UNIT-1

Important Terminology and Legislation Regarding Data Privacy

Learning Outcomes

By the end of this unit the learner will be able to:

- ✓ **Explain what a data privacy plan will include**
- ✓ **Know the important terminology and legislation regarding data privacy**

Unit 1

Important Terminology and Legislation Regarding Data Privacy

Elements of the Plan

Typically, you will want to include the following elements.

Personal Data Protection Policy

This is an overarching policy that outlines the responsibilities for data privacy in your organization, as well as guidelines for employees, rules governing data storage and use, and information on other aspects of general data privacy.

Internal Privacy Procedures

How will data be kept accurate? How long will we keep data? When should we delete data?

Information Request Procedure

What do we do when a client asks for their information? What rights do they have over the data we hold? How long do we have to respond?

Data Security Policy

What safeguards do we have in place to protect personal information? Who is responsible for ensuring data protection systems are working?

Data Breach Procedure

What do we do when there is a data breach? Who is in charge? How will an investigation be conducted? Who should be notified, and when?

Data Processing Agreements and Addenda

A collection of the data processing agreements or addenda in place with any third-party processors in use by the organization.

Internal Training Procedure

How will employees learn about the policies that are created? Does everyone need to learn everything? What learning methods might be most effective?

Additional Tips

Some other tips to keep in mind:

- ✓ Once a draft has been written, have several people from different areas of the company go through it. This will help you make sure you have covered all of the bases.

- ✓ Make sure the plan is readable. Use clear, concise language rather than jargon and big words.
- ✓ You may want to have the plan translated into languages other than English depending on your worker demographics.
- ✓ Choose the correct format. While a paper copy is a good idea, you may also want to post it on the company website or provide it in other formats.
- ✓ Supervisors should go over the plan with employees on a regular basis to make sure they read and understand it.

Refer to the information collected in your pre-assignment to give you a better sense of where your organization stands in this regard.

PRIVACY AWARENESS

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.

Both data protection and data privacy work together to ensure that the personal information of the individual's we work with is appropriately handled.

What is personal information? Personal information is defined as any **"information about an identifiable individual."** This includes information like:

- ✓ Name
- ✓ Email address
- ✓ Phone number
- ✓ Banking information, credit/debit card data, purchases, loan reports
- ✓ Social Insurance Number (SIN), or other identification numbers
- ✓ Race, ethnic origin, religion, education or income level
- ✓ Age, height, blood type, medical records

Why is Data Privacy So Important Anyway?

1. Customer Service and Experience
    a. Keeping the private information of customers protected, and upholding their personal rights, is a good way to keep customers **confident and comfortable** with the company. By demonstrating that we can protect their data, and working with them on any privacy concerns or requests, we show that **data privacy is important to us**, and that we can be trusted with personal information.
    b. As **customers are becoming more concerned about their data privacy**, a company that can be sensitive to privacy concerns, and deliver appropriate protective measures for personal data will be the **safer, and more comfortable choice** for customers.
2. Legislation
    a. We also have a legal requirement to protect the personal data of our customers and employees.
    b. Breaking the law can lead to a **variety of negative consequences**, including complaints, investigations, audits, and fines.
    c. The major legislation that we are dealing with is the European Union's **General Data Protection Regulation**, or **GDPR.**

What is the GDPR?

- ✓ The GDPR is a regulation adopted by the European Union governing personal data use and protection. Even though the GDPR is a regulation for the European Union, its scope includes **any business that processes the personal data of citizens of the European Union**, even if they do not physically operate in the EU.
- ✓ The GDPR outlines six principles to govern the protection of data. According to the GDPR, **personal data must be**:
    - o processed lawfully, fairly, and transparently.
    - o adequate, relevant, and limited to what is necessary for processing.
    - o accurate and kept up-to-date.
    - o kept in a form such that the data subject can be identified only as long as is necessary for processing.
    - o processed in a manner that ensures its security.

  and can only:
    - o be collected for specified, explicit, and legitimate purposes.
- ✓ All citizens of the European Union are granted certain rights under the GDPR in relation to their personal information:
    - o The right to be **informed**
    - o The right of **access**
    - o The right to **rectification**
    - o The right to **erasure**
    - o The right to **restrict processing**
    - o The right to **data portability**
    - o The right to **object**
    - o Rights in relation to **automated decision making and profiling**

- An organization has the responsibility to ensure that these rights are upheld.

How confident are you in your awareness of data protection and data security? Why do you feel this way?

Further Reading:

- ✓ Foulsham Mark and Brian Hitchen, *GDPR: Guiding Your Business To Compliance: A practical guide to meeting GDPR regulations,* Independent publisher, 2017.