Right to be forgotten as one of key principles of the EU Data Protection Law Reform

Marta Kołodziejczyk[1]

Ключові слова:

суб'єкт персональних даних, оператор персональних даних, обробник даних, основні права, право на забуття.

Key words:

data subject, data controller, data processor, fundamental rights, right to be forgotten.

On 25 January 2012 the EC proposed a comprehensive reform of the EC's 1995 data protection rules. Although the core principles of the Directive 95/46 were still valid, it could no longer meet the challenges of rapid technological developments and globalization, and as a result required revision. One of those is the right to be forgotten already included in the Directive 95/46/EC that guarantees the individuals the right to request the controller to delete unlawfully processed personal data. However, due to the fact that according to the European Commission it is difficult for an individual to enforce this right in the online environment, some amendments to the current legislative framework were proposed. As a result, on the 15 December 2015 the agreement, concerning legislative package proposed by the Commission in 2012 to update and modernize the data protection rules, was reached between the Council, Parliament and Commission. This package consisted of two legislative instruments: the general data protection regulation (intended to replace directive 95/46/EC) and the data protection directive in the area of law enforcement (intended to replace the 2008 data protection framework decision); it is to be expected that these legal acts enter into force in spring 2018.

Privacy and data protection – history and current state of law

Privacy and data protection as a specific field of law have been elaborated over the last four decades, notably in the context of the Council of Europe and the European Union, stimulated by the growing impact of information and communication technology. The concept of the "right to privacy" emerged in international law after the Second World War. This was illustrated in the Article 12 of the Universal Declaration of Human Rights (UN General Assembly, Paris 1948) according to which no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence. This declaratory level of protection became later lawful in Article 8 of the European Convention on Human Rights (Council of Europe, Rome, 1950), according to which everyone has the right to respect for his private and family life, his home and his correspondence, and no interference by a public authority with the exercise of this right is allowed except in accordance with the law and where necessary in a democratic society for certain important and legitimate interests. The above definition has been reflected in the series of judgments, e.g.: Leander v. Sweden (26.03.1987); Kopp v. Switzerland (25.03.1998); Amann v. Switzerland (16.02.2000), issued by the European Court of Human Rights in Strasbourg. However, in about 1970 the Council of Europe came to conclusion that Article 8 ECHR had a number of shortcomings, e.g. the uncertain scope of "private life", the emphasis on interference by public authorities, as well as lack of a more proactive approach against the possible misuse of personal information by companies or other organizations in the private sector. As a result the Data Protection Convention, also known as Convention 108 (Strasbourg 1981) had been adopted and has been ratified by 44 Member states of the Council of Europe, including all EU Member States. Parties to this convention guarantee every individual, whatever his nationality or residence, respect for his/her rights and fundamental freedoms; in particular right to privacy, with regard to automatic processing of personal data relating to him/her ("data protection"). In addition, the concept of "personal data" is defined as any infor-

[1] My scientific research focuses on EU Law and International Human Rights Law. I am a graduate of the Jagiellonian University Center for European Studies (master degree) and Warsaw University (Phd degree). During my professional career I had the opportunity to conduct my research under supervision of Prof. Adam Daniel Rotfeld at the Polish Institute of International Affairs (Warsaw), Council of the EU (Brussels), Renè Cassin International Institute for Human Rights (Strasbourg), European University Institute (Florence).

mation relating to an identified or identifiable ("data subject"). Hence, "data protection" is broader than "privacy protection" because it also concerns other fundamental rights and freedoms, and all kinds of data regardless of their relationship with privacy.

Let us now consider some of the key provisions of the above mentioned Convention; personal data are to be "obtained and processed fairly and lawfully" and "stored for specified and legitimate purposes and not used in a way incompatible with those purposes". Personal data should also be "adequate, relevant and not excessive in relation to the purposes for which they are stored", "accurate and, where necessary, kept up to date". Other crucial principles expressed in the text of the Convention are: "appropriate security measures", "additional safeguards for the data subject such as the right to have access to his or her own personal data, the right to obtain rectification or erasure of such data, and the right to remedy if such rights are not respected". To conclude, the Convention's philosophy is not that processing of personal data should always be considered as a breach of privacy, however, in its interests as well as other fundamental freedoms, any processing must always observe certain legal conditions. In this context, the core elements of Article 8 ECHR, such as interference with the right to privacy only on adequate legal basis, and where necessary for a legitimate purpose, have been transferred into a broader context. Furthermore, since 1997 the European Court of Human Rights has ruled in a number of cases that the protection of personal data is of "fundamental importance" for the right to respect of private life under Article 8 ECHR.

