*Eurasian Journal of Social Sciences, 9(1), 2021, 24-30*
DOI: 10.15604/ejss.2021.09.01.003

**EURASIAN JOURNAL OF SOCIAL SCIENCES**

**www.eurasianpublications.com**

# RISKS AND EXPLOITS EXPOSED BY GDPR

**Liviu Adrian Stoica**
Corresponding Author: Bucharest University of Economic Studies, Romania
Email: liviu.stoica@csie.ase.ro

**Robert Adrian Candoi Savu**
Bucharest University of Economic Studies, Romania
Email: robertzvs@yahoo.com

Received: February 22, 2021 Accepted: March 26, 2021

**Abstract**

This paper analyzes the flaws in the GDPR rules and regulations and tries to determinate the possibilities of exploiters to use the regulations in their favor to be able to commit wrongful deeds from the different correlations between companies and customers, companies and companies. It checks the ways of how the rules are exposed to flaws and how they can be used in a malicious way while effects are analyzed as impact on the business, on the free services offered and from the reduced ability to track cyber-crime. The study is focused on the improper aspects that can come from the GDPR like restricted technology access, poor customer services, huge business costs of adapting, restrictions on privacy and innovation and cybercrimes. The study is made about the exploits exposed to companies, to customers, inside or outside the territory of Europe. It analyses the relation between customer both to company inside or outside European territory including the aspects for the collaboration between companies no matter where they are located. The study is about exposing the negative aspects of implementing the GDPR rules and regulations with all that derive from this for informing the citizens on what they need to take into consideration while trusting different service providers thinking they are protected by the law.

**Keywords:** Risk, Exploit, GDPR, Vulnerability, Impact

## 1. Introduction

The General Data Protection Regulation (GDPR) 2016/679, first proposed in 2012, was adopted in 2016, superseding the Data Protection Directive 95/46/EC and set one set of data protection law on all European member states, which 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 is located in EU. It is impacting every entity that holds or uses European personal data inside or outside the European territory.

As in European Union (2016), we live in an informational world that make us all a 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, which 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 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 supervisory authority without undue delay and, where feasible, no later than 72 hours after having become aware of it.

Bisogni and Asghari (2020) investigate the relationship between data breaches and identity theft, including the impact of Data Breach Notification Laws (DBNL) on these incidents (using empirical data and Bayesian modeling). They collected incident data on breaches and identity thefts over a 13-year timespan (2005–2017) in the United States and their analysis shows that the correlation is driven by the size of a state. Enacting a DBNL still slightly reduces rates of identity theft; while publishing breaches notifications by Attorney Generals helps the broader security community learning about them. They conclude with an in-depth discussion on what the European Union can learn from the US experience.

Coyne's (2019) approach allows for a more nuanced view of the political climate in which LIBE operates and GDPR exists due to GDPR's current presentation as a model for other countries aiming to develop their own data privacy protection frameworks. As technological advancements in data processing and analysis create new vulnerabilities and opportunities for both public and private sector entities, it is essential to critically evaluate not only the regulatory standards that exist but also the opinions that inform them.

The majority of the businesses are unable to reliably quantify the current investment needed to adapt to the data protection. The medium and big companies need to appoint a permanent qualified Data Protection Officer which increases the company costs, including the proper software to secure the collected and stored data, the procedures to access the data and all the requirements which increase the company costs. This affects a lot of small business and their economic planning. All the costs that come from investing in better technology solutions to respond to request on data deletion, retention and portability will reflect in the company products or services by an increased price, in translation will affect directly the customers. This means all the data security and protection, which is a very good and needed approach come with a cost that affect both the company and the customers, better or lesser.

The article as it is presented can be considered as an approach on how to avoid the law and regulations made to trigger awareness about the flaws discovered in the law, which can be used by exploiters and try to correct them to keep the customers safe and avoid any kind of bad interpretation or behavior on the current rules imposed by the GDPR.

This paper is structured as follows: Section 2 presents the loopholes in GDPR whereas Section 3 discusses the Negative aspects derived from GDPR. Finally, Section 4 concludes the paper.

## 2. Loopholes in GDPR

The GDPR rules are the result of over four years of negotiations between the interested parties and is very wide and complex which, naturally, can have imperfections. Because of this aspect, where nothing is perfect and to cover everything that exist or could exist is almost 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 by finding loopholes while exploring the imperfections.

