The General Data Protection Regulation: Technical Implications of Compliance

Jaclyn Tsiang
COMP 116: Computer Security
May 7, 2018

Abstract

With massive data breaches occurring at an alarmingly frequent rate, the European Union is passing a set of new rules setting security standards for customer data collection. GDPR, or the General Data Protection Regulation, holds companies responsible for protecting personal data. GDPR widens the definition of personal data to include anything that can be mapped to an individual, including data like IP addresses and encrypted data. It places responsibility on both the controllers of the data, and those who process it. If a company is found to have mishandled data or left it vulnerable to a breach, it can be liable to serious fines. Additionally, GDPR requires companies to report security breaches and notify potential victims within a certain timeframe. These new regulations mean that many companies will have to scramble to build up their security measures and ensure that they comply with the GDPR requirements before the May 25, 2018 deadline. In this paper, I will explore the technical implications of various GDPR requirements.

Introduction

As breaches of sensitive data become more and more common globally, GDPR is the most extensive regulation on data protection to be passed in history. GDPR is part of a continuum of EU legislation focused on protecting personal data and privacy. It's predecessor is the EU's 1995 Data Protection Directive (DPD), which set initial standards for the processing of EU residents' personal data by companies [8]. While providing important baseline privacy and protection benchmarks, the effectiveness of DPD was hindered by privacy laws that differed between EU member states and thus limited DPD's implementation and enforcement [8]. Additionally, DPD is a directive, thus it is only enforceable once an EU Member State welcomes it into its national law. GDPR, on the other hand, is a regulation and therefore is immediately enforceable across the entire EU. Building off DPD, GDPR was created by the European Commission to be a more comprehensive, collaborative data protection framework that could be equally enforced within all EU Member States. GDPR officially goes into effect on May 25, 2018, at which time it can be officially enforced and organizations that do not meet compliance standards can begin to be penalized.

To the community:

While many companies, especially those outside of the EU, may not think too hard about the new GDPR, the regulation should not be brushed aside so easily as its scope is actually quite large. GDPR affects any company that deals with data from EU residents, whether that company is based in the EU or not. Even if the company does not have an office in the EU, if it collects information from a user from the EU, GDPR will apply. In addition, it is particularly important to note what information GDPR protects. GDPR greatly broadens the definitions of what constitutes as personal data to mean any data that can be mapped to an individual user. This means that companies must keep track of all personal data and who it belongs to, which many companies did not previously keep track of [12]. It is crucial for companies that fall under GDPR to understand the extensive technical implications of the regulation and make changes where needed in order to meet GDPR compliance and avoid harsh penalties.

What GDPR Compliance Means:

Due to the way in which many companies have built their system architectures inline with the traditionally corporate view of personal data, many will have to implement changes in order to comply with GDPR. One of the most important components of GDPR is its redefinition of personal data and who owns it. Under GDPR, personal data refers to any information that relates to an "identifiable natural person." The new definition encompasses information that was not

previously considered personal data, like online identifiers such as IP addresses and mobile device IDs, as well as personal data that has been encrypted [7]. Additionally, GDPR strictly places ownership of personal data collected by a company within the hands of that individual and relegates the company's role to that of a custodian to the data. GDPR ensures EU consumers' ownership over their data by granting them full rights to access, port, rectify or erase their data at any time [11]. Therefore, in order for to meet GDPR compliance, companies are required to have extensive mapping and inventorying architecture in place to keep track of the context and content of their personal data. GDPR also requires One other major component of GDPR is its establishment of mandatory breach reporting, which requires companies to notify data protection authorities of a breach within 72 hours [13]. There is a strong incentive for companies to comply with GDPR as the penalties for non-compliance are incredibly steep. For a less serious data breach, the penalty is a fine up to 10 million euros or 2% of the company's global annual turnover, whichever is greater [12]. A serious breach will result in a fine of up to 20 million euros or 4% of the company's global annual turnover [12]. The goal of these fines are to make compliance economically sensible to companies. Achieving compliance with GDPR means that many companies will have to make major changes to the way they handle their user's data and place greater emphasis on securing their systems.

