Justin Graham

09/17/2023

CYSE425

Policy Analysis Paper 1

Data retention policies are an important part of any company’s cybersecurity program. Data retention is how an organization stores and deletes their data. The time frame in which a company keeps specific types of data can vary depending on their policy and what kind of information they need to keep for longer periods of time. The basics of a data retention policy are to define the data by specifying what type of information needs to be collected and for what purpose. This can include employee records, billing information, contracts, or other electronic documents. Then the company needs to decide how they will store this data securely by using backups and sometimes encryption if necessary. Finally, they need a procedure to make sure that the data is correctly destroyed in the appropriate time frame to align with their policy. For this paper, I will focus on the General Data Protection Regulation (GDPR). Their policy towards data retention is that “organizations can only hold data when it is necessary. Its removal should occur when the intended function of the data is complete” (Lansford).

I chose this policy because I am very fond of the steps that the European Union took regarding its citizens privacy when it comes to online data. They took a stand against large corporations that would store and sell individual consumer data to third parties to make more money. Their new, more strict laws prevent companies and organizations from abusing their power of large computers and network abilities and protects individuals who have personal information on the internet.

The General Data Protection Regulation was brought into development by the European Union’s Parliament back in early 2014 when the European Parliament voted in favor of having a new regulation to replace their previous standard Article 29. It was finally passed and implemented in all the member states by the 25th of May 2018. The policy applies to any “organization that collects any personal data of any European Union member state citizen” (Castagna). Article 17 of the GDPR states that controller, the person who owns the data, has the right to have their data erased if it falls within one of their seven guidelines.

This policy affects all the countries within the European Union as well as any countries that do business with consumers in those countries. It is the first major policy that puts the accountability on the organizations to follow through with their data retention and deletion policy or receive heavy fines. Since it is not just limited to organizations that exist with the European Union member states, it poses a threat to many American companies that conduct business in those regions. It is the first step in preventing companies around the world form continuing to abuse consumer’s privacy and data.

Sources:

“Art. 17 GDPR – Right to Erasure ('right to Be Forgotten’).” *General Data Protection Regulation (GDPR)*, 12 June 2017, gdpr-info.eu/art-17-gdpr/.

Castagna, Rich, and Treacutea Lavery. “What Is GDPR? An Overview of GDPR Compliance and Conditions.” *WhatIs.Com*, TechTarget, 29 Jan. 2021, www.techtarget.com/whatis/definition/General-Data-Protection-Regulation-GDPR#:~:text=The%20General%20Data%20Protection%20Regulation,effect%20on%20May%2025%2C%202018.

Roberts, L. (2021). How to Create a Data Retention Policy | CIO Insight [Article]. *CIO Insight*, N.PAG-N.PAG.

Stylios, G. (2010). NEW EUROPEAN UNION POLICY ON DATA PROTECTION -- ACHIEVEMENTS AND PROBLEMS [Article]. *Proceedings of the International Conference on Information Technologies*, 113-126.