Mathematical Approach on the GDPR Complexity

Liviu Adrian Stoica, Chabbaki Ghizlane
Bucharest University of Economic Studies, Bucharest, Romania

The objective of this paper work is to create a mathematical approach that can quantify the complexity of the General Data Protection Regulation (GDPR) and, at the same time, the implementing of the rules in a company according to the actual benefits of doing so. The scope is to study the rules and regulations imposed by the law, the steps and requirements needed for implementing and to define the indicators that can be used in the mathematical definition of the model. Also, it checks the impact of each indicator in the system and identifies the factors that determine vulnerabilities, what damages are caused by these factors, the risk and impact level of the factors. It proposes a model to evaluate the indicators and the assignment of weights in formula evaluation of each indicator, so the risks of implementing the rules in the business will be smaller as well as the evaluation of the data protection terms of a company will be more balanced and optimal. The approach is from the point of view of the law imposed in implementing the model and the easiness and costs for the companies to do so, including the advantages or disadvantages and the risks they can expose to by doing so.

Keywords: GDPR, analysis, risks, complexity, mathematical formula

Introduction

General Data Protection Regulation (GDPR) (2016/679) was first proposed in 2012 and it was adopted in 2016. It replaces the Data Protection Directive (95/46/EC) and it establish one set of data protection law on all European member states that replace their own legislations aiming to give control to individuals over their personal data and to unify the regulation within the European Union (EU). It is affecting all organizations that have operations in EU or that are handling EU citizens data regardless if the main company is there or just a branch or subsidiary. It is impacting every entity that holds or uses European personal data inside or outside the European territory (Stoica, 2020).

We live in an informational world that make us all “data subjects” where our lives key aspects are determined by the data held about us. All social platforms, online companies, and all entities we interact with and have a contract or a service with store information’s about us that can determine our past, current, and even future behavior, identify our needs and almost every aspect of our life. All this data is at risk and open to compromise more than ever. Until now there was no law or legal approach that was forcing the “data owners” to report an incident in case of the data has been stolen or compromised, except if you fall victim to a direct or indirect consequence of the breach. Under GDPR, in the event of data breach the owners must notify the

---

Liviu Adrian Stoica, Ph.D., Finance Department, Bucharest University of Economic Studies, Bucharest, Romania.
Chabbaki Ghizlane, bachelor student, FABIZ student, Bucharest University of Economic Studies, Bucharest, Romania.
supervisory authority “without undue delay and, where feasible, not later than 72 hours after having become aware of it” (“GDPR-2016/679”, 2016).

Investing into better technology in response of the request on data deletion, retention and portability is a cost that is reflecting in the company products or services as an increased price affecting in a direct way all the actual customers or the potential customers, meaning that GDPR implementation, which is a necessary rule for stability and protection comes with a cost that affects both company and customers, better or lesser.

Is very hard to reliably quantify the investment needed to adapt to the GDPR rules and regulations by most of the companies? The big companies need a permanent qualified Data Protection Officer and all companies need adequate software for securing, collecting, storing, using the data affecting a lot of small business and their economic planning’s.

Vulnerability means a flaw or weakness in system security procedures, design, implementations or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system’s security policy (NIST SP 800-61 Rev. 2).

Problem Statement

The GDPR rules are the result of over four years of negotiations between the interested parties and are very wide and complex which, naturally, can have imperfections. Because of this aspect, where nothing is perfect a hundred percent and to cover everything that exists or could exist is almost impossible if not impossible the flaws uncovered can be exploited by some businesses and others that do not like to apply the law and they try to avoid it when they can try to find loopholes while exploring the imperfections (Stoica & Candoi-Savu, 2020).

The need of the mathematical approach comes from the need of an evaluation system of the implementing the GDPR and the benefits or the risks the new regulations expose for the business and for the customers. It tries to describe and evaluate the overall interaction between the customers and the companies, as is presented in Figure 1. GDPR relations between customers and companies, the implementation and set of rules based on the interaction, evaluating the compliance with the law, making the rules easier to be understood and implemented, both by the customers and the companies.

The model presents the overview complexity in interaction as the complexity of implementing the rules. Because of the structure of the law and the terms used, it takes time to understand it and to know what it requires for a full compliance. Both companies and customer must know their rights, what they are allowed to do, when and how they are allowed. For the companies the most important things to understand is how to collect, process, and store the data and for the customers about their legal rights on be informed how their data is collected, what data information it refers to, how it is processed and by who, and how they can cancel their data processing.
**Mathematical Approach on Interactions**

Based on the rules and regulations imposed by the law, we will try to determine first the complexity and the definition of the general overview of implementation in the relation with the customers and what the companies should do. For this we will take into account the minimum information needed for how to obtain the accord from the customer for the process of the data obtained, what data you’re not allowed to manipulate, what rights have the customers regarding the data, transparency of the companies regarding the data processing, storage and other operations regarding the data manipulated and used by the company, obtained from the customer (“Data Protection Under GDPR”, n.d.).

For the mathematical approach, for each indicator in the formula proposed, it will be used pe (points of evaluation) to can calculate and measure the indicators as a unified evaluation system.

\[
Oc = Ap + Ac + Tc + \sum_{i=1}^{nr} R_i + \sum_{j=1}^{no} RO_j, \quad \text{where:}
\]

\[
Oc = \text{overview coefficient,}
\]
\[
Ap = \text{allowing processing; it represents the coefficient that measures if the company complies with the rules that allow them to process the information from their customers. It is calculated based on:}
\]
\[
Ap = C_{DS} + CO_{DS} + LO_{B} + VI_{DS} + PI_{B} + LI_{B}, \quad \text{where:}
\]
\[
DS = \text{data subject, refers to the customer itself, the data collected from the customer;}
\]
\[
B = \text{business/company, actions taken in the company interests;}
\]
\[
C_{DS} = \text{consent of the data subject, 10 points;}
\]
\[
CO_{DS} = \text{need to fulfill a contractual obligation to the data subject (as example can be a telephone provider that needs to store the data of the client and in case of client not fulfilling the contractual obligations, they can blacklist him to not offer services again), 5 points;}
\]
LO\textsubscript{B} = need to fulfill a legal obligation (in interactions with the government to report the persons that benefit for some services, like in the medical business where you report the patients with their prescriptions), 5 points;

V\textsubscript{ID}\textsubscript{S} = protect the vital interests of the data subject (mostly applies in governmental operations like hospitals or at medics where they keep the record of the patients, or police), 5 points;

P\textsubscript{IA} = perform a task in the public interest (process data of people in an area based on age to make statistical dispersion of population), 5 points;

LIC\textsubscript{B} = legitimate interest of the company, as long as the fundamental rights and freedoms of the persons whose data are processed are not seriously affected. If the rights of the person prevail over the interests of the company, it’s not allowed to process the personal data, 5 points;

Ac = accord coefficient, refers to obtain the accord for processing from the DS by ensuring that DS understands the scope of the consent. Consent must be given freely, specifically, informed, and unambiguously, by means of a request submitted in clear and simple language.

Ac = DC + CE + ACC + PW + CDP, where:

DC = details of consent, 10 points;

CE = consent easiness, refers to the language and terms used in the consent proposal, how many special terms are used, how long are the phrases used, how ambiguous is the consent overall, 25 points;

ACC = acceptance of consent, refers to the easiness of accept the consent, such as checking an online box or signing a form, 5 points;

OW = opportunity to withdraw the consent, 10 points;

CDP = data processing detailed in the consent, from 0 to 15 points, increments of 1 point based on number of gathering personal information, details of processing, storage etc.;

Tc = transparency coefficient, refers to the information provided to DS about the entity processing the personal data and the purpose of that processing.

