The GDPR and its impact on the web

Daniel Anderson, Richard von Seck*
*Chair of Network Architectures and Services, Department of Informatics
Technical University of Munich, Germany
Email: ge72fat@mytum.de, seck@net.in.tum.de

***Abstract*—Processing of personal data is a key task for organizations and companies to optimize their business. To protect the consumers' privacy the General Data Protection Regulation (GDPR) was introduced in 2016 and became enforceable in 2018. The GDPR protects individuals by specifying how website operators can gain information about their customer. One core purpose is empowering people by giving them information on what their data is being used for. This paper introduces the tenets of the GDPR and presents the basic principles of data collection and processing, such as purpose limitation and data minimization. Furthermore, changes that have occurred on the web after the introduction of the regulation are discussed. A notable impact on web users is that they are now requested to give consent more often than before the law enforcement, less cookies are being collected, and users have the ability to inform themselves about data processing. However, the changes through the GDPR do not create more transparency on the web because the policies are too long and complex.**

***Index Terms*—gdpr, general data protection regulation, gdpr compliance**

1. Introduction

In the 21st century, internet is an essential part of most people's daily life. It is utilized for a multitude of different purposes, from purchasing clothes in a webstore to communicating with friends and family over social media to playing video games online. One thing that has become apparent in the last two years while browsing through the web is irritating pop-up windows or banners when visiting a website asking for consent to use cookies. Some might simply accept the use of cookies without giving it any further thought. Curious people might wonder what they are accepting and inform themselves what their data is being used for. For many people this is the first encounter where they become aware of data protection. Protection of personal data is specified to be a crucial right as stated in Article 8 of the Charter of Fundamental Rights of the European Union [1]: "Everyone has the right to the protection of personal data concerning him or her."
The GDPR [2] is a privacy and security law focusing on the protection of personal data within the European Union (EU) and the European Economic Area (EEA). Any information related to an identifiable natural person, i.e. an identification number or name, is considered personal data. The law protects every data subject no matter the nationality or residence. A data subject is an individual that organizations collect data about [3]. In this paper the terms "data subject", "user", "consumer", and "natural person" are used interchangeable. The GDPR applies to all organizations worldwide that collect or process personal data of EU citizens regardless of whether they have a presence in the EU [4]. There are two entities involved in the procedure of processing data. First, the controller which specifies the intent of the processing of personal data (Art. 4.7) and second, the processor that handles personal data for the controller (Art. 4.8). The regulation was introduced on 27 April 2016 and became enforceable on 25 May 2018. It replaced the 1995 Data Protection Directive (DPD) after Europe's data protection authority announced the DPD needed an update, following Googles lawsuit for scanning a user's emails in 2011 [5].
In the first part of this paper a brief overview over the core concepts and principles of the GDPR is given. The second part presents how the implementation of the data protection regulation has impacted the web and which changes have occurred.

2. Core Concepts

The following subchapters introduce key concepts and principles of the GDPR, show how consumers are protected by law, and specify special requirements that must be fulfilled by organizations to lawfully collect and process personal data.

2.1. Principles Regarding Personal Data

The GDPR consists of six core principles specifying how personal data must be collected and processed:

- Lawfulness, fairness, and transparency
- Purpose limitation
- Data minimization
- Accuracy
- Storage limitation
- Integrity and confidentiality

The first principle ensures that the data subject is always able to know what type of data is collected and what it is being used for. Transparency is further outlined in Section 2.6. Purpose limitation states that the collected information may only be used for the intended purpose and stored only for as long as necessary. Data minimization limits the data collection to only the relevant and necessary information. Only data that is relevant and necessary to fulfil the purpose should be gathered.

doi: 10.2313/NET-2020-11-1_01

The principle accuracy specifies that all stored data must be accurate and updated. Therefore, false data must be deleted or corrected in order to ensure that the personal data is accurate. Storage limitation states that the information should not be stored for a longer time period than necessary. As soon as the data has been processed for the specified purpose and is no longer needed, it should be erased. Archiving in the public interest can however be a reason to store the data longer. The last principle ensures that all personal data is appropriately secured. It implies that data must be protected from unauthorized access, mislaying, or demolition. Thus, it is inevitable to take precautions in order to guarantee the security of the stored personal data (Art. 5) [3].

2.2. Lawfulness of Processing

The GDPR specifies several principles one of which is the lawfulness of processing personal data. The regulation states that the processing is illicit unless the GDPR states it contrarily. Consequently, one of the following reasons must apply for it to be lawful. The user has given consent (Art. 6.1.a). The processing of data is a necessity in order to perform or enter a contract (Art. 6.1.b). Another valid reason could be the controller having legitimate interest in processing the data (Art. 6.1.f), e.g. a company has discovered a security leak on their website and wants to inform users of this fault. Furthermore, data processing is also permitted in the case of it being a legal obligation (Art. 6.1.c), e.g. a messaging platform noticing suspicious interaction among users. Processing is also permitted if it is necessary to protect the data subject's vital interest or it is in the public's best interest (Art. 6). Vital interest is defined as being interests that are essential for the life of the data subject (Recital 46), i.e. a hospital checking an individual's medical background.

