UDK: 342.721 DOI: https://doi.org/10.18485/iup_rlr.2020.ch10

Daniela Ježová*

PRINCIPLE OF PRIVACY BY DESIGN AND PRIVACY BY DEFAULT**

The paper introduces two concepts in data protection: privacy by design and privacy by default. Those concepts are closely connected. They already existed in data protection, although the data protection reform made them a legally binding concept. The article outlines the new ePrivacy Directive and its specification of the discussed concepts.

Keywords: Data protection, European Union, ePrivacy Directive, Digital Single Market, GDPR, Privacy by Design, Privacy by Default

1. INTRODUCTION

The European Union found it important to expand the current EU single market, which consists of the free movement of goods, services, labour and capital. The single market frees the EU territory of any barriers. Currently, the four freedoms included in the internal market need to reflect societal development and the digital era. After creating the Digital Single Market, the European Union can reach its full potential.[185] The creation of a Digital Single Market is definitely a priority of the Union. The Data protection reform is an important part of the formation of the digital single market where the goal is to free European Union of any digital barriers.

The Personal Data Protection Reform includes the General Data Protection Regulation[186],which was adopted in April 2016 and entered into force on 25 May 2018. It

* PhD, Assistant Professor, Institute of European Union Law, Comenius University in Bratislava Law Faculty, Slovak Republic. Email: daniela.jezova@flaw.uniba.sk.

** This contribution was supported by the European Union, grant Jean Monet Module, application No: 611579-EPP-1-2019-1-SK-EPPJMO-MODULE, title: *Digital Single Market as a New Dimension of EU Law*.

[185] Ježová, D.: EU Digital Single Market – Are we there yet?, In: AD ALTA: journal of interdisciplinary research, year 7, No. 2 (2017), p. 100.

[186] Regulation (EE) 2016/679 of The European Parliament and of The Council of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

includes Directive[187],which states that Member States must incorporate into their national law by 6 May 2018, as well as the upcoming new ePrivacy Regulation. The GDPR replaced the original Data Protection Directive no. 95/46/EC as of 1995.[188]Currently, another legislative piece for data protection which is up for discussion, is a legislative process for adopting the new Privacy and Electronic Communications Regulation[189], proposed by the European Commission on 10 January 2017. The new regulation should replace the 2009 Directive.

In this article several data protection issues will be discussed with the focus on the protection of the individual by default settings, by engineering software, data retention cases and cookies. The issues will be analysed from an EU perspective.

2. DATA PROTECTION

The reform of personal data protection is fundamental to the creation of a digital single market. It is a priority of the Union and its goal is the achievement of liberties associated with the EU single market to expand to the digital world.[190]The main pillar of the reform is the new regulation GDPR, which primarily strives to strengthen the rights of individuals to protection of their personal data and reduction of the administrative burden associated with their protection. Another goal was to enable the free flow of personal data in the digital single market area. The General data protection regulation can be called a significant milestone in data safety. Although the GDPR is a European Union Regulation, its territorial scope does not stop at European boundaries. Given the global economy with multinational groups and cross-border data transfer, international aspects have been taken into consideration upon creating the GDPR.[191] It means that the registered seat and the territory where the data is processed is not a significant factor for determining whether the controller should comply with the GDPR rules or not. The GDPR also altered the view on protected data.[192] The importance of the GDPR and its compliance is also emphasized by the structure of the fines and the penalty system which considers the annual turnover of the controlled subject.

---

[187] Directive (EU) 2016/680 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.

[188] Ježová, D., 2018. Data Protection Reform in the EU as a Part of the Forming Digital Single Market. In: European Studies, The review of European Law, Economics and Politics, vol. 5, 2018, p.: 295.

[189] Proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM/2017) 10 final, 2017/0003(COD).

[190] Ježová, D., 2017. Data Protection in Virtual World, In: Právnírozpravy 2017, Hradec Králové: Magnanimitas, 2017, p. 63, ISBN: 978-80-87952-18-4.

[191] Voigt, P., Bussche, A., 2017. The EU General Data Protection Regulation (GDPR) A Practical Guide, Springer – Verlag Berlin Heidelberg, 2017, p. 22.

[192] Ježová, D., 2018. Comparative Study of Slovak and Austrian Approach to GDPR, In: AD ALTA: journal of interdisciplinary research, year 8, No. 1 (2018), p.116 – 119.