Tc = Binf + Rppd + Lbr + Bdp + Sdd, where:

Binf = basic information about the company, should include as many details as possible like full name, address, ways to contact, etc., 1 point for each information provided and 5 points for each contact details of the data protection officer (if any);

Rppd = reasons why company processes personal data; it is based on Ap, and if it is detailed each indicator in Ap gets 5 points;

Lbr = legal basis on which company relies, 5 points;

Bdp = beneficiary of the data processed, who will receive the data (if applicable), 10 points;

Sdd = specific data details.

Sdd = LI + AM + TDS + R\textsubscript{DS} + WCW + LCO + ADMP, where:

LI = what legitimate interest in company pursues when processing data based on the legal basis invoked, 5 points;

AM = what measures apply to the transfer of data to a non-EU country, 1 point for each measure;

TDS = time for how long the data will be stored, 5 points;

R\textsubscript{DS} = what rights does the person enjoy in terms of data protection (right of access, correction, deletion, restriction, objection, portability, etc.), each right 3 points;

WCW = Ways for how consent can be withdrawn (when it is the legal basis for processing), 3 points for each way (can be by email, by phone, by postal office, etc.);
LCO = legal or contractual obligation to provide data, 5 points;
ADMP = automated decision-making process, information about the logic, significance, and consequences of the decision, 10 points;
i = right position;

nr = total number of rights;

R = rights of DS to access data and to data portability, free access to personal data (inform the DS the company is processing the data, provide the details of the processing like purpose of the processing, categories of personal data concerned, recipients of the data, etc., send him a copy of the personal data that is being processed in an accessible format), right of data portability where the DS can move their data to another company to be processed, right to correct data and the right to object when a person considers that his personal data is incorrect, incomplete, or inaccurate, that person has the right to correct or complete them without delay (if some of the shared data has been found to be incorrect, the company must inform everyone who viewed it, unless this would involve a disproportionate effort), right to request a restriction on the processing DS personal data during the period in which it is determined whether the interest of the company prevails over DS interest (in the case of direct marketing, company is always obliged to stop processing personal data if the person in question asks to do so), right to object at any time to the processing of DS personal data, when the company processes such data on the basis of its own legitimate interest or in order to perform a task in the public interest, right to erasure of data (“right to be forgotten”), when DS requests the data controller to delete his personal data (company can refuse only if processing is necessary to respect freedom of expression and information, company must keep the personal data in order to comply with a legal obligation; there are other reasons of public interest that justify the storage of data, such as those related to public health or scientific and historical research or must store the personal data for possible legal action), 10 points each right;

j = operation position;

no = total number of operations;

RO = record of operations; the company must be able to demonstrate that it is acting in accordance with the GDPR and is fulfilling all applicable obligations—in particular at the request of the Data Protection Authority or during its inspections, each record type stored has a value of 5 points (the name and contact details of the entity involved in the data processing, the reason (s) for processing the data, description of the categories of persons who provide personal data, the categories of organizations that receive personal data, the transfer of personal data to another country or organization, the period of storage of personal data, description of the security measures used when processing personal data).

As a presentation of the application of the formula there were taken four companies and analyzed based on the indicators and their scoring which are presented in Table 1. The test was conducted during August 2020 in Romania, in Bucharest on four small companies. For privacy purposes and GDPR rules they will not be named in the analysis. Two companies from IT sector, 1 and 2, and two companies from Pharmacy sector, 3 and 4.

Based on the formula applied we can identify where the companies have problems in complying with the regulations, like in the case of Pharmacy 2 where they do not offer the patient to give its consent but they store all the data for legal proposes or in the IT company where one of the companies is on marketing proposes and has a higher score because they invested more money in developing the needs of the company in data protection compared with the other IT company which is based on software service and stores less data and processes less information.
### Mathematical Approach on GDPR Complexity

In this approach we try to determine the complexity of the rules required by the GDPR law. How the law is made, how it is structured, and how easy it is to apply into the company. All the articles in the law are structured and grouped based on the applicability such as for company, for customers, or for the interactions between the company and the customers.