Although the Data Protection was put on the agenda of the Council of Europe and, as a result, exposed in the binding Conventions, this intergovernmental organization was less successful in terms of ensuring greater consistency across the EU. Some Member States were late in implementing the Convention, and those who did so arrived at different outcomes, in some cases even imposing restrictions on data flows with other Member States. Concerned that this lack of consistency could hamper the development of internal market involving a circulation of peoples and services, where the processing of personal data was to play an increasingly important role, the European Commission submitted a proposal for a Directive to harmonize the national laws on data protection in the private and most of the public sector. After four years of negotiations the Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data has been adopted. It specified the basic principles of data protection already included in the Convention 108 of the Council of Europe. In the first place, it required all Member States to protect the fundamental rights and freedoms of natural persons, and in particular the right to privacy with the respect to processing of personal data, in accordance with the Directive. In this context, the data could be processed only if the data subject has unambiguously given his consent, if processing was necessary for the performance of a contract to which the data subject was party, or for compliance with a legal obligation, for the performance of a government task, in order to protect the vital interests of the data subject, or to protect the legitimate interests pursued by the controller, except where such interests are overridden by the interests of the data subject. Furthermore, the Directive committed the controller to always inform the data subject about the purposes of the processing and other relevant matters in order to guarantee fair processing in respect of the data subject. In case of not fulfilling this condition, the data controller might become liable for committing an offence. Responsibility for compliance with national legislation on data protection belongs to supervisory authorities. Secondly, the Directive applies to the processing of personal data carried out "in the context of the activities of an establishment" of the controller on the territory of an EU Member State. In other words, where the controller is not established in the EU, the applicable law is that of the Member State in which the equipment used for processing is located. Thirdly, according to the Directive personal data may only be transferred to third countries that ensure adequate level of protection.

To conclude, the Directive 95/46/EC required the Member States neither to restrict nor prohibit the free flow of personal data between them for reasons connected with such protection. This provision aimed at achieving an equivalent high level of protection in all Member States and as a result assure a balanced development of the internal market. However, this goal has not been entirely fulfilled due to the fact that the distinctive features of this particular legal act – Directive – allowed Member States fairly broad discretion on its transposition. In this context, it is worth to refer to the Treaties; Article 16 (2) TFUE mandates the European legislators to adopt "the rules relating to the protection of individuals with regard to processing of personal data", without, however, specifying the type of legislative act to be chosen. As a consequence, in line with Article 289(1) TFEU on the ordinary legislative procedure, the rules can be laid down in a regulation, a directive, or a decision. Let us note that a regulation has general application being at the same time directly applicable (it does not require implementation by EU member states), whereas a directive sets forth the results to be achieved, but leaves the means for achieving them largely up to implementation into national law by the members states. As a consequence,

by now the Commission has launched several legal actions for improper implementation of the Directive; in March 2009, the Court of Justice in Luxembourg ruled (case against Germany) that the requirement of "complete independence" for a supervisory authority means that it should be free from any external influence. This has been also recently confirmed and elaborated in a case against Austria. That is why the choice of regulation will according to the European Commission reduce legal fragmentation among member states in respect to different national data protection laws. This will lead e.g. to a net savings for companies of about €2.3 billion a year in terms of administrative burden alone. But even the regulation cannot result in complete harmonization of all legal provisions affecting data protection or totally eliminate the need to amend national laws. This fact may confirm that the type of legal instrument used is not determinative with regard to harmonization; for example it is also possible for a directive to leave little margin for member state implementation (e.g. EU Consumer Rights Directive 2011/83/EU). To conclude, the final proposal contains two legislative instruments that form the core of the data protection reform package: in the first place, the Regulation, setting out the general EU framework for data protection; secondly, the Directive for the police and criminal justice sector which is due to replace Framework Decision 2008/977/JHA which covers the protection of personal data processed by police and judicial authorities in criminal matters.

