SCHULPROGRAMM

Anlagen

Schulisches Löschkonzept

(Beschluss der Schulkonferenz vom 24. 09. 2020)

Unsere Schule hat im Sinne von Art. 32 DS-GVO folgende Maßnahmen zur Sicherheit der Verarbeitung personenbezogener Daten im Bereich der Verwaltung getroffen. Technische und organisatorische Maßnahmen ergänzen sich dabei.

Schutz durch Pseudonymisierung und Verschlüsselung

Beide Verfahren stellen eine Möglichkeit dar, die Identifizierung von Betroffenen (Schüler, Eltern und Lehrkräfte) für den Fall unbefugten Zugriffs oder des Verlustes personenbezogener Daten, unmöglich zu machen oder zumindest zu erschweren.

Technische Maßnahme	**Organisatorische Maßnahme**
• Verschlüsselung von Festplatten auf Rechnern und Servern durch das Betriebssystem. (Verwaltung und Lehrkräfte)	
• Verschlüsselung von Datenbankdateien in Anwendungen wie SchiLD NRW, LOGINEO, Moodle	Anweisung durch Schulleitung: • Passwortschutz
• Verschlüsselung mobiler Datenträger wie USB Sticks und externer Festplatten.	Anweisung durch Schulleitung: • Lehrkräfte nutzen zum Transport von personenbezogenen Daten zwischen Schule und Wohnung nur sichere Datenträger. • BackUps in der Verwaltung grundsätzlich nur auf sicheren Datenträgern. • BackUps der Lehrkräfte zu Hause nur auf sicheren Datenträgern.
• SSL Zertifikat für Homepage der Schule.	• jährliche Erneuerung des SSL Zertifikats
• E-Mail Versand und Abruf nur über SSL/TLS, START TLS • Verschlüsselte E-Mails	• Anweisung der Schulleitung: Versand personenbezogener Daten ohne Verschlüsselung unzulässig
•	• Interne Anweisung, Dokumente, die als Vorlagen genutzt werden können, nach Ablauf der Aufbewahrungsfrist durch Löschen des Personenbezugs zu anonymisieren

Wahrung der Vertraulichkeit

Durch geeignete Maßnahmen wird sichergestellt, dass personenbezogene Daten aus der Schule nur einem gewünschten und zulässigen Empfängerkreis bekannt werden. In der Schule selbst können nur Personen, die durch ihre Funktion dazu berechtigt sind, auf die entsprechenden personenbezogenen Daten zugreifen. Außerhalb der Schule erhalten nur Dritte Zugriff auf personenbezogene Daten, denen die Schule diesen Zugriff ermöglicht.

Zutrittskontrolle

Maßnahmen, die sicherstellen, dass Unbefugte keinen Zutritt zu Räumen erhalten, in welchen Akten aufbewahrt werden bzw. Rechner oder Server stehen.

Technische Maßnahme	**Organisatorische Maßnahme**
Alarmanlage sichert Zutritt zum Gebäude	• Nur Schulleitung & Hausmeister können Alarmanlage deaktivieren. • Alarmanlage immer scharf geschaltet, wenn niemand im Gebäude ist.
Alarmanlage im Serverraum	• Zutritt nur für Schulleitung und IT Dienstleister
Schließanlage mit Sicherheitsschlössern	• Schlüssel werden nach Funktion vergeben. • Serverräume und Verwaltung sind nur für Funktionsträger und Schulleitung zu öffnen. • Räume der Schulverwaltung sind immer verschlossen, wenn sich kein Berechtigter dort aufhält. • Schlüssel werden **nicht** an nichtberechtigte Personen ausgeliehen
Türen zu Verwaltungsräumen nur mit Knopf/ kein Griff	

Zugangskontrolle

Maßnahmen, die verhindern, dass Unbefugte Computer nutzen oder Akten einsehen können.

Technische Maßnahme	**Organisatorische Maßnahme**
Aktenschränke abschließbar	• Aktenschränke stehen in der Verwaltung bzw. Archivraum. • Außerhalb der Arbeitszeit sind die Schränke verschlossen. • Nur Schulleitung und Sekretariat haben Schlüssel.
Unterlagen zum sonderpädagogischen Förderbedarf werden im Umschlag aufbewahrt	• Zugriff durch berechtigte Lehrkräfte werden mit Datum und Kürzel auf dem Umschlag markiert
Abstand Verwaltungsarbeitsplätze im Sekretariat	• Abdecken von Unterlagen mit