Today, personal data is very valuable and can be used as source of income for organizations and criminals alike. Therefore, the protection of data is necessary. In this context, the concept of privacy by design and privacy by default has to be considered a mandatory solution.

These concepts represent the evolution of privacy since they explicate the inclusion of privacy within the design of business processes and IT application support, in order to include all the necessary security requirements at initial implementation stages of such developments (privacy by design), or rather put in place mechanisms to ensure that only personal information needed for each specific purpose is processed "by default".

3. CONCEPT OF PRIVACY BY DESIGN

As mentioned above, the GDPR significantly changed rules of privacy. Although this concept is not new, and it has always been a part of the data protection law. Directive 95/46 of the European Union already referred to the requirement of the appropriate technical and organizational measures to be taken both when designing the system and during processing. Generally speaking, the concept of privacy by design means that if a system includes choices for the consumer on how much personal data will be shared with others, the default settings should be the most privacy friendly ones. Privacy by default generally means that if the system provides choices for the data subject regarding how much personal data he/she wants to share with others, the default settings should be the strictest ones[193]. Companies are encouraged to implement technical and organizational measures at the earliest stages of the design of the processing operations in a way that safeguards privacy and data protection principles right from the start. The key change by the GDPR is that it is now a legal requirement. Privacy by design and privacy by default are frequently discussed topics in connection with data protection and are two changes introduced by GDPR. Privacy by designs under GDPR means that data processors shall consider privacy at initial stages when designing and developing a product as well as services that involve processing personal data. The GDPR introduced the new requirements in this concept.

The aspect of the concept of Privacy by design is established in the GDPR recital 78[194] and article 25 para 1. Based on recital 78 "*appropriate technical and organisational measures be taken to ensure that the requirements of this Regulation are met*." Paragraph 1 of Article 25 GDPR stipulates that "*taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall […] implement appropriate technical and organisational measures*".

Based on the author Cavoukian, privacy by design is "the philosophy and methodology of embedding privacy into the design specifications of information technologies, business

[193] See also the definition prepared by the European Commission webpage available: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_en (01.09.2019).

[194] Part of the recital no. 78 GDPR: „The protection of the rights and freedoms of natural persons with regard to the processing of personal data require that appropriate technical and organisational measures be taken to ensure that the requirements of this Regulation are met."

practices, and networked infrastructures as a core functionality. Privacy by design means building in privacy right up front, directly into the design specifications and architecture of new systems and processes.."[195]

Privacy by design is a concept introduced in the 90´s by Ann Cavoukian, ex-commissioner of Information and Privacy in Ontario, Canada. Cavoukian defined 7 foundational principles of privacy by design in her work. The main principles are[196]:

a) proactive not reactive, preventative not remedial: explicit recognition of the value and benefits of proactively adopting strong privacy practices, early and consistently in order to prevent privacy risks from occurring (for example, preventing internal data breaches from happening);
b) privacy as the default setting: the collection of personal information must be fair, lawful and limited to that which is necessary for the specified purposes. The design of programs, information and communications technologies, and systems, should begin with non-identifiable interactions and transactions, as the default. Wherever possible, identifiability, observability, and linkability of personal information should be minimized;
c) privacy embedded into design: privacy is embedded into design of business processes, technologies, operations, and information architectures in a holistic, integrative and creative way;
d) full functionality – positive – sum, not zero-sum: accommodate all legitimate interests and objectives in a positive-sum "win-win" manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made. Privacy by Design avoids the pretence of false dichotomies, such as privacy vs. security, demonstrating that it is possible, and far more desirable, to have both.
e) end-to-end security – full lifecycle protection: privacy must be continuously protected across the entire life-cycle of the personal data. There should be no gaps in either protection or accountability. The security has special relevance here because without strong security, there can be no privacy
f) visibility and transparency: Privacy by Design seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification. Its component parts and operations remain visible and transparent, to both users and providers alike.
g) respect for user privacy: Above all, Privacy by Design requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options

---

[195] Cavoukian, A., 2011. Privacy by design in law, policy and practice. A white paper for regulators, decision-makers and policy-makers, 2011. Available: http://www.ontla.on.ca/library/repository/mon/25008/312239.pdf (01.09.2019), p. 3.

196 Cavokian, A.: Privacy by Design, The 7 Foundational Principles, Implementing and Mapping of Fair Information Practices, available at https://iapp.org/media/pdf/resource_center/Privacy%20by%20Design%20-%207%20Foundational%20Principles.pdf (01.03.2020).

