CHALLENGES OF GENERAL DATA PROTECTION REGULATION (GDPR)

Dragan Savić*,
Mladen Veinović

Singidunum University,
Belgrade, Serbia

Abstract:
The aim of this paper is The General Data Protection Regulation (GDPR), an overview of current achievements in this domain within the framework of existing knowledge in literature, international standards and the best practice as far as the GDPR is concerned. This paper is particularly dedicated to GDPR who harmonizes data protection requirements across all 28 Member States, introduces new rights for data subjects, and applies extra-territorially to any organization controlling or processing data on natural persons in the European Union.

Keywords:
privacy, computer security, controller, personal data, WP29.

1. INTRODUCTION

The EU General Data Protection Regulation (GDPR) comes into effect in all EU Member States on 25 May 2018. This Paper provides a framework to help understand the basic principles of the new GDPR focusing on the data processing and collection principles. It also enables determination of the appropriate legal grounds to collect, process or further process personal data for all types of research, the conditions that need to be followed and the associated data subject rights, as well as it helps asses the implications of the different legal grounds for statistical and/or scientific research.

Collection and processing of personal information is fundamental to the work of researchers, so the protection of collected and processed data is of the utmost importance. The guidance provided in the GDPR is regarded as general information and is not legal advice and should not be relied upon as such. Specific legal advice should be taken in relation to any specific legal problems or matters.

Creation of legal certainty and sustainability of the data protection measures in technologically neutral approach is the major goal of the Regulation, because every researcher, whether employed within an agency, working independently or within a client's research department, will need to ensure that they understand the legal basis used for collecting, utilization, storage, sharing and processing of personal data.

Correspondence:
Dragan Savić

e-mail:
dragansavic.rm@gmail.com

DOI: 10.15308/Sinteza-2018-23-30

Aim of the GDPR is coordination of different rules existing in individual Member States, so the legal fragmentation, complexities and uncertainties shaped with the Data Protection Directive are reduced. The Regulation also allows the reinforcement of the data subjects' 5 rights, so it is easier for them to regain control over their personal data. Several updates and introductions of new individual rights and procedures of importance are executed, even so, the GDPR still applies roughly to the data controllers and processors acting in the public and private sectors for profitable and not-profitable purposes.

2. GENERAL DATA PROTECTION REGULATION

The General Data Protection Regulation (2016/679) announced the largest reorganization of European privacy laws in the last 20 years. This Regulation was published in the Official Journal on 4 May 2016 and became active on 25 May 2016, but the most essential provisions will become applicable in all Member States from 25 May 2018. [1] Regulation is readily effective in every Member State without the need for further national legislation. Nevertheless, it is necessary that Member States enclose at least some executive legislation by creating national regulator, in order to make excessive use of any of the derogations available under it. [2] The Regulation itself is followed by the Criminal Law Enforcement Data Protection Directive (2016/680), which refers to the processing of personal data by law enforcement authorities and must be implemented in all Member States by 6 May 2018. This Directive, however, will not be considered further in this note. [3] [4] [5]

The General Data Protection Regulation (GDPR) is recently harmonized regulation applicable across Europe and it mandates the protection of data about people living in the European Union. Every organization collecting, processing and using such data must adhere to this regulation, regardless of where it originates from. [6] Correct name of the GDPR is Regulation (EU) 2016/689, and it updates, replaces, and extends the protections previously given in the directive on data privacy (Directive 95/46/EC) from 1995. Excluded from the GDPR is protection of personal data of individuals involved in criminal affairs and the protection regime for such circumstances is outlined in a complementary directive -Directive (EU) 2016/680). [5] [6]

Every Member State must appoint a regulator as a form of supervisory authority, which in return should allow greater harmonization. However, with large number of national derogations, different Member States will very likely interpret and enforce this Regulation differently. Jurisdiction over businesses working across borders should primarily have supervisory authorities from countries in which said businesses have their main establishments. [7] Yet, there are exceptions to this rule.