Effect on system architectures

In order to achieve GDPR compliance, many companies will have to implement major alterations to their system architectures. One of the rights GDPR guarantees to EU residents in regards to their data is the right to erasure, or the right to be forgotten. This determines that if a resident asks to have their data erased, withdraws their consent, or if their data is no longer necessary to serve its original purpose, then the company is obligated to erase that data "without undue delay" (*GDPR, Article 17*). As data is often kept across many different storage systems and is often not adequately tracked as it moves to different locations, companies must reconstruct their current system architectures very intentionally in order to ensure users' right to be forgotten.

There are several things to consider when architecting a solution that will allow a company to thoroughly delete data in a timely fashion. It is essential to understand 1) what personal data exists 2) where it is located 3) where the data is managed and processed within the organization 4) who can access it 5) timestamps of the data 6) if other data retention regulations apply. This can be particularly challenging due to the ease at which data proliferates within a company, meaning that data can end scattered in several separate systems. GDPR also requires an erasure system to be auditable to prove that once a query has been performed for the erasure of data, that data was identified and subsequently deleted. Organizations with centralized data management services will have the easiest time meeting compliance standards, as the complexity of erasing all

of a person's data will be greatly reduced. This approach, however, is more difficult to implement. Other organizations with more distributed data should consider building individual services on top of distributed data stores that enable erasure and auditing functions across locations. Architecting a GDPR-compliant data erasure solution must be done thoughtfully in order to ensure that no data is overlooked [10].

Another potential effect of GDPR on system architecture applies to organizations that use automated decision making processes. Designed to protect individuals' rights and combat problems of discrimination within biased algorithms, GDPR prohibits any "decision based solely on automated processing, including profiling" which "significantly affects" the data subject (GDPR, *Article 22*). Profiling is defined by GDPR as "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person" (GDPR, *Article 4*). GDPR demands for humans have the ability to intervene in algorithmic decision making and for data subjects to be able "to express their point of view and contest the decision" [6]. This holds data processors accountable for the decisions their algorithms make and places responsibility on organizations to ensure that their algorithms are transparent and fair. Organizations will need to reevaluate their current algorithmic design and potentially make alterations in order to comply to these demands.

Organizations processing data that may put individuals' rights and freedoms at high risk are also obligated by GDPR to perform data protection impact assessments (DPIA). GDPR requires a DPIA if an organization plans to "use systematic and extensive profiling with significant effects," "process special category or criminal offense data on a large scale" or "systematically monitor publicly accessible places on a large scale" [3]. A DPIA must describe the data processing being performed and its purpose, discuss necessity and proportionality, assess risk to individuals, and detail safeguards, security measures and mechanisms in place to mitigate those risks [3]. Additionally, certain organizations with more substantial data processing may be required to appoint a data protection officer to help monitor internal compliance, provide advice on data protection, and be a contact point for data subjects and supervisory authority. Appointing a data protection officer is mandatory under GDPR for organizations that are public authorities, have core activities that require heavy and systematic monitoring of individuals, or have core activities that consist of processing certain categories of data or data relating to criminal offenses [13].

Impact on US companies

While GDPR compliance is an EU-wide regulation, any organization that handles data of EU residents must comply as well. In the US, this is particularly significant as there is no single, comprehensive national law that regulates the collection and use of personal data. While there

have been several regulations that have been passed to protect specific types of personal data, like the Payment Card Industry Data Security Standard, which increased control over cardholder data, and the Health Insurance Portability and Accountability Act of 1996, which increased protection of medical information, most US companies have not had to deal any regulation as broad as GDPR [1]. US companies that interact with data from EU residents should proceed with caution when seeking with compliance with GDPR. Some might look at data classified as "Personally Identifiable Information" (PII) to assess compliance, however, this US privacy term does not align with GDPR's definition of personal data. Whereas PII clearly defines what constitutes as personal information including in the definition Social Security numbers, driver's license numbers and financial accounts, GDPR makes its definition of personal data purposefully broad [4]. Therefore it is not sufficient to assess compliance solely based off of PII. Additionally, US companies may be taken by surprise by the extent to which GDPR emphasizes users' rights to the processing of their data as they may be used to the American regulations that usually favor business over the consumer.

