DIE DATA GAME Toolbox

Kofinanziert von der Europäischen Union

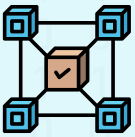
Von der Europäischen Union finanziert. Die geäußerten Ansichten und Meinungen entsprechen jedoch ausschließlich denen des Autors bzw. der Autoren und spiegeln nicht zwingend die der Europäischen Union oder der OeAD-GmbH wider. Weder die Europäische Union noch die OeAD-GmbH können dafür verantwortlich gemacht werden.

TOOL-SEKTIONEN

VERWALTUNG & TECHNOLOGIE

RECHTLICHE ANFORDERUNGEN & VERANTWORTUNG

DATENSCHUTZ & SICHERHEIT



ZUGANG, REGISTRIERUNG, VERWALTUNG

SICHERHEIT IN BILDUNGS-TECHNOLOGIEN

SPEICHERUNG & VERARBEITUNG

DATEN-BEHANDLUNG & -SICHERHEIT

TRAININGS- UND AUFKLÄRUNGS-PROGRAMME

SOCIAL-MEDIA-APPS

TOOLS

VERWALTUNG & TECHNOLOGIE

1. DPIA-VORLAGEN

Datenschutz-Folgenabschätzungen (DPIAs) sind wichtige Tools zur Bewertung potenzieller Risiken für die Daten der Lernenden vor Beginn eines Kurses oder Projekts. Sie helfen Organisationen dabei, Risiken im Zusammenhang mit der Datenverarbeitung zu identifizieren und zu mindern und gewährleisten die Einhaltung von Vorschriften wie der Datenschutz-Grundverordnung (DSGVO). DPIAs sind besonders wichtig im Bildungsbereich, wo häufig sensible personenbezogene Daten verarbeitet werden. Durch die Durchführung einer DPIA können Lehrkräfte die mit ihren Projekten verbundenen Datenschutzrisiken besser verstehen, Methoden zur Verringerung oder Beseitigung dieser Risiken ermitteln und Datenschutzmaßnahmen dokumentieren, um die Einhaltung der Vorschriften gegenüber den Aufsichtsbehörden nachzuweisen.

- GDPR EU
- IUBENDA
- TECHTARGET
- S.E.T.U.

2. PASSWORT-VERWALTUNG

Passwortverwaltungstools wie LastPass, 1Password und Bitwarden gewährleisten sichere, einzigartige Passwörter für den Zugriff auf Bildungssysteme und Datenbanken und verringern so das Risiko eines unbefugten Zugriffs. Diese Tools bieten Funktionen wie Passwortmanager und automatische Ausfüllfunktionen, die die Verwaltung mehrerer sicherer Passwörter erleichtern. Durch den Einsatz dieser Tools können Lehrkräfte ein hohes Maß an Sicherheit gewährleisten und gleichzeitig ihre Anmeldeprozesse vereinfachen. Dies trägt dazu bei, häufige Sicherheitsprobleme im Zusammenhang mit schwachen oder mehrfach verwendeten Passwörtern zu vermeiden.

- LASTPASS
- 1PASSWORD
- BITWARDEN

TOOLS

VERWALTUNG & TECHNOLOGIE

3. E-PLATTFORMEN

Schulungsmodule für Mitarbeiter:innen zu DSGVO und Datenverarbeitung, die auf Plattformen wie Coursera und Udemy verfügbar sind, sind unerlässlich, um sicherzustellen, dass Lehrkräfte die Datenschutzbestimmungen verstehen und einhalten. Diese Module bieten interaktive Lernerfahrungen, die den Mitarbeiter:innen helfen, die erforderlichen Fähigkeiten für den sicheren Umgang mit Daten von Lernenden zu entwickeln. Durch die Nutzung von Plattformen wie TalentLMS oder Articulate 360 können Bildungseinrichtungen maßgeschneiderte Schulungsprogramme erstellen, die ihren spezifischen Anforderungen entsprechen. Diese Schulungen sind für den Erhalt einer Datenschutzkultur im Bildungsbereich von entscheidender Bedeutung.

- COURSERA
- UDEMY
- TALENTLMS
- ARTICULATE 360

4. SCHUTZ & SICHERHEIT

Cybersicherheitsrahmen wie der CIS Controls Implementation Guide und das NIST Cybersecurity Framework bieten Richtlinien für die Sicherung institutioneller Systeme und Daten. Diese Rahmen beschreiben bewährte Verfahren für die Cybersicherheit und helfen Institutionen dabei, robuste Sicherheitsmaßnahmen zum Schutz vor Cyberbedrohungen umzusetzen. Durch die Befolgung dieser Rahmen können Bildungseinrichtungen sicherstellen, dass ihre Daten und Systeme gut geschützt sind und den Branchenstandards entsprechen. Dieser proaktive Ansatz trägt dazu bei, Datenschutzverletzungen zu verhindern und die Sicherheit der Institution zu gewährleisten.

- CIS CONTROLS
- NIST FRAMEWORK

TOOLS

VERWALTUNG & TECHNOLOGIE

5. VPN

Virtual-Private-Network (VPN)-Tools wie NordVPN und ExpressVPN sichern Internetverbindungen während virtueller Unterrichtsstunden, insbesondere in öffentlichen Netzwerken. Durch die Verschlüsselung der übertragenen Daten schützen VPNs vor Abhörversuchen und Man-in-the-Middle-Angriffen und gewährleisten, dass vertrauliche Informationen geheim bleiben. Dies ist besonders wichtig für Lehrkräfte, die häufig remote arbeiten oder öffentliche Netzwerke nutzen. Die Verwendung von VPNs trägt zum Erhalt der Sicherheit in der Kommunikation im Bildungsbereich bei.

- NORDVPN
- EXPRESS VPN

6. KOMMUNIKATION

- SIGNAL
- MS TEAMS

Datenschutzorientierte Kommunikationstools wie Signal und Microsoft Teams (mit erweiterten Sicherheitseinstellungen) verschlüsseln die Video- und Textkommunikation mit den Lernenden. Diese Tools bieten End-to-End-Verschlüsselung und sichere Authentifizierungs-mechanismen, wodurch sichergestellt wird, dass sensible Informationen, die während der Einheiten ausgetauscht werden, vertraulich bleiben. Durch die Verwendung dieser Tools können Lehrkräfte die Privatsphäre der Kommunikation wahren und gleichzeitig mit Lernenden oder Kolleg:innen zusammenarbeiten. Dies stärkt das Vertrauen und die Einhaltung der Datenschutzbestimmungen.

7. PRÜFUNG & ÜBERWACHUNG

Prüfungs- und Überwachungssoftware wie Splunk und SolarWinds überwachen den Datenzugriff und identifizieren potenzielle Sicherheitsverletzungen nach der Einheit. Diese Tools analysieren Protokolle und Netzwerkaktivitäten, um Sicherheitsvorfälle frühzeitig zu erkennen, sodass Institutionen umgehend Maßnahmen ergreifen können, um Schäden zu minimieren.

Durch den Einsatz dieser Tools können Lehrkräfte sicherstellen, dass Datensicherheitsmaßnahmen wirksam sind und den regulatorischen Standards entsprechen. Diese proaktive Überwachung trägt dazu bei, die Integrität von Bildungssystemen zu wahren.

TOOLS

VERWALTUNG & TECHNOLOGIE

8. MELDUNG BEI SICHERHEITS-VERLETZUNGEN

SPLUNK

SOLARWINDS

Splunk und SolarWinds überwachen in Echtzeit Protokoll- und Netzwerkdaten, um Hinweise auf unbefugte Zugriffe oder Datenlecks sofort zu erkennen. Wird ein Vorfall detektiert, stellt GDPR advisor rechtssichere Benachrichtigungsvorlagen bereit, mit denen betroffene Personen und Aufsichtsbehörden fristgerecht informiert werden können. Die Kombination aus automatischer Überwachung und standardisierten DSGVO-Meldevorlagen beschleunigt den Mitteilungsprozess, erhöht die Transparenz und reduziert das Risiko regulatorischer Sanktionen.

GDPR ADVISOR

9. ANONYME FEEDBACK-TOOLS

Feedback-Mechanismen wie Google Forms mit Verschlüsselung oder Mentimeter ermöglichen es Lehrkräften, während des Unterrichts Feedback von Lernenden zu Datensicherheitspraktiken zu sammeln. Diese Tools bieten sichere Plattformen für anonymes Feedback und helfen Lehrkräften dabei, Verbesserungsmöglichkeiten in ihren Datenverarbeitungsprozessen zu identifizieren. Durch den Einsatz dieser Mechanismen können Bildungseinrichtungen ihre Datensicherheitspraktiken verfeinern und das Vertrauen der Lernenden stärken. Diese Feedbackschleife ist für den Erhalt einer sicheren und reaktionsfähigen Bildungsumgebung unerlässlich.

GOOGLE FORMS

MENTIMETER

FORMS APP

TOOLS

RECHTLICHE ANFORDERUNGEN & VERANTWORTUNG

AKTIVITÄT 1

Präsentieren Sie ein Szenario, in dem eine Lehrkraft entscheiden muss, ob sie Daten von Lernenden an Dritte weitergeben soll.

- Diskutieren Sie, wie die Einhaltung der DSGVO die Entscheidung beeinflussen sollte.
- Quiz: Fügen Sie ein Quiz ein, um das Wissen über die Grundsätze der DSGVO zu testen.

Methodischer Leitfaden

- Ermutigen Sie Lehrkräfte, reale Szenarien zu verwenden, um mit ihren Lernenden über die DSGVO zu diskutieren.
- Schlagen Sie vor, das Bewusstsein für die DSGVO als Teil der Orientierung für Lernende einzubeziehen, insbesondere in Kursenmit Online-Lernen.
- Definieren Sie Schlüsselbegriffe wie personenbezogene Daten, Zustimmung und Datenverarbeitung.
- Stellen Sie Fallstudien oder Beispiele für Verstöße gegen die DSGVO und deren Folgen im Bildungsbereich zur Verfügung.

Definitionen und Schlüsselbegriffe

- **DSGVO (Datenschutz-Grundverordnung)**: Die DSGVO ist eine Verordnung der Europäischen Union, die Regeln für die Erhebung, Speicherung und Verarbeitung personenbezogener Daten festlegt, um den Datenschutz zu verbessern.
- **Personenbezogene Daten**: Alle Informationen, die eine Person direkt oder indirekt identifizieren können, wie z. B. Name, E-Mail-Adresse oder IP-Adresse.
- **Datenverantwortlicher**: Eine Stelle (z. B. eine Bildungseinrichtung), die den Zweck und die Mittel der Verarbeitung personenbezogener Daten festlegt.
- **Datenverarbeiter:in**: Eine Person oder Stelle, die Daten im Auftrag des Datenverantwortlichen verarbeitet (z. B. ein Cloud-Speicheranbieter).
- **Zustimmung**: Die ausdrückliche Zustimmung einer Person zur Verarbeitung ihrer Daten für bestimmte Zwecke, die freiwillig, informiert und eindeutig sein muss.

Beispiele/Fallstudien

- **Fallstudie 1**: Eine Online-Lehrplattform wurde Opfer einer Datenpanne, bei der persönliche Daten von Lernenden, darunter E-Mail-Adressen und Passwörter, offengelegt wurden.

RECHTLICHE ANFORDERUNGEN & VERANTWORTUNG

Der Verstoß ergab sich daraus, dass die Plattform ihre Sicherheitsprotokolle nicht aktualisiert hatte. Infolgedessen musste das Unternehmen hohe Geldstrafen wegen Nichteinhaltung der DSGVO zahlen und verlor das Vertrauen der Nutzer:innen.

- *Lektion*: Aktualisieren Sie regelmäßig die Sicherheitssysteme und überprüfen Sie die für die Datenverarbeitung verwendeten Plattformen.

Case Study 2: An educator recorded an online session and shared it publicly on a

complaint, citing unauthorised data usage. The institution was required to remove the recording and provide formal apologies.
Lesson: Always obtain consent for recording sessions and clarify where the recordings will be used.

Fallstudie 3: Eine Schule hat ein neues digitales Anwesenheitssystem eingeführt, ohne die Eltern darüber zu informieren. Die Eltern äußerten Bedenken hinsichtlich der Verarbeitung und Speicherung der Daten ihrer Kinder. Nach den Beschwerden führte die Schule eine Datenschutzprüfung durch und stellte bessere Kommunikationsrichtlinien zur Datenerfassung auf.
Lektion: Transparenz ist entscheidend – kommunizieren Sie allen Beteiligten den Zweck und die Methoden der Datenerfassung.

AKTIVITÄT 2

Schritt-für-Schritt-Anleitung zur Einhaltung der DSGVO im Online- und Präsenzunterricht

Eine Erwachsenenbildnerin führt Online-Sitzungen über eine beliebte Videokonferenzplattform durch. Während einer Sitzung zeichnet die der Lehrerin die Sitzung auf, um sie mit abwesenden Schüler:innen zu teilen. Die Lehrerin nutzt außerdem einen gemeinsamen Online-Ordner, um Kursmaterialien zu Verfügung zu stellen. Die Lernenden äußern jedoch Bedenken darüber, wie ihre personenbezogenen Daten (z. B. Videoaufzeichnungen, E-Mail-Adressen und Zugriffsprotokolle des gemeinsamen Ordners) gespeichert werden und ob diese ohne ihre Zustimmung weitergegeben werden könnten.

Schritt 1
Überprüfen Sie die DSGVO-Konformität digitaler Tools:

- Bevor Sie sich für eine Videokonferenzplattform entscheiden, überprüfen Sie deren Datenschutzrichtlinien, um sicherzustellen,

RECHTLICHE ANFORDERUNGEN & VERANTWORTUNG

dass sie den DSGVO-Vorschriften entsprechen. Überprüfen Sie beispielsweise, ob die Plattform Daten verschlüsselt und auf DSGVO-konformen Servern speichert.
- Wenn Sie ein neues Tool verwenden, stellen Sie sicher, dass Ihre Einrichtung einen Auftragsverarbeitungsvertrag (AVV) mit dem Anbieter unterzeichnet hat.

Schritt 2

Holen Sie die ausdrückliche Zustimmung zur Datenverarbeitung ein:

- Informieren Sie die Lernenden bevor Sie eine Einheit aufzeichnen oder personenbezogene Daten erheben, darüber, warum ihre Daten benötigt werden und wie diese verwendet werden.
- Beispiel: Verwenden Sie ein Einverständnisformular oder fügen Sie zu Beginn jeder Einheit einen deutlichen Hinweis ein, in dem der Zweck der Aufzeichnung angegeben ist.

Schritt 3

Sichere Kommunikationskanäle:

- Verwenden Sie passwortgeschützte Links, um Materialien zu teilen oder Unterrichtseinheiten durchzuführen.
- Beispiel: Anstatt Links mit offenem Zugriff zu teilen, verlangen Sie von den Lernenden, dass sie sich mit ihren Zugangsdaten anmelden, um auf gemeinsam genutzte Ressourcen zugreifen zu können.

Schritt 4

Beschränken Sie die Datenerfassung auf das Notwendige:

Erfassen Sie nur Daten, die für den Kurs unerlässlich sind. Fordern Sie beispielsweise keine persönlichen Daten wie Privatadressen an, es sei denn, dies ist unbedingt erforderlich.

Schritt 5

Informieren Sie die Lernenden über ihre Datenschutzrechte:

- Bauen Sie ein kurzes Modul oder eine Diskussion über die Rechte der Lernenden gemäß der DSGVO ein, z. B. über den Zugriff auf ihre personenbezogenen Daten sowie deren Korrektur oder Löschung.
- Beispiel: Verteilen Sie zu Beginn des Kurses ein Dokument, in dem diese Rechte zusammengefasst sind.

Schritt 6

Überprüfen und löschen Sie regelmäßig unnötige Daten:

- Prüfen Sie regelmäßig Ihre Datenspeicherungspraktiken. Löschen Sie beispielsweise alte Aufzeichnungen von Sitzungen und Zugriffsprotokolle, die für Bildungszwecke nicht mehr benötigt werden.

TOOLS

RECHTLICHE ANFORDERUNGEN & VERANTWORTUNG

AKTIVITÄT 3

Herausforderungen im Zusammenhang mit der DSGVO und dem Schutz der Privatsphäre von Lernenden

Eine Institution startet einen Online-Kurs und verlangt von den Lernenden, dass sie ein Anmeldeformular mit persönlichen Angaben, einschließlich Telefonnummern und demografischen Daten, ausfüllen. Ein Lernender beantragt nach Abschluss des Kurses die Löschung seiner Daten, was Fragen darüber aufwirft, wie die Institution die Daten der Lernenden verwaltet und löscht.

Sechs wichtige Schritte zur Einhaltung der DSGVO im Online- und Präsenzunterricht

Schritt 1
Rechtskonformität:
- Stellen Sie sicher, dass alle Datenerfassungsprozesse den Anforderungen der DSGVO entsprechen, indem Sie Transparenz wahren. Verwenden Sie beispielsweise eine Datenschutzerklärung, in der klar angegeben ist, warum Daten erfasst werden und wie sie verwendet werden.

Schritt 2
Datensicherheit:
- *Speichern Sie alle personenbezogenen Daten sicher, indem Sie verschlüsselte Speichersysteme verwenden und den Zugriff auf autorisiertes Personal beschränken.*

Schritt 3
Zustimmungsmanagement:
- Holen Sie vor der Verarbeitung von Daten der Lernenden deren ausdrückliche Zustimmung ein, beispielsweise für die Aufzeichnung von Unterrichtseinheiten. Einwilligungserklärungen sollten sicher aufbewahrt werden, damit sie später eingesehen werden können.

Schritt 4
Datenspeicherungsrichtlinien:
- Legen Sie fest, wie lange Daten gespeichert bleiben, und stellen Sie sicher, dass nicht mehr benötigte Daten gelöscht werden, sobald ihr Zweck erfüllt ist.

Schritt 5
Umgang mit Datenanforderungen:
- Beantworten Sie Anfragen von Lernenden, die Zugriff auf ihre Daten, deren Korrektur oder Löschung wünschen, umgehend.

TOOLS

RECHTLICHE ANFORDERUNGEN & VERANTWORTUNG

Schritt 6

Schulungen für Institutionen:

- Schulen Sie alle an der Kursdurchführung beteiligten Mitarbeiter:innen in Bezug auf die Einhaltung der DSGVO. Beispiel: Führen Sie einen Workshop für Lehrkräfte zu sicheren Datenverwaltungspraktiken durch.

WESENTLICHE AUSWIRKUNGEN DER DSGVO AUF DEN ONLINE- UND PRÄSENZUNTERRICHT

NEWS UPDATE

Dieser UNESCO-Bericht hebt das Gleichgewicht zwischen der Nutzung vonbildungsbezogenen Daten und dem Schutz der Privatsphäre der Lernenden hervor. Er befasst sich mit den wichtigsten Herausforderungen bei der Einhaltung der DSGVO, wie z. B. der Verwaltung von Einwilligungen, der Beantwortung von Datenzugriffsanfragen und der Umsetzung sicherer Datenverarbeitungsverfahren. Das Tool bietet Lehrkräften praktische Anleitungen zum Schutz der Daten von Lernenden bei gleichzeitiger Einhaltung der Datenschutzbestimmungen und ist damit eine unschätzbare Ressource für die Förderung sicherer und ethischer Datenpraktiken im Bildungswesen.

BEWERTUNG

Das Data Protection Self-Assessment Toolkit, das vom britischen Information Commissioner's Office (ICO) bereitgestellt wird, ist ein praktisches Tool, das Organisationen dabei helfen soll, ihre Einhaltung der Datenschutzvorschriften, einschließlich der DSGVO, zu bewerten. Dieses Tool begleitet Lehrkräfte durch verschiedene Aspekte der Compliance, wie Datensicherheit, rechtmäßige Verarbeitung und Rechteverwaltung. Es ist besonders nützlich, um Lücken in den aktuellen Praktiken zu identifizieren und Verbesserungen umzusetzen, sodass Lehrkräfte den Datenschutz sowohl in Online- als auch in Präsenzumgebungen sicher bewältigen können.

CHECKLISTE FÜR DEN ONLINE-UNTERRICHT

Vor der Einheit

Überprüfen Sie, ob alle verwendeten digitalen Plattformen (z. B. Videokonferenz-Tools,

TOOLS

RECHTLICHE ANFORDERUNGEN & VERANTWORTUNG

Online-Bewertungstests) mit der DSGVO konform sind, indem Sie deren Datenschutzrichtlinien und Datenschutzpraktiken überprüfen.

Holen Sie die ausdrückliche Zustimmung der Lernenden zur Erhebung und Verarbeitung ihrer personenbezogenen Daten ein (z. B. für Online-Anmeldungen, Bewertungsdaten usw.).

Sichern Sie den Zugriff auf Unterrichtsmaterialien, indem Sie Dateien mit einem Passwort schützen oder sichere Plattformen für den Austausch von Ressourcen verwenden.

Informieren Sie die Lernenden über ihre Datenschutzrechte, einschließlich ihres Rechts auf Zugriff auf ihre Daten und deren Löschung, und darüber, wie ihre Daten während des Kurses verwendet werden.

Während der Einheit

Verwenden Sie sichere Kommunikationsmittel (z. B. verschlüsselte E-Mails, passwortgeschützte Online-Foren), um sensible Informationen auszutauschen.

Stellen Sie sicher, dass die Interaktionen der Lernenden, Aufzeichnungen und Chat-Protokolle vertraulich behandelt werden und nur für relevante Parteien zugänglich sind.

Vermeiden Sie es, unnötige personenbezogene Daten zu erheben; fordern Sie nur das an, was für die Einheit erforderlich ist.

Nach der Einheit

Löschen Sie die Aufzeichnungen der Einheiten oder speichern Sie sie sicher und gewährleisten Sie, dass der Zugriff nur autorisiertem Personal vorbehalten ist.

Aktualisieren Sie die Unterlagen und stellen Sie sicher, dass die Zustimmung der Lernenden ordnungsgemäß dokumentiert ist.

Überprüfen und bewerten Sie regelmäßig die Datenverarbeitungsprozesse, um die kontinuierliche Einhaltung der DSGVO sicherzustellen.

TOOLS

DATENSCHUTZ & SICHERHEIT

Eine effektive Kommunikation und Transparenz in Bezug auf Datenschutz und Datensicherheit sind unerlässlich, um Vertrauen und Rechtskonformität im Bildungsbereich zu fördern. Da personenbezogene Daten zunehmend mit digitalem Lernen verflochten sind, müssen Lehrkräfte und Bildungseinrichtungen sicherstellen, dass die Lernenden darüber informiert sind, wie ihre Daten erfasst, verarbeitet und geschützt werden. Eine transparente Kommunikation hilft den Lernenden, ihre Rechte gemäß Datenschutzgesetzen wie der Datenschutz-Grundverordnung (DSGVO) zu verstehen, und stärkt das Vertrauen in das Engagement der Einrichtung für den Datenschutz.

Im Folgenden finden Sie einige Strategien für eine effektive Vermittlung von Datenschutz- und Sicherheitsfragen an Lernende.

