GDPR: The importance of consent and data protection

Nicole Zluky
Holy Family University

Bernice M. Purcell, DBA
Holy Family University

ABSTRACT

The objective of General Data Protection Regulation (GDPR) is to sustain integrity and protection of data in a technologically advanced and face-paced world. The GDPR helps ensure the safety of consumers' data and a simplified outline of a company's actual wants and needs with said information. Companies are subject to penalties and fines if they do not comply with the proper regulations in place. The GDPR brings forth an ample amount of data privacy by assuring companies underly their exact actions with a consumers' information, as well as specify what information is defined as private. Consent to share information should be a law, and now is in the EU. A data user should be able to have full control over what is displayed, shared or used on a greater scale. Implementation of GDPR standards is not difficult and provides benefits to the company. When implementing GDPR education and effective communications, particularly regarding employees with roles directly impacted by the standard, are crucial to success data protection.

Keywords: GDPR, privacy, data protection, data security

INTRODUCTION

"The digital future of Europe (EU) can only be built on trust" (Palmer, 2018). In January 2012, the European Commission began to create plans for a data protection modification across the European Union in order to assure the protection of their citizens' data. The General Data Protection Regulation (GDPR) went into full effect on May 25, 2018 (Palmer, 2018). Even though GDPR went live in the EU, companies across the globe have had to make huge changes in their budgeting and their overall planning to meet the guidelines due to international business dealings with the EU. This became a difficult task for many companies since not much had changed regarding data protection laws since the 1990s. The goal of GDPR is to enhance the rights of individuals and give them more control over their information.

REQUIREMENTS OF GDPR

The GDPR involves two main roles and six principles. The two main roles involved in GDPR are the data controller and the data processor. The data controller is "a person who (either alone or jointly in common with other persons) determines the purposes and the manner in which any personal data are, or are to be, processed" (Wray, 2017). The Data Processor is defined as "any person (other than an employee of the data controller) who processes the data on behalf of the data controller" (Wray, 2017). The data controller is responsible for providing the data subject with a privacy notice, which provides the data subject with a substantial amount of information regarding the contact details of the data protection office, where applicable, the purpose of the processing for which the personal data is intended and for what purpose, who will be receiving the data and if the data controller intends to share personal data with a third party.

The objective of the six principles is to provide the user full control of their data. The six principles of GDPR are as follows: (Reed, 2018, Page 20):

1. Data accuracy
2. Data minimization
3. Integrity and confidentially
4. Lawfulness (Fairness)/Transparency
5. Purpose Limitation
6. Storage Limitation

Matt Burgess (2018), a writer for wired.com, noted "... allowing people to have easier access to the data companies hold about them, a new fines regime and a clear responsibility for organizations to obtain the consent of people they collect information about."

The first principle, data accuracy, notes every step must be taken to erase or rectify data that is inaccurate or incomplete. "Individuals have the right to request that inaccurate or incomplete data be erased or rectified within 30 days" (Irwin, 2018). The GDPR does not define the definition of accuracy; however, inaccuracy is defined as "incorrect or misleading as to any matter of fact. (Information Commissioner's Office)." The GDPR also includes the right for individuals to have inaccurate personal data rectified or completed if it is incomplete.

Data minimalization means companies must limit the personal data collected, stored and used (Irwin, 2018). Data needs to be relevant and necessary for carrying out the purpose for

which the data is initially collected for. Data minimalization should meet the following checklist: adequacy (is enough to properly fulfil your stated purpose), relevancy, (has a rational link to that purpose) and limited to what is necessary (one does not hold more than one needs for that purpose). The GDPR does not define the terms to help a company decide what is adequate, relevant and limited. The data minimalization for a company depends upon that company's purpose for the data and why the purpose is necessary; a company's data should not contain include irrelevant details.

The third principle is integrity and confidentiality, which deals explicitly with security. The GDPR states that personal data must be "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" (Irwin, 2018). The GDPR could not be specific with the way the rule is directed due to a company's policy and technology constantly changing. A company must have a secure system in place to ensure a customer's data always maintains integrity and upholds a high level of confidentiality. A company should also consider policies pertaining to risk analysis, organizational policies and technical measures. Two very popular technical measures are pseudonymization and encryption. Since the chance exists for a technical incident to occur, it is also expected that a company should be able to restore access and availability to all personal data in a timely manner. Conducting frequent testing is also recommended in order to sustain the 'integrity and confidentiality', which is the main goal of the principle.

