1/2023
1 – 24

Buchtipp
Pixi-Bücher
Die Daten Füchse

DATENSCHUTZ KONKRET

Recht | Projekte | Lösungen

Chefredaktion: Rainer Knyrim

Datenschutz in der Schule

Früh übt sich – Datenschutz für Kinder und Jugendliche
Interview mit privacy4kids

In Schulen darf Datensicherheit kein Zufall sein!
Dominik Heidegger

Datenschutz in der Schule
Florian Novotny, Thomas Menzel

(Un-)Rechtmäßigkeit einer Veröffentlichung von Kinderfotos
Andreea Panazan

FAQ: Anmeldung Schulskikurs
Viktoria Haidinger

DSB: Information über Schulpflicht
EGMR: Fernsehinterview mit einem Kind
Viktoria Haidinger und Michael Löffler

Checkliste Auskunft nach Art 15 DSGVO
Hans-Jürgen Pollirer

ISSN 2313-5409
dako.manz.at
MANZ

Dominik Heidegger
Informationssicherheitsbeauftragter der Untis GmbH

In Schulen darf Datensicherheit kein Zufall sein!

Verschlüsselungsmechanismen; personenbezogene Daten; TOM; Authentifizierung; Autorisierung; Backup. Bildungseinrichtungen nutzen nicht erst seit der Corona-Pandemie Software und Apps für die Organisation des Schulalltags. Die dort verarbeiteten personenbezogenen Daten von Schüler*innen, Erziehungsberechtigten und Lehrkräften unterliegen besonderen Schutzmaßnahmen durch die DSGVO und verpflichten die Bildungseinrichtung und den Software-Hersteller zu einem verantwortungsvollen Umgang mit diesen sensiblen Informationen. Dieser Beitrag gibt einen Überblick über die technischen Standards und Datensicherheitsmaßnahmen, die zum Schutz der Daten zur Anwendung kommen.

Reguliert und einstudiert

Jede Schuleinrichtung muss sicherstellen, dass sie die personenbezogenen Daten aller Schulbeteiligten gem geltenden Gesetzen und Regulierungen schützt – umso mehr, wenn für die Organisation des Schulalltags eine Schulsoftware verwendet wird. Die DSGVO bringt einige verschärfte Anforderungen für Schulen und Hersteller von Schulsoftware mit sich, die in **folgenden Pflichten** resultieren:

- Pflicht, eine leicht zugängliche Datenschutzerklärung bereitzustellen;
- Pflicht, die Einwilligung der Schüler*innen oder Eltern zur Verarbeitung ihrer personenbezogenen Daten einzuholen (Einwilligungsformular mit Unterschrift);
- Pflicht, die Schüler oder Eltern über ihre Rechte iZm der Verarbeitung zu informieren, zB das Recht auf Auskunft, Berichtigung, Löschung und Widerspruch;
- Pflicht, Datenschutz durch technische und organisatorische Maßnahmen (TOM) sicherzustellen, zB Verschlüsselung, Authentifizierung, Zugriffssteuerungen;
- Pflicht, Datenpannen zu melden (Notfallpläne, Prozessbeschreibungen).

Um stets am aktuellen Stand zu bleiben, sollten diese Dokumente und Prozesse regelmäßig aktualisiert, involvierte Mitarbeitende geschult und Schüler*innen über Neuerungen informiert werden. Eine jährliche Kommunikation der Wichtigkeit von Datenschutz hält die Wachsamkeit hoch.

Was sind sensible personenbezogene Daten im Schulalltag?

Beispiele für sensible personenbezogene Daten im Schulalltag können sein:

- Gesundheitsdaten von Schüler*innen, Lehrkräften und Administration
- Informationen über ethnische oder religiöse Zugehörigkeit
- politische Meinungen
- Informationen über Verbrechen und Straftaten
- Informationen über sexuelle Orientierung

Diese Daten enthalten sensible Informationen zur Privatsphäre der betroffenen Person und sind daher besonders zu schützen, um Missbrauch zu verhindern.

TOM

TOM (technisch-organisatorische Sicherheitsmaßnahmen) sind ein wichtiger Bestandteil der DSGVO-Compliance. Diese stellen sicher, dass personenbezogene Daten angemessen geschützt werden, sowohl vor unbefugtem Zugriff als auch vor Verlust oder Beschädigung.