The magnitude of anticipated change is fairly large and requires immediate action in order to get ready for compliance. Affected organizations will need to follow consistent and interconnected approach in order to comply with EU operations. GDPR will allow individuals to have considerably strengthened rights to privacy that they can enforce directly against organizations. [7]

The supervisory authority is appointed for a minimum period of four years and by all means must be independent of the Member State. [8] However, Member State may establish more than one supervisory authority (as is the case today in Germany). Also, European Data Protection Board (the Board), made up of one representative from the supervisory authorities from each Member State should be formed. [8] This Board will be successor of the current representative body, the Article 29 Working Party, but will in the same time have much stronger role in providing guidance and coordinating enforcement of the GDPR through a consistency mechanism than mentioned Article 29 Working party. [9]

The most essential trait of the supervisory authorities on the Board is clear guidance. The Article 29 Working Party has issued a work plan setting out four priority areas for guidance [3]:

- the new right to "data portability";
- the notion of "high risk" and privacy impact assessments;
- certification; and
- the role of the data protection officer. [3]

The most important role within the framework for protecting our fundamental human right- right to privacy are data protection laws through which it is regulated how organizations collect and process personal data. The European data protection law is considered to be one of the most comprehensive and restrictive in the world. [10] The GDPR includes controllers and processors founded in countries outside EU but which are collecting and processing personal data relating to individuals within EU, and thus significantly raises the bar for similar organizations all over the World. [10]

For controllers, accomplishing conformity with the GDPR should help build and secure trust of the c

ustomers/users, as well as reputation and finally and most importantly- value. For processors, accomplishing conformity with the GDPR should help with assuring controllers that they are the right partner and are able to maintain competitive edge. [10] For other organizations that provide services to both controllers and processors - from marketing agencies to payroll providers - there is an opportunity to add considerable value to their customers through providing compliance-enabling solutions. [11]

3. HOW THE DGPR WORKS

The GDPR consists of 173 recitals and 99 operative provisions. Only the operative provisions have legal effects while the recitals do not (or at least should not have). [11] Even though the GDPR has direct effects and does not require any Member State to pass laws in order to implement this regulation, it allows Member States to implement certain aspects of the GDPR in their own way under what are known as 'derogations'. These derogations help introduce exemptions from the GDPR's transparency obligations and individual rights and permit transfers of personal data in limited circumstances. Most derogations are linked to matters such as national security and defense, protection of judicial independence and proceedings, prevention and detection of crime, budgetary and taxation matters, public health and security and other important public interests. [11]

Each Member State must appoint a supervisory authority as an independent body responsible for monitoring and enforcing conformity with the GDPR. The GDPR, also, creates a new body called the European Data Protection Board (EDPB). This new body will consist of members from each of the EU's supervisory authorities (though the ICO's position after the UK leaves the EU is unclear) with the addition of the European Data Protection Supervisor. [12] As an independent EU body EDPB will have legal status and responsibility for overseeing the consistent application of the GDPR, amongst other tasks. It will also be responsible for resolving any occurring disputes between supervisory authorities. [13]

The Regulation does not apply to personal data relating to deceased individuals, except in cases when such personal data is crucial to identify living individual (for example, medical records which identify a relative or joint bank account records). Even so, Member States may establish their own rules when it comes to this type of processing (and countries such as Bulgaria, Estonia and France have already done it) so some organizations use 'deceased suppression records' to ensure that their marketing databases are up-to-date. [14]

The GDPR will apply where data are entirely processed by automated means or in cases of partially manual processing of personal data so the filing system could be formed, either partial or complete. The Regulation identifies what personal data consists of: identification numbers, on-line identifiers (whether this should include IP addresses or not is debatable), location data and other factors relating to one individual's behavior. [15] This is why organizations that provide on-line services or are relying on the use of tracking technologies will need to review their data processing practice to ensure they follow the GDPR requirements. Also, new definitions of 'genetic data' and 'biometric data' are included within the definition of special category data in The Regulation. [15]

As mentioned, the GDPR will apply where personal data are processed entirely or partly by automated means or the manual processing of personal data, which forms part of a filing system or is intended to form part of a filing system. If that is not the case, if processing does not, or is not intended to form part of a filing system then it will not be in the GDPR's reach. [15] In practice though, this exception isn't applicable to most organizations since most records are formed in certain way based on certain criteria so the data are easily accessible.

