**Weekly Assignment 5**

We will now take a look at real regulations in GDPR.

Read more about GDPR first here:

<https://en.wikipedia.org/wiki/General_Data_Protection_Regulation>

You can view the actual regulations here (you don’t have to read this entire thing):

<https://gdpr.eu/tag/gdpr/>

Using the regulations above answer the following questions:

1. Does a US company need to follow GDPR regulations? If so, why? If not, why not?

Yes, a US company may need to follow GDPR regulations if it meets certain criteria. The General Data Protection Regulation (GDPR) applies to organizations outside the EU if they:

- Offer goods or services to individuals in the EU\*\*: This includes selling products or services, even if the company is not physically located in the EU.

- Monitor the behavior of individuals in the EU\*\*: This includes activities such as tracking and profiling individuals based on their online behavior within the EU.

The reason for this extraterritorial application is to protect the personal data and privacy of EU citizens regardless of where the data processing occurs.

2. What rights does an EU citizen have in GDPR on their data?

Under GDPR, EU citizens have several key rights regarding their personal data:

- Right to be informed: Individuals have the right to be informed about the collection and use of their personal data.

- Right of access: Individuals can request access to their personal data and obtain information about how it is being processed.

- Right to rectification: Individuals can request correction of inaccurate or incomplete personal data.

- Right to erasure (Right to be forgotten): Individuals can request the deletion of their personal data under certain conditions.

- Right to restrict processing: Individuals can request the restriction or suppression of their personal data under certain conditions.

- Right to data portability: Individuals can request to receive their personal data in a structured, commonly used, and machine-readable format, and they can transfer that data to another controller.

- Right to object: Individuals can object to the processing of their personal data for direct marketing, scientific or historical research, or statistical purposes.

- Rights related to automated decision-making and profiling: Individuals have the right to not be subject to a decision based solely on automated processing, including profiling, which produces legal or similarly significant effects on them.

3. In GDPR, what is a controller and a processor? What is the difference between a processor and processing?

- Controller: A controller is an entity (individual, organization, public authority, agency, or other body) that determines the purposes and means of the processing of personal data. The controller is responsible for ensuring compliance with GDPR requirements and for protecting the rights of data subjects.

- Processor: A processor is an entity that processes personal data on behalf of the controller. The processor acts on the instructions of the controller and does not have control over the purposes and means of the processing.

- Difference between a processor and processing:

- A processor is the entity performing the data processing activities on behalf of the controller.

- Processing refers to any operation or set of operations performed on personal data, whether automated or not, including collection, recording, organization, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure, dissemination, alignment, combination, restriction, erasure, or destruction of personal data.

4. What is Article 82 section 4 talking about?

Article 82 of the GDPR addresses the right to compensation and liability for damages caused by infringement of the regulation. Section 4 of this article states:

Where more than one controller or processor, or both a controller and a processor, are involved in the same processing and where they are, under paragraphs 2 and 3, responsible for any damage caused by processing, each controller or processor shall be held liable for the entire damage in order to ensure effective compensation of the data subject.”

This means that if multiple parties (controllers and/or processors) are involved in data processing that results in damage, each party can be held fully liable for the entire damage to ensure that the affected data subject receives full compensation. This is known as "joint and several liability. After compensating the data subject, the liable parties can seek to recover portions of the compensation from other responsible parties according to their respective degrees of responsibility.

When you are finished upload this document into Canvas for your submission.