data protection.[129] Controllers are obliged to inform the data subjects without delay and at the latest within one month of receipt of the request whether any action has been taken regarding any rectification or erasure pertaining to his/her personal data.[130]

---

[124] *Id.* art. 4, para. 8 (emphasis added).

[125] *Id*. art. 7.

[126] *Id.* art. 23, para. 1.

[127] *Id.* art. 23, para. 2.

[128] FEDERAL TRADE COMMISSION, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS (Mar. 2012), http://www.ftc.gov/os/2012/03/120326 privacyreport.pdf. Other recommendations include the "do not track mechanism," which can be used by consumers who do not want their online activities to be followed, and greater transparency by companies to disclose what type of data and for what purpose it is used.

[129] Draft Regulation, *supra* note 109, art. 11.

[130] *Id*. art. 12, para. 2.

G. Right to Rectification

Data subjects have the right to request that the controller rectify personal data that are inaccurate and communicate such rectification to the data subject.[131]

H. Right to Be Forgotten and to Erase

Data subjects have the right to obtain from the controller the erasure of personal data and assurance that the controller will abstain from further dissemination of such data, especially of data made available by the data subject related to his/her childhood and when one of the following reasons apply:

- The data are no longer needed in relation to the purpose for which they were initially collected or processed
- The data subject has withdrawn his/her consent on which the processing was based, or the storage period has expired
- The data subject objects to the processing of personal data on grounds related to his/her particular situation
- The processing of data is not compatible with the Regulation for other reasons[132]

On May 13, 2014, the Grand Chamber of the European Court of Justice (ECJ) delivered its judgment in a case involving a Spanish national and Google Inc., in which it upheld the request of the Spanish national to order Google to withdraw personal data related to him and to prevent further access to such data. (Judgment of the ECJ (Grand Chamber), Case C-131/12, Google Spain SL, Google Inc v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González (May 13, 2014), EURLEX, http://curia.europa.eu/juris/celex.jsf?celex=62012CJ0131&lang1=en&type=TXT&ancre=.)

I. Right to Data Portability

The draft regulation provides for a new right for data subjects not previously included in the Data Protection Directive: the right of data portability.[133] This right grants the data subject, when personal data are processed by electronic means, the right to obtain from the controller a copy of data that are processed in an electronic and structured format and, which allows for further use by the data subject.[134]

J. Right to Object

The right to object is entrusted to data subjects at any time during processing where the objection is based on grounds such as safeguarding the vital interests of the data subject, performing a task carried out in the public interest, or for purposes of the legitimate interests of the controller. As far as direct marketing, the data subject will have the right to object free of charge. Such a right will be available to the data subject in a manner that is easily understood and is distinct from other information.[135]

---

[131] *Id*. art. 16.

[132] *Id*. art. 17, para. 1.

[133] *Id*. art. 18.

[134] *Id*. para. 1.

[135] *Id*. art. 19, paras. 1–2.

K. Profiling

The draft regulation introduces a distinct article related to profiling measures, in contrast to the Data Protection Directive, which did not specifically address this issue. Article 20 of the draft regulation states that every data subject

> [s]hall have the right not to be subject to a measure which produces legal effects concerning this natural person or significantly affects this natural person, and which is based solely on automated processing intended to evaluate certain personal aspects relating to this natural person or to analyze or predict in particular the natural person's performance at work, economic situation, location, health, personal preferences, reliability or behavior.[136]

Profiling of a data subject is possible in the following instances:

- Processing of personal data is necessary for entering into or performing a contract that was initiated by the data subject and suitable safeguards have been added
- Processing is expressly authorized either in the laws of EU Member States or in EU legislation (national legislation must also provide additional safeguards to protect the legitimate interests of a data subject)
- The data subject has given his/her consent, subject to the specific requirements pertaining to consent, as included in article 7[137]

The Article 29 Working Party, in its Opinion 01/2012, agreed with the conditions on profiling.[138] However, it opined that the issue of profiling is a complex one in an online environment, that profiling should not be limited to automated processing, and that the term "significantly affects" is vague. It also opined that profiling should cover the creation of personal profiles by social networks or the creation of motion profiles by mobile applications.[139]

L. Protection of Minors

Article 8, paragraph 1 of the draft regulation requires that consent be given or authorized by a child's parent or legal guardian when the information society offers services directly to a child and the child concerned is below the age of thirteen. Only upon consent by the appropriate parent or legal guardian is the processing of a child's personal data lawful.[140] General contract law provisions of the EU Members with regard to the formation, validity, or effect of a contract as it relates to a child remain unaffected. The Commission has the power to adopt delegated acts

---

[136] *Id*. art. 20, para. 1.

