Bloomberg BNA | Bloomberg Law®: Privacy & Data Security

Reproduced with permission from Bloomberg Law: Privacy & Data Security, http://www.bna.com/bloomberg-law-privacy-data-security/.

Profile: EUROPEAN UNION

Cédric Burton and Sarah Cadiot, of Wilson Sonsini Goodrich & Rosati, Brussels, provided expert review of the EU Profile and wrote the Risk Environment section. They are grateful to Anna Ciesielska, legal intern in the firm's Brussels office, for her excellent research assistance.

I. Applicable Laws and Regulations

A. General Overview of EU Law

1. Sources of EU Law

Privacy is a fundamental right under the law of the European Union (EU). The constitutional aspects of EU law are provided in the Treaty on the Functioning of the European Union (TFEU) and the Treaty on European Union (TEU). The TFEU codifies the right to protection of personal data concerning individuals (art. 16). In addition, the Charter of Fundamental Rights of the European Union (the Charter) reaffirms rights provided in earlier European legal instruments in a single document that applies to the entire EU, and it includes the right to respect for one's private and family life, home and communications, and protection of personal data under Articles 7 and 8.

In parallel, the Council of Europe (CoE)—a separate institution from the European Union, composed of 47 countries—adopted the European Convention on Human Rights (ECHR) in 1950. Under the ECHR, the right to respect for one's private and family life, home, and correspondence is a fundamental right (art. 8). The ECHR prohibits interference with this right unless it is in accordance with the law and necessary in the interests of national security, public safety, or the economic well-being of the country; for the prevention of disorder or crime; for the protection of health or morals; or for the protection of the rights and freedoms of others. Member States of the CoE are signatories to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention) opened for signature in January 1981. In addition, amendments to the Convention were proposed in 1999, and an Additional Protocol in 2001.

While all EU countries are parties to the ECHR, the EU itself is not. However, the TEU binds the EU to join the ECHR (art. 6(2) of TEU). In this regard, a draft agreement on the accession of the EU to the ECHR was prepared and submitted to the Court of Justice of the European Union (CJEU) for opinion. On December 18, 2014, the CJEU declared that this draft agreement was not compatible with EU law, and there has been no significant progress since then.

2. EU Legal Instruments

Under the EU treaties (*i.e.*, TEU and TFEU), the EU institutions can pass various types of statutory acts. Some of them are directly binding on EU countries, namely: (i) regulations (*i.e.* , a legislative act that applies automatically in its entirety across the EU), (ii) directives (*i.e.* , a legislative act that sets out a goal and minimum requirements that all EU countries must implement into their national legal order within a certain period of time), and (iii) decisions (*i.e.*, a directly applicable act only to those to whom the decision is addressed, such as an EU country or a company). Non-binding acts include recommendations and opinions. In addition, the EU institutions and certain EU agencies can adopt technical or sector-specific requirements that are binding and apply across the EU.

3. EU Institutions

The EU institutions play a key role in the initiative, preparation, negotiation, adoption and/or enforcement of the different EU acts. The EU institutions comprise seven institutions, including the European Parliament, the European Council, the Council of the EU (Council—which is a different body from

the Council of Europe (CoE)), the European Commission (Commission), the Court of Justice of the European Union, the European Central Bank, and the Court of Auditors. In brief, the EU legislative process involves the Commission—often defined as the executive arm of the EU—which initiates the legislative proposals and has enforcement powers in certain sectors—and the European Parliament which shares the legislative power with the Council.

B. Privacy and Data Protection Directives and Regulations

The main legal instrument for EU data protection law is Directive 95/46/EC on the protection of personal data (Directive 95/46/EC). Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive 2002/58/EC), as amended by Directive 2009/136/EC, is a specific act regulating the processing of personal data in the electronic communications sector.

1. Directive 95/46/EC

a. General Information

Directive 95/46/EC is the primary legislative instrument for data protection at the EU level. It has been implemented in EU countries' laws. For instance, in France, Act No. 78-17 of January 6, 1978, has been modified to include the requirements of Directive 95/46/EC; in Italy, this Directive has been transposed to Legislative Decree No. 196 of June 30, 2003, Personal Data Protection Code. Directive 95/46/EC sets forth the minimum data protection standards. Directive 95/46/EC and its implementation into national law will be replaced by the upcoming General Data Protection Regulation.