Lawfulness (fairness)/transparency ensures an organization will make it a point that their data collection policy will not break the law and that no information is out of reach of the data subjects (Irwin, 2018). A company must be clear and candid with their customers from the beginning about their intentions with the customer's personal data. Lawfulness notes the use of the information has been identified regarding processing. Fairness requires that a customer's data is handled in a respectable way which is justified and does not deceive or mislead the person. Transparency denotes being open and honest and providing the customer with confidence in being informed when necessary.

The fifth principle, purpose limitation, requires that an organization collecting data is to ensure the data is used only for its intended purpose. A company can only use the personal data for a new purpose if either this is compatible with their original purpose, or the company is given consent for the new use by their customer. A company's purpose must be specified because it helps the data user understand how a company uses their data and provides them the right to decide whether to share their information and helps build public trust in how a company uses their personal data.

The final principle is storage limitation, which ensures an organization will delete personal information that is no longer relevant to their needs. Due to the abundance of businesses and types, there is no set period as to how long a company should keep a customer's information. Every company has different policy and procedures set in place.

The six principles should be utilized as guidelines for a company's day-to-day business. However, companies have found themselves in legal trouble due to their lack of one or more of the principles listed above. The overriding spirit of the six principles of GDPR is that the customer is always aware of all the steps and processes in which their information is being used.

THE ISSUE INSPIRING GDPR

The issue at hand can be simplified to how much personal information a company has on an individual, what is defined as personal information and what is done with this data. Personal information is considered as more than just information personally linked to that individual. The GDPR's definition is much broader than that; the definition of data includes MAC/IP addresses, tracking cookies, browser histories, location, and anything else that links an activity to an individual. It is easy for a company to have the ability to share this information with a third party or use the data to its own advantage. Data protection is vital on many levels; if data protection is found to be violated the company is subject to intense fines and penalties.

Fines are contingent upon the severity of the violation; such penalties include "fines up to €10,000,000, or 2% of total worldwide turnover, whichever is greater" or "fines of up to €20,000,000 or 4% of total worldwide turnover, whichever is greater" (Back Office Associates, 2018). The €10,000,000 fine (or 2% of total worldwide turnover) could be issued due to the following violations: "the processing of a child's data, processing that does not require identification or failure to the general obligations of controllers or processors" (Back Office Associates, 2018). Penalties leading to a higher fine, such as the €20,000,000 or 4% of total worldwide turnover, are due to: lawful principles for processing, data subject rights and transfers of personal data to a recipient in a third country or international organization" (Back Office Associates, 2018).

Large corporations such as Yahoo and Equifax were subjected to huge fines due to data breaches. Yahoo incurred fines of up to $35 million for having failed to disclose the 2014 data breach in which hackers stole the information of an estimated 500 million users. Though, Equifax was not penalized, it faced lawsuits from 50 states, totaling to 145 million users, for exposing the users' information, which was caused due to a missed patch within a business unit. A consent order was implemented and required Equifax to supply all its "technology assets, their locations and provide a formal process for patching" (Fazzini, 2018).

Having reasonable security is preferred over having many pages of regulations in place; GDPR-Article 29 can be summarized as denying unauthorized users from editing information, to make sure said user is only given access to what they're authorized to have access to and to only use the information towards completing their tasks (Irwin, 2018). It is important to lay out the privacy and security policies in simple terms, and to not mask the policies with large words and phrases; an individual should understand the intended use of his or her information. The overall goal is to ensure the confidentiality, availability, integrity and resilience of the data and to rule out corruption. The implementation of GDPR is meant to ensure this.

The GDPR can have tremendous impact on businesses, as illustratred by the Facebook and Cambridge Analytica Scandal. However, incorporating the GDPR principles is not an overwhelming task. An example of this is the GlaxoSmithKline.