[137] *Id*. para. 2

[138] Article 29 Data Protection Working Party, *Opinion 01/2012*, *supra* note 111.

[139] *Id*.

[140] Draft Regulation, *supra* note 109, art. 8, para. 1.

regarding specific criteria and requirements in order to obtain "verifiable consent," and the Commission may also establish standard forms for specific ways to obtain verifiable consent.[141]

VI. Role of Data Protection Authorities

A. EU Level: European Data Protection Supervisor

Similarly to the EU Member States, which are bound by the EU legislation on data protection, EU institutions and bodies are required to ensure that the right to privacy and the right of personal data protection are respected. The European Data Protection Supervisor, an independent supervisory authority, was established on the basis of article 41 of Regulation 45/2001,[142] and is in charge of ensuring that EU institutions adhere to the rules on protection of personal data. It also monitors the application of the said Regulation and other EU legislation on personal data and advises the Community institutions on any aspect affecting personal data.[143]

The draft regulation proposes the establishment of a European Data Protection Board (EDPB). The EDPB will be an independent body and will play an advisory role to the Commission. It will consist of the head of the supervisory authority of each Member State and the European Data Protection Supervisor.[144] It will replace the Article 29 Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, created under the Personal Data Protection Directive. National supervisory authorities will be required to communicate any draft measure that may, inter alia, affect the free movement of personal data to the EDPB and the Commission.[145]

B. Member States

Similarly to the Data Protection Directive, the draft regulation requires each Member to designate one or more public authorities to monitor the application of the rules of the Regulation. One supervisory authority will act as a contact point and participate in the EDPB. Members of national supervisory authorities must be appointed by the parliament or the government of each EU Member and be selected from among individuals whose independence is beyond any doubt.

The draft regulation expands the role of the supervisory authorities to cooperate with each other and with the Commission. Based on the decision of the ECJ in the case of *Commission v. Germany*, which dealt with the independence of supervisory authorities, the Draft Regulation

---

[141] *Id*. paras. 3–4.

[142] Regulation (EC) No. 45/2001 of the European Parliament and of the Council of 18 December 2000 On the Protection of Individuals with Regard to the Processing of Personal Data by the Community Institutions and Bodies and on the Free Movement of Such Data, 2001 O.J. (L 8) 1, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:008:0001:0022:EN:PDF.

[143] *See* EUROPEAN DATA PROTECTION SUPERVISOR, http://www.edps.europa.eu/EDPSWEB/edps/EDPS?lang=en (last visited June 25, 2012).

[144] Draft Regulation, *supra* note 109, art. 64.

[145] *Id*. art. 58.

also expands on the independence of supervisory authorities.[146] Each supervisory authority has competence within the territory of the Member State where it is located. The draft regulation proposes a "one-stop shop" by which a supervisory authority is granted additional competence when a controller or a processor is established in several Member States.[147] The supervisory authority is required to prepare annual reports describing the application and enforcement of data protection rules in the individual Member States.

The draft regulation makes a distinction between duties assigned to the supervisory authorities and powers bestowed on them. Supervisory authorities have the following duties:

- Monitoring the application of the provisions of the draft regulation
- Hearing and investigating complaints either on its own initiative or based on complaints by the data subject, which must be handled free of charge
- Approving binding rules
- Issuing opinions on the draft codes of conduct adopted pursuant to article 38(2)
- Promoting public awareness of the risks, rules, safeguards, and rights of individuals[148]

Some of the key powers of the supervisory authorities are the following:

- Notifying the controller or the processor of an alleged breach of the rules on processing of personal data and ordering both to remedy the situation
- Imposing a definite or temporary ban on processing
- Bringing to the attention of judicial authorities violations of the rules contained in the regulation
- Engaging in legal proceedings, in case an individual or a legal person initiates legal action against a decision of a supervisory authority
- Ordering the controller and processor to comply with the requests of data subjects
- Ordering the rectification, erasure, or destruction of data processed in violation of the draft regulation
- Imposing a ban on processing
- Suspending data flows to a recipient in a third country or to an international organization
- Issuing opinions on issues involving personal data protection[149]

---

[146] Case C-518/07, Judgment of the ECJ, Grand Chamber, March 9, 2010, European Commission v. Federal Republic of Germany, http://curia.europa.eu/juris/liste.jsf?language=en&num=C-518/07.

[147] Draft Regulation, *supra* note 109, art. 51.

[148] *Id.* art. 52.

[149] *Id.* art. 53.

C. Designation of Data Protection Officers

An additional safeguard envisioned by the draft regulation is the designation of a data protection officer by controllers or processors when the processing of personal data is carried out by a public authority or by an enterprise that employs 250 persons or more, or when the processing requires the regular and systematic monitoring of data subjects because of its scope and purpose.[150]

VII. Remedies, Liabilities, and Sanctions

In general, the rights of data subjects are clarified and improved by the draft regulation. Chapter VIII of the Draft Regulation is composed of seven articles and lists the following rights of data subjects: (a) to file a complaint with a supervisory authority, (b) to a judicial remedy against a supervisory authority, (c) to a judicial remedy against a controller or a processor, and (d) to compensation and liability. It also introduces common rules on court proceedings.[151]

Moreover, the draft regulation empowers supervisory authorities to impose effective, proportionate, and dissuasive penalties.[152] A supervisory authority is authorized to impose an administrative fine of €250,000 (about US$ 306,500) to a natural person who processes personal data without a commercial interest after a repeat noncompliance with the Draft Regulation. If it is an enterprise, or an organization that employs less than 250 persons, the fine will be up to 0.5% of its annual worldwide turnover.[153] A warning is issued with no fine to first time offenders, either individuals or companies.[154]

Another positive aspect is that the draft regulation reinforces the right of organizations and associations engaged in protecting the rights of data subjects to lodge a complaint with a supervisory authority.[155] This right can be exercised irrespective of a complaint initiated by a data subject.[156]

VIII. Territorial and Extraterritorial Application of the Draft Regulation

The territorial scope of the draft regulation extends to the processing of personal data when a controller or processor is established in the European Union.[157] It also has extraterritorial application when the processing of personal data of individuals who reside within

---

[150] *Id*. art. 35.

[151] *Id*. arts. 73–79.

[152] *Id*. art. 79, paras. 1–2.

[153] *Id*. art. 79, paras. 3–4.

[154] *Id*.

[155] *Id*. art. 73, para. 2.

[156] *Id*. art. 73, para. 3.

[157] *Id*. art. 3, para. 1.

the EU is undertaken by a processor who is not established in the EU, but the processing relates to one of the following two activities: (a) the provision of services and goods to individuals within the EU, or (b) the monitoring of their behavior.[158]

Similarly to the Data Protection Directive, a transfer of personal data to a third country or an international organization may take place, provided that the Commission has issued an adequacy decision. In such a case there is no need for further authorization.[159] Adequacy decisions will be published in the Official Journal of the European Union. The United States has already expressed its concern that US companies would be subject to stricter data protection rules.[160]

In the absence of an adequacy decision, a controller or processor may transfer personal data to a third country, provided that additional safeguards have been taken in a legally binding instrument, such as binding corporate rules or standard data protection clauses adopted by the Commission.[161]

Theresa Papademetriou
Senior Foreign Law Specialist
June 2012

[158] *Id*. art. 3.

[159] *Id*. art. 41.

[160] *US Lobbying Waters Down EU Data Protection Reform*, EURACTIV (Feb. 21, 2012), http://www.euractiv.com/specialreport-data-protection/us-lobbying-waters-eu-data-prote-news-510991.

[161] Draft Regulation, *supra* note 109, art. 42.