The territorial application of the GDPR covers much wider range than the Directive, used not only to regulate organizations established in the EU, but as well:

- EU-based entities, in relation to their activities, regardless whether the data is processed within the EU or outside of it;
- organizations from outside the EU, in relation to the offering of goods (and services) to data subjects in the EU or the monitoring of their behavior as far as their behavior takes place within the EU. [16]

4. KEY CHANGES IN GDPR

Key changes in GDPR include:

- a requirement to apply principles of 'privacy by design' and 'privacy by default' into the process of developing and launching new technologies, products, services, etc.;
- a new obligation to carry out privacy impact assessments;

- new rights to data portability and a right to be forgotten;
- a new requirement to notify data protection supervisory authorities if a data breach takes place;
- fines for non-compliance of up to EUR 20,000,000 or (if higher) 4% of the global annual turnover of the organization; and
- special rules around profiling and use of children's data. [16]

The GDPR applies to 'controllers' and 'processors'. A controller regulates all the purposes and means of processing personal data while processor is responsible for processing this data on behalf of a controller. The Regulation places very specific legal obligations on processor. For example, processor is required to keep records of collected personal data and processing activities; processor also has legal liability if it is found that they are responsible for a breach. [17] In addition to this, controller continues to be liable for their obligations even if processor is involved – the GDPR places further obligations on to ensure that controller's contracts with processors comply with the Regulation. [18]

The GDPR applies to processing carried out by organizations operating within the EU as well as to foreign organizations that offer goods or services to individuals in the EU. Even so, the GDPR does not apply to certain activities including processing covered by the Law Enforcement Directive, processing for national security purposes and processing carried out by individuals purely for personal/household activities. [19]

5. BASIC CONCEPTS AND DEFINITION

The basic definitions of "processing", "filing system", "controller", and "processor" are largely as in the Directive. The definition of "personal data" is also as in the Directive, but is supplemented to clarify that location data and on-line identifiers (e.g. IP addresses) also constitute personal data. [19] Withal, new definitions have been introduced, such as "profiling", "personal data breach", "pseudonymization", "biometric data", "data concerning health", "group of undertakings", and "cross-border processing". [20]

Consent is defined to mean any freely given, specific, informed and unambiguous indication of the data subject's will by which he or she, by a statement or clear affirmative action, confirms an agreement to the processing of personal data relating to him or her. [21]

The GDPR considerably increases the range of regulatory compliance for organizations which process data on behalf of data controllers – so-called 'data processors. [22] Data processors are required to implement any appropriate security measure, report data breaches to the controller, keep a register of data processing activities and seek controller's authorization before allowing third parties to sub-process personal data. Processors are also directly liable to implement sanctions for failure to comply with the GDPR. [23]

Complying with GDPR is mandatory. The GDPR applies every organization that controls or processes personal data on private persons in the European Union. [8] There is wide array of requirements and mandates that need to be in place when GDPR actually comes into force, of which is not the least that when a data breach occurs, the local data protection authority and all affected data subjects must be notified within 72 hours. [23]

In order to ensure that rights and freedoms of data subjects are not compromised the GDPR demands that data controllers and processors follow through both organizational and technical safeguards. Organizational safeguards include data protection impact assessments, data protection by design for both structured and unstructured data, and the appointment of a data protection officer who reports to the highest level of the organization. [23]

