**IS6574 Assignment 3**

Using this as your guide:

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

You still work for the same online company from Assignment 2. However now they have expanded their data to scientists with the European Union. These scientists in the EU can register their personal information with your company and then download the data that the USA government provides.

Your boss has now asked you what does the company need to do to become GDPR compliant?

List ALL of the GDPR requirements given the company’s business and architecture. Submit each requirement in this type of format:

|  |
| --- |
| Requirement Name (you set this) |
| Write the details of the requirement here. |

Hint: Each requirement should be at least a paragraph answer long answer. It should explain any technical change requirements if necessary. It should mention any special training if necessary. It should mention frequency of any type of activity such as log reviews, or server updates if necessary (examples include weekly, quarterly, annually etc.). You need to be thorough given the architecture of the company.

You will need to take some time and read through the GDPR regulations to determine what needs to be done at your business. (This assignment should not be done quickly with just some fast Google search where you hit on a few things.)

Treat this like you were actually assigned this task at your job and need to perform on it well.

When you are done you will likely have learned many interesting things about GDPR that you did not know when you started. You also should be much more qualified to discuss GDPR at a real job in the future should such a discussion come up.

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

**Requirement Name: Data Protection Officer (DPO) Appointment**

**Details:** The company must appoint a Data Protection Officer (DPO) to oversee GDPR compliance due to the handling of personal data of EU citizens. The DPO will be responsible for informing and advising the company on GDPR obligations, monitoring compliance, and serving as the contact point for data subjects and supervisory authorities. The DPO should have expert knowledge of data protection laws and practices. The company must ensure that the DPO has the necessary resources to perform their tasks and maintain their independence within the organization. Regular reports on compliance and issues must be submitted to senior management.

**Requirement Name: Lawful Basis for Processing**

**Details:** The company must identify and document the lawful basis for processing personal data of EU scientists. This could include consent, performance of a contract, legal obligation, vital interests, public task, or legitimate interests. The chosen lawful basis must be clearly communicated to the data subjects through a comprehensive privacy notice. This notice should be easily accessible on the company’s website and provided at the point of data collection. Regular reviews of the lawful basis and associated documentation should be conducted annually or whenever there are changes in processing activities.

**Requirement Name: Data Processing Agreements (DPA)**

**Details:** The company must establish Data Processing Agreements (DPAs) with any third parties that process personal data on its behalf. These agreements must outline the nature and purpose of the processing, the type of data involved, and the obligations of both parties to ensure data protection. The DPAs should be reviewed and updated annually or whenever there are changes in processing activities or third-party providers. This ensures that all parties are aware of their responsibilities and that the personal data is protected at all times.

**Requirement Name: Data Subject Rights**

**Details:** The company must implement processes to handle data subject rights requests, such as access, rectification, erasure, restriction of processing, data portability, and objection to processing. These processes should be well-documented and include response procedures within the required timeframes (typically one month). Regular training should be provided to employees on handling these requests and the importance of compliance. A dedicated team or individual should be responsible for managing these requests and ensuring timely and accurate responses.

**Requirement Name: Privacy by Design and Default**

**Details:** The company must incorporate data protection principles into the design of new products and services (Privacy by Design) and ensure that, by default, only the minimum necessary personal data is processed (Privacy by Default). This requirement may involve conducting Data Protection Impact Assessments (DPIAs) for high-risk processing activities and embedding privacy features in the development lifecycle of IT systems. Developers and IT staff should receive regular training on privacy principles and how to implement them in practice.

**Requirement Name: Data Breach Notification**

**Details:** The company must establish a procedure for detecting, reporting, and investigating personal data breaches. In the event of a data breach, the company must notify the relevant supervisory authority within 72 hours and communicate the breach to affected data subjects without undue delay if it poses a high risk to their rights and freedoms. Regular breach response drills and annual reviews of the breach notification procedure are recommended. This ensures that the company is prepared to respond quickly and effectively to any data breaches.

**Requirement Name: Data Protection Impact Assessment (DPIA)**

**Details:** The company must conduct DPIAs for processing activities that are likely to result in a high risk to the rights and freedoms of data subjects. The DPIA should assess the necessity and proportionality of the processing, identify and mitigate risks, and involve consultation with the DPO. DPIAs should be reviewed periodically and updated as necessary, especially when introducing new processing activities. This helps to ensure that the company’s data processing activities remain compliant with GDPR and that any risks to data subjects are minimized.

**Requirement Name: Record of Processing Activities (RoPA)**

**Details:** The company must maintain a detailed record of all processing activities under its responsibility. This record should include the purposes of processing, categories of data subjects and personal data, recipients of the data, data retention periods, and security measures in place. The RoPA should be updated regularly, and all changes in processing activities must be documented. This helps to ensure that the company has a clear understanding of its data processing activities and can demonstrate compliance with GDPR requirements.

**Requirement Name: Data Minimization and Retention**

**Details:** The company must ensure that personal data collected is adequate, relevant, and limited to what is necessary for the purposes for which it is processed (data minimization). Additionally, the company must establish data retention policies to ensure personal data is not kept longer than necessary. Regular audits should be conducted to ensure compliance with these policies, and outdated or unnecessary data should be securely deleted. This helps to reduce the risk of data breaches and ensures that the company is only processing the data that it needs.

**Requirement Name: Security Measures**

**Details:** The company must implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including pseudonymization and encryption of personal data, measures to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems, and regular testing of security measures. Annual security reviews and quarterly vulnerability assessments should be conducted to identify and mitigate risks. This helps to ensure that the company’s data processing activities are secure and that personal data is protected from unauthorized access and disclosure.

**Requirement Name: Employee Training and Awareness**

**Details:** The company must provide regular training to all employees on data protection principles and GDPR compliance. This training should cover topics such as data subject rights, data breach response, data minimization, and secure data handling practices. Training sessions should be held at least annually, with additional sessions for new employees and when there are significant changes to data protection policies or regulations. This helps to ensure that all employees understand their responsibilities under GDPR and are equipped to handle personal data appropriately.

**Requirement Name: Secure Data Transfers**

**Details:** The company must ensure that any transfer of personal data outside the EU complies with GDPR requirements. This includes using appropriate safeguards such as Standard Contractual Clauses (SCCs), Binding Corporate Rules (BCRs), or ensuring that the destination country has an adequacy decision from the European Commission. Regular reviews of data transfer mechanisms and audits of third-party compliance should be conducted. This helps to ensure that personal data remains protected when it is transferred outside the EU.