Sullivan (2019) examines the two major international data transfer schemes in existence today – the European Union (EU) model which at present is effectively the General Data Protection Regulation (GDPR), and the Asia-Pacific Economic Cooperation (APEC) Cross Border Privacy Rules system (CBPR), in the context of the Internet of Things (IoT).

One of the objectives of the GDPR is to protect the European population when their personal data is controlled by entities inside the EU and outside too. One loophole that can be identified at this level of protection can be appointed to the chance of organizations to collect the data and try to ignore the GDPR rules, by trying to make it escaped from the rules by passing it to other entities without legal protection. Even if the data is collected under the GDPR protection, in the legal way, it can be transferred to other entities to escape the protection of the law. If these

entities obtain the data indirectly, the GDPR should still apply but the application of the law might be only theoretical in these cases since they are considered data chains. The collected data under the GDPR consist from any data related to a living person, it gives obligations to the processors and rights to the individuals, but even so, users might lose some rights while organizations take advantages of this.

As Damian (2019) states, GDPR compliance is not straightforward: its text is not written by software or information engineers but rather, by lawyers and policy-makers. As a design aid to information engineers aiming for GDPR compliance, as well as an aid to software users' understanding of the regulation, this article offers a systematic synthesis and discussion of it, distilled by the mathematical analysis method known as Formal Concept Analysis (FCA). By its principles, GDPR is synthesized as a concept lattice, that is, a formal summary of the regulation, featuring 144372 records — its uses are manifold.

As analyzed by Voss (2017), extending the research before the GDPR, the protection of data was covering any organization processing the data in the European Union but did not guarantee the protection when the data was processed by an organization outside of the EU. With the GDPR, this changes in protection for all the European individual data processed by any company no matter if it is in EU or not, as observed by Kindt (2016) based on PrivazyPlan (2018) recital 23 of GDPR in order to ensure that natural persons are not deprived of the protection to which they are entitled under this Regulation, the processing of personal data of data subjects who are in the Union by a controller or a processor not established in the Union should be subject to this Regulation where the processing activities are related to offering goods or services to such data subjects irrespective of whether connected to a payment. The reason is to assure the population that their data is protected no matter where it is processed, like in the case when you access a website but you do not know where is the owner localized, or in the case when you go in a store to buy a product that is made in other country outside the EU and the store will say the product rules apply from the country of manufacture not the country of selling for the consummator rights which based on the low it is the opposite case.

As a test scenario, as presented in Figure 1, we can have an online catalogue of products. The company that hosts the catalogue is just presenting the items, as in marketing purposes with the prices equivalent in Euro and the entire site translated in English or other European country members' languages. We have a global portal with a large catalogue of items destined to the European consummators correlated with third party sellers from all over the world. This portal just promotes the merchandise under the GDPR rules and actually does not handle or collect any personal data. The potential customers can browse this portal anonymously and if they decide to buy a product, they will click the link accordingly for that product. The portal will redirect the customer to the real seller. The sellers of the products in the portal can be from Union or outside. The problem occurs when the customer is redirected to an outside of the Union seller. This is happening because the third-party seller does not sell directly to a European customer, it is just hosting the products on an online portal. This means that all the personal data interchange takes place outside the Union, directly with the seller that is not under the GDPR rules because its products are not supposed to be directed to the Union, they are worldwide. So, all the data exchanged between the customer and the seller are not under GDPR and is outside its scope.