von der Besuchertheke	personenbezogenen Daten auf dem Schreibtisch bei Anwesenheit nicht berechtigter Personen • Bildschirmausrichtung, so dass Einblick für nichtberechtigte Personen erschwert ist.
Verschließbare Lehrerfächer, Schreibtische, Rollcontainer für Akten	• Anweisung “Freier Schreibtisch” - nach Arbeitsschluss verbleiben keine Unterlagen mit personenbezogenen Daten auf den Schreibtischen.
Anmeldung/Authentifikation mit Benutzername und Passwort	• Vorgabe von Passwortrichtlinien zu Länge und Komplexität • Wechselfristen für Passwörter • Nutzung eines Passwort Managers • Begrenzung der Anzahl der Fehleingaben • Verwalten von Benutzerberechtigungen
Automatische Desktopsperre (Bildschirmschoner mit Passwortschutz) Automatischer Log-out • vom System • von Anwendungen	• Abmeldung nach 10 Minuten Inaktivität • Beim Verlassen des Arbeitsplatzes Aktivierung des Bildschirmschoners oder Log-out durch den Benutzer.
	• Prüfung der Identität des Anfragenden auf Berechtigung bei Anfragen nach Art. 15 DS-GVO
VPN für Fernzugriffe auf Server, Clients und Netzwerkgeräte	
Intrusion Detection System für Server und Netzwerk	• Vertragliche Regelung für Aufschaltung beim IT Dienstleister für zeitnahe Benachrichtigung und Reaktion
Firewall	• entsprechend dem technisch aktuellen Stand und werden aktuell gehalten
Virenschutz für Server, Clients und mobile Geräte der Verwaltung	• Regelmäßige Aktualisierung der Virenschutz-Software
	• getrennte Aufbewahrung von Zertifikatsdateien zur Entschlüsselung von verschlüsselt übermittelten personenbezogenen Daten von den entsprechenden Daten (z.B. SchiPS)

Zugriffskontrolle

Maßnahmen, die sicherstellen, dass Berechtigte nur Zugriff auf personenbezogene Daten haben, für welche eine dienstliche Notwendigkeit besteht.

Technische Maßnahme	Organisatorische Maßnahme
Abgestufte Rollenkonzepte bei Verwaltungsprogrammen Benutzer- und Gruppenrichtlinien für Betriebssystem und Netzwerk	• Zugriffsberechtigungen werden entsprechend Funktion vergeben • schriftliches Berechtigungskonzept vorhanden • Verwaltung der Rechte durch einen System Administrator • Beschränkung der Anzahl von Personen mit Administrationsrechten auf das notwendige Minimum • Regelmäßige Aktualisierung der Benutzerberechtigungen, z.B. Löschen von Berechtigungen bei Beendigung der Tätigkeit an der Schule
Nutzung eines Aktenschredders (mind. Sicherheitsstufe 3, cross cut)	• Anweisung der Schulleitung zur Vernichtung von Akten in kleinen Mengen (Datenschutzkonzept der Schule)
Vernichtung größerer Mengen an Akten über den zertifizierten externer Aktenvernichter des Schulträgers Vernichtung von Altgeräten, insbesondere Festplatten und anderen Datenspeichern/ Datenträgern durch zertifizierten externen Entsorger des Schulträgers	• Vertrag zur Datenverarbeitung im Auftrag • Angebot der Schule, die Entsorgung von dienstlich genutzten Privatgeräten von Lehrkräften, Datenträgern, USB Sticks, Festplatten usw. über den Entsorger des Schulträgers vorzunehmen
Protokollierung sämtlicher Zugriffe auf Anwendungen: bei der Eingabe, Änderung und Löschung von Daten	• Kontrolle, ob Protokollierung aktiviert ist • Anwendungen für die Verarbeitung von personenbezogenen Daten müssen Protokollierung von Zugriffen unterstützten (Auswahlkriterium bei Anschaffung)
	• Anweisung der Schulleitung: auf Verwaltungsrechnern dürfen keine Cloud-Dienste (z.B. Dropbox, Google Drive, …) installiert werden, für die es keine Autorisierung durch die Schulleitung gibt.

Weitere Maßnahmen:

- Lehrkräfte dürfen private Endgeräte nur mit Genehmigung durch die Schulleitung zur Verarbeitung personenbezogenen Daten aus der Schule nutzen und verpflichten sich, die dort geforderten technischen und organisatorischen Maßnahmen zur Wahrung der Vertraulichkeit umzusetzen.
- Vertragliche Regelung (Vertrag zur Auftragsverarbeitung) mit dem externen Dienstleister, welcher die Kopierer (Drucker, Faxgeräte) zur Verfügung stellt über die Wahrung der Vertraulichkeit durch fachgerechte Löschung der Festplatten der Kopierer (internen Datenspeicher bei Drucker und Faxgeräten) bei Wartung und Austausch der Geräte.
- Mit dem externen Reinigungsdienst wird ein Vertrag geschlossen, der diesen zur Vertraulichkeit und entsprechenden Unterweisung und Kontrolle seiner Mitarbeiter verpflichtet.

