https://doi.org/10.22364/iscflul.7.2.17

Vanya Panteleeva, *Ph.D.*
University of Ruse, Bulgaria

TRANSPOSITION OF DIRECTIVE (EU) 2016/680 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL OF 27 APRIL 2016 IN PERSONAL DATA PROTECTION ACT IN REPUBLIC OF BULGARIA

Summary

The digitalization of the world around us, also known as "the 4th Industrial Revolution", requires a rethinking of approaches to the protection of personal data and privacy. Various solutions are offered on global, regional and national scale, including regulatory, institutional, organizational and technological solutions.

In 2012, European Commission initiated the adoption of an entirely new legal framework for the protection of personal data within the Union. After 4 years of intensive negotiations, on 4 May 2016 the result was published in the Official Journal of the European Union: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing personal data and on the free movement of such data (General Data Protection Regulation) and Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 [1] on the protection of natural persons with regard to the processing of personal data by the competent authorities for the purposes of the prevention, investigation, detection or prosecution of crimes, or the enforcement of penalties and on the free movement of such data.

By the Act Amending and Supplementing the Personal Data Protection Act published in issue 17/2019 of State Gazette of Republic of Bulgaria was transposed the Directive (EU) 2016/680. This ensured homogeneous and high-level protection of personal data and facilitated the exchange of information with the competent authorities of other EU Member States, which is crucial for effective implementation of this cooperation.

The present paper analyses the Directive (EU) 2016/680 and its transposition in the national legislation concerning protection of personal data in the prevention, investigation, detection/prosecution of criminal offences and enforcement of criminal penalties.

Keywords: EU law, personal data protection, national law

[1] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

Introduction

In April 2016, EU Directive 2016/680 was adopted by the European Parliament and the Council, together with the General Data Protection Regulation (GDPR). This Directive regulates the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. The Directive (EU) 2016/680 and its transposition in the national legislation concerning protection of personal data in the prevention, investigation, detection/prosecution of criminal offences and enforcement of criminal penalties poses a number of questions reviewed in the current article.

1. EU Directive 2016/680

Personal data protection policy has a pronouncedly horizontal character, affecting almost all areas of life and business. This has been considered by European legislators when adopting the General Data Protection Regulation, which is a comprehensive and complex legal act.

From the standpoint of EU law, the regulation is directly applicable and obligatory in its entirety. Its purpose is to ensure uniform application of European Union law in all the Member States. The regulation, unlike the directive, does not need to be transposed. However, one of the challenges of the General Data Protection Regulation is the heterogeneous nature of its rules, which remain an option and, in some cases, oblige legislators in the Member States to adopt national implementing measures.

The General Data Protection Regulation (GDPR) has generated quite a lot of public attention from both sides – public and private sector. The new legal regime is applicable as of 25 May 2018. The GDPR replaces EU Directive 95/46/EC on the protection of personal data (in short, the Data Protection Directive, DPD)[2] and introduces several new elements in data subjects' rights (such as a right to data portability and the right to be forgotten), and new obligations for data controllers (such as data breach notifications, mandatory appointment of data protection officers and concepts like Data Protection Impact Assessments and Data Protection by Design and by Default). Another very important novelty that the GDPR brings is the possibility for the supervisory authorities to impose administrative fines in case of non-compliance.

It is important to note that Directive (EU) 2016/680 was adopted together with the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive

[2] Directive (Eu) 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.