Facebook and Cambridge Analytica Scandal

The Facebook and Cambridge Analytica scandal exemplifies the effects on a business violating GDPR. For Cambridge Analytica, the violation not only caused company fines, but it led to the company's demise. Joe Tuman, a San Francisco State University Communication Studies Professor stated, "The bottom line is, his [Mark Zuckerberg] platform, like many social media platforms, is monetized on the basis of the trading of private information. That is a big

part of the way that they make money. There is an incentive obviously enough in the capitalist system to make as much money as you can" (AP Archive, "US Facebook Analyst", 2018). In regard to the possible relation of the Facebook and Cambridge Analytica Scandal to the United States presidential election, Mark Zuckerburg stated, "We do not sell data to advertizers." Though that may be true, Facebook found a loophole by gathering the information users provided, such as their age, gender and interests to attract a specific target. Facebook then received specific requests from advertisers, to strategically place ads based on a users' input. While Facebook does not directly generate revenue from selling a users' information, they do produce revenue through their strategic ad placement. "The company's (Facebook) advertising revenue jumped 49% to $40 billion in 2017" (Yurieff, 2018). Prior to the recent changes made to Facebook's policies, when a user logged onto a third-party application, such as Spotify or Uber, using their Facebook accounts, the third-party application would then have access to the user's data (account), as well as their friends' data (accounts). However, Facebook has since updated their policies to better educate the user on their intensions (Yurieff, 2018).

According to a former Cambridge Analytica employee, the firm received the data through researcher Aleksandr Kogan, a Russian American who worked at the University of Cambridge; up to 87 million users' data was exposed. Mr. Kogan built a Facebook app that was essentially a quiz; not only did it collect data from users who took the quiz, but it exposed a loophole in Facebook API that allowed it to collect data from the Facebook friends of the user who took the quiz. Companies currently affiliated with Facebook may continue to conduct their business in the same fashion. However, those said companies are still responsible for complying with GDPR, as well as laws that apply to their company directly. (Yurieff, 2018)

GlaxoSmithKline (GSK) incorporates GDPR principles

The GDPR's six principles are not standardized rules; they are guidelines to be followed. An example of a company incorporating the GDPR methods into company policy is GlaxoSmithKline (GSK), a science-led global healthcare company. GlaxoSmithKline maps out the policies in which affect their customers, as well as their employees. GlaxoSmithKline has received approval for their Binding Corporate Rules (BCRs) in the following countries: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania (R&D only), Slovakia, Slovenia, Spain, Sweden, Switzerland and the UK. BCRs are an intra-group agreement between GSK companies, and their Public Policy Statement. Their Public Policy is designed to explain the BCRs and ensure an individual, who's personal information is being accessed, is aware of how it is being used (GSK's Binding Corporate Rules, n.d.).

GlaxoSmithKline has created their own policies using the six principles of GDPR. GSK notes they process their customers' information fairly and lawfully, their privacy policy displays the reason for processing, the legal basis for processing and special category information. GSK noted it only collects and retains a minimal amount of personal information necessary information to purse a specific purpose. It also explains how personal information will be used and their customers' rights. Personal information is not used for anything other than it's intended purposes, and GSK confirmed it uses security safeguards (GSK's Binding Corporate Rules, n.d.).

GlaxoSmithKline has published the following statement regarding its data security measures:

> Safeguarding your privacy: We implement appropriate technical and organizational security measures to prevent accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal information. These measures are appropriate to the risks associated with using personal information and incorporate state of the art technologies.
>
> Incident and breach management: We will notify data protection authorities of personal data breaches, unless those breaches are unlikely to result in a risk to your rights and freedoms. We will notify you of personal data breaches if such breach is likely to result in a high risk to your rights and freedoms, and (at our discretion) in certain other circumstances. We maintain a record of personal data breaches which includes facts about the personal data breach, its effects (if any) and the remedial action taken to resolve the breach. We will make these records available to competent data protection authorities on request.
>
> (GlaxoSmithKline Communications and Government Affairs, "GSK Public Policy Positions", 2018, pp. 3 - 4).

GDPR'S BUSINESS BENEFITS

The GDPR will resolve company problems by enhancing a company's cybersecurity; the regulation pushes the company to rethink and make improvements on their overall cybersecurity strategy. Another benefit to GDPR is improving data management; in order to stay compliant a company should focus on auditing all the data they possess. By auditing the data, it will enable the company to organize and refine data management processes. Auditing the data will also help reduce the unnecessary information not pertaining to the company's use. Auditing will also financially assist a company's cost in storing and processing the data. Former customers' information could strike a red flag, due to it no longer being necessary; an audit would help filter out this kind of data.

By complying with GDPR a company will also enhance their customers' loyalty and even their trust. By displaying a company is following the guidelines of GDPR, they may build a stronger trust and loyalty with their current clients and build a greater number of clients overall. The transparency and responsibility a company demonstrates in their consent to their customers will help build a stronger trust in their brand.

