

Frauenfeld, 25. August 2021

Richtlinie Datenschutz Mittelschulen

1 Grundlagen

Die Mittelschulen unterstehen dem kantonalen Gesetz über den Datenschutz (vgl. § 1 Abs. 2 Gesetz über den Datenschutz, TG DSG, RB 170.7). Zweck des Gesetzes ist der Schutz der Persönlichkeit und damit aller Personen, mit welchen die Mittelschulen in Kontakt stehen (§ 1 TG DSG).

Die vorliegenden Richtlinien sollen helfen, bei der Benutzung digitaler Hilfsmittel die datenschutzrechtlichen Vorgaben einzuhalten.

2 Klassifikation von Daten

Datenschutzrechtlich sind Sachdaten, Personendaten und besonders schützenswerte Personendaten zu unterscheiden. Für die Bearbeitung der einzelnen Datenkategorien gelten unterschiedliche Voraussetzungen. Die Bearbeitung von Sachdaten ist dabei datenschutzrechtlich weitgehend unbedenklich, soweit das Amtsgeheimnis eingehalten wird.

3 Personendaten

3.1 Adressen

Adressen von Schülerinnen und Schülern dürfen nur zu dem Zweck bearbeitet werden, zu dem sie erhoben wurden. Der Bearbeitungszweck ergibt sich aus den gesetzlich festgelegten Aufgaben der Schule. Die schulinterne Verwendung von Adressen, um beispielsweise auf Veranstaltungen oder Umfragen hinzuweisen, ist zulässig, soweit dies für den Bildungsauftrag geeignet und erforderlich ist. Die Lernenden und Mitarbeitenden sind bereits bei der Angabe ihrer Adressen zu informieren, dass diese von der Schule auch für solche Zwecke verwendet werden.

3.2 Besonders schützenswerte Personendaten

Als besonders schützenswerte Daten zählen: Noten und weitere Angaben über Leistung und Verhalten, Semesterzeugnisse, Absenzen, Aktennotizen über Disziplinarfälle, jegliche Daten, die im weitesten Sinne einen medizinischen Befund darstellen.

Besonders schützenswerte Personendaten dürfen nur bearbeitet werden, wenn sich dies aus einer ausdrücklich gesetzlichen Grundlage ergibt oder eine gesetzliche Aufgabe die Bearbeitung zwingend erfordert oder aber die Betroffenen ausdrücklich zustimmen oder ihre Zustimmung vorausgesetzt werden darf (§ 4 Abs. 3 Datenschutzgesetz). Konkret bedeutet dies:

- Die Erfassung, Speicherung und anderweitige Bearbeitung dieser Daten hat in geschützten Systemen zu erfolgen. Die Weitergabe ist nur an autorisierte Personen gestattet und hat geschützt zu erfolgen.

- Die Daten sind gemäss Angaben im Registraturplan aufzubewahren bzw. dem Staatsarchiv zu übergeben. ¹

3.3 Bearbeiten von Personendaten für nicht personenbezogene Zwecke

Bei der Schule vorhandene Personendaten dürfen für nicht personenbezogene Zwecke wie Statistiken bearbeitet werden. Voraussetzung ist, dass sie anonymisiert werden und aus den Auswertungen keine Rückschlüsse auf betroffene Personen möglich sind.

4 Bekanntgabe von Informationen von allgemeinem Interesse

Die Schule kann von Amtes wegen über Tätigkeiten von allgemeinem Interesse, etwa über Neuigkeiten, Anlässe, Schulprogramme und Stundenpläne informieren. Aufbau, Zuständigkeit und Ansprechpersonen können ebenso veröffentlicht werden. Dazu gehören beispielsweise die Namen, Funktionen, geschäftliche Telefonnummern und E-Mail-Adressen der Lehrpersonen, der Schulleitung und die der anderen Mitarbeitenden, soweit sie Funktionen für die Schule ausüben, die von allgemeinem Interesse sind.