According to the author Shaar, privacy by design should not be limited to developing clever technical solutions and incorporating them into systems. It is equally important to examine very early in the planning process whether and how to limit the amount of personal data to the absolute minimum necessary... Privacy by design goes beyond maintaining security. Privacy by Design includes the idea that systems should be designed and constructed in a way to avoid or minimize the amount of personal data processed. The key elements of data minimization are the separation of personal identifiers and content data, the use of pseudonyms and the anonymization or deletion of personal data as early as possible.[197] Authors Gurses, Troncoso and Diaz[198]focused on privacy by design and its principles which they found vague and with many open questions about their application when engineering systems" and they "show how starting from data minimization is a necessary and foundational first step to engineering systems in line with the principles of privacy by design.

EU law requires that controllers put in place measures to implement data protection principles effectively and to integrate the necessary safeguards to meet the requirements of the regulation and protect the rights of data subjects. These measures should be implemented both at the time of processing and when determining the means for processing[199]. When implementing these measures, the controller must to take into account the state of the art, the costs of implementation, the nature, scope and purpose of personal data processing and the risk and severity for the rights and freedoms of the data subject[200]. This principle is linked to article 24 GDPR where controller responsibility is laid out and refers to the implementation of all data protection principles and the compliance with the whole of the GDPR.

Article 25 is based on the realisation that the conditions for data processing are fundamentally set by the software and hardware used for the task. The accelerating pace of technical progress turns data protection through technology into the regulatory approach of the future. Technological concepts for preventive protection shall serve as the basis for minimally invasive data processing.[201]

When looking at the legal framework of the Council of European law such as Convention 108+[202], it is also required that controllers and processors assess the likely effect of processing personal data on the rights and freedoms of the data subjects before the processing (ex. art. 7). In addition, controllers and processors are obliged to design data processing in such a

---

[197] Schaar, P. 2010. Privacy by Design. Privacy by Design Issue of Identity in the Information Society Volume 3, Number 2, pp 267-274, available:https://link.springer.com/article/10.1007/s12394-010-0055-x (01.09.2019).

[198] Gurses, S., Troncoso, C., Diaz, C. Engineering Privacy by Design, available: https://software.imdea.org/~carmela.troncoso/papers/Gurses-CPDP11.pdf (01.09.2019).

[199] See Article 29 Working Party. 2017. Guidelines on Data Protection Impact Assessment (DPIA) (wp248rev.01) avialable: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236 (01.09.2019).

[200] See also ENISA 2015. Privacy and Data Protection by Design – from Policy to Engineering, available: https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design (01.09.2019).

[201] Voigt, P., Bussche, A., 2017. The EU General Data Protection Regulation (GDPR) A Practical Guide, Springer – Verlag Berlin Heidelberg, 2017, p. 62.

[202] Convention 108+ Convention for the protection of individuals with regard to the processing of personal data.

way as to prevent or minimise the risk of interference with those rights and fundamental freedoms (art. 10 para 2) and implement technical and organizational measures which take into account the implications of the right to the protection of personal data at all stages of the data processing.[203]

In his Preliminary Opinion on privacy by design[204], the European Data Protection Supervisor stated that a wider spectrum of approaches may be taken into account for the objective of "privacy by design" which includes a visionary and ethical dimension, consistent with the principles and values enshrined in the EU Charter of Fundamental Rights of the EU.

The principle of privacy by design can be identified as the key tool for increasing trust in information technology. Privacy must be approached through proactive measures, and not just as a reaction to breaches or other faults. The way to proactive action is to think about privacy from the beginning of a service/product lifecycle, in the design phase.

Compliance with data protection rules and the privacy by design principle shall be a cooperation between technical, legal and information technical knowledge in order to ensure correct implementation of the concept of privacy by design. In large companies, more experts shall be involved in the design process of the service/product.