95/46/EC (General Data Protection Regulation) (further referred to as GDPR), which indicates the attempt to ensure the integrity and complexity of data protection reform. This Directive focuses on the processing of personal data by organisations in the criminal law chain (e.g., the police, public prosecution services, courts and the prison system) within their legal tasks and competences (e.g., preventing, investigating, prosecuting and sentencing crimes and executing criminal penalties). For instance, when a law enforcement agency or a court processes personal data of their employees to pay the wages, the GDPR is the applicable legal act, since these data are not directly related to the implementation tasks under the scope of criminal investigation. Regarding such cases, Article 9, para. 1 of the Directive states that the GDPR shall apply. GDPR is also applicable in cases where competent authorities process personal data for archiving purposes in the public interest, for scientific or historical research purposes, or statistical purposes (Article 9, para. 2 of the Directive). The focus of the Directive's provisions is on the so-called competent authorities, which may not only include public authorities but also other bodies and entities entrusted by national law to exercise public authority and public powers in view of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. The Directive (EU) 2016/680 ought to be considered as a *lex specialis* for personal data protection in criminal law, whereas the GDPR is the *lex generalis* for personal data protection.

Directive's history runs mostly in parallel with that of the GDPR. The GDPR mainly builds upon and extends the notions of the EU Data Protection Directive (DPD) from 1995. This Directive was mostly based on the provisions in Convention 108 of the Council of Europe (also referred to as the Treaty of Strasbourg) from 1981.[3] The Council of Europe also published a recommendation that supplements Convention 108 for the use of personal data by the police in 1987.[4] This recommendation specified who had access to police data, under which conditions police data could be transferred to authorities in third countries, how data subjects could exercise their data protection rights and how independent supervision was organized. These recommendations, however, are not legally binding and many Member States have not fully implemented them. In 2008, the EU published Framework Decision 2008/977/JHA on the protection of personal data processing in the framework of police and judicial cooperation in criminal matters.[5] The aim of this decision was, on the one hand, the protection of personal data processed for the prevention, investigation, detection and prosecution of crimes and the execution of criminal penalties and, on the other hand, the facilitation and simplification of police and judicial cooperation between Member States.

Finally, in 2012, the European Commission presented the first draft for a Directive that would harmonize the processing of personal data in criminal law

[3] Council of Europe. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, No. 108, 28.01.1981.

[4] Council of Europe. Police Data Recommendation Rec(87)15, 17.09.1987.

[5] Europese Raad. Framework Decision 2008/977/JHA, 27.11.2008.

matters.[6] According to the Directive, the deadline for its implementation in national legislation was two years, with a final deadline in May 2018.

2. Transposition of Directive (EU) 2016/680 in Bulgarian Law. Personal Data Protection Act of Republic of Bulgaria

In 2019, in the Personal Data Protection Act of Republic of Bulgaria amendments were made concerning transposition of Directive (EU) 2016/680, and a new Chapter 8 was created concerning transposition of the Directive.

Art. 42, para. 1, defines the scope of Chapter 8

> *[..] the processing of personal data by competent authorities for the purpose of prevention, investigation, detection or prosecution of criminal offenses or execution of penalties, including prevention from threats to public order and security and their prevention.*

In Art. 3, No. 7 of the Directive, the European legislator provides the definition of "Competent authorities", which includes:

(a) any public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, and

(b) any other body or entity entrusted by Member State law to exercise public authority and public powers for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

The category "Competent authorities" is defined in Personal Data Protection Act, Art. 42, para. 4, as follows: "state bodies, which have the authority to prevent, investigate, detect or prosecute criminal offenses or enforce penalties, including the prevention from threats to public security and their prevention." So, these state bodies are entities involved in the criminal justice system framework, such as the police authorities, public prosecutors, courts and the prison system within their legal tasks such as preventing, investigating, prosecuting and sentencing crimes, as well as executing criminal penalties.

Most of the principals for data processing are common to the ones outlined by GDPR. The processing of personal data must be lawful, fair and used for specific purposes mentioned in the pertinent law. The purpose of the processing should

[6] 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 offences or the execution of criminal penalties, and the free movement of such data. COM(2012). Available at: https://eur-lex.europa.eu/legal-content/ENG/TXT/PDF/?uri=CELEX:52012PC0010&from=en%20 [last viewed November 3, 2019].

be explicit and legitimate, and determined when that data is collected. Individuals should be informed of the possible risks, rules, safeguards, and rights in relation to the processing of their personal data and how to use their rights. The main principles are defined in Personal Data Protection Act, Art. 45, para. 1:

- Lawfulness and fairness;
- Purpose specification and limitation;
- Data minimization;
- Accuracy;
- Storage limitation;

The time limits and storage of data is in the "hands" of the administrator of data.