Another crucial reason for the review of the Directive 95/46/EC has to do with the new institutional framework of the EU. The Lisbon Treaty (December 2009) emphasizes fundamental rights[1]; Article 16 provides for comprehensive data protection in all policy areas, regardless of whether it relates to the internal market, law enforcement, or almost any other part of the public sector. Not to mention about the separate right to the protection of personal data laid down in Article 8 of the Charter of Fundamental Rights that became legally binding on the EU institutions and national governments with the entry into force of the Treaty of Lisbon[2].

Reinforcement of the rights of data subjects

The need for reform of current EU data protection legislation can be explained by the rising impact of IT technologies on our lives. Specifically, at the time when the Directive was adopted the Internet barely existed, however, in nowadays reality the data processing is taking place on the web sites, by search engines or social networks. In a recent survey, more than two-thirds of Europeans – 72 per cent – expressed their concerns connected to uncontrolled usage of their data personal data by companies on the Internet[3]. In this context, the European Commission in its official comment focused on such challenges for the protection of personal data in the future as: the astounding capabilities of modern technologies; the increased globalization of data flows; and access to personal data by law enforcement authorities that is greater than ever. That is why the aim of the new legislative acts proposed by the Commission is to strengthen individuals rights by improving the ability to control their data[4] by clarifying the requirement of consent as one possible ground for lawful processing of personal data as well as reinforcing the rights of individuals to request the controller to delete unlawfully processed personal data (right to be forgotten).

Enhancing the responsibility of controllers and processors

In the first place, it is crucial to define the above terms; as a result, controller is defined as natural or legal person, public authority, organization, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data. Secondly, processor, on the other hand, is the natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller. Furthermore, as far as the controller's responsibilities are concerned (article 22 of the Regulation) in the framework of data protection reform, the new legislative acts (regulation, directive) focus on controllers' obligation to be able to "demonstrate" compliance with the Regulation by adoption of internal policies for ensuring such compliance. The effectiveness of such mechanisms must be verifiable either by internal or external data protection specialists or by data protection certification mechanism envisaged under Article 39. In addition, in order to give data subjects greater control over their personal data, the Regulation sets out further obligations

[1] Fuster G. The Emergence of Personal Data Protection as a Fundamental Right of the EU / G. Fuster. – Switzerland : Springer International Publishing, 2014. – P. 3–33.

[2] Gutwirth S. Reforming European Data Protection Law / S. Gutwirth, R. Leenes, P. de Hert. – New York ; London : Springer Dordrecht Heidelberg, 2015. – P. 3–15.

[3] Proposed EU Data Protection Regulation One Year Later: The Albrecht Report // Privacy &Security Law Report. – 2013. – 12 PVLR 99. – P. 1–7.

[4] Gutwirth S. Reforming European Data Protection Law / S. Gutwirth, R. Leenes, P. de Hert. – New York ; London : Springer Dordrecht Heidelberg, 2015. – P. 3–15.

for the controller by requiring him to apply the principles of "data protection by design" and "data protection by default" (Article 23).

In the first place, data protection by design means that controllers of data – whether companies or public bodies – take a positive approach to protecting privacy, by embedding it into both technology (for example hardware like computer chips or services like social networking platforms) and into their organizational policies (through, for example, the completion of privacy impact assessments). Secondly, privacy by default means that when a user receives a product or service, privacy settings should be as strict as possible, without the user having to change them. In this way, everyone feels comfortable to consciously choose the privacy setting within which he feels most comfortable with. Rather than allowing the service provider making a guess about what he might prefer. In addition, service providers should support their users in this by providing user-friendly methods to change privacy settings. Not to mention about the need for transparency enshrined in data processing practices.

Definition of consent in the EU law

It is worth to mention that the "consent" is currently defined in Articles 2(h) and 7(a) of Directive 95/46/EC as "any freely given specific and informed indication" of a data subject's wish to agree to the processing of his personal data. In addition, this agreement must be "unambiguously" given in order to make the processing of personal data legitimate. However, national laws have transposed this concept quite differently. Consequently national supervisory authorities tend to apply variable interpretations of consent. Furthermore, the meaning of "unambiguously" given consent is interpreted in a differentiated manner: in some member states consent has to be given "expressly" and in some cases even in writing, while other member states also accept some forms of implied consent. As a consequence, valid consent in one member state may not be legally valid in others, therefore creating uncertainty amongst controllers operating in several member states on whether a data processing operation is lawful or not. Hence, in the proposed Regulation the definition of "the data subject's consent" of Article 4(8) is remedied by adding the criterion "explicit" which allows to avoid the confusing parallelism with "unambiguous". Moreover, where consent is the legal ground for data processing, Article 7 states that the controller must be able to demonstrate that consent has taken place. A the same time, the Regulation reaffirms that the data subject may withdraw his or her consent at any time, bearing in mind that this will only take full legal effect for future processing. Furthermore, consent is excluded in Article 7(4) as a ground for processing in specific cases of significant imbalance between data controller and data subject, for example in the framework of an employment relationship. Similarly. Article 8 sets out further conditions for the lawfulness of consent for processing of personal data of children below the age of 13 years in relation to services offered to them on-line.