Effectiveness is at the heart of the concept of data protection by design. The requirement to implement the principles in an effective manner means that controllers must be able to demonstrate that they have implemented dedicated measures to protect these principles, and that they have integrated specific safeguards that are necessary to secure the rights and freedoms of data subjects. Each implemented measure must have an actual effect. This observation has two consequences. Firstly, it means that Article 25 does not oblige controllers to implement any prescribed technical and organizational measures or safeguards, as long as the chosen measures and safeguards are in fact appropriate when implementing data protection into data processing. Secondly, controllers must be able to demonstrate that they have implemented measures and safeguards to achieve the desired effect in terms of data protection. To do so, the controller may determine appropriate key performance indicators to demonstrate compliance. Key performance indicators may include metrics to demonstrate the effectiveness of the measures in question.[205]

Based on this study[206], it is proposed that from the very first moment a company predicts a business activity, it must include the required assessments in relation to the personal and processing data that will have to be incorporated in that activity. Based on this study

[203] EU publications. 2018. Handbook on European data protection law 2018 edition, available: https://publications.europa.eu/en/publication-detail/-/publication/5b0cfa83-63f3-11e8-ab9c-01aa75ed71a1 (01.09.2019).

[204] EDPS, opinion 5/2018. Preliminary Opinion on privacy by design, May 2018 available: https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf (01.09.2019).

[205] The European Data protection Board enacted guidelines: Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Adopted on 13 November 2019 available https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201904_dataprotection_by_design_and_by_default.pdf (01.03.2020) - version for public consultation.

[206] Romero, S., De-Pablos-Heredero: Contribution of Privacy by Design (of the Processes), In: Harvard Deusto Business Research, available https://www.researchgate.net/publication/322795436_Contribution_of_Privacy_by_Design_of_the_Processes (02.03.2020).

of privacy by design, it is a popular design philosophy, and therefore it is important to make it more concrete.[207]Based on another study[208], the results indicate that, contrary to the popular view that consumers are unlikely to pay for privacy, consumersmay be willing to pay a premium fee for privacy.

The proposal of the new ePrivacy Regulation introduces the concept of "Privacy by design" more deeply, whereby users opt for a higher or lower level of privacy.

4. PRIVACY BY DEFAULT

The concept of privacy by default stated in article 25 para 2 GDPR should ensure that personal data is processed with the highest privacy protection. By default, personal data isn't made accessible to an indefinite number of persons and only personal data that is necessary for a specific reason shall be obtained. The principles of data minimization and purpose limitation relate to the concept.

Privacy-friendly default settings usually provide for maximum privacy in such a way that users do not have to change the settings of a service or product upon first use or access in order to protect themselves. When users wish to change these settings, they should have to opt in and amend the settings by themselves.[209] (ex. to share more of their personal data with others).

In accordance with the principle of data minimization, by default, only the amount of personal data that is necessary for the processing shall be processed. The amount of personal data refers to the quantitative as well as qualitative considerations. Controllers must consider both the volume of personal data, as well as types, categories and level of detail of personal data. If personal data is not needed after the first processing, then it shall by default be deleted or anonymized. Any retention should be objectively justifiable and demonstrable by the data controller in an accountable way. Anonymization of personal data is an alternative to deletion, provided that all the relevant contextual elements are taken into account and the likelihood and severity of the risk, including the risk of re-identification, is regularly assessed.[210]

Article 25(2) further states that personal data shall not be made accessible, without the individual's intervention, to an indefinite number of natural persons. The controller must by default limit accessibility and consult with the data subject before publishing or otherwise making available personal data about the data subject to an indefinite number of natural persons.

---

[207] Colesky, M; Hoepman, J; Hillen, Ch.: "A Critical Analysis of Privacy Design Strategies," 2016 IEEE Security and Privacy Workshops (SPW), San Jose, CA, 2016, pp. 33-40.

[208] Tsai, J., Egelman, S., Cranor, L., Acquisti, A.: The Effect of Online Privacy Information onPurchasing Behaviour: An Experimental Study, In.: Information Systems Research, Vol. 22, No. 2, June 2011, pp. 254–268.

[209] Voigt, P., Bussche, A., 2017. The EU General Data Protection Regulation (GDPR) A Practical Guide, Springer – Verlag Berlin Heidelberg, 2017, p. 63.

[210] The European Data protection Board enacted guidelines: Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Adopted on 13 November 2019 available https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201904_dataprotection_by_design_and_by_default.pdf (01.03.2020) – version for public consultation.

