# #TOPIC 4

# MAIN IMPLICATIONS OF THE GDPR FOR ONLINE AND CLASSROOM TEACHING

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.

DATAGAME

Co-funded by the European Union

# Main implications of the GDPR for online and classroom teaching

The General Data Protection Regulation (GDPR) has profound implications for both online and classroom teaching, particularly as educators handle sensitive personal data. This regulation, effective since May 25, 2018, is designed to protect the privacy of individuals within the European Union (EU) and the European Economic Area (EEA). For educators, understanding the key aspects of GDPR compliance is crucial for ensuring the safety and privacy of learners' data while maintaining transparency and trust.

In the context of adult education, the GDPR brings new responsibilities for handling personal data, especially in online teaching environments where data is collected and processed more frequently. Adherence to GDPR not only safeguards learners' rights but also minimises the risks of potential violations that could lead to significant penalties for educational institutions.

This section explains how GDPR affects classroom and online teaching and provides practical tips for compliance. It provides practical tools and guidance to help educators navigate these legal requirements effectively.

| Section | Description |
|---|---|
| **Module Title** | Legal and Compliance: Main implications of the GDPR for online and classroom teaching |
| **Overview of the topic** | Introduce the GDPR, its significance for data protection, and its implications for adult education providers. |
| **Objective** | By the end of the module, educators will:<br>• Understand the principles of data protection under GDPR.<br>• Learn how to apply GDPR principles in online and classroom teaching.<br>• Be able to educate their learners on their rights under GDPR. |
| **Relevant Regulations/Standards** | GDPR Articles related to data processing, consent, data subject rights (e.g., Article 6: Lawfulness of processing; Article 13: Information to be provided where personal data are collected from the data subject). |
| **Implications for Adult Education** | Discuss how GDPR applies to adult education environments, focusing on how personal data is |

| | |
|---|---|
| | collected, processed, and protected during online and classroom teaching. |
| **Activities/Exercises** | • Scenario Discussion: Present a scenario in which a teacher needs to decide whether to share student data with a third party. Discuss how GDPR compliance should influence the decision.<br>• Quiz: Include a quiz to test knowledge of GDPR principles. |
| **Methodological Guidance** | • Encourage educators to use real-life scenarios to discuss GDPR with their learners.<br>• Suggest including GDPR awareness as part of the orientation for students, particularly in courses involving online learning. |
| **Explanatory Notes** | • Define key terms such as *personal data*, *consent*, and *data processing*.<br>• Provide case studies or examples of GDPR compliance breaches and their consequences in educational settings. |
| **Definitions and Key Terms** | • **GDPR (General Data Protection Regulation)**: The GDPR is a European Union regulation that sets rules for how personal data is collected, stored, and processed, aiming to enhance privacy protections.<br>• **Personal Data**: Any information that can directly or indirectly identify a person, such as name, email address, or IP address.<br>• **Data Controller**: An entity (e.g., an educational institution) that determines the purpose and means of processing personal data.<br>• **Data Processor**: A person or entity that processes data on behalf of the Data Controller (e.g., a cloud storage provider).<br>• **Consent**: Explicit permission given by individuals to process their data for specific purposes, which must be freely given, informed, and unambiguous. |
| **Examples/Case Studies** | **Case Study 1**: An online teaching platform suffered a data breach, exposing learners' personal information, including email addresses and passwords. The breach occurred because the platform did not update its security protocols. As a |

| | |
|---|---|
| | result, the organisation faced heavy fines for non-compliance with GDPR and lost user trust.<br>**Lesson**: Regularly update security systems and audit platforms used for data processing.<br>**Case Study 2**: An educator recorded an online session and shared it publicly on a social media platform. A learner, unaware that the session was recorded, filed a complaint, citing unauthorised data usage. The institution was required to remove the recording and provide formal apologies.<br>**Lesson**: Always obtain consent for recording sessions and clarify where the recordings will be used.<br>**Case Study 3**: A school implemented a new digital attendance system without informing parents. Parents raised concerns about how their children's data was being processed and stored. Following the complaints, the school conducted a data privacy audit and introduced better communication policies about data collection.<br>**Lesson**: Transparency is critical—communicate the purpose and methods of data collection to all stakeholders. |

# **GUIDE:** Instructional Guide for GDPR Compliance in Online Teaching

**Subtitle: Critical Scenario for GDPR Compliance in Online Teaching**

**Objective:** To obtain a clear understanding of GDPR compliance requirements in online and classroom teaching, focusing on safeguarding learners' personal data, ensuring lawful data processing, and minimising potential risks related to data protection breaches.

**Scenario:** An adult educator conducts online sessions using a popular video conferencing platform. During a session, the educator records the meeting to share with absent students. The educator also uses a shared online folder to distribute course materials. However, learners express concerns about how their personal data (e.g., video recordings, email addresses, and shared folder access logs) is being stored and whether it could be shared without their consent.

**Guidance:** Step-by-Step Advice for GDPR Compliance in Online and Classroom Teaching

1. **Verify GDPR Compliance of Digital Tools**:
   - Before choosing a video conferencing platform, review its privacy policy to ensure compliance with GDPR regulations. For example, check if the platform encrypts data and stores it in GDPR-compliant servers.
   - If using a new tool, ensure your institution has signed a Data Processing Agreement (DPA) with the provider.