Conclusion

As the single most comprehensive regulation on data protection in history, the impact of GDPR will be felt by companies and consumers worldwide. Complying with GDPR is an ongoing process and organizations must continue to reevaluate their data processing activities. Companies outside of the EU are not automatically exempt and must ensure that take care to check whether they are subjected to the regulation or not. Additionally, companies in countries with business-centered privacy laws like the US should be extra cautious when interpreting GDPR compliance as GDPR's definition of personal data does not leave much unprotected.

References

[1] “A Comprehensive Guide to the General Data Protection Regulation (GDPR).” *MarTech Today*, martechtoday.com/guide/gdpr-the-general-data-protection-regulation.

[2] “Data Protection Impact Assessments.” *ICO*, ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/.

[3] “Data Protection Officers.” *ICO*, ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-officers/.

[4] Dehaye, Paul-Olivier. “Personally Identifiable Information and GDPR Compliance.” *Medium*, Augmenting Humanity, 30 Sept. 2016, medium.com/personaldata-io/personally-identifiable-information-and-gdpr-compliance-5bb39dc886c0.

[5] Gjermundrød, Harald, et al. “PrivacyTracker: A Privacy-by-Design GDPR-Compliant Framework with Verifiable Data Traceability Controls.” *SpringerLink*, Springer, Dordrecht, 6 June 2016, link.springer.com/chapter/10.1007%2F978-3-319-46963-8_1.

[6] Goodman, Bryce, and Seth Flaxman. *European Union Regulations on Algorithmic Decision-Making and a “Right to Explanation.” European Union Regulations on Algorithmic Decision-Making and a “Right to Explanation,”* arxiv.org/pdf/1606.08813.pdf.

[7] Irwin, Luke. “GDPR: How the Definition of Personal Data Will Change.” *IT Governance Blog*, 19 June 2017, www.itgovernance.co.uk/blog/gdpr-how-the-definition-of-personal-data-will-change/ .

[8] Lord, Nate. “What Is the Data Protection Directive? The Predecessor to the GDPR.” *Digital Guardian*, 24 Apr. 2017, digitalguardian.com/blog/what-data-protection-directive-predecessor-gdpr.

[9] Narayanan, Arvind, and Vitaly Shmatikov. “Myths and Fallacies of ‘Personally Identifiable Information.’” *Communications of the ACM*, vol. 53, no. 6, 2010, p. 24., doi:10.1145/1743546.1743558.

[10] Reber, Jill. “Architecting for GDPR: The Right to Be Forgotten.” *Primitive Logic*, Nov. 2017, www.primitivelogic.com/insights/architecting-for-gdpr-the-right-to-be-forgotten/.

[11] Sirota, Dimitri, and IDG Contributor Network. “GDPR – What Security Pros Need to Know about the New Era of Privacy Regulations.” *CSO Online*, InfoWorld, 2 Aug. 2017, www.csoonline.com/article/3212924/privacy/gdpr-tldr-what-security-pros-need-to-know-about-the-new-era-of-privacy-regulations.html.

[12] Team, ITGP Privacy. *EU General Data Protection Regulation (GDPR): An Implementation and Compliance Guide - Second Edition*. IT Governance Ltd., 2017.

[13] “What the GDPR Means for Businesses.” *Science Direct*, Elsevier, 29 June 2016, www.sciencedirect.com/science/article/pii/S1353485816300563.