5. THE NEW ePRIVACY REGULATION

Recital 173 of the GDPR stipulates that the ePrivacy Directive shall be reviewed. Like in GDPR, the full harmonization concept is followed when changing the Directive to Regulation. In 2017, the new ePrivacy Regulation was introduced as a proposal adopted by the European Commission. The proposal is one of the actions needed for the creation of the Digital Single Market. In the Council, the examination of the proposal has been carried out in the Working Party on Telecommunications and Information Society (WP TELE). Within its WP TELE configuration, the EU Council made some progress and published several redrafts of the proposal since September 2017. The following issues were discussed: the need to clarify the relationship between ePrivacy and the GDPR; privacy settings; the legal grounds for data processing other than consent, as well as the applicability of the new rules to service providers assisting competent authorities for national security purposes, and the concept of public interests as a basis justifying restrictive measures.

Another point of discussion was related to data retention and to the related restrictions of rights, related to the current decision of the CJEU in the case Tele2 Sverige and Ministerio Fiscal[211]. This court decision makes an important clarification in the field of data retention. The CJEU drew a more precise line between admissible and inadmissible law enforcement access to data retained initially for commercial purposes by private providers of electronic communications services. In the previous case Tele 2 and Watson[212], the CJEU ruled that access to the retained data is limited to cases involving serious crimes. In the case of Digital Rights Ireland and Seitlinger and others[213], the CJEU criticised the general application of the Directive that required the collection of data on "all persons and all means of electronic communication as well as all traffic data without any differentiation, limitation or exception being made". In line with these criticisms, the CJEU found the Directive to be a disproportionate interference with the EU Charter. The right of respect for private life and the right to protection of personal data as provided for in Articles 7 and 8 of the EU Charter were central to the holding of the Court.[214]

The new regulation shall also interact with new technologies such as Machine-to-Machine, Internet of Things or Artificial Intelligence. The issue of processing of electronic communications data for the purposes of prevention/detection/reporting of child abuse imagery is also not closed.[215]Currently under the Finish presidency, the WP TELE examined the possible changes in the proposal of the new ePrivacy Directive dated on 10 January 2017.[216]

---

[211] Judgment of 2 October 2018, Tele2 Sverige and Ministerio Fiscal, C-207/16, EU:C:2018:788.

[212] Judgement of 21 December, Tele2 and Watson, C-203/15 and C-698/15, EU:C:2016:970.

[213] Judgment of 8 April 2014, Digital Rights Ireland and Seitlinger and others, C-293/12 and C-594/12, EU:C:2014:238.

[214] See Murphy, M. Data Retention in the Aftermath of Digital Rights Ireland and Seitlinger (2014). 24(4) Irish Criminal Law Journal 105.

[215] Progress report of the Presidency 2017/0003 (COD), 22 May 2019, available https://data.consilium.europa.eu/doc/document/ST-9351-2019-INIT/en/pdf (01.09.2019, 15.03.2020).

[216] Progress report of the Presidency 2017/0003(COD), 14447/19, 17 November 2019, available https://data.consilium.europa.eu/doc/document/ST-14447-2019-INIT/en/pdf (15.03.2020).

From the legal perspective the relationship between the new ePrivacy regulation and GDPR is that the new ePrivacy regulation will be *lex specialis* to GDPR. All matters concerning the processing of personal data not covered by ePrivacy regulations are covered by the GDPR as the general legal framework. As far as the new ePrivacy regulation is a part of the data protection reform the, penalties follow the pattern given by GDPR and can be calculated from the annual worldwide revenue of the undertaking.

The ePrivacy regulation relies on the definition of "electronic communication services" provided by the proposal for a Directive establishing the European Electronic Communication Code. Such an approach is intended to ensure equal protection of end-users when using functionally equivalent services. Therefore, the definition encompasses not only internet access services and services consisting wholly or partly in the conveyance of signals, but also interpersonal communication services, such as voiceover IP, messaging services and web-based e-mail services. The ePrivacy Regulation also covers interpersonal communications services that are ancillary to another service and have communication functionality.[217]

Privacy by default and Privacy by design concepts mostly include the options of cookies. Currently, the default settings for cookies in most current browsers are 'accept all cookies'. Therefore, providers of software enabling the retrieval and presentation of information on the internet should have an obligation to configure the software so that it offers the option to prevent third parties from storing information on terminal equipment; this is often presented as 'reject third party cookies'. End-users should be offered a set of privacy setting options, ranging from higher (for example, 'never accept cookies') to lower (for example, 'always accept cookies') and intermediate (for example, 'reject third party cookies' or 'only accept first party cookies'). Such privacy settings should be presented in a an easily visible and intelligible manner.[218]