Consent and GDPR

Article 4 of GDPR defines consent as: "'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her" (Irwin, 2018). The requirements of consent are as follows: freely given, specific, informed, and unambiguous and clear affirmative action. (Irwin, 2018). Consent is considered freely given so as long as there is a defining balance between the data user and the data controller. If data controllers withheld or offered a degraded version of their service to the data user, who refused or later withdrew consent from the company to have access to their information, such consent would not be valid.

Specific, informed, and unambiguous is the second type of consent GDPR follows (Irwin, 2018). It prevents data controllers from using unclear and legal terminology which may confuse the data user when accepting the terms of consent. Data Processors can no longer be indirect in their statements. An example of an undesirable statement may read "we may process your personal data…", instead it should be more direct and define it's wants. Clear Affirmative Action is the third type of consent of GDPR. The third type of consent constitutes the user MUST opt-in on their terms, and there is to be no hidden boxes (Irwin. 2018). For example, the data controller must express the use of cookies, and receive consent from the user to agreeing with their terms. GDPR also offers a data user to the right to withdraw their consent at any time.

RECOMMENDATIONS

Businesses have existing laws to support their customers' sensitive information; however, GDPR intertwines with those laws to make the overall regulations more efficient. The following suggestions can assist a company in maintaining compliance with GDPR. Training is a vital element in maintaining compliance with GDPR. A company must be sure to involve relevant information to the company regarding their training. Procedures should also be established in order to demonstrate what the training entailed. The procedures should include the different levels of employment, and the additional amount of training that would be required for management and above. After the training session has been completed a certificate of completion should be presented to all staff members who took part in the exercise. A record should also be retained regarding the company who conducted the training; these records display efforts of establishing GDPR within the company.

Now that training has been addressed, the next step is to appoint an employee, whose sole responsibility is to enforce all the polices set in place; the role is referred to as Data Protection Officer (DPO) or a Data Compliance Manager. Preferably, the employee appointed should have experience concerning legal aspect, as well as compliance. Appointing a DPO displays the company's efforts to maintain GDPR and lowers their risk of fines and penalties. A policy should be generated, containing the responsibilities of the DPO(s); policies will help with any questions presented to the company regarding a DPO's role. Once a DPO has been appointed, a company should follow up with a Data Protection Impact Assessment (DPIA). "A DPIA is an audit of an organization's own processes and procedures that measures how these processes affect or might compromise the privacy of the individuals whose data it stores, collects or processes. The DPIA achieves three things:

1. Ensures compliance with applicable legal, regulatory and policy requirements regarding privacy
2. Determines the risks and effects
3. Evaluates protections and alternative processes to mitigate potential privacy risks" (Grenacher, 2018)

A business should also conduct a data and risk audit, which would require the company to list all the personal data within the company's possession, and attempt to provide answers regarding:

- What the information is being used for?
- What is the company doing with the information?
- Do they contain more information than they need?
- What is the level of sensitivity of the information?

- Where is it stored?

Implementing guides and policies is always essential and would be beneficial to display that the processes are reviewed either quarterly, or as necessary for the company. How information is stored and protected is of extreme importance. If a company's policy states to retain the original hard copy, the company should make sure they possess alarms, locks, and possibly safes. If the information is electronic, the company should make sure packets are updated, firewalls and anti-viruses are installed, strong passwords are implemented, as well as pseudonymization and providing limited access to their customer's data. It is also imperative to securely delete unnecessary data within the company; policies should also be created listing the steps taken to securely delete the unwanted information.

Companies that share their data with a third party should confirm their legal contract notes a level of compliance regarding GDPR. Even though a company maybe GDPR complaint, an outside vender may not yet have adapted to the appropriate regulations, which can result to fines and penalties, due to being associated with the noncompliant company. As stated earlier in the paper, consent must be freely given; it must be very specific. A company must be very precise regarding their intentions of their customer's information. It is important to create guides and policies to better direct the customer. A company's terms and conditions page should not contain extensive legal terminology, and it should not contain pre-checked boxes. A privacy policy should be written in a simple language; it should pertinent information. Such as, the reason for the data, what information the company actually has, the length of time their data will be used for and also, educate the customer in regard to understanding that they have the right to discontinue the use of their information by the company.

