Colin Monroe

GDPR Case Study

Introduction

On May 25th, 2018 the General Data Protection Regulation (GDPR) will come into effect for all natural EU people. Unlike the previous data privacy legislation this is a regulation not a directive. This means that it is binding legislation that all businesses must adhere to.The main goal of the GDPR is to tighten data privacy laws and give more power back to the people. There are many provisions but the main ones are: the right to be forgotten, right to access and stronger consent requirements. The GDPR will be enforced by higher fines with the maximum being 20 million Euros or 4% of gross annual revenue whichever is higher (Matt Burgess, 2017). The right to be forgotten is that a company must erase all personal data if the person withdraws consent or the data is no longer relevant. The right to access is that a person may request from a company whether or not their data is being used and if so how. Consent is now required for any company to use personal data and must be presented in a clear fashion (Matt Burgess, 2017). While businesses have been given two years to comply with the GDPR there are still many questions about term definitions in the articles. This paper will use Article 17, “right to erasure”, as an example of how there are many poorly defined terms in the GDPR (Fillaronga, Kiesberg, Li, 2017). This has left many companies in the EU and US uncertain in how to proceed.

Literature Review:

Defined in the GDPR article 4 a data controller is “natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data;”. A data processor is a “natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller”.

Article 17 “Right to erasure” (‘right to be forgotten’)” of the GDPR states:

“The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

(a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;

(c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);

(d) the personal data have been unlawfully processed;

(e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;

(f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).”

Basically if a person no longer consents, the purpose that the data collected for is no longer relevant, or if directed by the law an organization must fully erase all of that person's data from all of their data repositories.

If you are US company that deals with EU citizens then you will need to comply with the GDPR. The impact of “the right to erasure” on US companies will be significant. All companies will now have to keep track of where a certain individual's personal information is being kept in all or their data storage. Every time that there is new data acquired about that person they will need to be able to link that with their old data to keep track of it. They will also have to be able to search that person out on backups and be able to delete that information (David Froud, 2017).

All major US companies that deal with data processing and collection will now have to hire a Data Protection officer under the GDPR (Matt Burgess, 2017). The DPO officer will be responsible for monitoring and auditing the company making sure that they are complying with the GDPR rules (Matt Burgess, 2017).

Findings

Many experts are concerned that the articles have poorly defined terms which leaves too much to interpretation. For example the word “erasure” is never defined

throughout the text of the article (Fillaronga, Kiesberg, Li, 2017). There could be many different ways to interpret this and already the discussion over what is the correct way to interpret “erasure” has begun. There is important when considering what technique a company must use to delete this data. If they do not at least use the seven pass DoD technique than that data still exists on the hard drive. So if this information is revealed at a later date has the organisation fulfilled their duty? Probably not but there will be a need to wait for precedents to be established at this point in time. Which means that this article is being substandard in its protection of data privacy.

There is concern over when organisations should be held to the provision that erasure must occur when data is no longer relevant. One could see companies forever holding onto this data claiming that it is part of further research. While it would be the DPO officer's responsibility to determine if something should no longer relevant. Under what guidelines and parameters can they deem that something is not relevant to some kind of research the company is doing.

There is also no plan laid out for the protection of personal data from the misuse of article 17. With the ability to obtain someone's credentials to prove their identity being fairly easy. Whether it be malicious actors or teenagers doing it for fun the ability to file false claims under this act is very possible (Daphne Keller, 2016). The likelihood that companies will sift through all of these claims to make sure that all are legitimate is unlikely (Daphne Keller, 2016). This is due to the fact that non compliance will cost them a lot more money than if they process a false claim. This could lead to a type of denial

of service attack. A malicious actor could file enough false claims with various companies and have all of your business and personal information deleted from the internet.

Recommendations

The best way for US companies to prepare for the GDPR is to make sure that it is integrated throughout your business and not considered a problem for IT. From the example of Article 17 we could see how poorly defined the terms were. So for the GDPR until there is some precedent set the recommendation would be to make sure to do the most thorough straightforward action. Do not try and skirt the system and try to convince people that encryption will equal erasure. Use the proper techniques and erase things so that they are not forensically recoverable. Make sure that you keep track of all information and no where each individual's information is stored. Do not try and create a dubious long lasting “research” program to keep individuals data. It is very hard to filter out and find false claims. Businesses should probably investigate further if there is an unusual request like for a longstanding business to be deleted.

Conclusion

The GDPR makes great strides in creating personal data privacy. However, some poor definitions within the articles have left many wondering how to proceed. As we saw in just Article 17 the main terms are open to interpretation. The lack of technical standard to go along with the terms leaves the possibility of substandard privacy

protection. There is also no motivation for companies to make sure that this article is not misused by others to delete data that is not their own. To protect themselves US companies should use the strictest standards when dealing with the GDPR.

Bibliography

Burgess, M. (November 7, 2017). GDPR will change data protection- here's what you need to know. Retrieved on 11/29/17 from http://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018

EU Parliament (April 14, 2016). GDPR Key Changes. Retrieved on 11/25/17 from https://www.eugdpr.org/key-changes.html

Fillaronga, E. Kiesberg, P. Li, T. (August 15, 2017) Humans Forget, Machines Remember: Artificial Intelligence and the Right to Be Forgotten. Retrieved on 11/28/17 from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3018186

Froud, D. (June 2, 2017). GDPR: Does the Right to Erasure Include Backups? Retrieved on 11/27/17 from http://www.davidfroud.com/does-right-to-erasure-include-backups/

Keller, D. (January 27, 2016). The new, worse 'right to be forgotten'. Retrieved on 11/28/17 from https://www.politico.eu/article/right-to-be-forgotten-google-defense-data-protection-privacy/

Official Journal of the European Union. (April 5, 2016). EU General Data Protection Regulation (EU-GDPR) Table of Contents. Retrieved on 11/27/17 from https://www.privacy-regulation.eu/en/index.htm