2.3. Consent

Consent is one of the six reasons defined in Article 6 of the GDPR as mentioned in Section 2.2 why permission for processing data is granted. Thus, one possible way to satisfy the GDPR requirements to process data is by getting consent from the data subject before processing their personal data. This can be done by simply having the user check of a tick-box. One of the core requisites is that consent must be a voluntary choice for the user, must be freely given, and shall be just as easy to withdraw at any time after it was granted (Art. 7.3). The request for consent shall be obviously distinguishable from others and presented in an appropriate way using foolproof language (Art. 7.2). The GDPR additionally protects children under the age of 16 by specifying that data collection is only lawful if authorized by a parent (Art. 8).

2.4. Special Cases of Data Processing

Next, the GDPR prohibits all processing of data belonging to special categories which consists i.a. of the race, ethnicity, political interest or religious belief of a natural person (Art. 9.1). Nevertheless, there are cases in which the processing is not prohibited. One example for this is if the data subject has given explicit consent for a specified purpose. This shows that even if the GDPR generally forbids the collection of some data, there are ways around it. The regulation further defines that personal data related to criminal conviction and offences is only to be processed under supervision of official authority (Art. 10).

2.5. Right to Erasure

The GDPR empowers the data subject by giving individuals the right to ask organizations to erase all the personal data that was collected. The right to erasure, also known as the right to be forgotten, forces the controller to delete personal data without "undue delay" if there is a legitimate reason, e.g. the data is no longer needed for the purposes which they were collected for or the user withdraws consent (Art. 17.1). Thus, if a user has the desire to have personal data removed, he can withdraw consent and request an erasure of his data. Also, the controller is obligated to notify the data subject and all other controllers in data processing about the erasure of the personal data if possible with reasonable effort (Art. 19).

2.6. Transparency for Data Subject

Transparency is defined so that any information that is brought to the public or to any person must be easily understandable, accessible, and succinct. The wording must be simple and comprehensible. If necessary, visualization should be used. Transparency is especially important in relation to the collection and processing of personal data of a data subject, as well as the reasoning and the identity of the controller. Especially when the data subject is a child, which means when the information targets children, the information must be communicated clearly and easy to understand. The information regarding privacy must be provided in a written document or electronically (Art. 12).

3. Impact on the Web

The GDPR regulations aim to impact the web in a way that it is more transparent. The following sections discuss different web interactions along with their technical implementations with the goal to determine if the transparency on the web has increased through the GDPR.

3.1. Privacy Policy

Firstly, many companies had to adapt their privacy policies in order to further be compliant with the requirements of the GDPR. Websites that did not have a privacy policy had to create one and if one already existed, they had to renew it based on the regulations. A factor that should not be left disregarded is that having a GDPR compliant privacy note does not necessary mean that it is transparent to a user. The length and difficulty to understand the provided information play an important role in comprehending the content. Sobers [6] measured the average reading time for privacy policies. An overview is presented in Figure 1. It shows the difference of reading time of the privacy policies across different websites from

doi: 10.2313/NET-2020-11-1_01

before the enforcement of the GDPR to afterwards. Eight out of the ten examples actually increased their wordcount of the privacy policy and thus the reading time has also gone up. Only Facebook and Reddit reduced the amount of words that are used in the privacy policy. In average the reading time increased from 17 minutes and 24 seconds to 20 minutes and 3 seconds. This refers to the average absolute reading time that a person needs to read through the entire privacy policy.

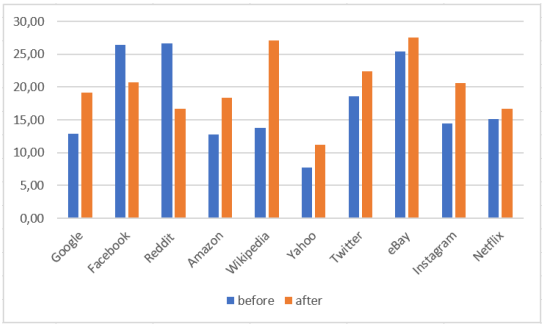

Figure 1: Reading Time in Minutes [6]

Furthermore, Sobers [6] analysed the reading difficulty of privacy policies. The reading level does not show a clear trend. The difficulty to understand the policy increased on five websites, decreased on two pages and remained at the same level on three sites. The platform eBay reached the highest reading level with 18 before the GDPR and 20 afterwards. This is at the reading comprehension level of a senior college student. However, it was not clearly stated which scale the author references for the comparison of the reading level. The goal to decrease privacy concerns and increase transparency was therefore not reached when looking at privacy policies [6].