AKTIVITÄT 1

Kommunikation und Transparenz: Kommunikation zu Datenschutz- und Sicherheitsfragen

- **DSGVO Artikel 12**: Transparente Informationen, Kommunikation und Modalitäten für die Ausübung der Rechte der betroffenen Person
- **DSGVO Artikel 13**: Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person
- **DSGVO Artikel 32**: Sicherheit der Verarbeitung

Szenario-Diskussion

Präsentieren Sie eine Situation, in der eine Lernende Bedenken hinsichtlich der während eines Online-Kurses gesammelten Daten äußert. Diskutieren Sie, wie Lehrkräfte diese Bedenken transparent ansprechen und gleichzeitig die Einhaltung der DSGVO gewährleisten sollten.

Rollenspiel-Aktivität

Lehrkräfte üben das Erklären von Datenschutzkonzepten wie Zustimmung und Datenspeicherung gegenüber Lernenden in einfacher und klarer Sprache.

TOOLS

DATENSCHUTZ & SICHERHEIT

Reflexionsübung

Bitten Sie die Lehrkräfte, ihre aktuellen Kommunikationspraktiken in Bezug auf den Datenschutz zu prüfen und Verbesserungsmöglichkeiten zu ermitteln.

Methodische Leitlinien

- Verwenden Sie **leicht verständliche Sprache**, wenn Sie Datenschutzthemen besprechen, um sicherzustellen, dass alle Lernenden die Inhalte verstehen. Transparenz ist entscheidend für den Aufbau von Vertrauen und die Einhaltung von Datenschutz- und Sicherheitsgesetzen.
- Teilen Sie **praktische Beispiele** für Datenschutzpraktiken innerhalb der Kursstruktur, z. B. wie Anwesenheitslisten sicher geführt werden.
- Integrieren Sie **Datenschutzdiskussionen** in den Lehrplan, um die Lernenden zu aktiven Beteiligten beim Schutz ihrer Daten zu machen.

Definitionen und Schlüsselbegriffe

- **Transparenz**: Die Praxis, Informationen über die Erhebung, Speicherung und Verwendung personenbezogener Daten offen zu teilen.
- **Datenschutzerklärung**: Ein Dokument, in dem dargelegt wird, wie eine Organisation personenbezogene Daten erhebt, verwendet und schützt.
- **Informierte Einwilligung**: Eindeutige Zustimmung von Personen, nachdem sie über die spezifischen Datenverarbeitungsaktivitäten informiert wurden.
- **Recht auf Information**: Das von der DSGVO vorgeschriebene Recht von Personen, zu erfahren, wie ihre Daten verarbeitet werden.
- **Meldung von Datenschutzverletzungen**: Die Verpflichtung, betroffene Parteien im Falle eines Datenschutzvorfalls unverzüglich zu benachrichtigen.

Beispiele/Fallstudien

- **Fallstudie 1**: Eine Universität führt ein neues Lernmanagementsystem ein, informiert die Studierenden jedoch nicht über die erhobenen Daten. Es kommt zu Beschwerden, die eine Überprüfung und öffentliche Erklärung der Datenschutzrichtlinien des Systems erforderlich machen.
- *Lektion*: Informieren Sie immer ausführlich über neue Tools und die damit verbundenen Datenerhebungsverfahren.

- **Fallstudie 2**: Ein Lehrer nutzt für den Unterricht eine Chat-Plattform und gibt dabei versehentlich persönliche Daten einer Schülerin weiter.

TOOLS

DATENSCHUTZ & SICHERHEIT

Die Schülerin meldet dies, woraufhin eine Schulung für Lehrkräfte zum Thema verantwortungsbewusste Kommunikation durchgeführt wird.

- *Lektion*: Beschränken Sie die Weitergabe personenbezogener Daten auf unbedingt notwendige Informationen.

- **Fallstudie 3**: Eine Institution stellt Lernenden unklare Datenschutzhinweise zur Verfügung. Nach einer juristischen Überprüfung werden die Hinweise in verständlicher Sprache neu formuliert, was zu mehr Zufriedenheit und Vertrauen bei den Lernenden führt.
- *Lektion*: Verwenden Sie in allen Mitteilungen zum Thema Datenschutz eine einfache und prägnante Sprache.

AKTIVITÄT 2

Förderung von Transparenz und Vertrauen bei der Datenverarbeitung

Ein Erwachsenenbildner sammelt im Rahmen einer Kursbewertung Daten von Lernenden über eine Online-Umfrageplattform. Die Lernenden äußern Bedenken über die mangelnde Klarheit darüber, wie ihre Antworten gespeichert, analysiert und weitergegeben werden. Einige Lernende zögern, teilzunehmen, und begründen dies mit Datenschutzbedenken und der möglichen missbräuchlichen Verwendung ihrer Daten.

Schritt-für-Schritt-Kommunikationsstrategien für mehr Transparenz

Schritt 1

Bieten Sie klare Erklärungen zur Datenerfassung

- Erläutern Sie klar und deutlich, warum Daten erhoben werden, wie sie verwendet werden und welche Vorteile dies für die Lernenden hat. Beginnen Sie die Umfrage beispielsweise mit einer Erklärung wie: „Diese Umfrage dient der Verbesserung der Kursqualität. Alle Antworten sind anonym und werden ausschließlich für Bildungszwecke verwendet."

Schritt 2

Verwenden Sie eine verständliche Sprache für Datenschutzrichtlinien

- Vermeiden Sie technischen Fachjargon, wenn Sie Lernenden Datenschutzrichtlinien erklären. Verwenden Sie stattdessen einfache Begriffe. Ersetzen Sie beispielsweise „Daten werden gemäß Artikel 6 der DSGVO verarbeitet und gespeichert" durch „Ihre Daten werden sicher gespeichert und ausschließlich zur Verbesserung Ihrer Lernerfahrung verwendet".

TOOLS

DATENSCHUTZ & SICHERHEIT

Schritt 3
Holen Sie vor der Datenerhebung ausdrückliche Zustimmung ein

- Bitten Sie die Lernenden um ihre Zustimmung in einem einfachen Opt-in-Format. Fügen Sie beispielsweise ein Kontrollkästchen mit dem Hinweis „Ich stimme der Teilnahme an dieser Umfrage zu und verstehe, wie meine Antworten verwendet werden“ ein.

Schritt 4
Ermutigen Sie zu Fragen und Diskussionen zum Thema Datenschutz

- Legen Sie fest, wie lange Daten gespeichert werden, und stellen Sie sicher, dass nicht mehr benötigte Daten nach Erfüllung ihres Zwecks gelöscht werden.

Schritt 5
Betonen Sie die Rechte der Lernenden

- Heben Sie die Rechte der Lernenden auf Zugriff auf, Korrektur oder Löschung ihrer Daten hervor. Verteilen Sie beispielsweise einen einseitigen Leitfaden, in dem diese Rechte und Kontaktinformationen für weitere Unterstützung zusammengefasst sind.

Schritt 6
Sorgen Sie für Transparenz bei Tools von Drittanbietern

- Informieren Sie die Lernenden, wenn Plattformen von Drittanbietern für die Datenerfassung oder -speicherung verwendet werden, und erklären Sie, wie diese Plattformen die Datenschutzbestimmungen einhalten. Beispiel: „Wir verwenden [Umfrageplattform], die mit der DSGVO konform ist, sodass die sichere Speicherung Ihrer Daten gewährleistet ist.“

Schritt 7
Informieren Sie regelmäßig über Updates und Änderungen bei der Handhabung von Daten

- Informieren Sie die Lernenden über alle Änderungen der Richtlinien zur Datenerfassung oder -speicherung. Versenden Sie beispielsweise eine kurze E-Mail mit einer Zusammenfassung der Updates, z. B.: „Wir haben unsere Datenspeicherungspraktiken verbessert, um Ihre Privatsphäre noch besser zu schützen.“

TOOLS

DATENSCHUTZ & SICHERHEIT

AKTIVITÄT 3

Förderung des Bewusstseins und Engagements der Lernenden im Bereich Datenschutz

Während eines Online-Kurses müssen die Lernenden Benutzerkonten auf einer kollaborativen Plattform erstellen, um an Diskussionen teilnehmen zu können. Einige Lernende äußern Bedenken hinsichtlich der Weitergabe persönlicher Daten und ihrer Möglichkeiten, die Verwendung ihrer Daten zu kontrollieren. Eine Lernende fragt, ob sie ihr Konto und die damit verbundenen Daten nach Abschluss des Kurses löschen kann.

Sechs wichtige Schritte zur Einbindung der Lernenden in das Thema Datenschutz

Schritt 1

Transparenz bei der Registrierung und Datennutzung

- Kommunizieren Sie klar und deutlich, warum personenbezogene Daten erfasst werden und wie sie verwendet werden. Fügen Sie beispielsweise zu Beginn des Kurses einen Hinweis wie den folgenden ein: „Ihre Kontodaten sind für die Teilnahme an diesem Kurs erforderlich. Wir versichern Ihnen, dass Ihre Daten ohne Ihre Zustimmung nicht weitergegeben werden.“

Schritt 2

Fördern Sie das Bewusstsein für die Rechte der Lernenden

- Informieren Sie die Lernenden über ihre Rechte gemäß der DSGVO, wie z. B. Datenzugriff, -korrektur und -löschung. Stellen Sie beispielsweise eine einseitige Zusammenfassung der Rechte gemäß der DSGVO zur Verfügung oder widmen Sie eine kurze Einheit der Erörterung dieser Rechte.

Schritt 3

Stellen Sie klare Opt-out-Optionen bereit

- Stellen Sie sicher, dass Lernende sich von optionalen Aktivitäten mit Datenaustausch, beispielsweise der Teilnahme an öffentlichen Diskussionen, abmelden können. Verwenden Sie beispielsweise Kontrollkästchen, damit Lernende entscheiden können, ob ihr Profil für andere Nutzer:innen auf einer Plattform sichtbar ist.

Schritt 4

Fördern Sie die Beteiligung der Lernenden an Datenpraktiken

- Beziehen Sie die Lernenden in Diskussionen darüber

DATENSCHUTZ & SICHERHEIT

ein, wie mit ihren Daten umgegangen wird, und fördern Sie so ihr Verantwortungsbewusstsein und ihr Verständnis. Organisieren Sie beispielsweise eine Gruppenaktivität, bei der die Lernenden eine hypothetische Richtlinie zur Datenweitergabe bewerten und Verbesserungsvorschläge machen.

Schritt 5

Optimieren Sie die Datenlöschungsprozesse

- Make it easy for learners to request the deletion of their accounts and associated data. Share instructions, such as: "To request the deletion of your account, please email [support@institution.com] with your account details. Your request will be processed within 14 days."

Schritt 6

Bauen Sie praktische Übungen zu Datenschutzkonzepten ein

- Nutzen Sie interaktive Aktivitäten, um die Bedeutung von Datenschutz und Datensicherheit zu verdeutlichen. Erstellen Sie beispielsweise ein Quiz zu Datenschutzszenarien oder diskutieren Sie reale Beispiele für Verstöße gegen die DSGVO und deren Folgen.

Beispiele/Fallstudien

Fallstudie 1: In einem Kurs wurde während der Einführungsphase das Modul „Datenschutz 101" vorgestellt, das Videos und Infografiken zur DSGVO umfasste. Die Lernenden gaben an, dass sie nach dem Kurs mehr Selbstvertrauen im Umgang mit ihren Daten hätten.

Fallstudie 2: Eine Lehrerin organisiert eine simulierte Debatte, in der die Lernenden für und gegen die Weitergabe bestimmter Arten personenbezogener Daten im Bildungsbereich argumentieren. Die interaktiven, diskussionsbasierten Aktivitäten regen zum kritischen Nachdenken über Datenrechte und -pflichten an.

Fallstudie 3: Eine Lernplattform verfügt über die Schaltfläche „Meine Daten löschen", die den Prozess der Datenlöschungsanfrage automatisiert. Die Lernenden begrüßen die Transparenz und die einfache Kontrollmöglichkeit.