The user also has the right to request records of all their available information, delete their information from a company's system or have the information amended due to incorrect information. Due to this, it is crucial to have an action in place for such circumstances. A plan should be put into action to:

1. verify the person requesting the information is in fact who they say they are
2. all the information they are requesting is accounted for
3. make the customer aware it will take a few weeks to gather all the information
4. document all the steps that have been taken.

It is important to document the steps taken for record keeping, as well as, to maintain organization.

Data breaches have made quite the dent in recent times and seem to be more and more common. A company should be prepared for these unfortunate events by making sure their products are protected and compliant. Security is key; it is not just the act of being secure that will help avoid fines and penalties, it is selecting a solution that best suites the company's needs. Antivirus software, network firewalls and encryption are just some of the important elements absolutely necessary to ensure the security of a customer's information. Companies must face facts; they are given access to very sensitive information such names, gender, religious preference, marital status and social security numbers. In the event of a data breach, a company should check to make sure a breach has even taken place; it might be a false alarm. If it were to be a true data breach, the next step is to identify what part of the information caused the data breach. A data breach must be communicated to its users within 72 hours. And as always make sure to document the data breach, where the problem occurred, when the communication was sent out to the data users and how it was/will be

resolved. A good way to stay on top of such heinous acts could be to run Data Breach Notifications; the notifications will display real-time activity and conduct an analysis of the situation.

CONCLUSION

Though GDPR is new from a legal standpoint, previous regulations have already made an impact on companies around the world. Data users are becoming more and more suspicious regarding what their information is being used for; however, GDPR can provide the user with a sense of ease by having control over their personal information again. The GDPR is a progressive and proactive move within the virtual world, and though it may seem to be a burden on companies, will strengthen the relationship and trust with their data users.

REFERENCES

Anon. (n.d.). Lecture presented at US Facebook Analyst in CA, San Francisco. Retrieved from http://www.aparchive.com/metadata/youtube/46a4be61a93ff1686c242699ffe56b17

Anon. Consent. (n.d.). Retrieved from https://www.gdpreu.org/the-regulation/key-concepts/consent/

Back Office Associates, 2018 *GDPR Webinar- The GDPR is here and I'm not ready! What do I do?*

Burgess, M. (2018, October 4). What is GDPR? The summary guide to GDPR compliance in the UK. Wired.com. Retrieved from https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018

Fazzini, K. (2018, June 27). Equifax gets new to-do list, but no fines or penalties. Retrieved from https://www.cnbc.com/2018/06/27/equifax-breach-consent-order-issued.html

Fimin, M. (2018, March 29). Five Benefits GDPR Compliance Will Bring To Your Business. Retrieved from https://www.forbes.com/sites/forbestechcouncil/2018/03/29/five-benefits-gdpr-compliance-will-bring-to-your-business/#c91792d482f9

GlaxoSmithKline Communications and Government Affairs. (2018, June). GSK Public Policy Positions. Retrieved from https://www.gsk.com/media/2934/binding-corporate-rules-policy.pdf

Grenacher, M. (2018, June 04). GDPR, The Checklist For Compliance. Retrieved from https://www.forbes.com/sites/forbestechcouncil/2018/06/04/gdpr-the-checklist-for-compliance/#5984cfdf5bec

GSK's Binding Corporate Rules. (n.d.). Retrieved from https://www.gsk.com/en-gb/about-us/policies-codes-and-standards/binding-corporate-rules/#_edn2

Irwin, L. (2018, January 31). The GDPR: Understanding the 6 Data protection principles. Retrieved from https://www.itgovernance.eu/blog/en/the-gdpr-understanding-the-6-data-protection-principles

Palmer, D. (2018, May 25). What is GDPR? Everything you need to know about the new general data protection regulations. Retrieved from https://www.zdnet.com/article/gdpr-an-executive-guide-to-what-you-need-to-know/

Popera, A. (2018, February 08). Pharmaceutical Company to pay $4.75 Million in TCPA Settlement. Retrieved from https://gryphoncompliance.com/pharmaceutical-company-to-pay-4-75-million-in-tcpa-settlement

Principle (d): Accuracy. (n.d.). Retrieved from https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/principles/accuracy/

Reed, S. (2018). *GDPR - Know Your Rights*. Middletown, DE.

Wray, D. (2017). *The little book of GDPR*. United States: Darren Wray.

Yurieff, K. (2018, April 11). Your Facebook data scandal questions answered. Retrieved from https://money.cnn.com/2018/04/11/technology/facebook-questions-data-privacy/index.html