Activity: Case Study – GDPR Compliance in Action

Objective:
Participants will analyze a real-world case study to understand how a company successfully implemented GDPR compliance after a data breach. The goal is to explore the challenges faced, the company's response in line with GDPR, and the lessons learned.

Duration:

30 minutes

Materials Needed:

1. **Case Study Handout or Slide**: A brief description of the real-world case study, highlighting the breach, response, and outcome.
2. **Projector or Whiteboard** (optional): To present key points and facilitate discussion.
3. **Notepads and Pens** or **Laptops/Tablets**: For participants to note their observations and key discussion points.

Case Study Example: Data Breach at XYZ Telecom

Scenario:
XYZ Telecom, a European telecommunications company, suffered a major data breach in which hackers gained access to personal customer information, including names, addresses, email addresses, and phone numbers. The breach occurred due to a vulnerability in their customer support portal, which hackers exploited. The company needed to respond in full compliance with GDPR regulations.

Key Points to Discuss:

1. The Breach:

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

- **How it Occurred**:
    - Hackers exploited a security vulnerability in XYZ Telecom's customer support portal, gaining access to personal customer data stored in the system.
- **Data Exposed**:
    - Personal identifiers such as customer names, addresses, phone numbers, and email addresses were exposed, but no payment details were compromised.

Discussion Question:

- What security vulnerabilities or failures led to this breach? How could XYZ Telecom have identified and patched this vulnerability earlier?

---

2. The Response:

- **Notifying Affected Individuals**:
    - In compliance with GDPR, XYZ Telecom notified affected customers within the required **72-hour window**. They sent emails and text messages to all affected customers, explaining the breach, what data was exposed, and offering guidance on steps to protect their information.
- **Assessing the Breach**:
    - XYZ Telecom conducted a **root cause analysis** and determined that the breach occurred due to a failure in their patch management system, which left the support portal vulnerable. They immediately fixed the vulnerability and ran additional security tests.
- **Updating Security Protocols**:
    - The company strengthened its security by implementing **multi-factor authentication (MFA)** for both internal employees and customers accessing sensitive data, performed more frequent system audits, and hired a third-party cybersecurity firm to conduct regular penetration tests.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Discussion Question:

- How did XYZ Telecom's response align with GDPR? What steps could they have taken differently to better protect customer data?

---

3. The Outcome:

- **Lessons Learned**:
    - XYZ Telecom learned the importance of regularly updating security systems and the need for stricter access controls. The breach highlighted vulnerabilities in their IT infrastructure that were subsequently addressed.
- **Changes Implemented**:
    - The company updated its internal **data protection policies**, requiring more frequent vulnerability scans and better staff training on cybersecurity. They also created a **Data Breach Response Plan** to ensure rapid, compliant responses to any future incidents.

Discussion Question:

- What long-term changes did XYZ Telecom implement to ensure compliance with GDPR and prevent future breaches? How can these lessons apply to other companies?

Activity Flow:

1. Case Presentation (10 minutes):

- The facilitator introduces the XYZ Telecom case study, explaining the breach, the data exposed, and the company's GDPR-compliant response.

2. Group Discussion (15 minutes):

- Participants will break into small groups to discuss the following:
    1. How the breach occurred and what weaknesses were exposed.
    2. The effectiveness of XYZ Telecom's response in compliance with GDPR.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

3. The lessons learned and the changes the company implemented to prevent future breaches.
4. What other actions could XYZ Telecom have taken to improve their response and data protection?

3. Presentation of Key Insights (5 minutes):

- Each group will briefly present their findings, highlighting key insights from the discussion. The facilitator will then wrap up the activity by summarizing the most important points and encouraging questions.

Expected Outcomes:

- **Understanding of GDPR compliance**: Participants will understand how a company can respond to a data breach in compliance with GDPR, including customer notification, breach assessment, and security protocol updates.
- **Real-world application**: Participants will analyze the challenges faced by a real company and the steps taken to ensure compliance, offering practical lessons applicable to other organizations.
- **Critical thinking**: The group discussion will encourage participants to think critically about the actions taken by XYZ Telecom and explore potential improvements in data protection strategies.

Additional Scenarios for Case Study Activities

1. **Scenario: Data Breach at E-Commerce Platform**
    - **Context**: A major online retailer experiences a breach where customer payment information is exposed due to a vulnerability in their checkout process. They must respond according to GDPR.
    - **Focus**: How to handle breaches involving financial data and protecting payment information.
2. **Scenario: Financial Institution Data Leak**

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

- **Context**: A bank discovers that an employee unintentionally leaked customer account details through unsecured email communication.
- **Focus**: How to implement GDPR-compliant policies for internal staff handling sensitive data.

3. **Scenario: Healthcare Provider Data Breach**
   - **Context**: A healthcare organization experiences a breach where patient medical records are accessed by unauthorized personnel due to weak access controls.
   - **Focus**: How to handle sensitive health information under GDPR and comply with health data privacy laws.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.