Datenschutz und Datensicherheit

Allgemeines

1. **Einwilligung und Informationspflicht**: Vor der Verarbeitung von Schülerdaten ist in der Regel die Einwilligung der betroffenen Schülerinnen und Schüler oder ihrer Erziehungsberechtigten erforderlich. Die Schülerinnen und Schüler und ihre Eltern sollen über den Zweck der Datenverarbeitung, die Art der verarbeiteten Daten, die Speicherdauer und ihre Rechte gemäß den Datenschutzbestimmungen informiert werden.

2. **Datenminimierung und Zweckbindung**: Es sollen nur die für den spezifischen Zweck notwendigen Daten erhoben und verarbeitet werden. Die Verarbeitung von Schülerdaten soll nur für die festgelegten Zwecke, z. B. für Lernplattformen, erfolgen und darf nicht für andere Zwecke genutzt werden. Eine umfassende Datensammlung ohne klaren Grund ist zu vermeiden.

3. **Datensicherheit**: Die Schülerdaten müssen angemessen vor unbefugtem Zugriff, Verlust, Diebstahl oder unbefugter Weitergabe geschützt werden. Technische und organisatorische Maßnahmen zur Datensicherheit sind unerlässlich.

4. **Aufbewahrungsfristen und Speicherbegrenzung**: Die Schülerdaten sollten nur so lange gespeichert werden, wie es für den angegebenen Zweck erforderlich ist. Nach Ablauf der Aufbewahrungsfristen müssen die Daten gelöscht werden.

5. **Rechte der Betroffenen**: Die Schülerinnen und Schüler haben Rechte bezüglich ihrer personenbezogenen Daten wie das Recht auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung und das Recht auf Datenübertragbarkeit. Diese Rechte müssen respektiert und erfüllt werden.

6. **Auftragsverarbeitung**: Wenn ein Drittanbieter, wie z. B. ein IT-Dienstleister, Zugriff auf die Schülerdaten hat, muss ein Auftragsverarbeitungsvertrag abgeschlossen werden, der die datenschutzrechtlichen Pflichten und Verantwortlichkeiten regelt. Die BBS Wirtschaft Worms nutzt das modulare Netz MNS+ (Land Rheinland-Pfalz), welches vom Dienstleister Netline verwaltet wird. Hierfür hat die Schule einen Auftragsverarbeitungsvertrag geschlossen.

7. **Sensible Daten**: Besondere Kategorien personenbezogener Daten (sensible Daten) wie Gesundheitsdaten oder religiöse Überzeugungen sollen mit besonderer Sorgfalt behandelt werden und nur nach strengen rechtlichen Vorgaben verarbeitet werden.

8. **Datenschutzverletzung und Folgenabschätzung**: In bestimmten Fällen, insbesondere bei hohen Datenschutzrisiken, kann eine Datenschutz-Folgenabschätzung erforderlich sein, um potenzielle

Risiken und Schutzmaßnahmen zu bewerten. Diese erfolgt durch den Datenschutzbeauftragten der BBS Wirtschaft Worms.

Konsequenzen

Zu 1. Einwilligung und Informationspflicht

Einwilligung: Die Einwilligung ist die freiwillige und ausdrückliche Zustimmung der Schülerinnen und Schüler oder ihrer Eltern zur Verarbeitung ihrer personenbezogenen Daten. Bevor wir die Schülerdaten erheben oder nutzen, müssen wir sicherstellen, dass Schülerinnen, Schüler und Eltern informiert werden, warum wir die Daten benötigen und wie sie verarbeitet werden. Die Einwilligung muss klar, spezifisch und freiwillig erfolgen.

Informationspflicht: Die Informationspflicht bedeutet, dass wir die Schülerinnen und Schüler und ihre Eltern über unsere Datenverarbeitungspraktiken informieren müssen. Wir kommunizieren klar, wer für die Datenverarbeitung verantwortlich ist, welchen Zweck die Daten haben, welche Datenarten wir verarbeiten, wie lange wir die Daten speichern und ob wir sie an Dritte weitergeben. Außerdem müssen wir sie über ihre Datenschutzrechte aufklären, z. B. das Recht auf Zugriff, Berichtigung und Löschung ihrer Daten.

Zu 2. Datenminimierung und Zweckbindung

Folgende Daten sind zulässig:

- **Identifikationsdaten**: Name, Geburtsdatum, Anschrift, Geschlecht, Klassenstufe.
- **Kontaktinformationen**: Telefonnummer, E-Mail-Adresse, Kontaktdaten der Eltern oder Erziehungsberechtigten.
- **Schulische Leistungsdaten**: Noten, Abschlüsse, Fehlzeiten
- **Gesundheitsdaten**: In einigen Fällen können relevante medizinische Informationen (7. sensible Daten) erforderlich sein, um die Gesundheit und das Wohlbefinden der Schülerin oder des Schülers zu schützen (z. B. bei Allergien oder besonderen medizinischen Bedürfnissen).
- **Informationen über die Teilnahme** an Aktivitäten und Veranstaltungen der Schule
- **Weitere Daten:** Ausbildungsbetriebe, deren Kontaktpersonen wie beispielweise Ausbilderinnen und Ausbilder mit den Identifikationsdaten und Kontaktinformationen.