The GDPR law has a total of 99 articles, organized by chapters and sections. We can identify the categories of articles, by their scope, as Definition which has 61 articles for the scope, territory, who and how verify the compliancy, etc., Company with 22 articles (with the most important and mandatory to implement: processing of special categories of personal data; processing of personal data relating to criminal convictions and offences; processing which does not require identification, information to be provided where personal data is collected from the data subject; information to be provided where personal data has not been obtained from

#### Table 1

| Indicator/score | Company 1 | Company 2 | Company 3 | Company 4 |
|-----------------|-----------|-----------|-----------|-----------|
| CDS             | 10        | 10        | 10        | 0         |
| CODS            | 5         | 0         | 0         | 0         |
| LOa             | 5         | 5         | 5         | 5         |
| V1DS            | 0         | 0         | 0         | 0         |
| PI\_B           | 0         | 0         | 5         | 5         |
| LIC\_B          | 0         | 0         | 5         | 5         |
| Ap              | 20        | 15        | 25        | 15        |
| DC              | 10        | 5         | 10        | 0         |
| CE              | 15        | 25        | 20        | 0         |
| ACC             | 5         | 5         | 5         | 0         |
| OW              | 5         | 10        | 5         | 0         |
| CDP             | 5         | 10        | 10        | 0         |
| Ac              | 40        | 55        | 50        | 0         |
| Binf            | 5         | 10        | 10        | 0         |
| Rppd            | 15        | 10        | 20        | 15        |
| Lbr             | 0         | 0         | 5         | 5         |
| Bdp             | 10        | 0         | 10        | 10        |
| Sdd             | 26        | 47        | 25        | 16        |
| LI              | 0         | 0         | 0         | 0         |
| AM              | 0         | 2         | 0         | 0         |
| TDS             | 5         | 5         | 5         | 5         |
| R\_DS           | 9         | 15        | 9         | 6         |
| WCW             | 12        | 12        | 6         | 0         |
| LCO             | 0         | 0         | 5         | 5         |
| ADMP            | 0         | 10        | 0         | 0         |
| Te              | 56        | 67        | 70        | 46        |
| \(\sum R\)     | 30        | 30        | 30        | 10        |
| \(\sum RO\)    | 10        | 20        | 40        | 40        |
| Oc              | 156       | 187       | 215       | 111       |

Source: authors own research.
the data subject; notification obligation regarding rectification or erasure of personal data or restriction of processing; automated individual decision-making, including profiling; restrictions; responsibility of the controller; records of processing activities; security of processing; notification of a personal data breach to the supervisory authority; communication of a personal data breach to the data subject; designation of the data protection officer; codes of conduct; penalties), Customers with seven articles (containing their rights: right of access by the data subject; right to rectification; right to erasure; right to restriction of processing; right to data portability; right to object; right to compensation and liability), and Interaction with nine articles (conditions for consent; conditions applicable to child’s consent in relation to information society services; principles relating to processing of personal data; lawfulness of processing; transparent information, communication and modalities for the exercise of the rights of the data subject; data protection by design and by default; data protection impact assessment; derogations for specific situations; representation of data subjects).

Based on the articles and law structure, the complexity can be split into implementation and rules to comply for the companies and understanding the rights and how to use them for the customers.

In Romania the Government adopted the LAW No. 190 of 18 July 2018 on measures to implement “Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Individuals With Regard to Processing of Personal Data and Regarding the Free Movement of These Data and Repealing Directive 95/46/EC (General Regulation on Data Protection)”. This law lays down the measures necessary for implementation at national level, mainly, of the provisions of Art. 6 Para. (2), Art. 9 Para. (4), Art. 37-39, 42, 43, Art. 83 Para. (7), Art. 85 and of Art. 87-89 of “Regulation (EU) 2016/679 European Parliament and of the Council of 27 April 2016 on Protection Individuals With Regard to the Processing of Personal Data and the Free Movement of Such Data and Repealing Directive 95/46/EC”, published in the Official Journal of the European Union, L series, No. 119 of 4 May2016, referred to as the General Data Protection Regulation.

