Paul Romer

CSD370

Module 2.2 Assignment

January 19, 2025

GDPR

The Mesusa Corporation (MeCo), which currently is based in Friday Harbor, WA, is in the process of expanding to include locations in Brazil and the UK. Paula Deers, who is the Compliance Officer, needs more information on GDPR and what needs to be done on her end to become compliant with GDPR principles. She would like you to provide her with a basic description of GDPR, how it came about, and a checklist to follow to achieve compliance.

Paula Deers,

GDPR or the General Data Protection Regulation is the updated privacy law for the European Union. It went into effect in May 2018. GDPR aims to ensure that data is collected and stored in a responsible manner. “The data that's collected must be for a specific and legitimate purpose and shouldn't be used in any way beyond that intention (TechTarget).” It’s known as the toughest security and privacy law in the world and is responsible for the ‘allow cookies’ banners on many websites.

GDPR applies to any website that has users from the European Union, regardless of where the business is located. It aims to ensure that visitors have a clear understanding that their data is collected, that they consent to have their data collected, that their data is stored securely, and that customers are notified in a timely manner if their data is breached. Companies that don’t follow these regulations could be subject to large fines.

Below is a checklist of some of the key requirements to be GDPR compliant.

1. **Assess Data Collection Practices**
   1. **Inventory Personal Data**: Identify and document all personal data your organization collects, processes, and stores. Understand its origin, purpose, and the legal basis for its processing.
   2. **Data Minimization**: Collect only the data necessary for your specified purposes. Avoid gathering excessive or irrelevant information.
   3. **Obtain Consent**: Obtain consent for data to be stored and processed.
   4. **Data Removal**: Implement mechanisms for individuals to withdraw consent easily.
2. **Enhance Data Security Measures**
   1. **Implement Technical Safeguards**: Use encryption, pseudonymization, and access controls to protect personal data. Regularly update security protocols to address emerging threats.
   2. **Conduct Regular Security Audits**: Periodically assess your systems for vulnerabilities and ensure compliance with security policies.
3. **Privacy Policies and Notices**
   1. **Transparent Communication**: Clearly inform individuals about how their data is collected, used, stored, and shared. Ensure privacy notices are easily accessible and written in plain language.
4. **Manage Data Breaches Effectively**
   1. **Establish Breach Detection and Response Protocols**: Develop procedures to identify, assess, and respond to data breaches promptly.
   2. **Notification Obligations**: Notify relevant supervisory authorities of a breach and inform affected individuals.

References:

* <https://www.techtarget.com/whatis/definition/General-Data-Protection-Regulation-GDPR>
* <https://www.investopedia.com/terms/g/general-data-protection-regulation-gdpr.asp>
* <https://www.wired.com/story/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018/>
* <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1552662547490&uri=CELEX%3A32016R0679>
* <https://en.wikipedia.org/wiki/General_Data_Protection_Regulation>