3.2. Browser Cookies

A cookie is information about a natural person that is generated by a website and stored on the computer by the browser. They can track a user's activity in a browser and remember information such as shopping history. Since the GDPR there has been an increase in the amount of cookie consent banners on websites complying with Article 6.1.a. This provides reasons for data processing to be lawful, one of which is collecting consent from the user. Lawfulness of processing is further discussed in Section 2.3. Companies had to create consent forms in order to be allowed to further collect individuals' data and adjust the way they process data. This mostly applies to consumers from Europe. According to Dabrowski et al. [7] unrestricted use of tenacious cookies has become significantly less for EU web users. Their study collects data sets measuring cookie behavior using Alexa Top 100,000 websites before the adoption of the GDPR in 2016 as well as after introduction in 2018. Measurements show that only 26% of websites, which collect cookies, avoid collecting them without consent from an EU visitor. The GDPR even has an impact on users outside of the EU. When comparing the results from 2016 to the results from 2018 US consumers profit from a reduction of up to 46.7% of the amount of cookies collected. Therefore, the new cookie policies have in theory positively impacted the users' privacy all around the world. On another note, this is also perceivable for consumers since they are obliged to give their consent on most websites that accept the cookies in order to further be able to access the page. Users are found to be disturbed by the frequent occurrence of disclaimers. They also seem to have more privacy concerns because they are now aware that their activities are being monitored and their data is being used. Looking at this from a practical point of view, only very few users are actually willing to click on the banner and read through how the cookies are being used. This as well as the point that was already addressed in regard to the privacy policy does not really add to a higher transparency. If users are not able to understand what is written in the cookies or if they are confronted with a humongous amount of words that they are not willing to read, the people are not really empowered, and the process does not become more transparent [8].

3.3. Third Party Presence

In the business environment there is an interdependency between websites. An interdependency i.e. exists if one website uses the services of another webpage in form of third party presence. An example of a third party presence is Google Analytics. Google Analytics is a service that tracks website activities such as session duration and bounce rate [9]. For a person's privacy this means that another entity has access to their activities and thus it is interesting to determine if the third party presence has decreased since May 2018.

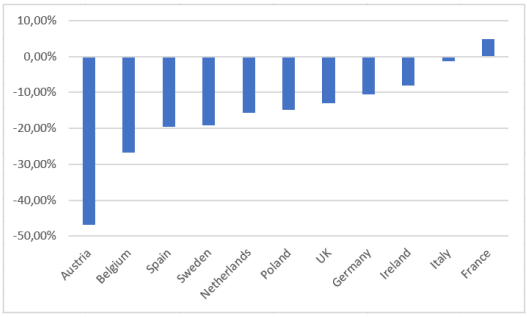

Figure 2: Comparing pre- and post May 25 average numbers of unique third parties for countries, listed as change in percent [10].

Sørensen and Kosta [10] show the percentage difference in the average numbers of unique third parties on websites before and after May 25th, 2018. An overview of the top ten countries with the strongest economies [11] is presented in Figure 2. Austria shows the biggest change with a decline of 46.79%. Whereas in France for example the average number of unique third parties actually grew 4.83%. It shows a decline in most countries and in the total number of third parties, but it must be noted that this is not a in depth inspection of each country. Therefore, it is not possible to conclude a significant impact of the GDPR on third party presence [10].

3.4. Newsletters

If a data subject had subscribed to a newsletter before the GDPR was enforced, the organization must have

collected the data in a lawful way, following the rules presented in Section 2.3 to further send messages. Organizations must be able to prove that they have the user's consent or have another lawful reason for processing data so they can continue sending messages to the data subject. Recital 32 of the GDPR specifies that consent must be "freely given, specific, informative and unambiguous". If this is not the case, their personal data has to be deleted from the mailing list. Companies are forbidden to use personal data for any other reason than specified. Thus, previous to the law a company could for example use the contact information of a user that bought an eBook to send them recurring email campaigns. Now, they must add another checkbox where the user must agree that their information can be used for other marketing actions. If this is not agreed upon, no emails or letters can be sent to them [12].

3.5. Data Exchange

Companies like Google and Facebook provide free usage of their platforms in exchange for user data. They track activities like browsing history, likes, and purchases. There have been numerous scandals in the past concerning data privacy and protection. This data is then purchased by advertisers so that they can better direct their ads. The GDPR regulations influence this business model severely. In general, these companies now have different policies for the countries to which the GDPR applies to and all other countries. For the data collection and processing of Europeans the controller now has to follow the rules that were discussed above such as get consent from the data subject, prove the lawfulness of storing the data, and maintaining the data. A factor that is also influenced by this is the data transfer across borders. If the data is for example transferred to the US, a country which does not ensure sufficient data protection, they have to sign on to the Privacy Shield or assure adequate security in a contract [13].