Technical safeguards include pseudonymization, encryption, and various capabilities for identifying and blocking data breaches, ensuring data security, and automatically identifying and classifying personal data, among others. [11] According to the GDPR "data breach" also includes "accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed", making thus prevention of unauthorized use or access to personal data a crucial element of the Regulation compliance. [9]

Non-compliance to the GDPR will be quite expensive. In addition to other financial consequences, there are two tiers of regulatory fines, a fine of up to €20 million or four percent of the annual worldwide turnover for the organization, whichever is higher. [14]

6. PRINCIPLES

The principles for protection of data under the Data Protection Act do not differ much from the principles stated within the GDPR. [24] The key addition is the

new accountability requirement: compliance with the principles needs to be demonstrated. Personal data shall be: [24]

- processed lawfully, fairly and in a transparent manner in relation to individuals (lawfulness, fairness and transparency);
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (purpose limitation);
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimization);
- accurate and, where necessary, kept up to date (data accuracy);
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed (storage limitation);
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures. [25]

The principles of accountability [3] and more explicitly underline in the GDPR than the DPA. The Regulation offers a new principle of accountability – requiring the controller to demonstrate active compliance with its legal responsibilities. This is achieved by integrating data protection throughout the organization's processes and culture, including by:

- maintaining a clear written record of all data operations which can be inspected by a regulator on demand;
- mechanisms and procedures for monitoring and verifying compliance (e.g. regular audit);
- measures to enhance awareness of data protection issues in the organization (e.g. training) up to senior managerial level;
- adoption of the principle of privacy by design – ensuring data protection principles are taken in to account at the early stages of designing new technologies, products and systems;
- adoption of the principle of privacy by default – ensuring that privacy protection is adopted as a default option;
- appointment of a Data Protection Officer (DPO) if required. [8]

The principle of transparency requires that any information and communication relating to the processing of personal data is easily accessible and easy to understand, and that clear and plain language is used. [3] [10] This principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed. [3] [10]

Significant effect of this requirement will be on the way organizations inform individuals of how their data will be processed. It will not, in any way, be acceptable to conceal information in thickly written privacy policies or terms and conditions. If consent is given without full transparency about the impacts of processing, it is stated in the GDPR that it will not be valid. The controller should be able to demonstrate compliance with the principles ("accountability"). [8] To demonstrate this conformation, 39 of the 99 articles require evidence. It is not necessary to register processing with the Supervisory Authorities under the Regulation but organizations (especially larger businesses) will need to keep detailed records of their processing.

7. PERSONAL DATA AND SENSITIVE PERSONAL DATA

Any information relating to an identifiable person who can be directly or indirectly identified, in particular by reference to an identifier, is considered to be 'personal data'. This definition allows that personal data, including name, identification number, location data or on-line identifier can be composed out of wide range of personal identifiers, and thus taking into account all the constant changes in technology and the way organizations collect information about people. Both automated personal data and manual filing systems where personal data are accessible according to specific criteria are covered with The GDPR. It is possible to include chronologically ordered sets of manual records containing personal data, as well. [25] Personal data that has been pseudonymized – e.g. key-coded – can fall within the reach of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

Sensitive personal data as "special categories of personal data" are brought up in the GDPR, and the definition of this kind of data now includes new fields such as biometric data. Genetic data, and biometric data which

are processed to uniquely identify an individual are specifically included in this special categories. Personal data relating to criminal convictions and offenses are not included, but similar extra safeguards apply to its processing. [25] This Regulation sets out new and elaborated rules regarding situations where data are used to undertake automated decisions impacting individuals (profiling). [25]

Biometric data are defined as personal data gathered using specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allows or affirms the unique identification of that natural person, such as facial images or fingerprint data. [11]

Profiling, on the other hand, is any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements. [11]

8. DATA SUBJECTS RIGHTS

The GDPR amplify the existing statutory rights data subjects have (e.g. to access their data files), through a wide range of entirely new or "refreshed" rights. These rights may be exercised freely (i.e. without charge to the data subject) and must generally be met within 30 days. The limited time allowed for responding to requests, as well as a removal of right to charge any kind of fee, will very likely inflict a significant burden on controllers forcing them to take steps to make data in their systems more easily accessible to data subjects.