Directive 95/46/EC applies in two broad situations. First, it applies to the data processing carried out in the context of the activities of an establishment of a data controller on the territory of an EU country. In addition, it applies when the data controller is not established in the EU, but makes use of equipment and means in the EU for the purposes of processing personal data, unless such equipment is used only for purposes of transit through the EU.

Directive 95/46/EC provides a set of specific definitions related to data protection (art. 2), including:

- "Personal data" means the information that relates to an identified or identifiable person; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;
- "Data controller" means a natural or legal person who determines the purposes and the means of data processing;
- "Data processor" means a natural or legal person who processes personal data on behalf of the data controller; and
- "Data processing" covers such operations as collection, recording, organization, alteration, disclosure, and all other possible uses of personal data.

b. Data Processing Principles

Directive 95/46/EC requires data controllers to comply with a number of data protection principles (art. 6), including:

- *Legal ground*. Data processing must be fair and lawful. Data controllers must rely on one of the legal grounds provided in Directive 95/46/EC, *i.e.*, consent of the individual; performance of a contract; legal obligation; processing being necessary to protect vital interests of the individual; performance of a task carried out in the public interest; or processing being necessary for the purposes of the legitimate interests of the data controller (art. 7).
- *Purpose limitation*. Data processing can only be conducted for specific, explicit and legitimate purposes. Data controllers may only process personal data as necessary for the purposes of the data processing, not for purposes that are incompatible with the purpose of collection.
- *Limited period of data retention*. Data controllers must not keep personal data for longer than it is necessary for the designated purposes.
- *Data quality*. Personal data must be accurate and kept up-to-date as necessary. Data controllers should take every reasonable step to ensure that personal data is not inaccurate or incomplete for the designated purposes.

c. Cross-border Data Transfer Restrictions

Directive 95/46/EC prohibits the transfer of personal outside the EEA to a country which does not provide an adequate level of data protection (art. 25–26). The Commission may determine that a third country ensures an adequate level of protection of personal data through its domestic law or through international commitments into which it has entered. Whether a third country provides an adequate level of data protection is determined based on an assessment of all the circumstances surrounding a data transfer, with particular consideration to the nature of the personal data, the purpose and duration of the proposed data processing, the country of origin and country of final destination, the general and sectoral rules of law in force in the third country, and the professional

rules and security measures in that country. In light of these criteria, the Commission may conclude that a country provides an appropriate level of data protection and adopt an adequacy decision to officially recognize this status.

So far, only ten countries have been recognized as providing an adequate level of protection to personal data (i.e., Andorra, Argentina, the Faroe Islands, Guernsey, the Isle of Man, the State of Israel, Jersey, New Zealand, Switzerland, the Eastern Republic of Uruguay). In addition, the Commission adopted an adequacy decision in relation to the Canadian Personal Information Protection and Electronic Documents Act (PIPEDA). This adequacy decision allows EU organizations to send certain personal data to Canadian recipients who are subject to PIPEDA without any additional safeguards. The up-to-date list of third countries and sectors recognized as providing an adequate level of protection to personal data can be found at the Commission's webpage.

In addition, the Commission had recognized the EU-U.S. Safe Harbor Framework as providing an adequate level of protection for the transfer of data to the U.S. to entities that self-certified to the Safe Harbor Framework. However, on October 6, 2015, the Court of Justice of the European Union invalidated the adequacy decision for the EU-U.S. Safe Harbor Framework. *Schrems v. Data Prot. Comm'r*, No. C-362/14 (E.C.J., 2015). On February 2, the EU Commission announced that it reached a political agreement on a new framework for data transfers between the EU and the U.S., the EU-U.S. Privacy Shield. See "Safe Harbor Resurrected as EU-U.S. Privacy Shield," *Privacy Law Watch* (Feb. 3, 2016). The details of this new framework are unknown at the time of preparation of this overview.

