



ТЕМА 7

СЪХРАНЕНИЕ И ОБРАБОТКА НА ДАННИ ЗА УЧАЩИТЕ



Съфинансирано от
Европейския съюз

Финансирано от Европейския съюз. Изразените възгледи и мнения обаче принадлежат изцяло на техния(ите) автор(и) и не отразяват непременно възгледите и мненията на Европейския съюз или на Европейската изпълнителна агенция за образование и култура (EACEA). За тях не носи отговорност нито Европейският съюз, нито EACEA.

Съхраняване и обработка на данните на учащите се

Инструмент 1:

Тема	Съхраняване и обработване на данните на учащите се
Описание на темата	Сигурното съхранение и отговорната обработка на данните на учащите се са критични компоненти на защитата на данните. Съхранението включва използване на криптирани бази данни, сигурни облачни решения и редовни одити, за да се гарантира целостта и поверителността на данните. Обработката се фокусира върху обработката на информацията за учащите в съответствие с изискванията на GDPR, като се използват техники като анонимизиране, когато е уместно, и се спазват ясни политики за запазване и изтриване. Тези практики гарантират, че данните на учащите се се съхраняват по сигурен начин и се управляват по етичен начин през целия им жизнен цикъл.
Заглавие на инструмента	Услуги за сигурна електронна поща
Връзка към инструмента	ProtonMail Tutanota
За инструмента	Сигурните имейл услуги като ProtonMail и Tutanota защитават имейл комуникацията със силно криптиране, като гарантират, че поверителната информация, обменяна чрез имейл, остава поверителна. Тези услуги често включват криптиране от край до край и защитени сървъри за предпазване на комуникациите. Това ниво на сигурност е от решаващо значение за образователните институции, където често се обменят чувствителни данни. Като използват тези услуги, преподавателите могат да запазят поверителността и целостта на имейл комуникациите.

Инструмент 2:

Тема:	Съхраняване и обработка на данни за учащите
Описание на темата	Сигурното съхранение и отговорната обработка на данните на учащите се са критични компоненти на защитата на данните. Съхранението включва използването на криптирани бази данни, сигурни облачни решения и редовни одити, за да се гарантира целостта и поверителността на данните. Обработката се фокусира върху обработката на информацията за учащите в съответствие с изискванията на GDPR, като се използват техники като анонимизиране, когато е уместно, и се спазват ясни политики за запазване и изтриване. Тези практики гарантират, че данните на учащите се съхраняват по сигурен начин и се управляват по етичен начин през целия им жизнен цикъл.
Заглавие на инструмента	Платформи за сигурно споделяне на файлове
Връзка към инструмента	• Tresorit • Sync • Работно пространство на Google
За инструмента	Сигурните платформи за споделяне на файлове като Tresorit, Sync и Google Workspace (с подходящ контрол на достъпа) безопасно разпространяват учебни материали, съдържащи поверителна информация. Тези платформи предлагат криптиране и сигурен контрол на достъпа, като гарантират, че само упълномощени потребители имат достъп до споделените файлове. Като използват тези платформи, преподавателите могат да защитят чувствителните данни, докато си сътрудничат с колеги или споделят ресурси с обучаеми. По този начин се повишава сигурността на данните и се поддържа съответствие с разпоредбите за защита на данните.

Инструмент 3:

Тема	Съхраняване и обработка на данни за учащите
Описание на темата	Сигурното съхранение и отговорната обработка на данните на учащите се са критични компоненти на защитата на данните. Съхранението включва използването на криптирани бази данни, сигурни облачни решения и редовни одити, за да се гарантира целостта и поверителността на данните. Обработката се фокусира върху обработката на информацията за учащите в съответствие с изискванията на GDPR, като се използват техники като анонимизиране, когато е уместно, и се спазват ясни политики за запазване и изтриване. Тези практики гарантират, че данните на учащите се съхраняват по сигурен начин и се управляват по етичен начин през целия им жизнен цикъл.
Заглавие на инструмента	Системи за управление на обучението (LMS) с функции за сигурност
Връзка към инструмента	• Moodle • Canvas
За инструмента	Системите за управление на обучението (LMS), като Moodle и Canvas, предлагат надеждни функции за сигурност, като контрол на достъпа въз основа на роли, регистриране на дейностите и криптиране на всички съхранявани данни. Тези функции гарантират, че само упълномощени потребители имат достъп до чувствителна информация, като поддържат целостта и поверителността на данните в LMS. С помощта на тези системи преподавателите могат сигурно да управляват учебните материали и да проследяват дейностите на обучаемите, като същевременно защитават чувствителните данни. Това спомага за поддържането на сигурна учебна среда.