We recognize 4 rights: [10] [16] [19]

- The right to receive a copy of the data;
- The right to data erasure (The data may require the controller to erase personal data on request in a range of scenarios – e.g. where the data are no longer required for their original purpose, or where consent to processing has been withdrawn).
- The right to object to processing (Individuals have the right to object to processing based on legitimate interests (including profiling), direct marketing, research and statistics. If exercised, this request must be respected unless the organization can show there are compelling grounds to continue with the processing which overrides the individual's rights, or if the processing is required to establish, exercise or defend legal claims).
- The right to data portability (This right allows a data subject to receive their personal data "in a structured, commonly used and machine-readable format" and to transmit data in that format to another controller).

9. NOTIFICATION OF DATA BREACHES

The GDPR requires the data controller to provide notification to the relevant supervisory authority of any personal data breaches. The notification must [8]:

- describe the nature of the breach;
- state the number of the data subjects affected by the breach;
- describe the likely consequences of the breach;
- describe the measures taken or proposed to be taken by the controller to remedy the breach. [10]

Every breach of security leading to the destruction, loss, alteration, unauthorized disclosure of, or access to, personal data is considered to be personal data breach.

When there is a risk to the rights and freedoms of individuals (e.g. damage to reputation, financial loss, loss of confidentiality with significant detrimental effect, discrimination) ICO/DPC has to be notified. Affected individuals, on the other hand, are to be notified when there is particularly high risk to their rights and freedoms. Relevant breaches must be reported to the Data Protection Commissioner within 72 hours of you becoming aware of the breach. [8]

In specific situations, the controller should also notify the data subjects affected by the breach which is why it is important that mentioned controllers have an internal breach reporting procedure in place and train their staff to understand what constitutes a data breach. [8]

10. TWELVE STEPS TO TAKE NOW GDPR

1. Make all key people in your business aware of the impact the GDPR will have on your business.
2. Document what personal data you hold, where it came from and who you share it with.
3. Review your current privacy notice and make the necessary changes.
4. Check that your procedures cover all the above rights that individuals have.

5. Update your subject access request procedure.
6. Document your legal basis for processing the various types of personal data you handle.
7. Review how you are seeking, obtaining and recording consent and then make the necessary changes.
8. Think about how to verify children's ages and gather parental consent for processing their personal data.
9. Ensure you have the right procedures in place to detect, reports and investigate a personal data breach.
10. Work out how and when to implement a Protection Impact Assessments PIA.
11. Designate a Data Protection Officer (if required) or someone to take responsibility for data protection compliance.
12. If you operate internationally, you will need to determine which data protection supervisory authority you come under. [10]

11. CONCLUSION

Organization maintaining data on EU residents will certainly need to ensure that they have the necessary capabilities to ensure compliance with the varied aspects of the Regulation. Not being able to comply will be potentially very damaging and, if the EU follows through on its promised fine structure, quite expensive.

That is why it is essential to already plan correct approach to GDPR compliance as well as win support of crucial people in organization. New procedures, for example to deal with the GDPR's new transparency and individuals' rights provisions, may be needed, and in large or complex business this could have significant budgetary, IT, personnel, governance and communications implications.

The biggest emphasis in the GDPR is placed on the documentation that data controllers must keep to demonstrate their accountability. Organizations are required to review their approach to governance and how they manage data protection as a corporate issue in order to comply with all the areas listed in this document. One aspect of this might be to review the contracts and other arrangements controllers have in place when sharing data with other organizations.