There are special categories of data, as race, ethnic origin, politics, religion or philosophical beliefs, trade union membership, genetics, biometrics (where used for ID purposes), health, sex life, or sexual orientation, for which shall be permitted, where absolutely necessary, adequate safeguards of the rights and freedoms of the data subject, and it is provided for in the EU law, or in the legislation of the Republic of Bulgaria, Personal Data Protection Act, Art. 51, para. 1. However, there is an exception provided in para. 2 of the same articles, stating: "When the processing under para. 1 is not provided for in the law of the European Union, or in the legislation of the Republic of Bulgaria, the data under para. 1 may be processed when absolutely necessary, there are appropriate safeguards for the rights and freedoms of the data subject, and:

1. processing is to protect the vital interests of the data subject or another natural person, or
2. if processing refers to data that is obviously made public by the data subject."

Both Directive 2016/680 and of Personal Data Protection Act provide for data subject's rights, including a right to information and a right to access. The right to rectification (Art. 16, para. 1 of the Directive, Art. 56, para. 1 of the Personal Data Protection Act) applies to incorrect or incomplete data. Data subjects have the right to obtain from the data controller the rectification of inaccurate personal data relating to him or her. When data are incomplete, data subjects have the right to have incomplete personal data completed.

For personal data administrator and personal data processor, a list of obligations with regard to the processing of personal data is included in both Directive 2016/680 and the Personal Data Protection Act. Both personal data administrator and personal data processor maintain registers in writing and electronic formats. The registers include data about name and contact details of the administrator, the processor or the processors of personal data; the purposes of the personal data processing; the categories of recipients, to whom the personal data have been, or will be disclosed, including recipients in third states or international organizations; a description of the categories of data subjects and categories of personal data; where applicable, information on whether profiling is being carried out; where applicable, the categories of transfer of personal data to a third state, or international organization; the legal basis for the processing operation, including the transmission

of the data, for which the personal data have been intended; when possible, the deadlines for deletion of the different categories of personal data; where possible, a general description of the technical and organizational security measures under Art. 66.

One of the main goals of Directive 2016/680 is the protection of personal data of data subjects. Since many countries outside the EU are not offering such protection in their legal systems, there are strict rules in the Directive for the transfer of personal data to recipients in third countries. [7] The transfer of personal data to third countries (non-EU Member States) and international organizations is prohibited. Nevertheless, there are exceptions. Personal data in criminal law may be transferred outside the EU – only to competent authorities and only when there is a sufficient legal protection for data subjects in the receiving jurisdiction. Such protection can be based on an adequacy decision (Art. 36), appropriate safeguards (Art. 37), When such protection is absent, the transfer of personal data outside the EU may still take place in very specific situations (Art. 38–39), for instance, in case of immediate and serious threats to public security.

According to Section IV of Personal Data Protection Act, titled "Transfers of personal data to third countries or international organizations"[8]:

> *A competent authority may transfer personal data [..] to a third state or to an international organization, [..] when:*
>
> *1. the transfer is necessary for the purposes referred to in Article 42 (1);*
>
> *2. the personal data are transferred to a controller in a third country or international organisation that is an authority competent for the purposes referred to in Article 42 (1);*
>
> *3. where personal data received from another Member State of the European Union are transmitted, that Member State has given its prior authorisation to the transfer in accordance with its national law;*
>
> *4. where:*
>
> *(a) the European Commission has adopted a decision to the effect that the third country, territory or one or more specified sectors in the third country concerned, or the international organisation concerned, ensure an adequate level of protection, or*
>
> *(b) in the absence of a decision under Littera (a), appropriate safeguards have been provided or exist pursuant to Article 74, or*
>
> *(c) in the absence of a decision under Littera (a) and of appropriate safeguards under Littera (b), the transfer of the personal data is necessary in the cases referred to in Article 75;*
>
> *5. in the case of an onward transfer to another third country or international organisation, the competent authority that carried out the original transfer or*

[7] Bamberger K. A. and Mulligan D. K. Privacy on the Ground: Driving Corporate Behavior in the United States and Europe. The MIT Press.