2. **Obtain Explicit Consent for Data Processing**:
   - Before recording sessions or collecting personal data, inform students about why their data is needed and how it will be used.
   - Example: Use a consent form or include a clear notice at the start of each session stating the purpose of recording.
3. **Secure Communication Channels**:
   - Use password-protected links for sharing materials or conducting sessions.
   - Example: Instead of sharing open-access links, require students to log in with their credentials to access shared resources.
4. **Limit Data Collection to What Is Necessary**:
   - Only collect data that is essential for the course. For instance, do not request personal details like home addresses unless absolutely necessary.
5. **Educate Learners on Their Privacy Rights**:
   - Include a short module or discussion about students' rights under GDPR, such as accessing, correcting, or deleting their personal data.
   - Example: Share a document summarising their rights at the beginning of the course.
6. **Regularly Audit and Delete Unnecessary Data**:
   - Review data storage practices periodically. For example, delete old session recordings and access logs that are no longer required for educational purposes.

# **GUIDE:** Learners' registration and data access

**Subtitle: GDPR-related challenges and safeguarding for learner privacy**

**Objective:** To provide adult educators with the knowledge and tools to address common GDPR-related challenges, fostering an environment that respects and safeguards learner privacy.

**Scenario:** An institution launches an online course and requires learners to fill out a registration form with personal details, including phone numbers and demographic data. A learner requests their data to be removed after completing the course, raising questions about how the institution manages and deletes learner data.

**Guidance: Six Critical Steps for GDPR Compliance in Online and Classroom Teaching**

1. **Legal Compliance**:
   Ensure all data collection processes meet GDPR requirements by maintaining transparency. For example, use a privacy notice that clearly states why data is collected and how it will be used.
2. **Data Security**:
   Store all personal data securely, using encrypted storage systems and limiting access to authorised personnel only.

3. **Consent Management**:
   Before processing learner data, obtain explicit consent, such as for session recordings. Consent forms should be stored securely for future reference.
4. **Data Retention Policies**:
   Define how long data will be stored and ensure unnecessary data is deleted after its purpose is served.
5. **Handling Data Requests**:
   Respond promptly to learners who request access to, correction of, or deletion of their data.
6. **Institutional Training**:
   Educate all staff involved in course delivery about GDPR compliance.
   Example: Conduct a workshop for educators on secure data management practices.

# CHECKLIST

**Title: Data Privacy Compliance Checklist for Online and Classroom Teaching**

**Pre-session**

| | |
|---|---|
| ☐ | Verify that any digital platforms used (e.g., video conferencing tools, online assessments) comply with GDPR by reviewing their privacy policy and data protection practices. |
| ☐ | Obtain explicit consent from students for collecting and processing their personal data (e.g., for online registrations, assessment data, etc.). |
| ☐ | Secure access to teaching materials by password-protecting files or using secure platforms for sharing resources. |
| ☐ | Inform students about their data protection rights, including their right to access and erase their data, and how their data will be used during the course. |

**During session**

| | |
|---|---|
| ☐ | Use secure communication tools (e.g., encrypted email, password-protected online forums) for sharing sensitive information. |
| ☐ | Ensure that student interactions, recordings, and chat logs are kept confidential and are only accessible to relevant parties. |
| ☐ | Avoid collecting unnecessary personal data; only request what is required for the session. |

| | |
|---|---|
| **Post-session:** | |
| ☐ | Delete or securely store session recordings, ensuring that access is restricted to authorised personnel only. |
| ☐ | Update records and ensure proper documentation of student consent. |
| ☐ | Regularly audit and review data handling practices to ensure ongoing GDPR compliance. |
| **Notes:** This checklist helps educators systematically address GDPR requirements for each phase of an online or classroom session, providing a practical, step-by-step approach to ensure compliance. | |

| **Topic** | **Legal and Compliance: Main implications of the GDPR for online and classroom teaching** |
|---|---|
| **Description of the topic** | This topic focuses on understanding the implications of GDPR for educational settings, both online and in the classroom. It aims to equip educators with knowledge about data privacy regulations, enabling them to handle personal data responsibly, ensure compliance, and foster a culture of transparency and accountability in education. |
| **Title of tool** | Minding the data: protecting learners' privacy and security |
| **Link to the tool** | https://www.right-to-education.org/resource/minding-data-protecting-learners-privacy-and-security |
| **About the tool** | The UNESCO report highlights the balance between leveraging educational data and protecting learner privacy. It addresses key GDPR compliance challenges, such as managing consent, responding to data access requests, and implementing secure data handling practices. The tool offers actionable guidance for educators to safeguard learner data while ensuring compliance with privacy regulations, making it an invaluable resource for promoting safe and ethical data practices in education. |

| Topic | **Legal and Compliance: Main implications of the GDPR for online and classroom teaching** |
|---|---|
| **Description of the topic** | Understanding and complying with GDPR is crucial for educators who handle personal data in online or classroom teaching. This involves ensuring the secure collection, storage, and use of data, addressing data protection rights, and demonstrating accountability. Tools like self-assessments can help educators evaluate their current practices and identify areas for improvement. |
| **Title of tool** | Data protection self assessment |
| **Link to the tool** | https://ico.org.uk/for-organisations/advice-for-small-organisations/checklists/data-protection-self-assessment/ |
| **About the tool** | The Data Protection Self-Assessment Toolkit, provided by the UK Information Commissioner's Office (ICO), is a practical tool designed to help organisations evaluate their compliance with data protection laws, including GDPR. This tool guides educators through various compliance aspects, such as data security, lawful processing, and rights management. It is especially useful for identifying gaps in current practices and implementing improvements, enabling educators to confidently manage data privacy in both online and classroom environments. |