Wahrung der Integrität

Eingangskontrolle

Maßnahmen, die es erlauben, nachträglich zu überprüfen, ob personenbezogene Daten, welche in das Datenverarbeitungssystem der Verwaltung eingegeben wurden, auch den angelieferten Daten entsprechen. Die Eingabe wird über eine Protokollierung auf Ebene des Systems oder der Anwendung kontrolliert.

Technische Maßnahme	**Organisatorische Maßnahme**
technische Protokollierung der Eingabe, Änderung und Löschung von Daten	• stichprobenartige Kontrolle der Protokolle durch … (z.B. Schulleitung/ Administrator)
manueller Abgleich von aus Formularen übernommenen Daten	• Aufbewahrung von Formularen, aus denen Daten in die automatisierte Verarbeitung übernommen wurden (z.B. original Zeugnisnotenlisten der Lehrkräfte) • Aufbewahrung von Klassenbüchern, Kursbüchern, Listen und anderen Unterlagen entsprechend den Vorgaben von VO-DV I §9 • Aufbewahrung von Unterlagen der Lehrkräfte entsprechend den Vorgaben von VO-DV II §9 • Ausdruck von Kontrolllisten der in die automatisierte Verarbeitung eingegeben Daten • Sichtprüfung von Zeugnissen vor Ausgabe auf Richtigkeit

Weitergabekontrolle

Maßnahmen, die sicherstellen, dass personenbezogene Daten bei der digitalen Übermittlung oder der Speicherung oder beim Transport auf externen Datenträgern nicht unbefugt gelesen, kopiert, verändert oder gelöscht werden können.

Technische Maßnahme	**Organisatorische Maßnahme**
gesicherte Online Plattform zum Austausch von personenbezogenen Daten (z.B. Logineo NRW, Moodle, iServ, ...)	• Dienstanweisung zur Nutzung der Online Plattform zum Austausch von personenbezogenen Daten • Vertrag zur Auftragsverarbeitung mit dem Anbieter der Plattform
Verschlüsselte externe Datenträger	• Ausgabe des Notenmoduls von SchiLD NRW nur auf sichere USB Sticks/ über sichere Plattform
verschlüsselte E-Mails	
VPN Verbindung (z.B. zum externen Server bei Nutzung von virtuellen Desktops wie Citrix in der Verwaltung)	
verschlüsselte Verbindungen wie sftp, https bei der Online-Übermittlung	• Anweisung der Schulleitung, nur entsprechende Verbindungen zum Datenaustausch z.B. zwischen Standorten zu nutzen
Sichere Transportbehälter	• Bereitstellung von sicheren Transportbehältern vom Entsorger für Akten, Datenträger usw.
	• Anweisung der Schulleitung: die Weiterleitung dienstlicher E-Mails auf private E-Mail Konten ist untersagt
Cloud Dateimanager Logineo NRW, E-Mail, Kalender, Adressbuch	• die Anbindung über die Schnittstellen ist Lehrkräften nur nach Genehmigung durch die Schulleitung gestattet
Daten-Safe von Logineo NRW	• die Anbindung des Daten-Safe über WebDav ist blockiert

Wahrung der Verfügbarkeit und Belastbarkeit

Maßnahmen, mit welchen personenbezogene Daten vor zufälligem Verlust oder Zerstörung geschützt werden.

Wahrung der Verfügbarkeit

Maßnahmen zur Wahrung der Verfügbarkeit sollen sicherstellen, dass die verarbeiteten personenbezogenen Daten auch nach einem Zwischenfall weiterhin zur Verfügung stehen, um den Betrieb wieder ans Laufen zu bekommen.

Technische Maßnahme	**Organisatorische Maßnahme**
Spiegelung von Festplatten (RAID)	• regelmäßige Tests von Datenwiederherstellung

Backups
Sicherung auf externes Medium
	• Aufbewahrung von Datensicherungen an einem externen Ort.
	• Verwahrung externer Datenträger mit Sicherungsdateien in einem feuersicheren Safe
	• Beschreibung von:
	  ○ Rhythmus der Sicherungen
	  ○ Sicherungsmedien
	  ○ Sicherungsort
	  ○ Aufbewahrungszeit

Sicherungsdateien	• Erstellen einer Datensicherung vor größeren Verarbeitungsschritten (z.B. Gruppenprozessen oder Schuljahreswechseln bei SchiLD NRW)
Analoge und digitale Sicherheitskopien	• Anfertigen von Kopien von Abschlusszeugnissen auf Papier und als PDF
Partitionierung von Festplatten	• Trennung von Betriebssystem und Daten auf verschiedenen Partitionen oder Festplatten
Datenschutztresor	• Aufbewahrung von schulisch gelagerten externen Datenträgern für die Datensicherung

Wahrung der Belastbarkeit

Maßnahmen, die sicherstellen sollen, dass die Datenverarbeitungssysteme vor Beeinträchtigung von technische Störungen und Umwelteinflüsse geschützt sind.