Beispiele für technische und organisatorische Maßnahmen:

- Verschlüsselungsmethoden
- Authentifizierungs- und Autorisierungsmechanismen
- Zugriffssteuerungen
- Auditing- und Überwachungsfunktionen
- Firewall- und Intrusion Detection/Prevention Systems (IDPS)
- Datensicherungs- und Notfallwiederherstellungsmaßnahmen
- Compliance mit relevanten Regulierungen und branchenüblichen Standards

Verschlüsselungsmechanismen

Es gibt verschiedene Arten von Verschlüsselungsmethoden, die abhängig von der Art der Daten und der Höhe des Risikos von Missbrauch oder Verlust für verschiedene Anwendungsfälle geeignet sind. Es wird zwischen Daten „at rest", „in transport" und „in use" unterschieden:

- **Daten at rest:** Daten befinden sich auf einem Speichermedium (Festplatte, USB-Stick etc). Empfohlene Technologien:
  - AES (Advanced Encryption Standard) mit einem Schlüssel von mindestens 256 Bit
  - RSA (Rivest-Shamir-Adleman)
  - Twofish
- **Daten in transport:** Daten werden über ein Netzwerk übertragen. Empfohlene Technologien:
  - HTTPS (HTTP Secure)
  - SSL (Secure Sockets Layer) und sein Nachfolger TLS (Transport Layer Security)
- **Daten in use:** Daten werden derzeit von einer Anwendung verarbeitet. Geeignete Verschlüsselungsmethoden:
  - Full Disk Encryption (FDE)
  - Transparent Data Encryption (TDE)
- **Empfohlene Technologien:**
  - SSL oder TLS für die Verbindungen zwischen Anwendungen
  - IPSec (Internet Protocol Security) für die Datenübertragung auf Netzwerkebene
  - Bitlocker (Windows), FileVault (MacOS) für die Festplattenverschlüsselung

Die 7 W's hinter den 7 Bergen

Authentifizierung und Autorisierung stellen sicher, dass nur autorisierte Benutzer*innen auf sensible personenbezogene Daten zugreifen können.

Die wichtigste Frage hier lautet: **W**er will **w**ann auf **w**elche Daten **w**ie, **w**oher und **w**arum zugreifen?

„Authentifizierung" ist der Prozess, bei dem die Identität eines Benutzers verifiziert wird, bevor dieser Zugriff auf die Daten erhält.

- **Passwortbasierte Authentifizierung:** Anmeldung mit Benutzername und Passwort
  - Passwort Manager erleichtern die Verwaltung von komplexen Passwörtern.
- **Zwei-Faktor-Authentifizierung:** Bestätigung der Anmeldung mit einem einmaligen Code per SMS oder Authenticator-App
  - Die Verwendung von Authenticator-Apps (Microsoft-/Google-Authenticator) zur Generierung der Codes wird empfohlen.
- **Biometrische Authentifizierung:** Eingabe der biometrischen Daten wie Fingerabdruck, Gesicht oder Stimme bei der Identifizierung von Administratoren.
  - Technologien wie Gesichtserkennung, Fingerabdruck- und Iris-Scanner werden immer häufiger verwendet, um die Authentifizierung zu vereinfachen und zu verbessern.

Mit der **„Autorisierung"** erhält der Benutzer Zugriffsrechte auf bestimmte Daten oder Anwendungen, nachdem seine Identität bestätigt wurde.

- **Rollen-basierte Autorisierung:** Zugriffsrechte basierend auf der Rolle des Benutzers
  - Verwaltung von Berechtigungen mit Identity- und Access-Management-Systemen (IAM)
- **Regelbasierte Autorisierung:** Zugriffsrechte basierend auf Regeln
  - Die Verwendung von Policy-Engines ermöglicht die Definition des Zugriffs auf Daten basierend auf Attributen wie Benutzer, Zeit, Ort und Art.
- **Verfahrensbasierte Autorisierung:** Zugriffsrechte basierend auf spezifischem Kontext der Anfrage, wie zB den zeitlichen oder örtlichen Aspekten der Anfrage.
  - OAuth 2.0 ist ein Autorisierungsprotokoll, das es Benutzern ermöglicht, ihre Identität auf einer Drittanbieteranwendung zu bestätigen, ohne dass die Anmeldeinformationen weitergegeben werden müssen.

Authentifizierung und Autorisierung gehen Hand in Hand. Bei der Wahl des Authentifizierungs- und Autorisierungsmechanismus sollten die Art der Daten und die Höhe des Risikos von Missbrauch oder Verlust genau kalkuliert werden.