Absent an adequacy decision, companies can transfer personal data to a third country if they implement a data transfer mechanism, such as Standard Contractual Clauses (SCCs) or Binding Corporate Rules (BCRs).

- SCCs are sets of model contracts adopted by the Commission. The Commission adopted three different sets of SCCs, i.e., two sets for data transfers between data controllers and one set for data transfers between a data controller and a data processor. SCCs are automatically recognized as a valid legal basis for data transfers if they are executed unamended. However, some filings with national data protection authorities (DPAs) or DPA authorizations are still required in certain EU countries. If companies make material changes to the SCCs or use their own clauses, the clauses will need to be approved by DPAs in the relevant EU countries.
- Mainly designed for large multinational companies, BCRs are a form of a code of conduct made binding on all entities of a group. BCRs are subject to approval by DPAs under EU cooperation and mutual recognition procedures. One of the main advantages of BCRs is that they can be tailored to a company's culture or business model. BCRs must contain a number of privacy principles and commitments as required by the Article 29 Data Protection Working Party (*e.g.*, audits, training, and complaint-handling systems to ensure their effectiveness, and an element proving the BCRs are binding). See Article 29 Working Party Guidance on BCRs.

In addition to the above mechanisms, Article 26 of Directive 95/46/EC provides for certain derogations from the prohibition of data transfers to a country that does not provide an adequate level of protection; in particular when:

- the individual has given unambiguous consent to the data transfer;
- the data transfer is necessary for the performance of a contract between the individual and the data controller or implementation of pre-contractual measures taken at the individual's request;
- the data transfer is necessary to conclude or perform a contract made in the interest of the individual between the data controller and a third party;
- the data transfer is legally required on public interest grounds, or to establish, exercise, or defend legal claims;
- the data transfer is necessary to protect vital interests of the individual; or
- the data transfer is made from a register intended to provide information to the public and open to consultation by the public or any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.

d. Sensitive Data

Directive 95/46/EC provides that certain types of personal data must receive a higher level of protection and can only be processed in limited situations. This special category of data is considered to be sensitive data. Sensitive data is personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and health or sex life. The processing of sensitive data is generally limited to situations in which the individual gives explicit consent, or when data processing is necessary for purposes of carrying out the obligations and specific rights of the data controller in the field of employment law (if authorized by national law

providing for adequate safeguards), or other limited circumstances set forth under Article 8.

e. Individuals' Rights

Directive 95/46/EC provides that individuals can exercise certain rights in relation to the processing of their personal data. In particular, individuals can obtain from the data controller (i) the confirmation as to whether their personal data is processed; (ii) the communication of such data in an intelligible form; and (iii) information about the logic behind any automatic data processing of their personal data. In addition, individuals have a right to rectification, erasure or blocking of the data relating to them. Individuals can request the data controller to notify any third parties to whom the personal data have been disclosed of any such rectification, erasure or blocking (art. 12). Under certain conditions, individuals also have a right to object to the processing of personal data relating to them (art. 14).

Individuals must be able to seek redress with the DPA and the courts for violations of applicable data protection rules involving the processing of personal data relating to them (art. 22–24).

2. ePrivacy Directive

In addition to Directive 95/46/EC, Directive 2002/58/EC (as amended by Directive 2009/136/EC)—the ePrivacy Directive—provides specific rules for electronic communications service providers, such as telecommunications companies and Internet service providers. In particular, the ePrivacy Directive provides a number of rules on how those service providers must manage their subscribers' or users' data, and enumerates their rights. See Commission, *The ePrivacy Directive*.

The key elements regulated by the ePrivacy Directive include the rules on confidentiality of information; cookies and other similar technologies; data breach notification requirements; spamming; and the processing of location data and traffic data. The ePrivacy Directive was complemented by Commission Regulation (EU) No 611/2013, which provides further details regarding data breach notification requirements.