Technische Maßnahme	Organisatorische Maßnahme
Rauchmelder in allen Räumen, inkl. Serverraum	• regelmäßige Funktionskontrolle durch Hausmeister
automatische Überwachung von Temperatur und Feuchtigkeit im Serverraum	• regelmäßige Funktionskontrolle durch IT Dienstleister
	• keine sanitären Anschlüsse im oder oberhalb des Serverraums
Nutzung von Überspannungsschutz im Serverraum, an den Clients und Netzwerkkomponenten	• Nutzung von zertifizierten Komponenten
USV (unterbrechungsfreie Stromversorgung) im Serverraum	• regelmäßiger Funktionstest
Partitionierung von Festplatten	• Trennung von Betriebssystem und Daten auf verschiedenen Partitionen oder Festplatten
Virenschutz auf Server und Clients	• automatische Aktualisierung • Prüfung von externen Medien beim Anschluss ans Verwaltungsnetz
	• Alarmmeldung bei unberechtigten Zugriffsversuchen am Server
Datenschutztresor	• Aufbewahrung von schulisch gelagerten externen Datenträgern für die Datensicherung

Wahrung der Wiederherstellbarkeit nach einem Zwischenfall

Welche Maßnahmen werden getroffen, um nach einem Zwischenfall das System wieder möglichst zeitnah wiederherstellen zu können, so dass das System in möglichst vollem Umfang funktionsfähig ist, und die Verarbeitung personenbezogener Daten nahtlos anschließen kann.

Technische Maßnahme	**Organisatorische Maßnahme**
System BackUp von Server und Arbeitsplatz Rechnern	• regelmäßige Sicherung • Lagerung der Sicherung außer Haus • Notfallplan für Wiederherstellung auf dem normalen System/ auf Ersatzrechnern • Notfallplan für Wiederherstellung eines minimalen Verwaltungssystems auf einem einzelnen mobilen Rechner

Datensicherheit durch Kontrolle und Evaluation

Datenschutz-Maßnahmen	
Technische Maßnahme	**Organisatorische Maßnahme**
	• Schulleitung überprüft ADV Arbeitsplätze der Verwaltung regelmäßig auf Einhaltung der datenschutzrechtlichen Vorgaben.
	• Schulleitung bittet Lehrkräfte mit Genehmigung zur Verarbeitung personenbezogener Daten aus der Schule auf privaten Endgeräten um Auskunft zu getroffenen Maßnahmen zum Schutz der verarbeiteten Daten
Die Schule verfügt über ein Löschkonzept	• Die Schule hat keinen internen Datenschutzbeauftragten: Verantwortlich: OStD H.-U. Holtkemper Vertretung: StD J. Ritzenhoff
Die Schule verfügt über ein Datenschutzkonzept, darin integriert: • Anweisung “Freier Schreibtisch” • Passwort Richtlinie • Umgang mit Dienst E-Mails • Verschlüsselung von externen	• Die Schulleitung sensibilisiert Mitarbeiter und Lehrkräfte jährlich zum Thema Datenschutz • Das schulische Datenschutzkonzept ist im internen Bereich der Schul Cloud Plattform für alle Mitarbeiter und Lehrkräfte jederzeit einsehbar/

Datenträgern	wird allen Mitarbeitern und Lehrkräften ausgehändigt ● Neue Mitarbeiter und Lehrkräfte erhalten das schulische Datenschutzkonzept und werden vor Dienstbeginn zum Thema Datenschutz sensibilisiert
Informationsblatt zur Datenerhebung gem. Art. 13 bzw. Art. 14	● Die Schule informiert Betroffene entsprechend DS-GVO Art. 13 (bei Datenerhebung beim Betroffenen) und 14 (bei Datenerhebung bei Dritten)
Schema “Umgang mit Auskunftsanfragen nach Art. 15 DS-GVO”	● Bearbeitung von Auskunftsanfragen von Betroffenen nach dem schulischen Schema
	● Führen eines Verfahrensverzeichnisses über alle Verarbeitungstätigkeiten der Verwaltung ● regelmäßige Aktualisierung des Verfahrensverzeichnisses