Festen Zugriff beweisen

Zugriffssteuerungen sind Mechanismen, die den Zugriff auf sensible personenbezogene Daten steuern und beschränken. Schulen und Software-Hersteller sollten eine Kombination dieser Methoden und Technologien anwenden, um sicherzustellen, dass nur autorisierten Benutzern Zugriff gewährt wird:

- **Berechtigungen und Rollen:** Die Zuweisung von Rollen für bestimmte Benutzer, die festlegen, welche Daten sie einsehen und Aktionen sie in der Schulsoftware ausführen dürfen (siehe Autorisierung).
- **Diskretionäre Zugriffssteuerung (DAC):** Zugriffsrechte können Benutzern explizit zugewiesen werden, indem Daten oder Aktionen für bestimmte Benutzer oder Gruppen freigegeben oder blockiert werden (bspw Access Control Lists [ACLs].
- **Mandantenbasierte Zugriffssteuerung (MAC):** Basiert auf der Trennung der Daten in logischen Bereichen, die als Mandanten bezeichnet werden, und der Steuerung des Zugriffs auf diese Bereiche (bspw. Multitenancy Software).
- **Nondiscretionary Access Control (NDAC) oder Nondiscretionary Security:** Jeder Benutzer hat einen bestimmten Zugriff auf bestimmte Daten oder Aktionen, der durch Regeln beschränkt wird (bspw. durch Firewall und Intrusion Prevention System [IPS] Technologie).

Intelligente Feuerwände

Firewalls und Intrusion Detection/Prevention Systems (IDPS) sollten an strategischen Punkten im Netzwerk eingesetzt werden, um Systeme vor unerwünschten Zugriffen und Angriffen zu schützen.

- **Firewalls** kontrollieren und beschränken den Datenverkehr zwischen Netz-

werken. Sie blockieren unerwünschten Verkehr. Next-Generation Firewalls (NGFWs), die tiefgreifende Paketinspektionstechnologien verwenden, um den Datenverkehr zu überwachen und zu steuern, sind in der Lage, spezifische Anwendungen, Inhalte und Benutzeridentitäten zu identifizieren und zu steuern.

- **Intrusion Detection/Prevention Systems** (IDPS) erkennen und verhindern unerwünschte oder schädliche Aktivitäten im Netzwerk. Next-Generation Intrusion Prevention Systems (NGIPS) verwenden fortgeschrittene Technologien wie Machine Learning und künstliche Intelligenz, um bekannte als auch unbekannte Angriffe zu erkennen und zu verhindern.

Eine effektive Überwachung der Sicherheitsprotokolle und regelmäßige Updates von Firewalls und IDPS sind wichtige Maßnahmen zum Schutz vor Angriffen. Die gemeinsame Implementierung mit anderen Sicherheitstechnologien wie Zugriffssteuerungen und Verschlüsselung verstärken die Datensicherheit zusätzlich.

Hast du auch genug Backup?

Regelmäßige Datensicherungen und Notfallwiederherstellungsmaßnahmen ermöglichen es, im Fall eines Ausfalls oder eines Angriffs schnell auf eine gesicherte Kopie aller Daten zurückzugreifen. Damit wird das Risiko minimiert, dass wichtige Daten verloren gehen und der Schulbetrieb für längere Zeit unterbrochen wird.

Datensicherung ist die regelmäßige Erstellung von Sicherungskopien der Daten. Dies kann durch die Verwendung von Backup-Software und -Systemen erfolgen, die automatisch die Daten auf eine externe Festplatte, ein NAS-Gerät oder in die Cloud sichern. Cloud-basierte Backup-Lösungen, Virtualisierungstechnologien und Software-Defined Storage (SDS) sind geeignete Optionen.

Notfallwiederherstellungen sind Maßnahmen, um schnell auf die gesicherte Kopie der Daten zurückgreifen zu können und um die Auswirkungen eines Ausfalls oder Angriffs zu minimieren. Virtualisierungstechnologien oder Cloud-basierte Disaster-Recovery-Systeme können dazu verwendet werden. Ein Notfallwiederherstellungsplan und regelmäßige Tests sind wichtige Präventionsmaßnahmen.

Geprüft, durchgesehen, abgestempelt und fertig

Nach dem Motto „Vertrauen ist gut, Kontrolle ist besser" sollten sich Schulen und deren Datenschutzbeauftragte nicht ausschließlich auf die Aussagen des Softwareherstellers verlassen, sondern in regelmäßigen Abständen durch Audits selbst überprüfen, ob die TOM tatsächlich implementiert wurden.