DATENSCHUTZ & SICHERHEIT

CHECKLISTE FÜR DIE EINBINDUNG VON LERNENDEN IN DATENSCHUTZFRAGEN

Vor der Einheit

- *Erstellen Sie Schulungsmaterialien, die die Grundsätze der DSGVO und die Rechte der Lernenden erläutern (z. B. Infografiken, kurze Videos oder Folien).*
- *Informieren Sie bei der Kursanmeldung klar über die Richtlinien zur Datennutzung und geben Sie an, wie Daten gespeichert, verwendet und geschützt werden.*
- *Stellen Sie den Lernenden Opt-in-Zustimmungsformulare für Aktivitäten zur Verfügung, mit denen eine Datenverarbeitung einhergeht, wie beispielsweise die Aufzeichnung von Unterrichtseinheiten oder die Weitergabe von durch die Lernenden erstellten Inhalten.*
- *Richten Sie für Kursmaterialien und -aktivitäten sichere Plattformen mit Verschlüsselung und passwortgeschütztem Zugang ein.*

Während der Einheit

- *Wiederholen Sie zu Beginn der Einheit die Rechte der Lernenden und stellen Sie sicher, dass sie verstehen, wie sie Zugriff auf ihre Daten oder deren Löschung beantragen können.*
- *Moderieren Sie Diskussionen oder Aktivitäten, um die Lernenden dazu anzuregen, sich mit ihren Rechten und Pflichten im Bereich Datenschutz auseinanderzusetzen.*
- *Vermeiden Sie es, sensible Informationen in Gruppengesprächen weiterzugeben, außer wenn dies ausdrücklich erforderlich ist und alle Beteiligten damit einverstanden sind.*
- *Minimieren Sie die Datenerfassung, indem Sie nur die für die Teilnahme an der Einheit erforderlichen Informationen anfordern.*

Nach der Einheit

- *Stellen Sie den Lernenden im Anschluss Ressourcen zu den Rechten und Praktiken der DSGVO zur Verfügung (z. B. Links zu hilfreichen Artikeln oder Leitfäden).*
- *Bearbeiten Sie Datenanfragen umgehend, z. B.*

TOOLS

DATENSCHUTZ & SICHERHEIT

Anfragen zur Löschung oder Korrektur von Daten.

Prüfen Sie die gesammelten Daten und löschen Sie alle Informationen, die für Bildungszwecke nicht mehr erforderlich sind.

Dokumentieren Sie Ihre Zustimmungs- und Compliance-Maßnahmen, um Ihre Einhaltung der DSGVO-Grundsätze nachzuweisen.

UNTERSTÜTZUNG VON LEHRKRÄFTEN BEI DER EINBINDUNG VON LERNENDEN IN DEN DATENSCHUTZ

Stärkung der nächsten Generation
Zehn Regeln für den Online-Datenschutz

Diese Ressource, die von Expert:innen aus den Bereichen Bildung und Datenschutz entwickelt wurde, bietet Lehrkräften praktische Tools und Strategien, um Datenschutz effektiv zu vermitteln. Sie enthält Unterrichtspläne, interaktive Aktivitäten und Fallstudien, die den Lernenden dabei helfen, die Bedeutung des Datenschutzes in einer digitalen Welt zu verstehen. Das Tool steht im Einklang mit den Grundsätzen der DSGVO und konzentriert sich auf wichtige Themen wie Zustimmung, Transparenz und sichere Datenpraktiken. Mit dieser Ressource können Lehrkräfte die Lernenden dazu befähigen, fundierte Entscheidungen über ihre Online-Präsenz und den Datenschutz zu treffen.

Verbesserung des Datenschutzes im Bildungswesen
Die Compliance-Checkliste für Schulen

Diese Ressource, die von der Education Authority Northern Ireland (EA NI) bereitgestellt wird, ist speziell darauf zugeschnitten, Schulen und Lehrkräfte bei der Einhaltung der DSGVO im Bildungsbereich zu unterstützen. Sie bietet detaillierte Anleitungen zum Schutz personenbezogener Daten, zum Umgang mit Datenschutzverletzungen, zur Bearbeitung von Anfragen betroffener Personen und zur Umsetzung sicherer Datenverarbeitungsverfahren. Darüber hinaus enthält das Tool Vorlagen und Checklisten, die Schulen beim Aufbau eines robusten Datenschutzrahmens unterstützen. Es ist eine unverzichtbare Referenz für die Förderung von Transparenz, die Gewährleistung einer rechtmäßigen Datenverarbeitung und die Förderung einer Kultur der Verantwortlichkeit in Bildungseinrichtungen.

ZUGANG, REGISTRIERUNG, VERWALTUNG

Die Registrierung der Lernenden und die Benutzerverwaltung sind wesentliche Prozesse in jedem Bildungssystem, insbesondere auf Online-Lernplattformen oder in Einrichtungen, die verschiedene Kurse und Programme anbieten. Diese Prozesse gewährleisten, dass sich die Lernenden erfolgreich für Kurse anmelden können und dass die Administrator:innen ihre Profile und den Zugriff auf verschiedene Ressourcen effizient verwalten können.

Adult Education Programme
Perspektive der Nutzer:innen: How to register and Enrol on our new website

Dieses Video-Tutorial bietet einen umfassenden Überblick über eine neu gestartete Website für das Erwachsenenbildungsprogramm. Die Moderatorin erklärt die Funktionen der Website und den Registrierungsprozess und konzentriert sich dabei darauf, die Benutzererfahrung auf Grundlage des Feedbacks von Lernenden einfacher und effizienter zu gestalten.

Adult Education Programme
Perspektive der Administrator:innen: How to register a new adult student

In diesem Video wird den Zuschauer:innen gezeigt, wie ein:e Moderator:in eine:n neue:n erwachsene:n Nutzer:in für das Musical Ladder Portal registrieren und einladen kann. Das Video demonstriert Schritt für Schritt, wie ein Konto für erwachsene Lernende eingerichtet wird, damit diese auf alle Funktionen und Tools des Portals zugreifen können. Es enthältAnleitung dazu, wie man eine Einladung an den:die neue:n Nutzer:in sendet und ihn:sie durch den Registrierungsprozess führt, um sicherzustellen, dass er:sie bereit ist, seine:ihre musikalische Reise zu beginnen. Die Zuschauer:innen werden dazu ermutigt, den Kanal zu abonnieren, um über alle neuen Funktionen und Verbesserungen des Musical Ladder Portals auf dem Laufenden zu bleiben.

Das Beispiel konzentriert sich zwar auf den Bereich Musik, die im Video gezeigten theoretischen Tipps sind jedoch ebenso relevant für die breitere Funktionalität des Tools im Bereich „Benutzerverwaltung“.

TOOLS

ZUGANG, REGISTRIERUNG, VERWALTUNG

LEITFADEN ZU ANMELDEFORMULAREN FÜR BILDUNGSPROGRAMME

Bewährte Praktiken

Genaue Informationen sind entscheidend:

- Stellen Sie sicher, dass alle Felder mit genauen und aktuellen Informationen ausgefüllt sind. Fehler bei grundlegenden Angaben wie Ihrem Namen, Ihrem Geburtsdatum oder Ihren Kontaktdaten können Ihre Anmeldung oder die Kommunikation mit der Einrichtung verzögern.

Kontrollieren Sie Ihre Kontaktdaten:

- Überprüfen Sie, ob Ihre Kontaktdaten korrekt sind. So kann die Einrichtung Sie bei Bedarf erreichen.

Geben Sie Ihren vollständigen Bildungsweg an:

- Machen Sie ehrliche Angaben zu Ihrem höchsten Bildungsabschluss. Dies hilft den Lehrkräften dabei, den Unterricht auf Ihren akademischen Hintergrund abzustimmen.

Geben Sie besondere Bedürfnisse oder erforderliche Anpassungen an:

- Falls Sie körperliche oder lernbezogene Behinderungen haben, geben Sie dies bitte auf dem Formular an. So kann die Einrichtung die erforderlichen Anpassungen und Unterstützung bereitstellen.

Respektieren Sie die Vertraulichkeit:

- Beachten Sie, dass Ihre personenbezogenen Daten durch Datenschutzgesetze (DSGVO) geschützt sind. Die Einrichtung darf Daten nur im Rahmen der Programmevaluierung oder an Prüfungsorganisationen weitergeben.

Praktische Tipps

Name und Kontaktdaten:

- Tipp: Verwenden Sie immer Ihren vollständigen Namen und stellen Sie sicher, dass alle Kontaktdaten (E-Mail-Adresse, Telefonnummer und Notfallkontakt) korrekt sind. Wenn Sie Probleme mit Ihren Kontaktdaten haben, wenden Sie sich an den Helpdesk der Einrichtung.

TOOLS

ZUGANG, REGISTRIERUNG, VERWALTUNG

Bildungsstand:

- Tipp: Machen Sie ehrliche Angaben zu Ihrem Bildungsstand. Auch wenn Sie Ihre Ausbildung außerhalb der USA abgeschlossen haben, geben Sie diese Informationen an. Wenn Sie sich über Ihren höchsten Abschluss oder Grad nicht sicher sind, sehen Sie in Ihren Zeugnissen oder Diplomen nach.

Arbeitsstatus:

- Tipp: Seien Sie bei der Angabe Ihres Arbeitsstatus ehrlich hinsichtlich Ihrer aktuellen Beschäftigungssituation. Unabhängig davon, ob Sie beschäftigt sind, Arbeit suchen oder nicht arbeiten, kann die Einrichtung so Ihre Verfügbarkeit und Ihren Unterstützungsbedarf besser einschätzen.

Spezielle Anpassungen:

- Tipp: Wenn Sie eine Behinderung haben, füllen Sie den Abschnitt aus, in dem um Anpassungen gebeten werden kann. Dabei kann es sich um zusätzliche Zeit für Aufgaben oder Hilfsmittel für Barrierefreiheit handeln. Geben Sie genau an, welche Anpassungen Sie benötigen.

Datenschutz:

- Tipp: Lesen Sie den Abschnitt zur Vertraulichkeit sorgfältig durch. Sie werden gebeten, Ihre Zustimmung zur Verwendung Ihrer Daten für Programmevaluierungs- und Testzwecke zu geben. Dadurch wird sichergestellt, dass Ihre Daten geschützt sind, aber auch, dass Ihre Fortschritte nachverfolgt werden können und Ihnen die bestmögliche Lernerfahrung geboten wird.

Abschließende Unterschriften:

- Tipp: Überprüfen Sie vor dem Absenden das gesamte Formular auf Vollständigkeit. Vergewissern Sie sich, dass Sie alle Felder korrekt ausgefüllt und an den erforderlichen Stellen unterschrieben haben. So vermeiden Sie Verzögerungen bei der Bearbeitung Ihrer Anmeldung.

CHECKLISTE FÜR VERWALTUNG UND REGISTRIERUNG

Stellen Sie sicher, dass der Registrierungsprozess mit der DSGVO konform ist, indem Sie nur die erforderlichen personenbezogenen Daten erfassen.

TOOLS

ZUGANG, REGISTRIERUNG, VERWALTUNG

Stellen Sie den Lernenden einen klaren Datenschutzhinweis zur Verfügung, in dem erklärt wird, wie ihre Daten verwendet und gespeichert werden.

Holen Sie von den Lernenden eine dokumentierte Einwilligung zur Verwendung ihrer Daten ein, einschließlich aller Medien (z. B. Fotos, Videos), die während des Unterrichts geteilt werden.

Verwenden Sie eine sichere Online-Plattform für die Verwaltung der Konten der Lernenden und der Zugriffsberechtigungen.

Richten Sie einen rollenbasierten Zugriff ein, um die Administratorrechte auf autorisiertes Personal zu beschränken.