\[
GDPR_{\text{complexity}} = \text{Company}_{\text{complexity}} + \text{Customers}_{\text{complexity}}
\]

\[
\text{Company}_{\text{complexity}} = \ln \sum_{j=1}^{\text{nc}} \text{Costs}_j \times \ln \sum_{i=1}^{\text{nr}} \text{Rules}_i + \text{Supervisory}_{\text{complexity}}, \quad \text{where:}
\]

- \( \text{nc} = \text{total number of costs;} \)
- \( j = \text{position of cost;} \)
- \( \text{Costs} = \text{the costs needed to implement the rules, as cost with new job position for Data Officer, costs with software of collecting data, costs to data security, storage etc., 5 points for each cost;} \)
- \( \text{nr} = \text{total number of rules;} \)
- \( i = \text{position of rule;} \)
- \( \text{Rules} = \text{all the rules that the company need to respect to comply with the law, as types of data they can collect, information they need to provide to customers, etc., 5 points for each rule;} \)
- \( \text{Supervisory} = \text{the definition of the government control body, what is needed for collaboration, how hard is to get the authorizations etc., on a scale from 1-5 points;} \)

\[
\text{Customer}_{\text{complexity}} = \ln \sum_{i=1}^{\text{nr}} (Right_i \times q), \quad \text{where:}
\]

- \( i = \text{position of right;} \)
- \( \text{nr} = \text{number of rights;} \)
Right = right of the customer, as access to data, correct the data, etc., each with a value of 5 points;
q = coefficient of how easy is to do each of the rights, with a value from 1 to 3, where 1 is easy, 2 medium, and 3 hard.

In Romania the Supervisory complexity has a score of 4 points because the lack of transparency in the government, the ways of contact, all the papers required to comply etc.

\[ \min(\text{Company complexity}) = \ln 40 \times \ln 180 = 19 \text{ points} \]
\[ \text{Customer complexity} = \ln 60 = 4 \text{ points} \]

The GDPR complexity in Romania should be 27 points, where 20 should be minimum and 40 maximum, which it means that to actually understand and implement the GDPR is easy, even for those that do not have experience in the field. With more commercial on marketing networks about the rights of the customers, the GDPR implementation should be very easy and flawless.

Conclusions

Considering the proposed model for evaluation for the implementation of the rules and regulation in the interaction between the companies and the customers, it is very easy for each company to calculate its own score and to check what they need to improve, considering a higher score means a higher compliance with the law. For the customers it is easier to understand their rights and how to interact with the companies regarding their own data and to understand better to what they are exposed and how they can change that.

Overall, the whole analyze about the GDPR points out that was a mandatory law for protection of the privacy of the people, which is not very complex to understand and is quite easy to implement. Of course, because of the costs required for a full comply on the data process, manipulation, and storage, the small business can be affected in a negative way on their development but at the same time, having this system their trust from the customers increases which means their total number of customers increases so the balance between costs and benefits is equilibrated.

References

Damian, A. T. (2019). Design principles for the General Data Protection Regulation (GDPR): A formal concept analysis and its evaluation, Article 101469. Retrieved from https://www.sciencedirect.com/science/article/pii/S0306437919305216 (Accessed on 5 October 2020)

Data protection under GDPR. (n.d.). Retrieved from https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_en.htm (Accessed on 5 October 2020)

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 95/46/EC (General Data Protection Regulation). (2016). Retrieved from https://eur-lex.europa.eu/eli/reg/2016/679/oj (Accessed on 1 October 2020)

Stoica, L. A., & Candoi-Savu, R. A. (2020). Risks and exploits exposed by GDPR. 32 EBES Conference Proceedings. Istanbul/Turkey on July 1-3, 2020.