In this regard, the recent case of Planet49[219] shall be mentioned. The decision deals with the consent under GDPR regarding the question about consent and the cookies. The official press release from the CJEU eliminates any confusion. It is titled *Storing cookies requires internet users' active consent* and makes it clear that "*a pre-ticked checkbox is therefore insufficient*". Any cookies not strictly necessary are prohibited from being pre-checked, regardless of whether the data processed is categorized as personal or not. Consent is not valid if given by way of pre-checked checkboxes which the users must deselect to refuse their consent. The court of Justice also stated that the expiration date of cookies and third-party sharing should be disclosed when obtaining consent, different purposes should not be held together in one consent requirement. In the case of Planet 49, the Court did not discuss one key element of consent, whether it was given freely, since this had not been an element of consent, whether it has been freely given, since this

[217] Asensio, P.: Data Protection in the Internet: A European Union Perspective: In.: Vincente, D., M., de Vasconcelos Casimiro, S. (ed), Data protection in the Internet, Springer, 2020, Switzerland, p. 469.

[218] Recital 23 of the Proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM/2017) 10 final, 2017/0003(COD).

[219] Judgment of 1 October 2019, Planet49, C-673/17, EU:C:2019:801.

had not been raised by the referring court. However, it applied a strict approach to the three other elements of consent; that it should be specific, informed and unambiguous.[220]

6. CONCLUSION

'Privacy by design' is an increasingly popular paradigm. It is the principle or concept that privacy should be promoted as a default setting of every new ICT system and should be built into systems from the design stage.[221]

We have seen a number of stages in user desires and needs for privacy through the last century, driven by advancements in technology: a) Privacy 1.0 – leave me alone in my domestic sphere (Warren and Brandeis, b) Privacy 2.0 – let me control what is known about me outside the domestic sphere (Westin), c) Privacy 3.0 – let me control how I am known, i.e. moving beyond a take-it-or-leave-it choice.[222] Currently we are at the stage of Privacy 3.0, and may even be entering a new stage of Privacy 4.0.

The growing digital world needs strict rules on data protection. Making the concepts Privacy by Design and Privacy by Default legally binding puts more pressure on software designers to put data safety in the first place while creating the system. In the recent case law, The CJEU also emphasized that the default setting when using cookies shall contain only the necessary elements of consent, no other consent is considered as valid in case there are opt out options.

[220] Docksey, Ch.: The EU Approach to the protection of rights in the digital environment: today and tomorrow – State obligations and responsibilities of private parties – GDPR rules on data protection, and what to expect from upcoming ePrivacy regulation, In: Human Rights Challenges In Digital Age: Judicial Perspective, Council of Europe, 2020 p. 71.

[221] Koops, B., Leenes, R.: Privacy regulation cannot be hardcoded. A critical comment on the 'privacy by design'provision in data-protection law. In: International Review of Law, Computers & Technology, 2014, 28.2: 159-171.

[222] Edwards, L.: Data Protection and e-Privacy: From Spam and Cookies to Big Data, Machine Learning and Profiling, In.: Law, Policy and the Internet, Hart, 2019, p. 163.

LIST OF REFERENCES

Article 29 Working Party. 2017. Guidelines on Data Protection Impact Assessment (DPIA) (wp248rev. 01) available: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236 .

Asensio, P.: Data Protection in the Internet: A European Union Perspective: In.: Vincente, D., M., de Vasconcelos Casimiro, S. (ed), Data protection in the Internet, Springer, 2020, Switzerland, p. 469.

Cavokian, A.: Privacy by Design, The 7 Foundational Principles, Implementing and Mapping of Fair Information Practices, available on https://iapp.org/media/pdf/resource_center/Privacy%20by%20Design%20-%207%20Foundational%20Principles.pdf (01.03.2020).

Cavoukian, A., 2011. Privacy by design in law, policy and practice. A white paper for regulators, decision-makers and policy-makers, 2011. Available: http://www.ontla.on.ca/library/repository/mon/25008/312239.pdf (01.09.2019), p. 3.

Colesky, M; Hoepman, J; Hillen, Ch.: "A Critical Analysis of Privacy Design Strategies," 2016 IEEE Security and Privacy Workshops (SPW), San Jose, CA, 2016, pp. 33-40.

Convention 108+ Convention for the protection of individuals with regard to the processing of personal data.