In the context of reinforcing the rights of data subject, it is worth to emphasize that the proposed Regulation enhances administrative and judicial remedies when data protection rights are violated. In particular Article 76(1) enables certain associations, for example consumer protection associations whose statutory aim includes the protection of personal data, to bring actions, on behalf of one or a group of data subjects whose rights may have been violated, to court. Similarly, article 73(3) of the proposed Regulation provides that these data protection NGOs, in cases of personal data breaches, may address a supervisory authority in any member state in their own right; without obligation to obtain data subject's authorization to act on his behalf.

As far as the national authorities responsibilities for data protection are concerned, the proposed Regulation strengthens their potential for initiating legal actions by: a) clarifying the conditions for the establishment and for ensuring the complete independence of supervisory authorities in member states (Articles 46-50); b) providing for fully harmonized provisions for the competences, duties, and powers of the supervisory authorities (Articles 51 to 54); c) and as a result creating legal basis and conditions for an efficient cooperation between supervisory authorities established in EU Member States (Articles 55 to 56); d) introducing the one-stop-shop rule that gives companies operating in more than one member state, a single supervisory authority responsible for monitoring their personal-data processing activities in the EU, rather than force a company to deal with multiple bodies in different countries.

Right to be forgotten

In order to strengthen the level of protection guaranteed to individuals the European Commission published on the January 1, 2012 the Proposal for a Regulation on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data ("GDPR"), which updates the former Data Protection Directive. Although this legal act gives the individual the right to access, rectify, delete or block their

data, unless there are legitimate reasons, provided by law, for preventing this. However, the way in which these rights can be exercised is not harmonized, and therefore exercising them is actually easier in some Member States than in others. As a result, it is difficult, according to the European Commission, for an individual to enforce this right in the on-line environment. Hence, the unified regulation will give all European Union citizens a right to be forgotten online, in other words the right for an individual user to have his or her personal online data removed from the web. It is worth to mention that this legal rule has been officially acknowledged in the judgment Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González (Google Spain v. AEPD), issued by the European Court of Justice. The case concerned a reference for a preliminary ruling made by the Spanish High Court to the CJEU, which arose out of a dispute between Google Inc. and Google Spain on the one hand, and Mr Costeja González and the Spanish Data Protection Agency on the other. Let us now dwell on the facts of the above mentioned case; In 2010, Mario Costeja González, a Spanish national, filed a complaint with the Spanish Data Protection Agency ("Agencia Española de Protección de Datos", "AEPD") against La Vanguardia Ediciones SL, a large publisher of daily news in Spain, as well as Google Spain and Google Inc.[5]. González, the data subject seeking erasure, contended that whenever a Google search of his name was carried out, the top results listed linked the Internet user to two property auction notices for the recovery of social security debts that Mr Costeja González had owed 16 years earlier, which still appeared on La Vanguardia's website. Furthermore, the applicant claimed that these articles "although truthful, injured his reputation and invaded his privacy"[6]. That is why, González demanded that the Spanish newspaper erase them because they were no longer relevant, since the proceedings had concluded more than a decade ago[7]. The newspaper publisher refused to erase the articles because the Ministry of Labor and Social Affairs had ordered their publication[8]. Next, the plaintiff demanded that Google remove the link to those stories and thereby eliminate any association to his name. The applicant sought to obtain an order to the effect that the newspaper should alter, delete, or protect this information, and that Google should either delete or conceal the links to those pages. As far as the procedural History of Google Spain v. AEPD is concerned, the Spanish Data Protection Agency (AEPD) ruled that Google was responsible as a data controller for removing results about the plaintiff from its search engine[9]. After the AEPD's decision, Google brought action before the Audiencia Nacional, Spain's highest court, which referred the case to the Court of Justice of the European Union. As a consequence, on June 25, 2013, Advocate General Niilo Jääskinen issued his advisory opinion, finding that Google had no responsibility to remove any links on its search engine based on a privacy claim[10]. He reasoned that suppressing legitimate and legal information already in the public domain would interfere with freedom of expression and undermine the objectivity of information o the Internet[11]. However, the CJEU rejected the Advocate Generals's argument and recognized a broad right to be forgotten under Spain's implementation of Directive 95/46/EC[12]. The court found, in the first place, that Google, as an indexer of information, was processing personal data and therefore subject to the Directive's obligations for data controllers (remark: Google Spain SL, Case C-131/12).