Richten Sie Passwortrichtlinien ein, die sichere Passwörter vorschreiben, und ermutigen Sie die Lernenden, diese regelmäßig zu aktualisieren.

Überprüfen und aktualisieren Sie regelmäßig die Angaben in den Konten der Lernenden, um die Richtigkeit und Relevanz der Daten zu gewährleisten.

Deaktivieren Sie die Konten von Lernenden, die nicht mehr eingeschrieben sind oder ihren Kurs abgeschlossen haben.

Verwenden Sie verschlüsselte Speicherlösungen für sensible Daten der Lernenden, wie z. B. Ausweisdokumente.

Geben Sie den Lernenden auf Anfrage Zugriff auf ihre Daten und die Möglichkeit, ihre Informationen zu aktualisieren oder zu löschen.

Informieren Sie die Lernenden über ihre Rechte in Bezug auf ihre Daten sowie über die Schritte, die sie unternehmen können, um Datenschutzbedenken zu melden.

Erstellen Sie eine Sicherungskopie der Registrierungsdaten der Lernenden und bewahren Sie diese gemäß den Richtlinien zur Datenspeicherung sicher auf.

AKTIVITÄT 1

Fallstudien-Diskussionen

Präsentieren Sie eine Fallstudie, in der Nutzerdaten

TOOLS

ZUGANG, REGISTRIERUNG, VERWALTUNG

während des Registrierungsprozesses unsachgemäß behandelt wurden. Lassen Sie die Teilnehmer:innen die potenziellen Risiken diskutieren und wie diese durch geeignete Datenschutzmaßnahmen hätten vermieden werden können.

Rollenspiel

Teilen Sie die Teilnehmer:innen in Paare ein, wobei eine:r als Administrator:in und der:die andere als Schüler:in fungiert. Der:Die Administrator:in erklärt während des Anmeldeprozesses die Datenschutzrichtlinien und stellt sicher, dass der:die Schüler:in versteht, welche Daten erfasst werden und wie sie verwendet werden.

Methodischer Leitfaden: Förderung der aktiven Beteiligung

Beziehen Sie die Lernenden in Diskussionen über reale Szenarien ein, damit sie darüber reflektieren, wie Datenschutzgrundsätze in der Erwachsenenbildung angewendet werden. Ermutigen Sie sie, Erfahrungen aus ihren eigenen Institutionen auszutauschen.

Vereinfachen Sie komplexe Konzepte

Datenschutzgesetze können komplex sein. Zerlegen Sie die wichtigsten Grundsätze (wie Zustimmungserklärung, Datenspeicherung und Zugriffsrechte) in einfache, verständliche Begriffe. Verwenden Sie Beispiele aus der täglichen Arbeit in der Erwachsenenbildung, um diese Konzepte zu verdeutlichen.

Fördern Sie die gemeinschaftliche Problemlösung

Nutzen Sie Gruppenübungen, um die Zusammenarbeit zu fördern. Lassen Sie die Lernenden beispielsweise eine Checkliste zum Datenschutz für den Benutzerverwaltungsprozess in ihrer eigenen Einrichtung entwickeln.

Zur Erinnerung

Die Einwilligung gemäß DSGVO muss freiwillig, spezifisch, informiert und eindeutig sein. Das bedeutet, dass Nutzer:innen aktiv der Verarbeitung ihrer Daten zustimmen müssen und nicht nur darüber informiert werden dürfen.

Definitionen und Schlüsselbegriffe:

Benutzerverwaltung

Der Prozess der Verwaltung von Benutzerkonten und personenbezogenen Daten innerhalb eines Systems, einschließlich Registrierung, Aktualisierung und Löschung.

Datenverarbeitung

Die Erhebung, Speicherung, Verarbeitung und

TOOLS

ZUGANG, REGISTRIERUNG, VERWALTUNG

Weitergabe personenbezogener Daten.

Datenschutz
Schutz personenbezogener Daten vor unbefugtem Zugriff, unbefugter Nutzung und unbefugter Weitergabe.

Zustimmung
Ein Schlüsselelement der DSGVO, das sich auf die freiwillige Einwilligung einer betroffenen Person in die Verarbeitung ihrer personenbezogenen Daten bezieht.

Datenschutzverletzung
Ein Vorfall, bei dem personenbezogene Daten unbefugt eingesehen, weitergegeben oder vernichtet werden.

Datenaufbewahrung
Die Datenaufbewahrung bezieht sich darauf, wie lange personenbezogene Daten aufbewahrt werden. Die Institutionen sollten klare Aufbewahrungsfristen für Daten festlegen und sicherstellen, dass personenbezogene Daten nur so lange gespeichert werden, wie es für den Zweck, für den sie erhoben wurden, erforderlich ist.

Beispiele/ Fallstudien

Fallstudie 1: DSGVO-Konformität bei der Anmeldung
Eine Volkshochschule führt ein Online-Anmeldesystem ein, bei dem die Lernenden die Datenschutzrichtlinie lesen und ihr zustimmen müssen, bevor sie ihre Anmeldeformulare einreichen. Dadurch wird sichergestellt, dass das Zentrum die DSGVO-Anforderung einer informierten Zustimmung erfüllt.

Fallstudie 2: Umgang mit sensiblen Daten in einer sicheren Umgebung - Ein Berufsbildungsanbieter verwendet eine sichere, verschlüsselte Datenbank, um die Anmeldedaten der Lernenden zu speichern. Nur befugtes Personal kann auf die Daten zugreifen, und die Lernenden werden über ihre Rechte informiert, auf ihre Daten zuzugreifen, sie zu aktualisieren oder auf Anfrage zu löschen.

TOOLS

SICHERHEIT IN BILDUNGSTECH-NOLOGIE

Die rasche Einführung von Bildungstechnologien (EdTech) in Schulen und Einrichtungen hat die Lehr- und Lernerfahrung verändert. Sie hat jedoch auch erhebliche Herausforderungen in Bezug auf Datenschutz und Sicherheit mit sich gebracht. Dieses Thema konzentriert sich auf die Identifizierung, Bewertung und Abschwächung von Risiken, die mit der Nutzung digitaler Tools und Plattformen im Bildungsbereich verbunden sind. Durch die Förderung der Aufklärung und des Bewusstseins für den Datenschutz und die Sicherheit können Schulen und Einrichtungen fundierte Entscheidungen über die Integration von Technologien treffen und dabei den Schutz der Daten ihrer Gemeinschaft in den Vordergrund stellen.

UNESCO-Leitfaden zum Datenschutz beim Online-Lernen

Die UNESCO bietet ein umfassendes Handbuch mit dem Titel "Personal Data and Privacy Protection in Online Learning": Leitfaden für Schüler. Lehrer und Eltern". Diese Ressource bietet Strategien zum Schutz persönlicher Daten vor, während und nach Online-Lernsitzungen.

Der iKeepSafe-Lehrplan zum Datenschutz

Die Internet Keep Safe Coalition (iKeepSafe) hat einen Lehrplan entwickelt, der sich auf den Datenschutz in der Bildung konzentriert. Es befasst sich mit Bedenken im Zusammenhang mit der Nutzung von Bildungstechnologien und bietet Anleitungen zum Schutz persönlicher Daten von Schülern.

SPADATAS Projekt

Das SPADATAS-Projekt zielt darauf ab, das Bewusstsein für die Fragilität von Daten im Bildungsbereich zu schärfen. Es bietet Werkzeuge und Rahmenbedingungen für den Schutz der Privatsphäre, der Sicherheit und der Vertraulichkeit von Schülerdaten, die den Schulen helfen, die Auswirkungen datengestützter Entscheidungen zu verstehen.

TOOLS

SICHERHEIT IN BILDUNGSTECH-NOLOGIE

eLearning-Industrie zum Datenschutz

Ein Artikel mit dem Titel „Datenschutz und Sicherheit beim eLearning“ erörtert die Bedeutung des Datenschutzes bei eLearning-Plattformen. Er skizziert Schritte und bewährte Verfahren, um die Sicherheit und Integrität dieser Plattformen zu gewährleisten.

Privacy is key: Holding EdTech accountable

Common Sense Media bewertet beliebte EdTech-Plattformen hinsichtlich der Sicherheit und des Schutzes der Privatsphäre von Schülern. Ihre Erkenntnisse helfen Pädagogen und Eltern, fundierte Entscheidungen über die von ihnen verwendeten Tools zu treffen.

Einschlägige Vorschriften/Normen

***ISO/IEC 27001**: Eine internationale Norm für Informationssicherheits-Managementsysteme, die einen Rahmen für die Verwaltung der Datensicherheit in digitalen Werkzeugen bietet.*

Übung zur Analyse der Datenschutzrisiken

Lehrkräfte bewerten ein bestimmtes Bildungsinstrument, identifizieren potenzielle Datenschutzrisiken und schlagen Abhilfemaßnahmen vor.
Beispielhafte Aufforderungen: "Erfasst dieses Tool unnötige persönliche Informationen? Wie werden die Daten der Lernenden gespeichert und weitergegeben?"

Diskussion der Fallstudie
Analysieren Sie ein reales Beispiel einer Datenschutzverletzung im Bildungswesen und diskutieren Sie, wie diese hätte verhindert werden können.

Methodischer Leitfaden:
Ermutigung zu offenen Diskussionen über das Gleichgewicht zwischen technologischem Nutzen und Bedenken hinsichtlich der Privatsphäre.

SICHERHEIT IN BILDUNGSTECH-NOLOGIE

Verwenden Sie visuelle Hilfsmittel (z. B. Infografiken), um komplexe Vorschriften für die Lernenden zu vereinfachen.

Bieten Sie reale Szenarien an, um theoretisches Wissen mit praktischen Anwendungen zu verbinden.

Definitionen und Schlüsselbegriffe

Datenverschlüsselung
Eine Methode zur Sicherung von Informationen durch Umwandlung in einen Code, um unbefugten Zugriff zu verhindern.

Phishing
Eine Cyberattacke, bei der Personen dazu verleitet werden, persönliche Daten preiszugeben.

Beispiele/Fallstudien

Fallstudie 1: Eine Volkshochschule führte ein Lernmanagementsystem (LMS) ein, ohne die Richtlinien zur gemeinsamen Nutzung von Daten zu überprüfen. Nach einer Datenpanne, bei der persönliche Daten von Lernenden preisgegeben wurden, sah sich die Einrichtung mit rechtlichen Schritten konfrontiert und verlor das Vertrauen der Lernenden. Dies verdeutlicht die Notwendigkeit einer gründlichen Überprüfung der Technologie und der Einhaltung der Vorschriften.

TOOLS

SPEICHERUNG UND VERARBEITUNG

1. SICHERE POSTDIENSTE

Sichere E-Mail-Dienste wie ProtonMail und Tutanota schützen die E-Mail-Kommunikation mit einer starken Verschlüsselung, die sicherstellt, dass sensible Informationen, die per E-Mail ausgetauscht werden, vertraulich bleiben. Diese Dienste beinhalten oft eine Ende-zu-Ende-Verschlüsselung und sichere Server zum Schutz der Kommunikation. Dieses Sicherheitsniveau ist für Bildungseinrichtungen, in denen häufig sensible Daten ausgetauscht werden, von entscheidender Bedeutung. Durch die Nutzung dieser Dienste können Lehrkräfte die Vertraulichkeit und Integrität der E-Mail-Kommunikation wahren.