3.6. Trust

The GDPR has not succeeded in increasing trust in the digital economy. More than 80% of European citizens have the feeling that they do not really have any control over the information they reveal on the internet [14]. This problem possibly arises due to the points that were discussed in relation to the privacy policy and cookies. Even though two thirds of Europeans are aware of the existence of the GDPR, there does not seem to be a strong relationship between the awareness of the data protection regulations and the actual feeling of safety in the web [14]. The reasoning for this might be that the GDPR is quite complicated to understand. However, it should be possible for every natural person affected by the GDPR to be able to understand its contents. Also, the awareness for the regulations should be raised so that more people can feel safer when browsing the internet.

4. Conclusion

The GDPR has definitely had an impact on the web. However, not all changes are positive. In theory, there has been a notable increase in transparency. Europeans now have the possibility to inform themselves about what data is collected and how it is processed. Also, less cookies are being collected. Nevertheless, all the transparency that is now given can lead to an incorrect sense of security because even though a website ensures you of your privacy, it does not necessarily mean that they actually follow this correctly. Also, even though it is now possible to be knowledgeable about one's privacy protection, this does not necessarily lead to more transparency in the web. The length and difficulty to read and understand privacy policies or cookies negatively impacts the transparency. It is furthermore important to create more awareness and understanding of the GDPR for it to be more effective and provide a sense of security to the users. For future research it would be interesting to get a better insight into the effect of third party presence and how the awareness of this can be raised for data subjects by the controller. Another interesting topic is to inspect whether the websites actually follow the data protection regulations that they claim to secure.

References

[1] European Parliament, "Charter of fundamental rights of the european union (2007/c 303/01)," https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012P/TXT&from=EN, 2007, online; accessed 26 March 2020.

[2] E. Parliament, "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)," https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN, 2016, online; accessed 26 March 2020.

[3] "General data protection regulation faq," https://www.into.ie/app/uploads/2019/10/GDPR_FAQ.pdf, 2018, online; accessed 02 May 2020.

[4] C. Tankard, "What the gdpr means for businesses," *Network Security*, vol. 2016, no. 6, pp. 5–8, 2016.

[5] Ben Wolford, "What is gdpr, the eu's new data protection law?" https://gdpr.eu/what-is-gdpr/, online; accessed 28 March 2020.

[6] Rob Sobers, "The average reading level of a privacy policy," https://www.varonis.com/blog/gdpr-privacy-policy/, 2018, online; accessed 28 March 2020.

[7] A. Dabrowski, G. Merzdovnik, J. Ullrich, G. Sendera, and E. Weippl, "Measuring cookies and web privacy in a post-gdpr world," in *Passive and Active Measurement*, D. Choffnes and M. Barcellos, Eds. Cham: Springer International Publishing, 2019, pp. 258–270.

[8] O. Kulyk, A. Hilt, N. Gerber, and M. Volkamer, "This website uses cookies: Users' perceptions and reactions to the cookie disclaimer," https://www.researchgate.net/publication/325923893_This_Website_Uses_Cookies_Users'_Perceptions_and_Reactions_to_the_Cookie_Disclaimer, 2018, online; accessed 02 May 2020.

[9] B. Plaza, "Google analytics for measuring website performance," *Tourism Management*, vol. 32, no. 3, pp. 477–481, 2011.

[10] J. Sørensen and S. Kosta, "Before and after gdpr: The changes in third party presence at public and private european websites," 05 2019.

[11] Bruno Urmersbach, "Bip (bruttoinlandsprodukt) in den mitgliedsstaaten der eu in jeweiligen preisen im jahr 2018," https://de.statista.com/statistik/daten/studie/188776/umfrage/bruttoinlandsprodukt-bip-in-den-eu-laendern/, 2019, online; accessed 29 March 2020.

[12] Kyle McCarthy, "Examining the impact of gdpr one year in," https://www.act-on.com/blog/examining-the-impact-of-gdpr-one-year-in/, 2019, online; accessed 26 March 2020.

[13] K. Houser and W. Voss, "Gdpr: The end of google and facebook or a new paradigm in data privacy?" *SSRN Electronic Journal*, 07 2018.

[14] Eline Chivot and Daniel Castro, "What the evidence shows about the impact of the gdpr after one year," https://www.datainnovation.org/2019/06/what-the-evidence-shows-about-the-impact-of-the-gdpr-after-one-year/, 2019, online; accessed 28 March 2020.

doi: 10.2313/NET-2020-11-1_01