[8] https://www.cpdp.bg/en/index.php?p=element&aid=1194

another competent authority in the Republic of Bulgaria authorises the onward transfer, after taking into due account all relevant factors, including the seriousness of the criminal offence, the purpose for which the personal data was originally transferred and the level of personal data protection in the third country or an international organisation to which personal data are onward transferred.

(2) Transfers of personal data without the prior authorisation by another Member State of the European Union in accordance with Item 3 of Paragraph (3) shall be permitted only if the transfer of the personal data is necessary for the prevention of an immediate and serious threat to public order and security of a Member State of the European Union or a third country or to essential interests of a Member State of the European Union and the prior authorisation cannot be obtained in good time. In such cases, the authority of the Member State of the European Union that provided the personal data, which is competent to give prior authorisation under Item 3 of Paragraph (1), shall be informed.

In case of an intended data transfer without an adequately substantiated decision or appropriate safeguards, exceptions in Art. 75 of Personal Data Protection Act may apply to specific situations. Such data transfers may be allowed, for instance, when necessary to protect vital or legitimate interests of individuals, to prevent immediate and serious threats to public security.

The supervision of rules in processing of personal data for the purposes of prevention, investigation, detection or prosecution of criminal offenses or execution of penalties, including prevention from threats to public order and security and their prevention by the court, the prosecution and investigative bodies in the performance of their functions of bodies of the judiciary is carried out by the Inspectorate.

Conclusions

The review on the Personal Data Protection Act and Directive (EU) 2016/680 leads to the general conclusion that the aforementioned legislation is a positive development in data protection policy of the EU and Member States. However, it should be pointed out that, in order to enable an effective criminal law enforcement, there are also inevitable differences. As it has been mentioned, Personal Data Protection Act is *lex specialis* and aims to set specific rules for the personal data processing in criminal law.

Acknowledgement

The study was supported the contract of University of Ruse "Angel Kanchev", № BG05M2OP001-2.009-0011-C01, "Support for the development of human resources for research and innovation" at the University of Ruse "Angel Kanchev". The project is funded with support from the Operational Programme "Science and

Education for Smart Growth 2014–2020" financed by the European Commission, European Social Fund.

BIBLIOGRAPHY

Literature

1. Bamberger K. A. and Mulligan D. K. Privacy on the Ground: Driving Corporate Behavior in the United States and Europe, The MIT Press, 2015.
2. Gonzales Fuster G. The Emergence of Personal Data Protection as a Fundamental Right of the EU. Heidelberg: Springer, 2014.
3. Pajunoja L. J. The Data Protection Directive on Police Matters 2016/680 protects privacy – the evolution of EU´s data protection law and its compatibility with the right to privacy. Master's thesis, Helsinki: University of Helsinki, 2017.

Legislative acts

1. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0680 [last viewed November 3, 2019].
2. Directive (EU) 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. Available at: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A31995L0046 [last viewed November 3, 2019].
3. Council of Europe. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, No. 108, 28.01.1981. Available at: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108 [last viewed November 3, 2019].
4. Council of Europe. Police Data Recommendation Rec (87)15, 17.9.1987. Available at: https://rm.coe.int/168062dfd4 [last viewed November 3, 2019].
5. Framework Decision 2008/977/JHA, 27.11.2008. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32008F0977 [last viewed November 3, 2019].
6. Закон за защита на личните данни [Personal Data Protection Act]. Available at: https://www.cpdp.bg/en/index.php?p=element&aid=1194 [viewed April 9, 2020].