GDPR Readiness: Creating a Data Privacy Plan

Elements of the Plan

- Personal Data Protection Policy
- Internal Privacy Procedures
- Information Request Procedure
- Data Security Policy
- Data Breach Procedure
- Data Processing Agreements and Addenda
- Internal Training Procedure

What is Data Protection?

Data protection has to do with protecting data you hold from unauthorized access. Examples of this include encryption, firewalls, backups, and secured servers. A data breach would be the result of insufficient data protection.

What is Data Privacy?

Data privacy has more to do with managing who has authorized access to the information you hold. If an individual has given you consent to store their billing information and you give this to another company to use without the individual's permission, this would be a data privacy violation. Using that same information within your own company but for another non-consenting (and therefore unauthorized) process is also a violation.

Data Mapping: The First Step

The first step to developing an organization's privacy practices is identifying what pieces of personal data are collected, where it goes in the organization, who can access it, and what processing is done on it. It is important to create a data map that is thorough and complete. Some tips to keep in mind when you create your data map:

- Keep it as simple as possible while still containing all of the information it needs.
- Use different shapes or colours to differentiate between employees, processors, clients, and third-parties.
- The flow of data, and processing actions should be shown with arrows.
- Be sure to consider the flow of data both externally and internally.

What is Data Breach Procedure?

A Data Breach Procedure will outline the following information:

- How an employee can report a suspected data protection incident
- Who will be responsible for leading the containment effort (often a member of the IT department), and who should be involved in this process
- Who will lead an investigation into the incident, and who else may become involved
- A process for notifying individuals and supervising authorities if a data breach is severe
- A procedure for evaluating the incident after the fact to make informed decisions for the future

The Data Breach Procedure should make it clear that any significant data breaches must be reported to individuals and the supervising authority within **72 hours**.

Information Request Procedure

The Information Request Procedure outlines the steps that should be taken when an individual contacts the organization regarding their personal information. Citizens are granted certain rights in regard to their personal information under the GDPR, and a proper information request procedure should outline a process to be taken to uphold each right.

The rights that should be addressed in the procedure include: