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 are 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.
2. **Establish Legal Grounds for Processing**
   1. **Determine Lawful Basis**: Ensure that all data processing activities have a valid legal basis, such as consent, contractual necessity, legal obligation, vital interests, public task, or legitimate interests.
   2. **Obtain Explicit Consent**: Where consent is required, ensure it is freely given, specific, informed, and unambiguous. Implement mechanisms for individuals to withdraw consent easily.
3. **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.
4. **Update 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.
   2. **Include Mandatory Information**: Specify the data controller's identity, data processing purposes, legal bases, data retention periods, and individuals' rights.
5. **Facilitate Data Subject Rights**
   1. **Right of Access**: Enable individuals to access their personal data upon request.
   2. **Right to Rectification and Erasure**: Allow individuals to correct inaccurate data and delete data when appropriate.
   3. **Data Portability**: Provide personal data in a structured, commonly used, and machine-readable format upon request.
   4. **Right to Object and Restrict Processing**: Respect individuals' rights to object to or restrict certain data processing activities.
6. **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 within 72 hours of a breach and inform affected individuals when there's a high risk to their rights and freedoms.
7. **Appoint a Data Protection Officer (DPO)**
   1. **DPO Designation**: Appoint a DPO if your organization processes large-scale sensitive data or engages in regular and systematic monitoring of individuals. The DPO will oversee compliance and act as a liaison with supervisory authorities.
8. **Conduct Data Protection Impact Assessments (DPIAs)**
   1. **Evaluate High-Risk Processing**: For processing activities likely to result in high risks to individuals' rights, perform DPIAs to identify and mitigate potential impacts.
9. **Ensure Third-Party Compliance**
   1. **Review Data Processor Agreements**: Ensure contracts with third-party processors mandate GDPR compliance and outline responsibilities for data protection.
   2. **Monitor Third-Party Practices**: Regularly assess third-party compliance with data protection standards.
10. **Implement Privacy by Design and Default**
    1. **Integrate Data Protection into Operations**: Embed data protection principles into all processing activities and business practices from the outset.
    2. **Default Privacy Settings**: Configure systems to ensure that, by default, only necessary personal data is processed.

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>