- **Überprüfung der Dokumentation**: Schulen und Datenschutzbeauftragte können die Dokumentation der TOM durchsehen, um sicherzustellen, dass alle erforderlichen Maßnahmen enthalten sind und umgesetzt wurden.
- **Audits**: Eine Überprüfung von unabhängigen Auditor*innen zeigt auf, ob die TOM tatsächlich von Software-Herstellern implementiert wurden.
- **Compliance-Berichte**: Compliance-Berichte, die aufzeigen, wie die TOM implementiert wurden und welche Schritte ergriffen wurden, können eingeholt werden.
- **Vertragsklauseln**: Mit entsprechenden Vertragsklauseln kann festgehalten werden, dass die Implementierung der TOM kontrolliert wird sowie regelmäßige Überprüfungen und Audits stattfinden.

Fazit

Die Verarbeitung von personenbezogenen Daten in Schulsoftware stellt eine große Verantwortung dar, die sowohl von Bildungseinrichtungen als auch von Software-Herstellern ernst genommen werden sollte. Da sich der Bereich Datenschutz und Informationssicherheit rasend schnell weiterentwickelt, sollten die implementierten Prozesse regelmäßig überprüft und auf den neuesten Stand gebracht werden. Schulen und Datenschutzbeauftragte sollten daher eng mit Software-Herstellern zusammenarbeiten, um sicherzustellen, dass ihre Anforderungen erfüllt werden, und auch die Möglichkeit haben, Audits durchzuführen. Beiderseitiges Vertrauen und eine offene Kommunikation sind daher Voraussetzung für eine langfristige Zusammenarbeit und den bestmöglichen Schutz der personenbezogenen Daten aller Schulbeteiligten.

Dako 2023/3

Zum Thema

Über den Autor

Dominik Heidegger ist Informationssicherheitsbeauftragter der Untis GmbH und setzt sich für die Themen Informationssicherheit und Datenschutz in Unternehmen ein.
E-Mail: dominik.heidegger@daszeugs.com

Impressum gem. § 24 MedienG

Offenlegung gem. § 25 MedienG und Angaben zu § 5 ECG abrufbar unter https://www.manz.at/impressum

MIX Paper from responsible sources FSC® C130095 FSC www.fsc.org

Medieninhaber und Herausgeber: MANZ'sche Verlags- und Universitätsbuchhandlung GmbH. **Anschrift:** Kohlmarkt 16, 1010 Wien. **Verlagsadresse:** Johannesgasse 23, 1010 Wien (verlag@manz.at). **Redaktion:** Dr. Rainer Knyrim (Chefredakteur); Mag. Viktoria Haidinger, LL.M.; DI. Michael Löffler; Prof. KommR Hans-Jürgen Pollirer, Ing. Dr. Christof Tschohl. **E-Mail:** dako@manz.at **Verlagsredaktion:** Dr. Elisabeth Maier, Johannesgasse 23, 1010 Wien, E-Mail: elisabeth.maier@manz.at **Hersteller:** Printera Grupa d.o.o., 10431 Sveta Nedelja. **Herstellungsort:** Sveta Nedelja, Kroatien. **Verlagsort:** Wien, Österreich. **Zitiervorschlag:** Dako 2023/Nummer. **Anzeigenkontakt:** Stefan Dallinger, Tel: (01) 531 61-114, Fax: (01) 531 61-596, E-Mail: stefan.dallinger@manz.at **Bezugsbedingungen:** Die Dako erscheint 5 × jährlich. Der Bezugspreis 2023 (10. Jahrgang) beträgt € 179,– (inkl Versand in Österreich). Einzelheft € 43,00. Auslandspreise auf Anfrage. Nicht rechtzeitig vor ihrem Ablauf abbestellte Abonnements gelten für ein weiteres Jahr als erneuert. Abbestellungen müssen schriftlich bis spätestens 18. November des laufenden Abojahres beim Verlag einlangen. **Formatvorlagen:** Zum Download unter www.manz.at/formatvorlagen **Hinweis:** Auf eine geschlechtergerechte Sprache wird geachtet. Wird jedoch von einzelnen Autoren zugunsten der leichteren Lesbarkeit bloß die männliche oder die weibliche Form verwendet, sind immer beide Geschlechter gleichermaßen gemeint. **AZR:** Alle Abkürzungen entsprechen den „Abkürzungs- und Zitierregeln" (AZR), 8. Aufl (Verlag Manz, 2019). **Grafisches Konzept:** Michael Fürnsinn für buero8, 1070 Wien (buero8.com).