UNIT 2

Writing a Data Privacy Plan

Learning Objectives:
By the end of this unit the learner will be able to:
Map the flow of data in an organization visually Understand and write an information request procedure

Unit 2

Writing a Data Privacy Plan

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. A data map is a clear, visual way to accomplish this.

It is important to create a data map that is thorough and complete. A good way to do this is by consulting with employees in many different areas of your organization to see what data they collect in the course of their work, and what they do with it.

TIPS TO KEEP IN MIND

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. This will ensure that the data map is easily understood by everyone.
- 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 (with customers or clients) and internally (with employee records).

Test Your Knowledge

Using the Case Study Data Map, develop a generic Data Map using your own company processes.

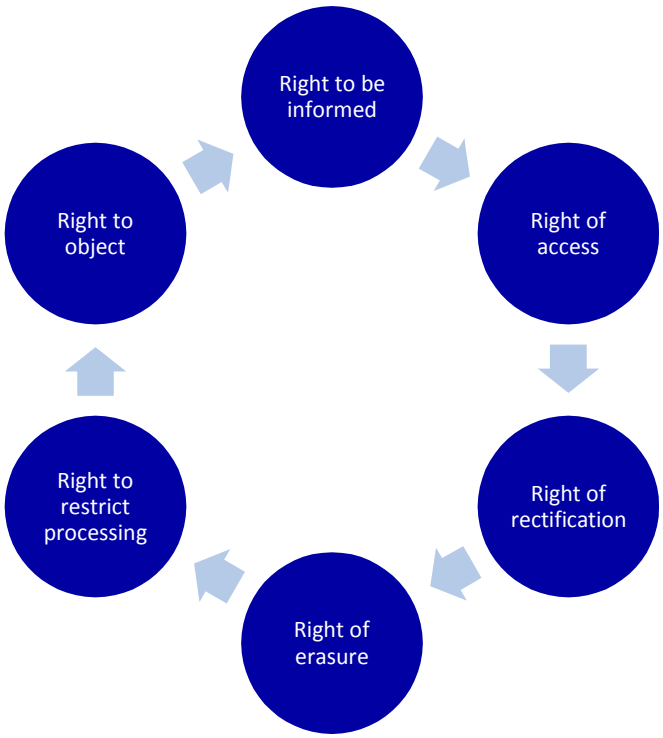
Data Map

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:



- **Right to be informed**: an individual can ask for confirmation that the organization has collected their personal information
- **Right of access:** an individual can ask for a copy of their personal information
- **Right of rectification:** an individual can ask for their personal information to be corrected if evidence of an inaccuracy is given
- **Right of erasure:** in certain circumstances, an individual can ask that their personal data be erased from the organization's records.
- **Right to restrict processing:** an individual can ask that their data only be stored and not processed.

- **Right to object:** an individual can object to the use of their personal data in a particular processing function.

This procedure should be clear so that any employee that handles an information request can easily follow the procedure.

The procedure should make clear that every information request must be responded to, and fulfilled, within a calendar month (or 28 days as a rule).

TEST YOUR KNOWLEDGE

Develop a general Information Request Procedure that addresses the steps that should be taken when any type of information request is received. Don't worry about addressing each of the rights individually.

Information Request Procedure

INTERNAL DATA PROCEDURES

The internal data procedures will outline the way data should be handled by employees within your organization. It addresses data accuracy, data retention, and data erasure, as well as the way these procedures will be monitored and inspected internally.

An organization has a responsibility to take reasonable measures to ensure the accuracy of the data they hold. There should be a process in place to keep stored data fresh, and a process to rectify data when informed by the individual.

Data should only be retained as long as it is useful for the purpose it was collected. Personal data should also only be retained as long as the individual does not withdraw their consent. The procedure should outline specific timelines around how long data should be kept, and where it will be stored.

When data no longer needs to be retained, or when an individual requests it (in certain circumstances), data should be properly erased. The process outlined in this procedure should cover the secure, complete deletion action, as well as the specific timeline on how often certain pieces of data will be deleted.

The procedure should also outline who is responsible for ensuring employees follow the procedure, and what actions may be taken if a non-compliance occurs.

TEST YOUR KNOWLEDGE

Develop an Internal Data Procedure that covers each of the elements presented: accuracy, retention, erasure, and monitoring compliance.

Internal Data Procedure

Further Reading:

- ✓ Kolah Ardi, *The GDPR Handbook: A Guide to Implementing the EU General Data Protection Regulation,* Kogan Page, 2018.