**GDPR Compliance for Mesusa Corporation (MeCo)**

Liz Hinz

CSD370-A339: Secure Software Development

Professor Nathan Braun

March 30, 2025

**GDPR Compliance for Mesusa Corporation (MeCo)**

Security and data protection are desired and prioritized by a significant amount of users. When expanding business outside of the United States and into locations such as Brazil and the UK, regulations set in these areas must be considered when conducting business. Based on past experiences, the EU set legal guidelines to secure users' information. GDPR, also known as the General Data Protection Regulation, is a vital piece of regulation. It protects people's information in the EU through set requirements. By understanding the different aspects of GDPR and its origins, a strong foundation is crafted for these new branches.

All EU data must comply with the General Data Protection Regulation. After security breaches of sensitive information invoked by Snowden and the invalidation of the Safe Harbor provisions due to lesser protections, GDPR ensures that data is shared safely between online trades of differing countries (Conklin & Shoemaker, 2022, p. 221).

Above all else, the General Data Protection Regulation focuses on data protection and privacy (Conklin & Shoemaker, 2022, p. 221-226). One of the requirements of GDPR is an appointed data protection officer (Conklin & Shoemaker, 2022, p. 222). Overall, individuals are given the “Right to Information, Right to Access, Right to Rectification, Right to Restrict Processing, Right to Object, Right to Erasure, and Right to Data Portability” (Conklin & Shoemaker, 2022, p. 224). Further, safeguards such as binding corporate rules, module contract clauses, and legally binding documents” must all be considered to maintain the proper protections for international data transfer (Conklin & Shoemaker, 2022, p. 224).

Enclosed is a checklist for GDPR practices from GDPR (2019) website that helps to ensure all software is compliant:

“Lawful Basis & Transparency

* Conduct an information audit to determine what information you process and who has access to it.
* Have a legal justification for your data processing activities.
* Provide clear information about your data processing and legal justification in your privacy policy.

Data Security

* Take data protection into account at all times, from the moment you begin developing a product to each time you process data.
* Encrypt, pseudonymize, or anonymize personal data wherever possible.
* Create an internal security policy for your team members, and build awareness about data protection.
* Knows when to conduct a data protection impact assessment, and have a process in place to carry it out.
* Have a process in place to notify the authorities and your data subjects in the event of a data breach.

Accountability & Governance

* Designate someone responsible for ensuring GDPR compliance across your organization.
* Sign a data processing agreement between your organization and any third parties that process personal data on your behalf.
* If your organization is outside the EU, appoint a representative within one of the EU member states.
* Appoint a Data Protection Officer (if necessary)

Privacy Rights

* It’s easy for your customers to request and receive all the information you have about them.
* It’s easy for your customers to correct or update inaccurate or incomplete information.
* It’s easy for your customers to request to have their personal data deleted.
* It’s easy for your customers to ask you to stop processing their data
* It’s easy for your customers to receive a copy of their personal data in a format that can be easily transferred to another company.
* It’s easy for your customers to object to you processing their data.
* If you make decisions about people based on automated processes, you have a procedure to protect their rights.”

When expanding the offices to include Brazil and the UK, GDPR guidelines must be considered to guarantee compliance. This information will aid when preparing to expand into new territories. Reviewing the standards set in these areas to adhere to current business practices is essential.

**References**

Conklin, WM. A., & Shoemaker, D. P. (2022). *CSSLP Certified Secure Software Lifecycle Professional: Exam Guide.* McGraw-Hill Education.

GDPR. (2019). *GDPR Checklist for Data Controllers*. GDPR.EU. <https://gdpr.eu/checklist/>