Secondly, the court drew upon Articles 12(b) and 14(a) of the Directive to hold that Google owed a duty to erase information from its search index (Google Spain SL, Case C-131/12) Thirdly, the CJEU rejected Google's argument that imposing a duty to remove personal data violated the principle of proportionality, and that such removal must be addressed to the publisher of the website because the publisher was responsible for making the information public. Furthermore, court reasoned that search engines make access to this information effortlessly available, because they enable users to obtain information about a data subject by simply typing the

---

5 Google Spain SL. v. Agencia Española de Protección de Datos : Case C-131/12 (May 13, 2013) [Electronic resource]. – Access mode : http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&doclang=EN.

6 Lee D. What Is the "Right To Be Forgotten?" / D. Lee [Electronic resource]. – Access mode : http://www.bbc.com/news/technology-27394751.

7 Google Spain SL. v. Agencia Española de Protección de Datos : Case C-131/12 (May 13, 2013) [Electronic resource]. – Access mode : http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&doclang=EN.

8 Opinion of Advocate General Jääskinen 19, Google Spain SL v. Agencia Española de Protección de Datos (Case C-131/12, May 13, 2014) [Electronic resource]. – Access mode : http://curia.europa.eu/juris/document/document.jsf?text=&docid=138782&doclang=EN.

9 Google Spain SL. v. Agencia Española de Protección de Datos : Case C-131/12 (May 13, 2013) [Electronic resource]. – Access mode : http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&doclang=EN.

10 Opinion of Advocate General Jääskinen 19, Google Spain SL v. Agencia Española de Protección de Datos (Case C-131/12, May 13, 2014) [Electronic resource]. – Access mode : http://curia.europa.eu/juris/document/document.jsf?text=&docid=138782&doclang=EN.

11 Opinion of Advocate General Jääskinen 19, Google Spain SL v. Agencia Española de Protección de Datos (Case C-131/12, May 13, 2014) [Electronic resource]. – Access mode : http://curia.europa.eu/juris/document/document.jsf?text=&docid=138782&doclang=EN.

12 Google Spain SL. v. Agencia Española de Protección de Datos : Case C-131/12 (May 13, 2013) [Electronic resource]. – Access mode : http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&doclang=EN.

subject's name[13]. What is more, due to their preeminent role in organizing data, search engines like Google are far more likely to interfere with the data subject's right to privacy than the original website publisher. (Id. 87.) Google, on the other hand, argued that the least cost avoider for removing access to the information was the website and not the search engine. Hence, the requirement of a search engine to remove content from its index would take insufficient account of the fundamental rights of publishers of websites, of other internet users and of the operator itself. In the context of the above mentioned judgment of the Court of Justice of the European Union it is worth to mention that the British House of Lords observed that the judgment of the Court is unworkable due to the fact that it does not take into account the effect the ruling will have on smaller search engines which, unlike Google, are unlikely to have the resources to process the thousands of removal requests they are likely to receive. In addition, the House of Lords sub-committee, noted that the expression, "right to be forgotten" is misleading because Information can be made more difficult to access, but it does not just disappear. Furthermore, they argue that it is "wrong in principle" to leave it to search engines to decide whether or not to delete information, based on "vague, ambiguous and unhelpful" criteria[14].