- PROTON MAIL
- TUTANOTA

2. SICHERE DATEIFREIGABE

Sichere Plattformen für die gemeinsame Nutzung von Dateien wie Tresorit, Sync und Google Workspace (mit entsprechenden Zugangskontrollen) ermöglichen die sichere Verteilung von Lernmaterialien mit sensiblen Informationen. Diese Plattformen bieten Verschlüsselung und sichere Zugriffskontrollen, die sicherstellen, dass nur autorisierte Nutzer auf freigegebene Dateien zugreifen können. Durch den Einsatz dieser Plattformen können Lehrkräfte sensible Daten schützen, während sie mit Kollegen zusammenarbeiten oder Ressourcen mit Lernenden teilen. Dadurch wird die Datensicherheit erhöht und die Einhaltung der Datenschutzbestimmungen gewährleistet.

- TRESORIT
- SYNC
- GOOGLE WORKSPACE

TOOLS

SPEICHERUNG UND VERARBEITUNG

3. LMS-SYSTEME MIT SICHERHEIT

Lernmanagementsysteme (LMS) wie Moodle und Canvas bieten robuste Sicherheitsfunktionen wie rollenbasierte Zugangskontrollen, Aktivitätsprotokollierung und Verschlüsselung aller gespeicherten Daten. Diese Funktionen stellen sicher, dass nur befugte Nutzer auf sensible Informationen zugreifen können und die Datenintegrität und Vertraulichkeit innerhalb des LMS gewahrt bleibt. Durch den Einsatz dieser Systeme können Lehrkräfte Lernmaterialien sicher verwalten und die Aktivitäten der Lernenden verfolgen, während gleichzeitig sensible Daten geschützt werden. Dies trägt zur Aufrechterhaltung einer sicheren Lernumgebung bei.

MOODLE CANVAS

4. SFTP FÜR SICHERE DATEIÜBERTRAGUNGEN

Secure File Transfer Protocol (SFTP) Tools wie FileZilla und WinSCP gewährleisten eine sichere Dateiübertragung bei der gemeinsamen Nutzung oder Übermittlung von Aufgaben. SFTP verschlüsselt die Daten während der Übertragung und verringert so das Risiko des Abfangens von Daten oder des unbefugten Zugriffs. Mithilfe dieser Tools können Lehrkräfte Dateien sicher mit Lernenden oder Kollegen austauschen und dabei die Vertraulichkeit und Integrität sensibler Informationen wahren. Dies ist wichtig, um die Daten der Lernenden bei der Übertragung von Dateien zu schützen.

FILEZILLA WINSCP

5. TOOLS FÜR DIE AUFBEWAHRUNG UND LÖSCHUNG VON DATEN

Tools zur Datenaufbewahrung und -löschung

TOOLS

SPEICHERUNG UND VERARBEITUNG

wie BleachBit und Eraser löschen die Daten von Lernenden sicher, wenn sie nicht mehr benötigt werden, und gewährleisten so die Einhaltung von Richtlinien zur Datenaufbewahrung. Diese Tools überschreiben Daten mehrfach, so dass sie nicht wiederherstellbar sind und das Risiko eines unbefugten Zugriffs verringert wird. Durch den Einsatz dieser Tools können Bildungseinrichtungen die Datensicherheit aufrechterhalten und die gesetzlichen Vorschriften zur Datenentsorgung einhalten. Dies trägt dazu bei, potenzielle Datenschutzverletzungen zu verhindern und die Einhaltung von Vorschriften zu gewährleisten.

BLEACH BIT

ERASER

6. TOOLS ZUR SICHERUNG UND WIEDERHERSTELLUNG

Regelmäßige Sicherungs- und Wiederherstellungspläne mit Tools wie Acronis und Veeam stellen sicher, dass die Daten der Lernenden sicher gesichert sind und im Falle eines Datenverlusts oder Systemausfalls wiederhergestellt werden können. Diese Tools bieten robuste Backup-Lösungen, die die Datenintegrität und -verfügbarkeit aufrechterhalten und so die Kontinuität der Institution gewährleisten. Durch die Implementierung dieser Pläne können Lehrkräfte wichtige Daten schützen und sich schnell von möglichen Störungen erholen. Dies trägt dazu bei, die Stabilität des Bildungsbetriebs aufrechtzuerhalten.

ACRONIS

VEEAM

TOOLS

DATEN-BEHANDLUNG & -SICHERHEIT

BEWÄLTIGUNG DER HERAUSFORDERUNGEN DES DATENSCHUTZES

Praktische Schritte zur Bewältigung der wichtigsten Herausforderungen beim Umgang mit dem Datenschutzrecht

Der CST-Blogartikel beleuchtet Strategien für Schulen zur Bewältigung von Datenschutzherausforderungen, die sich eng an der Erwachsenenbildung zum Thema Datenschutz orientieren. Er befasst sich mit häufigen Problemen wie der Beantwortung von Anfragen zum Thema Datenschutz (Subject Access Requests, SARs), dem sicheren Umgang mit Daten und der Eindämmung von Cyber-Bedrohungen - wichtige Anliegen in Bildungseinrichtungen. Schulen werden ermutigt, ihr Personal zu schulen, Daten sicher zu speichern und Cybersicherheitspraktiken einzuführen, die als praktische Beispiele für die Sensibilisierung erwachsener Lernender für den Datenschutz dienen. Diese Erkenntnisse unterstützen den Aufbau eines soliden Datenschutzbewusstseins in Bildungseinrichtungen.

Schulung zum Thema Datenschutz und Privatsphäre

Das Video mit dem Titel „Schulung zu Datenschutz und Privatsphäre - Lektion 1“ ist eine pädagogische Ressource, die die Komplexität des Datenschutzes und der Datenschutzpolitik erklären soll. Sie wurde vom Synthesia-Team erstellt und soll diese manchmal schwierigen Themen vereinfachen und klären.

Sicherheit im Internet

Dieses Video enthält praktische Tipps für die Sicherheit bei der Erkundung des Internet. Es wird betont, wie wichtig es ist, mit den online ausgetauschten Informationen vorsichtig umzugehen, und es werden Hinweise gegeben, wie man sich vor möglichen Online-Risiken schützen kann. Ziel ist es, das Bewusstsein für Online-Sicherheitspraktiken zu schärfen und einen verantwortungsvollen Umgang mit dem Internet zu fördern.

TOOLS

DATEN-BEHANDLUNG & -SICHERHEIT

Die Daten im Blick: Schutz der Privatsphäre und der Sicherheit der Lernenden

Der UNESCO-Bericht "Minding the Data: Protecting Learners' Privacy and Security" untersucht das Gleichgewicht zwischen der Nutzung von Bildungsdaten für Verbesserungen und dem Schutz der Privatsphäre von Schülern. Er hebt die Risiken des Datenmissbrauchs hervor, fordert eine solide Datenschutzpolitik und fördert die Zusammenarbeit bei der Entwicklung internationaler Strategien. Diese Ressource ist besonders wichtig für die Sensibilisierung von Lehrenden und Lernenden für den Datenschutz in digitalen Bildungsumgebungen.

CHECKLISTE

Sicherstellung des Online-Unterrichts:

Vergewissern Sie sich, dass die verwendete digitale Plattform mit der DSGVO übereinstimmt, indem Sie die Datenschutzrichtlinien der Plattform hinsichtlich der Datenverarbeitung überprüfen.

Einrichten eines Passwortschutzes oder von Zugangsbeschränkungen für Lehrmaterial für einen sicheren Zugang

Vergewissern Sie sich der dokumentierten Zustimmung der Lernenden, wenn Sie Fotos von der Unterrichtsstunde machen wollen.

Wählen Sie sichere Kommunikationskanäle für den Austausch von Details der Sitzung

Vorbereitung für eine sichere Online-Lehrveranstaltung

Wählen Sie eine vertrauenswürdige Plattform (z. B. Zoom, Microsoft Teams) und machen Sie sich mit den Grundeinstellungen vertraut.

Stellen Sie sicher, dass Ihre Internetverbindung sicher ist, und vermeiden Sie die Nutzung öffentlicher

Wi-Fi Aktualisieren Sie Ihr Gerät mit den neuesten Sicherheits-Patches und installieren Sie Antiviren-Software

TOOLS

DATEN-BEHANDLUNG & -SICHERHEIT

Einrichten eines passwortgeschützten Meeting-Links, um den Zugang auf autorisierte Teilnehmende zu beschränken

Planen Sie, nur das Minimum an notwendigen Informationen von den Teilnehmern zu erheben (z. B. Vornamen oder Aliasnamen)

Bereiten Sie Unterrichtsmaterialien im Voraus vor und bewahren Sie sie an einem sicheren Ort auf.

Wahrung der Privatsphäre und Sicherheit beim Online-Unterricht

Achten Sie darauf, nur berechtigte Teilnehmende zur Sitzung zuzulassen (z. B. über eine Wartezimmerfunktion)

Vermeiden Sie die Weitergabe von Namen, E-Mails oder persönlichen Daten der Teilnehmenden während der Sitzung.

Verwenden Sie sichere Methoden für den Austausch von Materialien (z. B. die von der Platt-form bereitgestellten Tools für die gemeinsame Nutzung von Dateien)

Erinnern Sie die Teilnehmenden an die grund-legenden Datenschutzregeln, z. B. dass sie den Link zur Besprechung nicht weitergeben oder die Sitzung nicht ohne Erlaubnis aufzeichnen dürfen.

Überwachung der Chat- und Bildschirmfreigabefunktionen, um sicherzustellen, dass keine unbefugten Inhalte freigegeben werden

Datenschutz und Nachbereitung nach der Sitzung

Speichern oder teilen Sie keine unnötigen Teilnehmerdaten (z. B. Namen oder Anwesen-heitslisten)

Stellen Sie sicher, dass etwaige Sitzungs-aufzeichnungen sicher aufbewahrt und nur an autorisierte Teilnehmer:innen weitergegeben werden.

Geben Sie alle weiterführenden Materialien oder Ressourcen über sichere Plattformen weiter (z. B. E-Mail oder private Links)

TOOLS

DATEN-BEHANDLUNG & -SICHERHEIT

Ermutigen Sie die Teilnehmenden, Tipps zum Schutz ihrer Daten zu lesen und stellen Sie entsprechende Ressourcen zur Verfügung.

Evaluieren Sie die Sitzung und notieren Sie eventuelle Datenschutz- oder Sicherheitsprobleme, um zukünftige Sitzungen zu verbessern.

AKTIVITÄT 1

Ein Erwachsenenbildner bereitet eine Online-Sitzung für eine Gruppe von Lernenden vor, die mit den Grundprinzipien des Datenschutzes nicht vertraut sind. Bei der Anmeldung werden die Lernenden gebeten, ihre E-Mail-Adressen anzugeben, und während der Sitzung könnten sie versehentlich persönliche Informationen im Chat preisgeben. Die Lehrkraft muss sicherstellen, dass die Privatsphäre geschützt wird und die Lernenden wissen, wie sie sich online sicher verhalten können.

Vor der Einheit

Wählen Sie sichere Plattformen: Verwenden Sie vertrauenswürdige Tools wie Zoom oder Microsoft Teams. Stellen Sie sicher, dass diese aktualisiert und mit DSGVO-konformen Einstellungen konfiguriert sind.

Minimieren Sie die Datenerfassung: Fragen Sie bei der Registrierung nur nach den wichtigsten Informationen (z. B. Vorname, E-Mail). Vermeiden Sie die Erhebung unnötiger persönlicher Daten.

Bereiten Sie Datenschutzregeln vor: Bereiten Sie einfache Datenschutzgrundregeln für die Sitzung vor und teilen Sie diese mit, z. B. „Teilen Sie keine sensiblen Informationen im Chat“. Teilen Sie diese Regeln den Teilnehmern im Vorfeld mit.

Testen Sie die Plattform: Machen Sie sich mit Funktionen wie dem Stummschalten von Teilnehmern, dem Sperren von Meetings und der Aktivierung von Warteräumen vertraut.