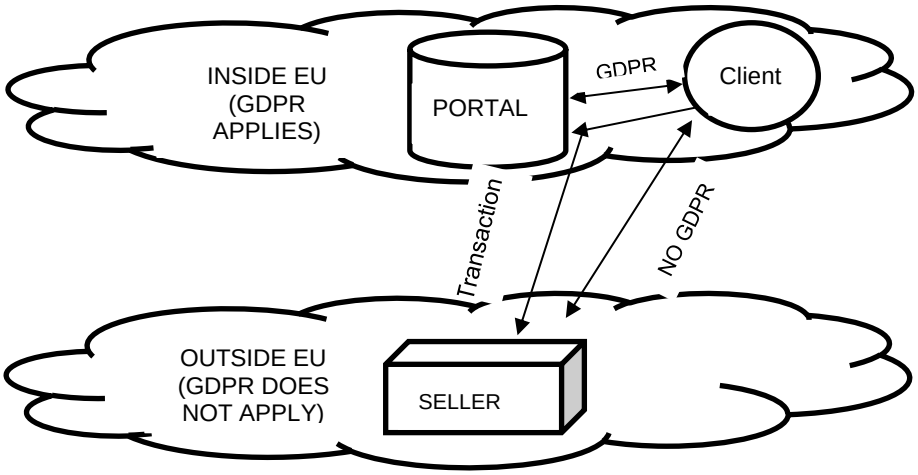
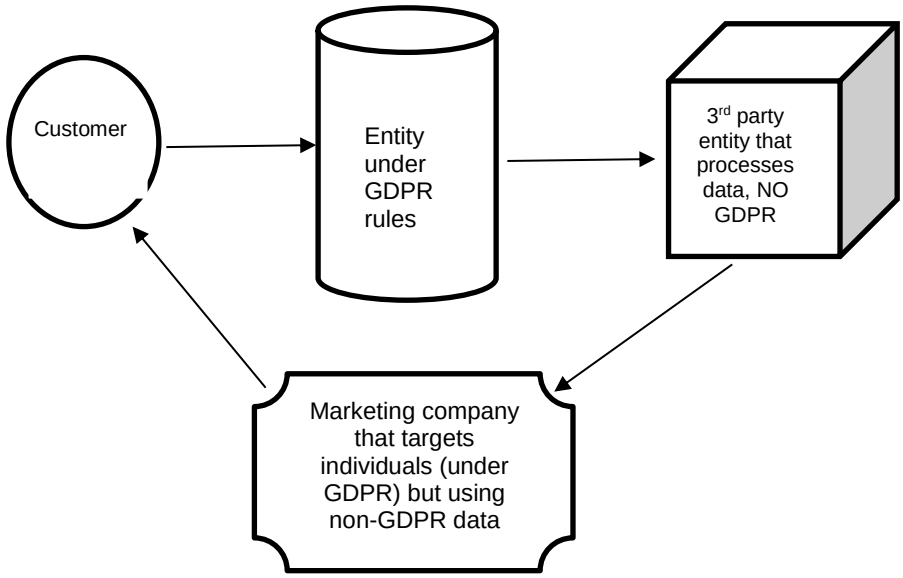



**Figure 1. An example of online portal data transactions**
**Source**: authors own study based on the proposed example

Based on Article 3.2 of GDPR European Union (2016) that states this Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to PrivazyPlan (2018) Recital 24, the monitoring of their behavior as far as their behavior takes place within the Union it would be covering the profiling and tracking of individuals in the EU. Regulation that covers the provision of electronic communications services to end-users in the Union mention that a non-EU provider needs to designate a representative in the EU aiming to cover the personal data collection via cookies in the websites used. This still does not cover the full potential of the loophole, because the sites can be cookie less and not store any information at all, just the seller (the 3rd party) will store all the data about the customer to be able to make an analyze about its shopping behavior and sell it to marketing companies for targeting in promotions.

**Figure 2. An example of customer losing rights about his own data**




**Source**: authors own study based on proposed example

Another loophole can appear from European Union (2016) Article 3.2 paragraph (a), the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union when the entity that process the data is subject of GDPR just if that data processed is used for offering goods or services to EU customers. We can have the example where a company outside or inside EU collects the customer data, legally, with their consent in the scope of a better offer for their needs. The problem appears when the entity sells the data to another entity that just make analyses and predictions based on the data collected. Since the analyze is not based on targeting directly the consummators is out of the scope of the GDPR and in this way a 3rd party now has access to all the private information, without giving the customers the opportunity to delete the data stored or access any information about it. If this 3rd party company makes a prediction of consummators based on an area on a certain product, it can sell the information to a marketing entity that can target that area directly with customized products without broking any GDPR rules or regulations, as presented in Figure 2.

Another loophole can be found in transparency, which from the point of data collection, everything should be transparent. Eugenia *et al*. (2018) analyze the recent enforcement of the GDPR, which has put extra burdens to data controllers operating within the EU. Beyond other challenges, the exercise of the Right to be Forgotten by individuals who request erasure of their personal information has also become a thorny issue when applied to backups and archives.