- *Data breach notification requirement*. Provider of a publicly available electronic communications service must notify competent authorities and, in certain situations, individuals of data breaches which lead to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service in the EU (art. 4(3) of the ePrivacy Directive).
- *Cookies and other similar technologies*. Article 5(3) of the ePrivacy Directive requires prior informed consent from a subscriber or user before a company stores information or gains access to information already stored in the terminal equipment of a subscriber or user. In practice, subscribers or users must provide appropriate consent to the use of cookies, except if cookies are used for the sole purpose of carrying out the transmission of a communication or are strictly necessary for the provider of the service explicitly requested by the subscriber or user. See also Commission, *Cookies*.
- *e-Marketing*. The use of automated calling and communication systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail for the purposes of direct marketing is only allowed with individuals' prior opt-in consent. However in some limited situations, providing individuals with an opportunity to opt-out is sufficient (art. 13, 2). In any event, individuals have the right to object, free of charge, to the processing of their personal data when they are processed for purposes of direct marketing (art. 13 of the ePrivacy Directive).

3. Data Retention

Separate directives have addressed data retention issues, such as Directive 2006/24/EC relating to the retention of data processed in connection with publicly available electronic communications services or on public communications networks (Data Retention Directive). However, the CJEU invalidated the Data Retention Directive in April 2014 in *Digital Rights Ireland Ltd. v. Minister for Commcn's, Marine & Natural Res.* (C-293/12 joined with C-594/12, April 8, 2014), finding that it did not comply with the Charter. The CJEU found that the data retention requirement under the Data Retention Directive entailed a wide-ranging and particularly serious interference with individuals' fundamental right to privacy and data protection. In the CJEU's view, the interference was disproportionate and not limited to what was strictly necessary, in violation of the Charter.

4. "Right to be Forgotten"

In 2014, in *Google Spain SL v. Agencia Española Protección de Datos* (C-131/12, May 13, 2014), the CJEU concluded that Articles 12 and 14 of Directive 95/46/EC includes a "right to be forgotten." In particular, the CJEU ruled that an individual can request search engine operators to delete data concerning him/her (including information and hyperlinks in the list of search results for his/her name) where the data is inadequate, irrelevant, or excessive in relation to

the purposes of the processing by the search engine. In the particular circumstances of the case, the individual's fundamental rights under Articles 7 and 8 of the Charter override the economic interest of the search engine operator and the interest of the general public in having access to that information. Such conclusion can be drawn after a case-by-case assessment.

II. Regulatory Authorities and Enforcement

Enforcement actions are taken at the country level by national DPAs. At the EU level, the Article 29 Data Protection Working Party (Working Party) is an influential body, but it does not have enforcement powers towards companies or individuals as such.

A. National Data Protection Authorities

National DPAs are the main enforcers of EU data protection law. Each national DPA is responsible for enforcing its own national data protection law in its country.

Directive 95/46/EC provides that DPAs must have (i) investigative powers (*e.g.* , powers of access to data and powers to collect all information necessary to perform their supervisory duties); (ii) effective powers of intervention (*e.g.*, powers of delivering opinions before processing operations are carried out; powers of ordering the blocking, erasure or destruction of data; powers of imposing a ban on data processing; powers of warning the data controller; or power of referring the matter to national parliaments); and (iii) the power to engage in legal proceedings where national law on data protection has been violated or to bring such violations to the attention of courts (art. 28(3)).

Sanctions for violations of national data protection law are regulated locally, not by Directive 95/46/EC. Only a few DPAs have the power to impose fines against companies directly (*e.g.*, France, the UK). However, courts have the power to fine companies for violation of EU data protection law.

In addition, as required by Directive 95/46/EC, individuals have the right to bring complaints before their national DPA in order to seek compensation for damages suffered as a result of a data controller's unlawful data processing (art. 23(1)). Decisions of national DPAs are appealable to a court in the EU country (art. 28(3)). Without prejudice to the right to bring complaints before national DPA, individuals have the right to seek a judicial remedy for any breach of the rights provided in Directive 95/46/EC as implemented into applicable law (art. 22).