To conclude, according to the recent judgment (ECJ Ruling C-131/12) of the EU Court of Justice where the information is inaccurate, inadequate, irrelevant or excessive for the purposes of the data processing (§ 93 of the ruling) individuals have the right – under certain conditions – to ask search engines to remove links with personal information about them. In this vein, in case of giving consent as a child not being aware of risks by envisaged processing, the new law allows this individual to remove any such data which were made public on Internet at that time. At the same time, the Court explicitly clarified that the right to be forgotten is not absolute but will always need to be balanced against other fundamental rights, such as the freedom of expression and of the media (§ 85 of the ruling). It is also worth to mention that, according to the judgment of the European Union Court of Justice, "the right to be forgotten" cannot amount to a total deletion of history (Joint Cases C-92/09 and C-93/09 Volker and Markus Schecke and Eifert (2010) ECR 1-000, § 48). Hence, a case-by-case assessment is needed considering the type of information in question, its sensitivity for the individual's private life and the interest of the public in having access to that information. The role the person requesting the deletion plays in public life might also be relevant. Moreover, the traditional right to erasure ("right to be forgotten") expressed in the Regulation is further strengthen in such a way that the controller who has made the personal data public is obliged to inform third parties processing the data that the data subject has requested the controller to erase any links to, or copies or replications of that personal data. However, appreciating this provision the EDPS recognizes that it may be in some cases a huge effort to inform all third parties who may be processing such data, as there will not always be clear understanding of where the data may have been disseminated[15]. To conclude, "the right to be forgotten and to erasure" are likely to be one of the most controversial provisions of the proposed Regulation. Especially if compared to USA standards of data protection. While in Europe the intellectual roots of the right to be forgotten can be found in French law, which recognizes le droit à l'oubli-or the "right of oblivion" – a right that allows a convicted criminal who has served his time and been rehabilitated to object to the publication of the facts of his conviction and incarceration. In America, by contrast, publication of someone's criminal history is protected by the First Amendment, leading Wikipedia to resist the efforts by two Germans convicted of murdering a famous actor to remove their criminal history from the actor's Wikipedia page[16].

Right to access and right to data portability

In line with the current state of EU data protection law any person must be able to exercise his right of access to personal data relating to him, so that they can verify the accuracy of the data and the lawfulness of the processing. However, in a reality of the vast amount of personal data being processed in the on-line environment, the easier access to one's own personal data must be further assured. That is why article 15 of the proposed Regulation adds new elements, such as the controller's obligation to inform the data subjects about the applied storage period, and of the rights to rectification, to erasure and to lodge a complaint with the competent supervisory authority. Moreover, the Regulation introduces a new right; the data subject's "right to data

[13] Google Spain SL. v. Agencia Española de Protección de Datos : Case C-131/12 (May 13, 2013) [Electronic resource]. – Access mode : http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&doclang=EN.

[14] European Union Committee – Second Report EU Data Protection law: a "right to be forgotten"? (23 July 2014) [Electronic resource]. – Access mode : http://www.publications.parliament.uk/pa/ld201415/ldselect/ldeucom/40/4002.htm.

[15] Kunert Ch. The European Commission's Proposed Data Protection Regulation: A Copernican Revolution In European Data Protection Law / Ch. Kunert // The Bureau of National Affairs. – 2012. – [Electronic resource]. – Access mode : http://www.bna.com.

[16] Rosen J. The right to be Forgotten / J. Rosen // Stanford Law Review Online. – 2012. – № 64. – P. 88–92 ; Rustad M. Reconsupteulizing the right to be forgotten to enable transatlantic data flow / M. Rustad, S. Kulevska // Harvard Journal of Law & Technology. – 2015. – Vol. 28. – № 2. – P. 351–416.

portability". Hence, article 18 provides the right to obtain from the controller a copy of the personal data "in a structured and commonly used electronic format", allowing for any further use by the data subject, in particular allowing the data subject to transfer this personal data from one automated processing system of the controller to and into another, without being prevented from doing so by the controller.