Based on Article 15 (European Union, 2016), which states the data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information, the citizens will know what is happening with their data, have the right to correct any errors if they spot them, ask for processor to delete any data or stop processing it. To do and exercise their rights, they need to know who is the entity that stores and processes their data. Other analysis was made by Cheng (2018) that after serious concerns about the invasion of digital footprint information privacy due to intense commercial promotion through data mining has led to the emergence of privacy by design in the form of the Do Not Track (DNT) mechanism. Article 13 regarding to collected personal data relating to a data subject give the entity that processes the information the obligation to inform the customer that he works with 3rd parties but without forcing him to provide the name of the recipients (European Union, 2016). Under Article 14, the recipient needs to inform the customer that it has its data but the 3rd party cannot identify the recipient because partial data was collected and based of lack of contact details, customer will not be informed (European Union, 2016). As example, if the customer receives a targeted message from a company that he does not recognize he can ask only then for his data to be removed but not prior to avoiding the unnecessary spam since he does not have the information on who actual owns his data.

Recital 61 says where the origin of the personal data cannot be provided to the data subject because various sources have been used, general information should be provided which make the customer almost impossible to erase all data history from the entities that hold it (PrivazyPlan, 2018). Based on this, all the profiling obtained from derivate data creates the same situation, when customer cannot avoid the targeted marketing until it happens to him, and only from the entity that targeted him, not all 3rd party entities that could have shared his personal data.

## 3. Negative aspects derived from GDPR

Except the loopholes that can be used to avoid the rules and regulations, GDPR can come with negative aspects as big entities like multinationals and companies were strengthened by the cost of implementing all the rules and regulations of the GDPR. It is an advantage of big companies that have a larger budget to pay for software upgrades and professionals, giving a greater share of the market to the already established competitors, while customers are less likely to try new platforms and tools. As an example, big companies such Google, Facebook, Amazon do not feel an effort on costs to implement the rules, while small companies struggle to implement the necessary rules because of the high costs, limiting the new products offered on the market, as similar example was analyzed by Cradduck (2020). Small and medium entities are weakened, even if the GDPR was announced years before implementation, most of the small and medium

companies are not full digitized. Most of them need to modernize their web platforms and markets and it is difficult for start-ups that need a huge start investment to comply with all the rules.

Another limitation or negative impact resulted from the implementation of the GDPR can be observed from the limit to the free speech and expression by the implementing of the rules, lot of media from the sites that were blocked to the public access from European Union, like some newspapers in USA, sites for e-commerce, games and other services especially those that export digital media and services and almost all the low business entities with sites that provide free content in exchange of collecting and processing customers data. Zhang (2019) examines the impacts of companies' voluntary adoption of the GDPR as well as the readability of privacy statements on US customers' intention to disclose information and their trust in a company.

The GDPR law can be considered to threaten the innovation and research, such as machine learning, big data mining, artificial intelligence, Blockchain that requires data processing which are minimized on their use of data and automate decision-making. Frei *et al.* (2011) used personal data collected from telephone provider and it makes it very hard for such articles and work of researches when it is needed the consent of all the customers for the analysis. Another example can be church that needs the consent of its members to target the meetings in the neighborhood.

Increases in cybersecurity risk considering the Internet Corporation for Assigned Names and Numbers issued a specification that allows registrants to be anonymous which avoids the information's in the WHOIS query used by cybersecurity professionals and researchers or trade markers. Starchon and Tomas (2019) discussed the example of mobile operators that affect our everyday lives with reference to assigned problem of collecting, processing and managing a relatively large amount of our personal data. The problem comes from the right of public to know versus the individual's right to privacy.

This situation might create risks for identity theft and online fraud because companies need to increase the data pools to respond to consumer information requests, which is a target for hackers and identity thieves, treating anonymous users as sensitive data and option for all-or-nothing choice for the customers.

## 4. Conclusion

GDPR, even without being perfect for covering all aspects that can appear or exist, is already having a positive effect on all entities that use personal data and it offers more protection and more usable rights to customers. Reducing the loopholes and adding more regulations based on society development will have a good impact on its overall success. A high transparency on an entity does not mean it is not avoiding the GDPR, it maintains the customer responsibility to investigate how the platforms collect and use personal data.

As no rule or regulation can be totally flawless, GDPR came to ensure the privacy of people adding as many benefits as it can, trying to limit the eventually identity theft and commercial abuse, while opening some opportunities for the bad people to stay anonymous and try to exploit the goodness of normal people. Until a future with more companies adapted to this transparency and business correctitude, people still need double check the transactions and the information that companies collect and how they process, indeed, not as much and detailed as before the GDPR was implemented.