B. Article 29 Working Party

The Working Party is an independent, advisory body established under Article 29 of Directive 95/46/EC. It includes a representative from each DPA, a representative of the European Data Protection Supervisor (EDPS), and a representative of the Commission. The Working Party is responsible for the uniform application of EU data protection law as implemented into local law within the EU. In addition, the Working Party provides opinions on the level of protection in the EU and in third countries (i.e., outside the EU and the EEA), and makes recommendations for protecting personal data of EU individuals. While the Working Party mostly plays an advisory role, it has more and more influence on both the legislative-making process and the enforcement actions taken by national DPAs. In particular, it is the body where DPAs discuss matters of pan-EU importance, including enforcement actions, with a view to take a consistent approach within the EU.

See the Working Party's official website for more of its recommendations and opinions.

C. European Data Protection Supervisor

The EDPS is an independent supervisory authority devoted to protecting personal data and privacy, and promoting good practices in data processing in EU institutions and bodies. The EDPS monitors the EU administration's processing of personal data, and advises on policies and legislation that affect privacy. The EDPS also cooperates with similar authorities to ensure consistent application of EU data protection rules. For example, the EDPS sent recommendations (in English) to the EU co-legislators negotiating the upcoming General Data Protection Regulation.

Strictly speaking, the EDPS does not have any enforcement powers against companies. However, the opinions of the EDPS are becoming more and more influential for EU data protection law.

The EDPS can also intervene before the CJEU in cases involving data protection issues, as it did in *Schrems v. Data Prot. Comm'r*.

D. Other EU Institutions and Bodies

Other EU institutions and bodies involved in data protection issues include the CJEU, the Article 31 Committee, the EU Ombudsman and the European Network Information Security Agency. The CJEU has issued several groundbreaking judgments in the last few years, including in *Digital Rights Ireland Ltd. v. Minister for Commc'ns, Marine and Natural*

Res. in 2014, and, most recently in *Schrems v. Data Prot.Comm'r* in 2015. The number of cases involving data protection issues brought to the CJEU is growing.

III. Risk Environment

At the EU level, there is no EU body with enforcement powers towards companies and individuals. Thus, the risk environment related to data processing remains at the national level and diverges from one EU country to another. In particular, some national DPAs are usually more business friendly than others, and the enforcement powers of each DPA vary greatly among EU countries. However, the Working Party plays a significant role in the EU. While Working Party's opinions and recommendations are not legally binding on independent DPAs, they provide a good indication of how DPAs may likely apply their national data protection provisions.

In addition, beside the risk of enforcement actions and sanctions by DPAs at national level, reputational risks also play an important role in the EU. In particular, the Working Party and DPAs have the right to issue public recommendations or opinions which can be very damaging for companies, even if not directly enforceable.

The risk environment for EU data protection law is evolving fast. DPAs have more resources and have gained experience in interpreting and enforcing EU data protection law. Cooperation among DPAs and enforcement significantly stepped up over the last few years. This trend will only increase with the expected entry into force of the General Data Protection Regulation (which will give significant powers to DPAs including, in certain situations, the power to fine up to 20,000,000 euros or up to 4% of a company global turn-over, whichever is higher,) in spring 2018.

IV. Emerging Issues and Outlook

A. General Data Protection Regulation

In 2012, the Commission published its proposal for a General Data Protection Regulation (GDPR) which will replace Directive 95/46/EC. The European Parliament and the Council proposed their own respective versions of the GDPR in 2014 and 2015. Subsequently, the text of the GDPR was negotiated at "Trilogue" meetings—*i.e.*, negotiations between representatives of the Council, the Commission, and the European Parliament. A political agreement on the text of the GDPR was reached by the European Parliament and Council on December 15, 2015. See "EU Privacy Regulation Clears First Ratification Hurdle," *Privacy Law Watch* (Dec. 18, 2015).

The GDPR introduces important changes to EU data protection law that will have a significant impact on companies doing business in the EU. In particular, the GDPR will:

- extend the geographical scope of EU data protection law. In particular, the GDPR will apply to companies without EU establishment which offers goods or services to, or monitors the behavior of, EU individuals;
- provide new rights to individuals, such as the right to data portability;
- replace existing filing requirements with record-keeping obligations and impose prior consultation with DPAs for high-risk data processing operations;
- require the appointment of a data protection officer in certain cases;
- oblige data controllers to notify the competent DPA, and in certain cases the individuals, about personal data breach incidents. Notifications to the competent DPA would need to be made without undue delay and, where feasible, no later than 72 hours after being aware of the breach, provided the breach likely involves risks to individuals' rights and freedoms;
- implement a "one-stop shop" so data controllers can interact mainly with one DPA if they are established in more than one EU country; and
- impose high fines for non-compliance with data protection rules. For the most severe violations, fines can be up to 20,000,000 euros or 4% of the annual global turnover, whichever is higher.