Territorial scope

Let us now concentrate on the most significant provisions of the proposals for two legislative instruments that form the core of the data protection reform package: in the first place, the Regulation, setting out the general EU framework for data protection; secondly, the Directive for the police and criminal justice sector which is due to replace Framework Decision 2008/977/JHA which covers the protection of personal data processed by police and judicial authorities in criminal matters. Article 3 of the proposed Regulation contains the rules governing its territorial scope. In spite of innovation in this respect there is a lot of continuity which is evidenced in the concept, already reflected in the Directive 95/46, of "the processing of personal data in the context of the activities of an establishment" in the EU as the basic test for determining when the EU data protection law applies (Article 3(1)). However, at the same time, under Article 3(2) of the Regulation, data controllers not established in the EU may become subjects to the EU law when their processing activities are related to "the offering of goods or services" to data subjects residing in the EU, or to the monitoring of the behavior of EU residents. The goal of these changes is to bring more non-EU-based companies offering services over the internet liable for data protection breaches under EU law. On the other hand, the proposed Directive aiming at achieving greater harmonization of EU member states' rules on data protection in the area of police and criminal justice sector applies to domestic processing operations. This is necessary as neither article 8 of the EU Charter of Fundamental Rights nor Article 16 TFEU make a distinction between domestic and cross-border processing operations, but refer to processing activities that fall within the scope of EU law and the free movement of personal data. In addition, both the proposals for the Regulation and for the Directive are addressed to member states only, and therefore do not apply to the processing of personal data by the Union institutions, bodies, offices, and agencies, that will continue to apply Regulation (EC) № 45/2001.

In the context of the above described proposals for two legislative instruments, regulation and directive, that form the core of the data protection reform package, it is worth to mention the opinion of the European Data Protection Supervisor (EDPS) on the Commission's proposal. In the first place, EDPS welcomed the proposal for Data Protection Regulation as "a huge step forward" towards more effective and consistent protection of personal data across the EU (EDPS, 2012). However, the architecture of the package in itself – a Directive and a Regulation – signals that there might be a problem with its comprehensiveness. The main weakness of the package is that the level of protection in the proposed Directive is substantially lower than in the proposed Regulation.

Ensuring protection of personal data by police and criminal justice authorities

The scope of the draft Directive is similar to the draft Regulation, but there are important differences. In the first place, police and justice are the areas where the use of personal information inevitably has an enormous impact on the lives of private individuals. That is why it is difficult to understand why the Commission, instead of proposing comprehensive legislative framework, has decided to frame the data protection into two separate, unequal in terms of data protection guarantees, legislative acts; namely, the regulation and the directive. Moreover, the choice for a self-standing instrument is regrettable and constitutes a missed opportunity to clarify and ensure the consistent application of rules applicable to situations in which activities of the private sector and of the law enforcement sector interact with each other and borderlines are becoming increasingly blurred. Examples of these situations are the transfer of Passenger Name Record (PNR) data and data on financial transfers to law enforcement authorities. Furthermore, the Directive fails to include important elements regarding the retention of personal data, transparency towards individuals, keeping personal data up to date, and ensuring it is adequate, relevant and not excessive. Similarly the European Data Protection Supervisor regrets in particular that "the Commission does not propose stricter rules for the transfer of personal data outside the EU; data protection authorities are not given mandatory powers to effectively control the processing of personal data in this area; the possibilities for the police to access data processed in the private sector are not regulated. To conclude, the proposed directive might cause fragmentation in the EU Data Protection System, rather than introducing consistency.

Final remarks

The above described reform constitutes a huge step forward for data protection in Europe, considered by some as "Copernican revolution". The proposed rules will strengthen the rights of individuals and make controllers more accountable for how they handle personal data. What is more, according to the recent judgment (ECJ Ruling C-131/12) of the EU Court of Justice where the information is inaccurate, inadequate, irrelevant or excessive for the purposes of the data processing (§ 93 of the ruling) individuals have the right – under certain conditions – to ask search engines to remove links with personal information about them. Furthermore, the role and powers of national supervisory authorities (alone and together) are effectively reinforced. The fact that the proposed Regulation would be directly applicable in the Member States and would liquidate many complexities and inconsistencies stemming from the different implementing laws of the Member States constitutes another advantage. On the other hand, the Directive for data protection in the law enforcement area provides for an inadequate level of protection, by far inferior to the proposed Regulation. Furthermore, the proposed instruments taken together do not fully address factual situations which fall under both policy areas, such as the use of PNR or telecommunication data for law enforcement purposes An advantage of the proposed Directive is that it covers domestic processing, and thus has a wider scope than the current Framework Decision.