Инструмент 4:

Тема	Съхраняване и обработка на данни за учащите
Описание на темата	Сигурното съхранение и отговорната обработка на данните на учащите се са критични компоненти на защитата на данните. Съхранението включва използване на криптирани бази данни, сигурни облачни решения и редовни одити, за да се гарантира целостта и поверителността на данните. Обработката се фокусира върху обработката на информацията за учащите в съответствие с изискванията на GDPR, като се използват техники като анонимизиране, когато е уместно, и се спазват ясни политики за запазване и изтриване. Тези практики гарантират, че данните на учащите се съхраняват по сигурен начин и се управляват по етичен начин през целия им жизнен цикъл.
Заглавие на инструмента	SFTP за защитен трансфер на файлове
Връзка към инструмента	• FileZilla • WinSCP
За инструмента	Инструментите за сигурен протокол за прехвърляне на файлове (SFTP) като FileZilla и WinSCP осигуряват сигурен трансфер на файлове при споделяне или изпращане на задачи. SFTP криптира данните по време на прехвърлянето, като намалява риска от прихващане на данни или неоторизиран достъп. С помощта на тези инструменти преподавателите могат безопасно да обменят файлове с обучаеми или колеги, като запазват поверителността и целостта на чувствителната информация. Това е от съществено значение за защита на данните на учащите по време на прехвърлянето на файлове.

Инструмент 5:

Тема:	Съхраняване и обработка на данни на учащи се
Описание на темата	Сигурното съхранение и отговорната обработка на данните на учащите се са критични компоненти на защитата на данните. Съхранението включва използването на криптирани бази данни, сигурни облачни решения и редовни одити, за да се гарантира целостта и поверителността на данните. Обработката се фокусира върху обработката на информацията за учащите в съответствие с изискванията на GDPR, като се използват техники като анонимизиране, когато е уместно, и се спазват ясни политики за запазване и изтриване. Тези практики гарантират, че данните на учащите се се съхраняват по сигурен начин и се управляват по етичен начин през целия им жизнен цикъл.
Заглавие на инструмента	Инструменти за запазване и изтриване на данни
Връзка към инструмента	• BleachBit • Eraser
За инструмента	Инструментите за запазване и изтриване на данни като BleachBit и Eraser сигурно изтриват данните на учащите се, след като вече не са необходими, като гарантират спазването на политиките за запазване на данни. Тези инструменти презаписват данните многократно, като ги правят невъзстановими и намаляват риска от неоторизиран достъп. Чрез използването на тези инструменти образователните институции могат да поддържат сигурността на данните и да спазват законовите изисквания за унищожаване на данни. Това помага да се предотвратят потенциални нарушения на данните и да се поддържа съответствие.

Инструмент 6:

Тема:	Съхраняване и обработване на данни за учащи се
Описание на темата	Сигурното съхранение и отговорната обработка на данните на учащите се са критични компоненти на защитата на данните. Съхранението включва използването на криптирани бази данни, сигурни облачни решения и редовни одити, за да се гарантира целостта и поверителността на данните. Обработката се фокусира върху обработката на информацията за учащите в съответствие с изискванията на GDPR, като се използват техники като анонимизиране, когато е уместно, и се спазват ясни политики за запазване и изтриване. Тези практики гарантират, че данните на учащите се се съхраняват по сигурен начин и се управляват по етичен начин през целия им жизнен цикъл.
Заглавие на инструмента	Инструменти за архивиране и възстановяване
Връзка към инструмента	• Acronis • Veeam
За инструмента	Редовните планове за архивиране и възстановяване с помощта на инструменти като Acronis и Veeam гарантират, че данните на учащите се са надеждно архивирани и могат да бъдат възстановени в случай на загуба на данни или повреда на системата. Тези инструменти предоставят надеждни решения за архивиране, които поддържат целостта и наличността на данните, като осигуряват институционална приемственост. Чрез прилагането на тези планове преподавателите могат да защитят критичните данни и бързо да се възстановят от потенциални смущения. Това спомага за поддържане на стабилността на образователните операции.