The GDPR will apply directly in EU countries and take effect around spring 2018, two years from the date of publication.

The GDPR will be accompanied by a new directive (see the Commission's proposal from 2012) applying to the processing of personal data for the purposes of prevention, investigation, detection or

prosecution of criminal offences, or the execution of criminal penalties. The European Parliament and Council also agreed on the text of this new directive on December 15, 2015, as the GDPR and this directive are part of the broader reform of EU data protection rules.

B. European Court of Justice Invalidates U.S.-EU Safe Harbor Framework

In October 6, 2015, the CJEU in its judgment *Schrems v. Data Prot. Comm'r* (Case C-362/14, Oct. 6, 2015) invalidated the Commission's Safe Harbor adequacy decision, Decision 2000/520 (July 26, 2000). The U.S.-EU Safe Harbor Framework (Safe Harbor Framework) was a mechanism that provided a legal basis for data transfers between the EU and the U.S. It was developed by the U.S. Department of Commerce in consultation with the Commission, and was formally recognized as a valid data transfer mechanism by the European Commission's adequacy decision in 2000. It included seven privacy principles and fifteen FAQs that companies must comply with in order to self-certify to the Safe Harbor Framework. By self-certifying, companies voluntarily and publicly commit to abiding by these privacy principles, which are then enforced by the U.S. Federal Trade Commission. The Safe Harbor Framework was a useful compliance tool for U.S. companies collecting personal data from EU individuals.

Max Schrems, an Austrian individual, complained about the alleged lack of adequate protection of personal data regarding data transfers under the Safe Harbor Framework. In particular, his complaint concerned the data transfers operated by Facebook between its EU and U.S. headquarters. Schrems claimed that the Safe Harbor Framework did not guarantee a sufficient level of protection with respect to transfers of personal data because of alleged U.S. mass surveillance programs. The complaint was handled by the Irish DPA which rejected it by arguing that it was bound by Decision 2000/520 and could therefore not investigate data transfers taking place under the Safe Harbor Framework. Schrems appealed the Irish DPA's decision to the Irish High Court which brought the case to the CJEU.

The CJEU invalidated Decision 2000/520 for a number of reasons. According to the CJEU, the broad national security exception contained in the Safe Harbor Framework that allows for disclosures of personal data to law enforcement authorities does not satisfy the standards of fundamental rights in the EU. In particular, the CJEU held that this exception enables disproportionate interference with the privacy rights of EU individuals. In addition, the CJEU emphasized the lack of judicial remedy or redress for EU individuals, including the right to have the data accessed, rectified, or erased, and the lack of oversight powers by national DPAs.

Following the CJEU decision, the Commission underscored the need to reach an agreement on a new Safe Harbor Framework. Any new Safe Harbor agreement will need to meet the criteria set forth by the CJEU in its judgment. The Safe Harbor negotiations actually started before the CEJU judgment when, following the Snowden revelations, the Commission issued 13 recommendations to enhance the Safe Harbor Framework on November 27, 2013.

On February 2, 2016 the EU Commission announced that it reached a political agreement on a new framework for data transfers between the EU and the U.S., the EU-U.S. Privacy Shield. See "Safe Harbor Resurrected as EU-U.S. Privacy Shield," *Privacy Law Watch* (Feb. 3, 2016). The details of this new framework are unknown at the time of preparation of this overview.