Анотація

У статті розглядається пакет пропозицій щодо реформ законів Європейського Союзу про охорону інформації, у якому висвітлюється деяка кількість головних змін порівняно із сучасними законами про охорону інформації; особлива увага приділяється праву на забуття. Саме тому текст структуровано таким чином: 1) приватне життя та охорона інформації – історія й сучасний стан закону; 2) посилення прав суб'єктів інформації: а) зростання відповідальності операторів та обробників персональних даних; б) погодження із законом Європейського Союзу; в) право на забуття; г) право на доступ і право на перенесення даних; 3) охорона персональних даних поліцією та органами кримінальної юстиції.

Summary

This article gives some insight into the EU data protection reform package highlighting a number of main changes in comparison to the current data protection rules, with the special focus given to the right to be forgotten. That is why the text is structured in the following way: 1) privacy and data protection – history and current state of law; 2) reinforcement of the rights of data subjects: a) enhancement of the responsibilities of controllers and processors; b) consent in the EU law; c) right to be forgotten; d) right to access and right to data portability; 3) protection of personal data by police and criminal justice authorities.

Literature:

1. Google Spain SL. v. Agencia Española de Protección de Datos : Case C-131/12 (May 13, 2013) [Electronic resource]. – Access mode : http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&doclang=EN.
2. Council Framework Decision 2008/977/JHA of 27 November 2008 [Electronic resource]. – Access mode : http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:350:0060:0071:en:PDF.
3. Directive (EC) 95/46 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) OJ L281/31.
4. EDPS Opinion of 7 March 2012 [Electronic resource]. – Access mode : https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-03-07_EDPS_Reform_package_EN.pdf.
5. EU Consumer Rights Directive. Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council (2011) OJ L304/64.
6. European Union Committee – Second Report EU Data Protection law: a "right to be forgotten"? (23 July 2014) [Electronic resource]. – Access mode : http://www.publications.parliament.uk/pa/ld201415/ldselect/ldeucom/40/4002.htm.

7. Fuster G. The Emergence of Personal Data Protection as a Fundamental Right of the EU / G. Fuster. – Switzerland : Springer International Publishing, 2014. – 300 p.
8. Gutwirth S. Reforming European Data Protection Law / S. Gutwirth, R. Leenes, P. de Hert. – New York ; London : Springer Dordrecht Heidelberg, 2015. – 315 p.
9. Hustinx P. EU Data Protection Law – Current State and Future Perspectives / P. Hustinx // Ethical Dimensions of Data Protection and Privacy : High Level Conference (Tallin, Estonia, 9 January 2013) / Center for Ethics, University of Tartu. – Tallin, 2013. – P. 3–8.
10. Kosta E. Consent in European data protection law / E. Kosta. – The Hague : Martinus Nijhoff Publishers, 2013. – 400 p.
11. Kunert Ch. The European Commission's Proposed Data Protection Regulation: A Copernican Revolution In European Data Protection Law / Ch. Kunert // The Bureau of National Affairs. – 2012. – [Electronic resource]. – Access mode : http://www.bna.com.
12. Opinion of Advocate General Jääskinen 19, Google Spain SL v. Agencia Española de Protección de Datos (Case C-131/12, May 13, 2014) [Electronic resource]. – Access mode : http://curia.europa.eu/juris/document/document.jsf?text=&docid=138782&doclang=EN.
13. Craig P. EU Law: Text, Cases and Materials / P. Craig, G. de Búrca. – 5th ed. – Oxford : Oxford University Press, 2011. – 120 p.
14. Proposed EU Data Protection Regulation One Year Later: The Albrecht Report // Privacy &Security Law Report. – 2013. – 12 PVLR 99. – P. 1–7.
15. Reding V. The European data protection framework for the twenty-first century / V. Reding // International Data Privacy Law. – 2012. – Vol. 2. – № 3. – P. 119–129.
16. Regulation (EC) № 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to processing of personal data by the Community institutions and bodies and on the free movement of such data (2001) OJ L 008/1.
17. Rosen J. The right to be Forgotten / J. Rosen // Stanford Law Review Online. – 2012. – № 64. – P. 88–92.
18. Rustad M. Reconsupteulizing the right to be forgotten to enable transatlantic data flow / M. Rustad, S. Kulevska // Harvard Journal of Law & Technology. – 2015. – Vol. 28. – № 2. – P. 351–416.
19. Lee D. What Is the "Right To Be Forgotten?" / D. Lee [Electronic resource]. – Access mode : http://www.bbc.com/news/technology-27394751.

Marta Kołodziejczyk,
academic of the Bielsko-Biala School of Finance and Law