Zu 3. Datensicherheit

Aspekte, auf die bei der Datensicherheit geachtet werden muss:

Zugriffskontrolle: Stellen Sie sicher, dass der Zugriff auf personenbezogene Daten auf autorisierte Benutzerinnen und Benutzer beschränkt ist. Implementieren Sie starke Passwörter und verwenden Sie möglichst eine Zwei-Faktor-Authentifizierung, um unautorisierte Zugriffe zu verhindern. Hierbei ist es nützlich Eselbrücken zu nutzen für die Erstellung eines Passwortes, etwa "Die Sonne scheint im Sommer 2023!" => Passwort: "DSsiS23!"

Verschlüsselung: Sensitive Daten sollen während der Übertragung und Speicherung verschlüsselt werden, um sicherzustellen, dass sie nur von berechtigten Personen gelesen werden können. E-Mail-Verkehr ist in der Regel unverschlüsselt. Die Schülerdaten müssen beim Versenden selbst verschlüsselt werden. Beispielsweise wird eine Notenliste in eine ZIP-Datei komprimiert verschlüsselt. Das Passwort bekommt ein Dritter über einen sicheren Zweitkanal mitgeteilt. Eine weitere Möglichkeit wäre, die Schüler- und Klassennamen abzukürzen, sodass keine Zuordnung von Dritten möglich ist. Bsp.: Peter Maier => „PeMa“

Datensicherung: Regelmäßige Backups aller wichtigen Daten sind essenziell, um Datenverlust durch Hardwareausfälle, Malware oder menschliches Versagen zu vermeiden.

Sicherheit der IT-Infrastruktur: Stellen Sie sicher, dass alle verwendeten Geräte und Netzwerke, einschließlich Server, Computer und drahtlose Netzwerke ausreichend geschützt und auf dem neuesten Stand sind.

Aktualisierung von Software und Systemen: Halten Sie Betriebssysteme, Anwendungen und Antivirenprogramme auf dem neuesten Stand, um bekannte Sicherheitslücken zu schließen und Malware-Angriffe zu verhindern.

Physische Sicherheit: Sorgen Sie dafür, dass physische Zugänge zu Räumlichkeiten und Datenträgern beschränkt und geschützt sind. Bsp.: Externe Festplatten und USB-Sticks wegschließen.

Zu 4. Aufbewahrungsfristen

Die entsprechenden Aufbewahrungsfristen sind wie folgt geregelt (Auszüge):

Klassen- und Kursbücher: 3 Jahre;

(Schul-)Gliederungspläne und Schulstatistiken: 3 Jahre;

Prüfungslisten und sonstige Nachweise über das Bestehen von Abschlussprüfungen, Zweitschriften von Abschluss- und Abgangszeugnissen: 60 Jahre;

Krankengeschichten: 30 Jahre.“

Quelle: https://schulemedienrecht.bildung-rp.de/themen/unterrichtsorganisation-und-klassenverwaltung/notenverwaltung-archivierung-und-loeschfristen/?L=0 (Letzter Zugriff: 22.11.2023)

Gilt für digitale sowie für analoge Medien.

Zu 5. Rechte der Betroffenen

Recht auf Auskunft: Die Schülerinnen und Schüler und Eltern haben das Recht zu erfahren, welche Daten von ihnen verarbeitet werden. Ausnahme: Bei Schülerinnen und Schülern, die sich bei Volljährigkeit an der Schule angemeldet haben, erfolgt keine Auskunft an Eltern, es sei denn die Schülerinnen und Schüler stimmen dem zu.

Recht auf Berichtigung: Wenn Daten unrichtig oder unvollständig sind, haben die Betroffenen das Recht auf Korrektur.

Recht auf Löschung: Unter bestimmten Umständen können die Betroffenen verlangen, dass ihre Daten gelöscht werden.

Recht auf Einschränkung der Verarbeitung: In bestimmten Situationen können die Betroffenen die vorübergehende Einschränkung der Datenverarbeitung verlangen.

Recht auf Datenübertragbarkeit: Die Betroffenen können ihre Daten in einem übertragbaren Format erhalten, um sie zu einem anderen Anbieter zu übertragen.