Directive (EU) 2016/680 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.

Docksey, Ch.: The EU Approach to the protection of rights in the digital environment: today and tomorrow – State obligations and responsibilities of private parties – GDPR rules on data protection, and what to expect from upcoming ePrivacy regulation, In: Human Rights Challenges In Digital Age: Judicial Perspective, Council of Europe, 2020 P. 71.

EDPS, opinion 5/2018. Preliminary Opinion on privacy by design, May 2018 available: https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf (01.09.2019).

Edwards, L.: Data Protection and e-Privacy: From Spam and Cookies to Big Data, Machine Learning and Profiling, In.: Law, Policy and the Internet, Hart, 2019, p. 163.

ENISA 2015. Privacy and Data Protection by Design – from Policy to Engineering, available: https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design.

EU publications. 2018. Handbook on European data protection law 2018 edition, available: https://publications.europa.eu/en/publication-detail/-/publication/5b0cfa83-63f3-11e8-ab9c-01aa75ed71a1 (01.09.2019).

Gurses, S., Troncoso, C., Diaz, C. Engineering Privacy by Design, available: https://software.imdea.org/~carmela.troncoso/papers/Gurses-CPDP11.pdf (01.09.2019).

Ježová, D., 2017. Data Protection in Virtual World, In: Právnírozpravy 2017, Hradec Králové: Magnanimitas, 2017, p. 63, ISBN: 978-80-87952-18-4.

Ježová, D., 2018. Comparative Study of Slovak and Austrian Approach to GDPR, In: AD ALTA: journal of interdisciplinary research, year 8, No. 1 (2018), p. 116 – 119.

Ježová, D.:, 2017. EU Digital Single Market – Are we there yet?, In: AD ALTA: journal of interdisciplinary research, year 7, No. 2 (2017), p. 100.

Judgement of 21 December, Tele2 and Watson, C-203/15 and C-698/15, EU:C:2016:970.

Judgment of 1 October 2019, Planet49, C-673/17, EU:C:2019:801.

Judgment of 2 October 2018, Tele2 Sverige and Ministerio Fiscal, C-207/16, EU:C:2018:788.

Judgment of 8 April 2014, Digital Rights Ireland and Seitlinger and others, C-293/12 and C-594/12, EU:C:2014:238.

Koops, B., Leenes, R.: Privacy regulation cannot be hardcoded. A critical comment on the 'privacy by design'provision in data-protection law. In: International Review of Law, Computers & Technology, 2014, 28.2: 159-171.

Murphy, M. Data Retention in the Aftermath of Digital Rights Ireland and Seitlinger (2014). 24(4) Irish Criminal Law Journal 105.

Progress report of the Presidency 2017/0003 (COD), 22 May 2019, available https://data.consilium.europa.eu/doc/document/ST-9351-2019-INIT/en/pdf (01.09.2019).

Progress report of the Presidency 2017/0003(COD), 14447/19, 17 November 2019, available https://data.consilium.europa.eu/doc/document/ST-14447-2019-INIT/en/pdf (15.03.2020).

Proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM/2017) 10 final, 2017/0003(COD).

Regulation (EE) 2016/679 of The European Parliament and of The Council of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Romero, S., De-Pablos-Heredero: Contribution of Privacy by Design (of the Processes), In: Harvard Deusto Business Research, available https://www.researchgate.net/publication/322795436_Contribution_of_Privacy_by_Design_of_the_Processes (02.03.2020).

Schaar, P. 2010. Privacy by Design. Privacy by Design Issue of Identity in the Information Society Volume 3, Number 2, pp 267-274, available: https://link.springer.com/article/10.1007/s12394-010-0055-x (01.09.2019).

Single Market. In: European Studies, The review of European Law, Economics and Politics, vol. 5, 2018, p.: 295.

The European Data protection Board enacted guidelines: Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Adopted on 13 November 2019 available https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201904_dataprotection_by_design_and_by_default.pdf (01.03.2020) - version for public consultation.

Tsai, J., Egelman, S., Cranor, L., Acquisti, A.: The Effect of Online Privacy Information onPurchasing Behaviour: An Experimental Study, In.: Information Systems Research, Vol. 22, No. 2, June 2011, pp. 254–268.

Voigt, P., Bussche, A., 2017. The EU General Data Protection Regulation (GDPR) A Practical Guide, Springer – Verlag Berlin Heidelberg, 2017.