Since *Schrems v. Data Prot. Comm'r*, companies are left with legal uncertainty around data transfers to the U.S. and a limited number of alternative data transfer mechanisms. For more information on the CJEU's decision and the reaction of data controllers, see "Following the CJEU's Landmark Ruling that the U.S.-EU Safe Harbor Is Invalid, What's Next for EU Transfers of Personal Data to the U.S.?," *World Data Protection Report* (Oct. 23, 2015), and "Invalidation of the Safe Harbor: Will It Cause the Adoption of Data Silos?," *Privacy Law Watch* (Nov. 2, 2015).

C. Other Recent Important Decisions for Businesses

Weltimmo *Decision—Which DPA has jurisdiction?*

In *Weltimmo s.r.o. v. Nemzeti Adatvédelmi és Információszabadság Hatóság*, (Case C-230/14, Oct. 1, 2015), a Slovak company "Weltimmo" ran a website targeting Hungarian customers. Some Hungarian customers complained about the processing of their personal data to the Hungarian DPA. While the company had registered its offices in Slovakia, Weltimmo also had a representative in Hungary. The questions were whether the Hungarian DPA was competent, and whether Hungarian data protection law was applicable. The CJEU ruled that the presence of only one representative can, in some circumstances, suffice to constitute an establishment if that representative acts with a sufficient degree of stability for the provision of the services concerned in the EU country in question. According to the CJEU, the concept of "establishment" extends to any real and effective activity—even a minimal one—exercised through stable arrangements (assessed on a case-by-case basis). The CJEU also upheld that a national DPA is competent

for the companies that are established in its jurisdiction. It cannot impose penalties on companies established outside its own country. Therefore, if a company does not have an establishment in the EU country where the infringing act occurred, the DPA of that country may not impose penalties. Instead, it should request the DPA of the EU country where the company is established to investigate the matter and to potentially sanction the company in accordance with its own applicable data protection law.

D. Umbrella Agreement

The EU-U.S. Umbrella Agreement (Umbrella Agreement) is a draft international agreement that has been negotiated between the EU and the U.S. since 2011. It will establish a data protection framework for EU-U.S. law enforcement cooperation. In particular, it would apply to the exchange of personal data between the U.S. and EU for the purposes of prevention, detection, investigation, and prosecution of criminal offenses, including terrorism.

One of the key issues that must be solved before the Umbrella Agreement can be enacted relates to EU citizens' right to seek judicial redress in the U.S. This right would be granted to EU citizens by a new bill which was introduced in the U.S. in March 2015, H.R. 1428 – Judicial Redress Act of 2015, and passed by the Senate on February 9. 2016. See "Senate Passes Amended Judicial Redress Act," *Privacy Law Watch* (Feb. 10, 2016). This bill would extend certain redress provisions of the U.S. Privacy Act of 1974 to EU citizens. According to the Commission, the Umbrella Agreement will not be signed and formally adopted until after the Judicial Redress Act has been promulgated in the U.S. (*see* Commission, *Questions and Answers on the EU-US data protection "Umbrella agreement,"* Sept. 8, 2015).

At a high-level, the Umbrella Agreement includes:

- *Purpose and use limitation principle* – data transfers should be made for specific purposes authorized by a legal basis;
- *Rules on onward transfers* – the requirement that any data transfer to a non-U.S., non-EU country or international organization would be subject to the consent of the competent authority of the country that originally transferred the data;
- *Retention period principle* – personal data could be retained only for as long as necessary or appropriate;
- *Individuals' rights to access and correct their personal data* – subject to limitations in the law enforcement context; and
- *Notification of data breaches to the competent authority* – and, where appropriate, the individual.

E. Other Ongoing Efforts to Reform Data Protection in the EU

In May 2015, the Commission adopted its Digital Single Market Strategy, which consists of several initiatives intended to be completed by late 2016 to move towards a single set of data protection rules and stimulate commerce. Some of the planned features highlighted in the Commission's Press Release (May 6, 2015) include improving access for consumers and businesses to digital goods and services by making cross-border e-commerce easier, reducing "geo-blocking," in which a consumer is denied access to a website and downloading because of his/her location, and reviewing the ePrivacy Directive. On December 9, 2015, the Commission announced the first legislative proposals under the Digital Single Market Strategy, relating respectively to the reform of the copyright regime and improving access to cultural content across the EU (See Press Release).