Widerspruchsrecht: Die Schülerinnen und Schüler und Eltern können der Verarbeitung ihrer Daten aus bestimmten Gründen widersprechen.

Zu 6. Auftragsverarbeitung

Wir nutzen als Schule bestimmte Dienstleistungen oder Software von anderen Unternehmen, um unsere Lehrmaterialien zu verwalten oder den Schulbetrieb zu organisieren (Bsp.: „Schulmanager-Online.de“, Office 365, Schulcampus (Land Rheinland-Pfalz), MNS+, MindView, AC-Profil, Schulverwaltungsprogramm). Diese Unternehmen könnten Zugriff auf die personenbezogenen Daten unserer Schülerinnen und Schüler haben, z.B. Namen, Noten oder Kontaktdaten.

Die Auftragsverarbeitung besagt, dass wir sicherstellen müssen, dass diese Unternehmen genauso verantwortungsbewusst mit den Schülerdaten umgehen wie wir selbst. Das bedeutet, dass wir mit ihnen einen Vertrag abschließen müssen, der festlegt, wie sie die Daten behandeln dürfen und dass sie die Daten nur für die vereinbarten Zwecke nutzen dürfen.

Wir sind als Schule auch dann noch für die Daten unserer Schülerinnen und Schüler verantwortlich, wenn wir externe Dienstleister einbinden. Deshalb ist es wichtig, sorgfältig auszuwählen, mit wem wir zusammenarbeiten, und sicherzustellen, dass diese Dienstleister Datenschutzmaßnahmen ergreifen, um die Schülerdaten zu schützen.

Die Auftragsverarbeitung hilft uns also dabei, die Privatsphäre unserer Schülerinnen und Schüler zu wahren und sicherzustellen, dass ihre Daten in sicheren Händen sind, egal ob sie von uns selbst oder von externen Dienstleistern verarbeitet werden.

Die Nutzung von Software auf Dienst- und Schulrechnen, die nicht durch den Datenschutzbeauftragten geprüft wurde, ist nicht gestattet.

ACHTUNG:

Die Nutzung von Office 365 verstößt ohne eigene Anpassung der Datenschutzverordnung des Landes Rheinland-Pfalz. Quelle: https://www.datenschutz.rlp.de/de/themenfelder-themen/microsoft-office-365/ (Letzter Zugriff: 22.11.2023)

Zusammengefasst gibt es folgende Möglichkeiten:

- Die Schülernamen und Klassennamen werden abgekürzt, so kann keine Zuordnung erfolgen. Bsp.: Sandro Wagner => San Wag
- Die Schülerdaten in der Cloud werden separat vom Nutzer (Lehrkraft) verschlüsselt.

Die Deaktivierung der Erfassung von Telemetriedaten im Betriebssystem sollte als zusätzliches Mittel angesehen werden.

WhatsApp ist nicht zulässig, da die genutzten Server sich nicht innerhalb der EU befinden. Signal dagegen ist erlaubt. Es muss auch hier das Einverständnis von den Schülerinnen und Schülern eingeholt werden.

Das neue Datenschutzabkommen zwischen der EU und den USA, bekannt als „EU-U.S. Data Privacy Framework“, wurde im Juni 2023 ins Leben gerufen (Quelle: Das „EU-U.S. Data Privacy Framework” – Das neue Datenschutzabkommen zwischen der EU und den USA (datenschutzkanzlei.de)). Es bildet die Grundlage für einen Beschluss der Europäischen Kommission, in dem das Datenschutzniveau für zertifizierte Unternehmen in den USA für angemessen erklärt wird. Besitzt ein Unternehmen dieses Zertifikat, ist die Nutzung in der EU unter Einhaltung des Datenschutzes möglich.

Zu 7. Sensible Daten (s. Oben)

Zu 8. Datenschutzverletzung und Folgeabschätzung

Datenschutzverletzungen müssen umgehend dem Datenschutzbeauftragten Karel Klug, klug@bbsw.biz-worms.de mitgeteilt werden. Es erfolgen anschließend Maßnahmen, um die Datenschutzverletzung abzumildern. Im letzten Schritt wird die Datenschutzverletzung vom Datenschutzbeauftragten an https://www.datenschutz.rlp.de/de/themenfelder-themen/datenpannen/ (Letzter Zugriff: 22.11.2023) gemeldet, von wo aus weitere Hilfsmaßnahmen eingeleitet werden.

Bsp.: Es werden persönliche Daten per E-Mail in CC an Personen versendet, die nicht dafür vorgesehen waren. Im ersten Schritt werden die unbeabsichtigten Personen darum gebeten, die erhaltene E-Mail zu löschen. Weiter werden alle Personen in der E-Mail über diese Panne informiert und anschließend erfolgt die Meldung der Datenpanne per URL an das Land Rheinland-Pfalz.