As a future for the research, to extend the results and make the customers more aware on the exploits that can appear from trying to avoid the law and to keep them as safe as possible, we recommend the analysis of each article, or combination of articles of European Union (2016) to check how they can be avoided or misinterpreted in the benefit of the exploiters to increase the awareness for the citizens and keep their personal data safe from exploitation ensuring the browsing anonymity while the transactions are fair and secured.

**Acknowledgment:** This paper was co-financed from the Human Capital Operational Program 2014-2020, project number POCU / 380/6/13/125245 no. 36482 / 23.05.2019 "Excellence in interdisciplinary PhD and post-PhD research, career alternatives through entrepreneurial initiative (EXCIA)", coordinator The Bucharest University of Economic Studies".

**References**

Bisogni, F., and Asghari, H., 2020. More than a suspect: An investigation into the connection between data breaches, identity theft, and data breach notification laws. *Journal of Information Policy*, 10, pp. 45-82. https://doi.org/10.5325/jinfopoli.10.2020.0045

Cheng, F. C., and Wang, Y. S., 2018. The Do Not Track mechanism for digital footprint privacy protection in marketing applications. Journal of Business Economics and Management, 19(2), pp. 253-267. https://doi.org/10.3846/jbem.2018.5200

Coyne, H., 2019. The untold story of Edward Snowden's impact on the GDPR. *The Cyber Defense Review*, 4(2), pp. 65-80.

Cradduck, L., Stevens, S., and Cowan, M., 2020. Data sharing, international property practices and the GDPR: communicating with your consumers. *Property Management*, 39(1), pp. 22-33. https://doi.org/10.1108/PM-05-2020-0033

Damian, A. T., 2019. Design principles for the General Data Protection Regulation (GDPR): A formal concept analysis and its evaluation. *Information Systems*, 91, pp. 1-14. https://doi.org/10.1016/j.is.2019.101469

Eugenia, P., Michota, A., Efthimios, A., Matthias, P., and Constantinos, P., 2018, Backups and the right to be forgotten in the GDPR: An uneasy relationship. *Computer Law & Security Review*, 34, pp. 1247-1257. https://doi.org/10.1016/j.clsr.2018.08.006

European Union, 2016. Council Regulation, 2016 (EU) 2016/679 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, Official Journal [online] L119. Available at: <https://eur-lex.europa.eu/eli/reg/2016/679/oj> [Accessed on 17 April 2020].

Frei, P., Poulsen, A. H., Johansen, C., Olsen, J. H., Steding-Jessen, M., and Schüz, J., 2011. *Use of mobile phones and risk of brain tumors: update of Danish cohort study*. [online] Available at: < https://pubmed.ncbi.nlm.nih.gov/22016439/> [Accessed on 10 April 2020].

Kindt, E. J., 2016. Why research may no longer be the same: about the territorial scope of the new data protection regulation. *Computer Law & Security Review*, 32(5), pp. 729-748. https://doi.org/10.1016/j.clsr.2016.07.007

PrivazyPlan, 2018. Practical guide for implementing the EU GDPR. Available at: <http://www.privacy-regulation.eu/privazyplan/en/> [Accessed 20 April 2020].

Starchon, P. and Tomas, P., 2019, GDPR principles in data protection encourage pseudonymization through most popular and full-personalized devices - mobile phones, *Procedia Computer Science,* 151, pp. 303-312. https://doi.org/10.1016/j.procs.2019.04.043

Sullivan, C., 2019. EU GDPR or APEC CBPR? A comparative analysis of the approach of the EU and APEC to cross border data transfers and protection of personal data in the IoT era. *Computer Law & Security Review*, 35, pp. 380-397. https://doi.org/10.1016/j.clsr.2019.05.004

Voss, W. G., 2017. First the GDPR, Now the Proposed ePrivacy Regulation. *Journal of Internet Law*, 21(1), pp. 3-11.

Zhang, Y., Wang, T., and Hsu, C., 2019. The effects of voluntary GDPR adoption and the readability of privacy statements on customers' information disclosure intention and trust. *Journal of Intellectual Capital*, 21(2), pp. 145-163. https://doi.org/10.1108/JIC-05-2019-0113