Different parts of the GDPR will have different impact on different organizations (for example, the provisions relating to profiling or children's data), so it will be useful to map out which parts of the Regulation will have the greatest impact on concrete business model and then give those areas necessary importance in planning process.

New antitrust-type sanction regime is in the focus of attention of the GDPR. With the threat of fines of up to 4% of annual worldwide turnover or €20 million, data protection will be taken more seriously. But, there is a risk of taking this too far and hold up innovation. That is why those advising on the Regulation will be under significant pressure to both provide sensible advice and avoid the risk of punitive sanctions. In the short term, privacy advice is going to need a little more thought, a good deal of pragmatism and a pinch of courage.

In closing, GDPR is coming fast, it almost certainly applies to your organization, and so the consequences of getting it wrong are severe. However, there are also positive consequences of getting it right, including a strong foundation for working with businesses in Europe, a clear understanding of consumer preferences, and strong internal data protection and security controls that foster trust with customers and partners alike.

REFERENCES

[1] P. Voigt, A. von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide*, Springer, 2017.

[2] CMS Law, Tax, Towards GDPR compliance, Your Action Plan, European Economic Interest Grouping 2017-2018.

[3] Simmons & Simmons, *New General Data Protection Regulation –overview and practical tips*, 2017.

[4] Bates Wells Braithwaite, Arts Council England, *A practical guide to lawful fundraising for arts and cultural organizations*, 2017.

[5] Association of financial mutual - AFM, *Implementing the General Data Protection Regulation, A practical guide for members of AFM*, 2017.

[6] NALC, *Reform of data protection legislation and introduction of the General Data Protection Regulation, Legal Briefing* L03-17, 2017.

[7] Business Information Factsheet, *A Guide to the General Data Protection Regulation (GDPR)*, 2017.

[8] European Commission, Communication from the commission to the European parliament and the council, *Stronger protection, new opportunities - Commission guidance on the direct application of the General Data Protection Regulation as of 25 May 2018*, Brussels, 2018.

[9] Hunton & Williams, *The Proposed EU General Data Protection Regulation, A Guide for in-house lawyers*, 2015.

[10] Information Commissioners Office - ICO, *Data protection, Guide General Data Protection Regulation (GDPR)*, 2018.

[11] Mason Hayers & Curran, *Getting Ready for The General Data Protection Regulation, A Guide by Mason Hayes & Curran,* Dublin, London, New York & San Francisco, 2018.

[12] G. Latchams, A practical guide to the General Data Protection Regulation, Version 1.0, 2017.

[13] Bird & Bird, *Guide to the General Data Protection Regulation*, 2017.

[14] Charity Finance Group (CFG), *Inspiring Financial Leadership, General data protection regulation: a guide for charities*, 2017.

[15] S. Blanchard, R. Smith, L. BlueVenn, *The General Data Protection Regulation(GDPR) A practical guide for businesses*, 2016.

[16] IT governance, *EU General Data Protection Regulation, A Compliance Guide*, 2016.

[17] Independent booksellers forum, *Guides to practical bookselling, General Data Protection Regulation (GDPR)*, 2017.

[18] SAGE, *General Data Protection Regulation (GDPR): The Sage quick start guide for businesses*, 2017.

[19] European Federation for Print and Digital Communication, INTERGRAF, *INTERGRAF Guide to the European data protection regulation for European printers*, 2016.

[20] DLA Piper, *A guide to the general data protection regulation*, 2016.

[21] Tectrade, *GDPR A practical guide*, Varonis, 2017.

[22] TLT, LLP, Get ready - *An essential guide to the General Data Protection Regulation*, 2017.

[23] Linklaters, *The General Data Protection Regulation A survival guide*, 2016.

[24] ESET, *Quick guide to the EU General Data Protection Regulation*, 2017.

[25] An Comisineir Cosanta Sonrai, *The GDPR and You General Data Protection Regulation Preparing for 2018*, 2017.