TOOLS

DATEN-BEHANDLUNG & -SICHERHEIT

Während der Einheit

Beginnen Sie mit Bewusstseinsbildung: Erläutern Sie zu Beginn der Sitzung kurz, warum Datenschutz wichtig ist, und nennen Sie Beispiele für häufige Risiken (z. B. Phishing-E-Mails, unsichere Websites).

Sichere Praktiken vorleben: Vermeiden Sie es, die vollen Namen zu nennen oder persönliche Informationen über die Teilnehmenden weiterzugeben. Nennen Sie sie beim Vornamen oder bei Pseudonymen.

Sichere Beteiligung: Nutzen Sie interaktive Tools wie Umfragen oder Frage- und Antwortfunktionen, um die Lernenden einzubeziehen, ohne dass sie persönliche Informationen preisgeben müssen.

Überwachen Sie den Chat: Achten Sie auf die versehentliche Weitergabe sensibler Daten im Chat und sprechen Sie diese an. Erinnern Sie die Teilnehmer:innen bei Bedarf an die Datenschutzregeln.

Nach der Einheit

Sichern Sie Materialien: Speichern Sie etwaige Aufzeichnungen in einem passwortgeschützten Ordner und geben Sie sie nur an autorisierte Personen weiter.

Ressourcen bereitstellen: Geben Sie einen einfachen Leitfaden oder eine Checkliste für den sicheren Umgang mit dem Internet heraus, die auf den Inhalt der Sitzung zugeschnitten sind.

Reflektieren und Verbessern: Notieren Sie eventuelle Probleme mit dem Datenschutz während der Sitzung und passen Sie Ihre Vorgehensweise für das nächste Mal an.

AKTIVITÄT 2

Einschlägige Vorschriften/Standards

Datenschutzrichtlinie für elektronische Kommunikation (ePrivacy-Richtlinie) *- legt Regeln für den Schutz der Privatsphäre im Internet und den Datenschutz in der elektronischen Kommunikation fest*

TOOLS

DATEN-BEHANDLUNG & -SICHERHEIT

Definition und Schlüsselbegriffen

Datenschutzverletzung *- Ein Vorfall, bei dem auf sensible Daten ohne Genehmigung zugegriffen wird oder diese offengelegt werden.*

Datenverletzung *– Ein Vorfall, bei dem sensible Daten ohne Genehmigung abgerufen oder offengelegt werden.*

Verschlüsselung - Der Prozess der Umwandlung von Informationen in ein sicheres Format, um unbefugten Zugriff zu verhindern.

Aktivitäten/Übungen

Rollenspiele *- Teilen Sie die Lernenden in Gruppen ein, um gängige Datenschutzrisiken zu simulieren (z. B. Phishing-E-Mails oder zu viele Beiträge in sozialen Medien) und Lösungen zu diskutieren.*

Daten-Audit *- Die Lernenden listen die persönlichen Informationen auf, die sie online weitergeben, und diskutieren, wie sie ihren digitalen Fußabdruck verringern können.*

Methodischer Leitfaden

Beginnen Sie die Sitzung mit einer nachvollziehbaren Geschichte oder Fallstudie, um die Bedeutung des Datenschutzes zu verdeutlichen.

Verwenden Sie eine einfache Sprache, um Konzepte zu erklären, und vermeiden Sie Fachjargon.

TOOLS

TRAININGS- UND AUFKLÄRUNGS-PROGRAMME

Schulungs- und Sensibilisierungsprogramme sind für Organisationen unerlässlich, um die Einhaltung von Datenschutzvorschriften wie der Allgemeinen Datenschutzverordnung (DSGVO) oder anderer nationaler und internationaler Gesetze zu gewährleisten.
Diese Programme klären Mitarbeitende, Verwaltungsangestellte und andere Interessen-gruppen über die Bedeutung des Datenschutzes und der Datensicherheit auf und fördern gleichzeitig eine Kultur der Compliance. Indem sie der Aufklärung und Bewusstseinsbildung durch gut strukturierte Schulungsprogramme Priorität einräumen, können Organisationen die Herausforderungen des Datenschutzes wirksam angehen und einen soliden Rahmen für die Einhaltung der Vorschriften schaffen.

GDPR Data Privacy Professional (GDPR DPP) Schulung

Dieser von DPO Europe angebotene Kurs hilft bei der Integration der GDPR-Anforderungen in Informationssicherheitsstrategien und gewährleistet den Datenschutz in allen IT-Infrastrukturen. Er behandelt den sicheren Umgang mit personenbezogenen Daten in Übereinstimmung mit der GDPR.

Intensivkurs zum zertifizierten Datenschutzbeauftragten (CDPO)

Dieser von der DELTA Data Protection & Compliance Academy angebotene Online-Intensivkurs vermittelt Einzelpersonen die Kenntnisse und Fähigkeiten, die sie benötigen, um als Datenschutzbeauftragte zu fungieren und die Einhaltung der DSGVO in ihrem Unternehmen sicherzustellen.

Datenschutzbeauftragter (DSB) Online-Schulung

InfosecTrain bietet ein umfassendes Verständnis der DSGVO-Compliance, das Aspekte wie organisatorische Prozesse, Datenschutzrichtlinien, Zustimmungsmechanismen und Datenschutzfolgenabschätzungen abdeckt.

TOOLS

TRAININGS- UND AUFKLÄRUNGS-PROGRAMME

Globales Schulungsprogramm zur Sensibilisierung für den Datenschutz

TeachPrivacy bietet ein Programm an, das den Mitarbeitern globaler Organisationen eine grundlegende Schulung zum Thema Datenschutz bietet und für multinationale Unternehmen, einschließlich solcher mit Sitz in der EU, geeignet ist.

Auffrischungskurs und Fortgeschrittenenkurs zum Datenschutz

Die EIPA bietet einen Kurs an, der dazu beitragen soll, das Wissen über den Datenschutz aufzufrischen und zu aktualisieren, und der von Experten und Praktikern geleitet wird, die auf dem Gebiet des Datenschutzes führend sind.

KnowBe4 Sicherheit Sensibilisierungsschulung

KnowBe4 bietet interaktive Schulungen zur Sensibilisierung für Cybersicherheitsrisiken wie Phishing und Social Engineering. Die Kurse helfen, das Wissen aufzufrischen und sicherheitsbewusstes Verhalten im Arbeitsalltag zu stärken.

SkillSoft Schulung zur Einhaltung von Vorschriften

Skillsoft bietet eine breite Palette von Compliance-Schulungen an, darunter auch Module zu Datenschutz und Privatsphäre. Die Inhalte sind so konzipiert, dass sie Unternehmen bei der Einhaltung gesetzlicher Vorschriften unterstützen und sicherstellen, dass die Mitarbeiter:innen ihre Rolle bei der Aufrechterhaltung der Datensicherheit verstehen.

OneTrust Datenschutz & Data Governance

OneTrust bietet Tools für das Datenschutzmanagement, einschließlich Schulungsressourcen, die Organisationen bei der Einhaltung der globalen Datenschutzgesetze unterstützen. Die Plattform hilft bei der Verwaltung von Einwilligungen, Daten-Mapping und Bewertungen und bietet einen umfassenden Ansatz für Data Governance.

TOOLS

TRAININGS- UND AUFKLÄRUNGS-PROGRAMME

TrustArc-Plattform für Datenschutzmanagement

TrustArc bietet eine Reihe von Tools, die Unternehmen bei der Einhaltung von Datenschutzbestimmungen unterstützen. Die Plattform umfasst Schulungsmodule, Risikobewertungen und die Verwaltung von Datenbeständen, um die Einhaltung von Datenschutzvorschriften zu gewährleisten.

DataGuard Compliance-Lösungen

DataGuard bietet umfassende Datenschutz- und Compliance-Dienstleistungen, einschließlich auf die Bedürfnisse von Unternehmen zugeschnittene Schulungsprogramme. Ihre Lösungen konzentrieren sich auf die Integration des Datenschutzes in die Geschäftsprozesse und gewährleisten die kontinuierliche Einhaltung von Vorschriften wie der GDPR.

AKTIVITÄT 1

Einschlägige Vorschriften/Standards

ISO/IEC 27701: Befürwortet regelmäßige Schulungen als Teil von Datenschutz-Informationsmanagementsystemen.

Nationale Gesetze und Verhaltenskodizes: Lokale Anpassungen der GDPR oder spezifische Datenschutzgesetze (z. B. DSGVO in Österreich) betonen oft die Notwendigkeit der Schulung und Sensibilisierung der Mitarbeitenden.

Datenschutzschulungen: Dies ist ein dynamischer Bereich in der Erwachsenenbildung, der sich darauf konzentriert, Mitarbeitenden, Ausbilder:innen und Entscheidungsträger:innen mit dem Wissen auszustatten, um die Einhaltung der Vorschriften zu gewährleisten. Die Ausbilder:innen müssen reale Szenarien einbeziehen, aktives Engagement fördern und auf die verschiedenen beruflichen Kontexte der Lernenden eingehen.

Definition und Schlüsselbegriffe

Compliance - Einhaltung rechtlicher und regulatorischer Anforderungen.

TOOLS

TRAININGS- UND AUFKLÄRUNGS-PROGRAMME

Personenbezogene Daten: Alle Informationen, die direkt oder indirekt eine Person identifizieren können.

Minimierung der Datenmenge: Erhebung nur der Daten, die für einen bestimmten Zweck erforderlich sind.

DSB (Datenschutzbeauftragte:r): Eine Rolle, die von der DSGVO für bestimmte Organisationen vorgeschrieben ist, um die Einhaltung und als Bindeglied zu den Aufsichtsbehörden zu fungieren.

Sensibilisierungskampagne: Eine strukturierte Anstrengung, um Mitarbeiter über Datenschutzpraktiken zu informieren und aufzuklären, mit Hilfe von Postern, E-Mails oder Workshops.

Methodischer Leitfaden

Verwendung von Fallstudien und Beispielen aus der Praxis, um Konzepte nachvollziehbar und umsetzbar zu machen.

Fördern Sie eine interaktive Lernumgebung mit Diskussionen, Rollenspielen und szenariobasiertem Lernen.

Stellen Sie einfache Checklisten und Vorlagen zur Verfügung, die den Lernenden helfen, die Konzepte an ihren Arbeitsplätzen anzuwenden.

Aktivitäten/Übungen

Compliance-Workshop *- Teilen Sie die Teilnehmer in Gruppen auf und präsentieren Sie Fallstudien zu Datenschutzverletzungen. Die Gruppen diskutieren, was schief gelaufen ist, und schlagen Lösungen vor, um künftige Verstöße zu verhindern. D.h. "Welche Sicherheitsvorkehrungen hätten den unbefugten Zugriff auf Kundendaten in diesem Szenario verhindern können?"*

Interaktives Rollenspiel *- Die Teilnehmer:innen simulieren eine:n Datenschutzbeauftragte:n, der eine interne Schulung durchführt und sich dabei auf die Grundsätze der DSGVO oder die Beantwortung eines Antrags auf Zugang zu personenbezogenen Daten konzentriert.*

TOOLS

SOCIAL-MEDIA-APPS

Beruflich orientierte Erwachsene stellen einen vielversprechenden Markt für Hochschulen dar, die mit rückläufigen Einschreibungen von traditionellen Studenten konfrontiert sind. Allerdings haben erwachsene Lernende oft mehrere Verpflichtungen und komplexe Lebensumstände zu bewältigen, was die Einschreibung in akademische Programme zu einer entmutigenden Aufgabe machen kann. Um diese Zielgruppe zu unterstützen, ist es wichtig, Prozesse zu rationalisieren und Barrieren zu beseitigen, einschließlich derer, die mit den in der Lehre verwendeten Social-Media-Tools zusammenhängen. Die Vereinfachung des Informationszugangs, das Angebot personalisierter Unterstützung und die Nutzung benutzerfreundlicher Plattformen können die Bildungserfahrungen erwachsener Lernender erheblich verbessern.

Rationalisieren Sie die Einschreibung von erwachsenen Lernenden: Leitfaden für bewährte Praktiken

In diesem Leitfaden werden konkrete Schritte zur Vereinfachung der Immatrikulationsverfahren und zur Beseitigung von Hindernissen für erwachsene Lernende beschrieben. Zu den Strategien gehören die Bereitstellung klarer und zugänglicher Informationen, das Überdenken der Bewerbungsanforderungen, das Angebot flexibler Fristen und die Verbesserung der Bewertung von Transferleistungen. Darüber hinaus wird die Bedeutung intuitiver Technologien, individueller Beratung und finanzieller Unterstützung hervorgehoben, die alle darauf abzielen, den Immatrikulationsprozess für erwachsene Lernende integrativer und effizienter zu gestalten.

Maximierung des Engagements von erwachsenen Lernenden in Online-Umgebungen

Skillrise, eine Initiative der ISTE (International Society for Technology in Education), stellt ein umfassendes Rahmenwerk zur Verfügung, das Lehrkräften und Institutionen dabei hilft, ansprechende und effektive digitale Lernerfahrungen für erwachsene Lernende zu schaffen. Das Tool skizziert einen strukturierten Ansatz zur Integration von Bildungstechnologie, der Faktoren wie Bereitschaft, Teamkapazität, Bedürfnisse der Lernenden und Implementierungsstrategien berücksichtigt.

TOOLS

SOCIAL-MEDIA-APPS

Einsatz digitaler Werkzeuge im Unterricht: Soziale Medien

Dieses Video zeigt, wie sich soziale Medien und digitale Tools positiv auf das akademische Umfeld auswirken können, indem sie das Engagement fördern und die Lernerfahrungen verbessern.
Der Inhalt zeigt praktische Möglichkeiten zur Integration von Social-Media-Plattformen, Tools für die Zusammenarbeit und kreativen Medien wie Podcasts in Ihre Lehrmethodik. Erfahren Sie, wie Sie Studierende inspirieren und das Beste aus diesen digitalen Tools machen können, um interaktive, moderne Lernumgebungen zu schaffen.

LEITFADEN ZUR NUTZUNG VON SOCIAL MEDIA APPS FÜR UNTERRICHTSZWECKE

Apps für soziale Medien haben die Art und Weise verändert, wie Lehrkräfte mit Lernenden inter-agieren und Inhalte vermitteln. Wenn diese Platt-formen im Bildungsbereich strategisch eingesetzt werden, können sie die Zusammenarbeit, Kreativität und das Engagement fördern. In diesem Leitfaden werden bewährte Verfahren und praktische Tipps für die effektive Einbindung von Social-Media-Apps in Ihren Unterricht vorgestellt, um die Beteiligung der Teilnehmenden und die Lernergebnisse zu verbessern.

Bewährte Praktiken

Wählen Sie die richtige Plattform für Ihr Publikum:

- Nicht alle Social-Media-Apps sind für jeden Bildungsbedarf geeignet. Berücksichtigen Sie bei der Auswahl einer Plattform die Altersgruppe, die Lernziele und die Datenschutzbedenken. LinkedIn eignet sich zum Beispiel hervorragend für berufliche Netzwerke und karrierebezogene Inhalte, während Plattformen wie Instagram oder Facebook für den Austausch von Multimedia-Inhalten und interaktive Diskussionen genutzt werden können.

Klare Richtlinien und Erwartungen festlegen:

- Legen Sie klare Regeln für die Nutzung sozialer Medien im Unterricht fest.

TOOLS

SOCIAL-MEDIA-APPS

Dazu gehört, wie oft die Lernenden Beiträge veröffentlichen dürfen, welche Inhalte angemessen sind und wie sie respektvoll mit Gleichaltrigen umgehen sollen. Wenn Sie diese Erwartungen von Anfang an klar kommunizieren, können Missverständnisse vermieden werden.

Professionelle Grenzen wahren:

- *Trennen Sie Ihre persönliche Präsenz in sozialen Medien von Ihren beruflichen Lehrkonten. So stellen Sie sicher, dass* Ihre Teilnehmenden mit Ihnen in einem lern-orientierten Kontext interagieren können, während Ihre Privatsphäre gewahrt bleibt.

Integrieren Sie soziale Medien in Ihre Lernziele:

- Stellen Sie sicher, dass die Nutzung sozialer Medien mit Ihren Bildungszielen übereinstimmt. Ob für Diskussionen, Gruppenprojekte oder den Austausch von Ressourcen – soziale Medien sollten einen klaren pädagogischen Zweck erfüllen, um ihren Nutzen zu maximieren.

Fördern Sie Zusammenarbeit und Kommunikation:

- Soziale Medien können das gegenseitige Lernen und die Zusammenarbeit zwischen Gleichaltrigen fördern. Schaffen Sie Räume, in denen die Lern-enden Fragen stellen, Ressourcen aus-tauschen und sich gegenseitig unterstützen können. Ermutigen Sie die Teilnehmenden, eigene Inhalte wie Blogbeiträge, Videos oder Infografiken zu erstellen, um ihre Lernerfahrung zu vertiefen.

Praktische Tipps

Wählen Sie die richtige App für die Freigabe von Inhalten aus:

- Tipp: Wenn Sie Multimedia-Inhalte teilen möchten, können Plattformen wie YouTube, Instagram oder TikTok Ihnen dabei helfen, die Lernenden visuell anzusprechen. Sie können Videos, Tutorials oder Live-Stream-Dis-kussionen hochladen. Achten Sie nur darauf, dass die Videos barrierefrei sind und gegebenenfalls Untertitel enthalten.

Private oder geschlossene Gruppen erstellen:

- Tipp: Für eine besser kontrollierte Kommunikation können Sie private Gruppen auf Plattformen wie Facebook oder Discord erstellen. In diesen Bereichen können die Lernenden miteinander interagieren.

TOOLS

SOCIAL-MEDIA-APPS

ohne sich Gedanken über die Öffentlichkeit machen zu müssen. Außerdem bleiben die Diskussionen so übersichtlich und zielgerichtet.

Verwenden Sie Hashtags zur Organisation:

- Tipp: Verwenden Sie auf Plattformen wie Twitter und Instagram spezifische Hashtags, um Inhalte zu organisieren. So können die Teilnehmeden relevante Beiträge leicht finden und kursbezogene Diskussionen verfolgen. Ermutigen Sie die Studierenden dazu, verwenden Sie den Hashtag, wenn Sie kursbezogene Inhalte veröffentlichen, um die Sichtbarkeit und Interaktion zu verbessern.

Ermutigen Sie die Schüler zu Beiträgen:

- Tipp: Bitten Sie die Schüler, Inhalte zum Thema zu erstellen und zu teilen. Dazu könnte das Teilen relevanter Artikel, das Reflektieren von Diskussionen im Unterricht oder das Posten eigener kreativer Arbeiten gehören. Belohnen Sie die Lernenden für ihre Beiträge, um ihr Verantwortungsbewusstsein und ihr Engagement zu fördern.

Überwachen und moderieren:

- Tipp: Behalten Sie die Interaktionen in den sozialen Medien im Auge, um sicherzustellen, dass die Umgebung respektvoll und lernfördernd bleibt. Überprüfen Sie regelmäßig die Beiträge auf unangemessene Inhalte, stellen Sie sicher, dass die Teilnehmenden die Richtlinien befolgen, und gehen Sie etwaige Probleme umgehend an.

Live-Interaktion integrieren:

- Tipp: Nutzen Sie Live-Streaming-Tools wie Instagram Live, Facebook Live oder YouTube Live, um Frage-und-Antwort-Runden, Gastvorträge oder Echtzeitdiskussionen zu veranstalten. So schaffen Sie einen interaktiven Raum, in dem die Lernenden direkt mit den Inhalten und den Lehrkräften interagieren können.

Umfragen und Abstimmungen erstellen:

- Tipp: Nutzen Sie Plattformen wie Twitter oder Instagram Stories, um kurze Umfragen oder Abstimmungen zu Unterrichtsinhalten zu erstellen. Dies kann eine unterhaltsame und ansprechende Möglichkeit sein, Feedback zu sammeln oder den Wissensstand zu überprüfen.

TOOLS

SOCIAL-MEDIA-APPS

CHECKLISTE

Sichere Online-Unterrichtsstunde
Schritt für Schritt

Überprüfen Sie, ob die Social-Media-App die DSGVO einhält, indem Sie deren Datenschutzrichtlinien und Datenverarbeitungsmethoden überprüfen.

Passen Sie die Datenschutzeinstellungen der App an, um den Zugriff auf Unterrichtsmaterialien und Interaktionen auf angemeldete Teilnehmer:innen zu beschränken.

Holen Sie von den Lernenden eine dokumen-tierte Einwilligung zur Verwendung ihrer Daten ein, einschließlich aller Medien (z. B. Fotos, Videos), die während des Unterrichts geteilt werden.

Erstellen Sie private Gruppen, Chats oder Bereiche innerhalb der App für sichere und kontrollierte Diskussionen.

Stellen Sie sicher, dass alle gemeinsam genutzten Unterrichtsmaterialien, Beiträge oder Medien keine personenbezogenen Daten (PII) enthalten.

Richten Sie sichere Passwörter ein und aktivieren Sie die Zwei-Faktor-Authentifizierung (2FA) für Konten, die für Unterrichtszwecke verwendet werden.

Überwachen und moderieren Sie Gruppenaktivitäten, um Datenverstöße oder Missbrauch der Plattform zu verhindern.

Ermutigen Sie die Lernenden, datenschutzorientierte Profile oder Pseudonyme zu verwenden, wenn sie Bedenken hinsichtlich der Offenlegung ihrer Daten haben.

Überprüfen Sie nach jeder Sitzung die App auf unnötige Dateien, private Nachrichten oder temporäre Daten und löschen Sie diese.

Vermeiden Sie es, sensible oder personenbezogene Daten (PII) auf der Plattform weiterzugeben, wie z. B. Adressen oder vollständige Namen.

TOOLS

SOCIAL-MEDIA-APPS

Informieren Sie die Lernenden über ihre Rechte hinsichtlich des Datenschutzes und erklären Sie ihnen, wie ihre Daten verwendet werden. Erstellen Sie einen Notfallplan für Datenverstöße, einschließlich Maßnahmen zur Benachrichtigung der betroffenen Personen und zur Risikominimierung.

Nutzen Sie soziale Medien effektiv zum Lernen?

Ich verstehe, wie die Nutzung sozialer Medien mein Lernen verbessern und interaktiver gestalten kann.

Ich habe die Social-Media-App(s) ausgewählt, die meinen Lernzielen und Vorlieben am besten entsprechen.

Ich bin zuversichtlich, dass meine Privatsphäre geschützt ist, und weiß, wie ich die Einstellungen anpassen muss, um online sicher zu sein.

Ich kenne die Grundregeln für respektvolle und produktive Online-Diskussionen.

Ich kann Ideen, Projekte oder Fragen so einbringen, dass sie zum Lernen in der Gruppe beitragen.

Ich nehme an Umfragen, Quizzen oder Challenges teil, um das Lernen unterhaltsamer und dynamischer zu gestalten.

Ich verwende Hashtags oder Gruppentags, um relevante Beiträge zu finden und alles zu organisieren.

Ich habe kein Problem damit, um Hilfe oder Erläuterungen zu bitten, wenn ich etwas auf der Plattform nicht verstehe.

Ich denke darüber nach, wie Social-Media-Aktivitäten mit meinen persönlichen Lernzielen zusammenhängen.

Ich gebe Feedback dazu, was funktioniert und was nicht, damit alle von einer besseren Lernerfahrung profitieren können.