Private Kontaktangaben oder Fotos dürfen nur mit Einwilligung der Betroffenen veröffentlicht werden. Als Informationsträger kommen hauptsächlich die Schulwebsite, das Intranet oder Printmedien in Frage. Schülerlisten mit Vor- und Nachnamen können im Intranet oder in Printmedien ², nicht aber auf der Schulwebsite aufgeführt werden.

5 Soziale Medien

Die Verwendung von sozialen Medien unter Verwendung von Personendaten gilt ebenfalls als Datenbearbeitung, weshalb auch in diesem Bereich zwischen Personendaten und besonders schützenswerten Personendaten zu unterscheiden ist. Da die Lernenden für die Nutzung sozialer Medien auch eigene Daten bekannt geben müssen, muss die Datenbearbeitung über die sozialen Medien mit Einwilligung erfolgen. Bei jüngeren Schülerinnen und Schülern erfolgt die Einwilligung durch die Eltern. Dadurch besteht die Gefahr von Ungleichbehandlungen von Schülerinnen und Schülern, deren Eltern beispielsweise nicht in die Nutzung sozialer Medien einwilligen und denen dadurch wichtige Schulinformationen entgehen. Die auf diesem Weg bekannt gemachten schulischen Informationen müssen daher auch auf andere Weise zugänglich sein.

¹ Im Staatsarchiv sind diese 100 Jahre lang geschützt und danach für die Öffentlichkeit freigegeben.

² Diesbezüglich gab es schon Reklamationen. Beispielsweise: «Wieso die Schülerliste der Absolventen in der Zeitung veröffentlicht werde?» Die Antwort des Datenschutzbeauftragten lautete jeweils, dass davon auszugehen sei, dass die Schülerinnen und Schüler stolz seien, es geschafft zu haben und deshalb deren Zustimmung vorausgesetzt werden könne. Aufgrund der europäischen Vorgaben werden sich aber in Zukunft betreffend der Zustimmung zwangsläufig Änderungen ergeben. So wird im EU-Raum bereits heute verlangt, dass eine Einwilligung nur gültig sei, wenn diese aufgeklärt und beweisbar sei und wenn zudem auf das Widerrufsrecht hingewiesen werde. Diese kommende Praxis kann bei vorschnell veröffentlichten Printmedien problematisch werden.

Die Verwendung sozialer Medien ist infolge der heiklen umfassenden Datenerfassung, -speicherung und Weiterbearbeitung durch die Betreiber auf ein Minimum zu beschränken. Auf den Austausch besonders schützenswerter Personendaten ist zu verzichten.

Wird über Messenger kommuniziert, sind vor allem die Verschlüsselung, der Serverstandort und die Möglichkeit der anonymen Nutzung datenschutzrelevant. Es ist von Vorteil, Anbieter zu berücksichtigen, die europäische Standorte und eine Ende-zu-Ende-Verschlüsselung anbieten (beispielsweise Threema).

5.1 WhatsApp

Mit dem Einsatz von WhatsApp werden Personendaten Dritter bearbeitet, da die Kontaktdaten freigeschaltet werden. Eine Einwilligung dieser Drittpersonen liegt nicht vor. Damit stellt die Nutzung von Whatsapp in der Schule einen Verstoß gegen § 4 ff. Datenschutzgesetz (TG DSG; RB 170.7) dar.

Alternativen: Es gibt Messengerdienste, die weniger problematisch sind, z.B. Threema. Eine App, die vorbehaltlos empfohlen werden kann, gibt es jedoch noch nicht, vgl. <https://www.datenschutz-tg.ch/ds/signal-telegram-threema-und-whatsapp.html>. Als beste Alternative bietet sich die Schulmailadresse an.

6 Auslagerung

Die Schule kann das Bearbeiten von Informationen Dritten übertragen, also auslagern. Dies ist beispielsweise bei der Nutzung von Produkten wie Dropbox, Office 365 oder einer anderen Software der Fall. Auch das Betreiben der Website durch externe Dienstleister, Abklärungen durch externe Fachpersonen oder das Verfassen von Berichten durch Externe gehören zu den Auslagerungen.

Produkte, bei denen die datenschutzrechtlichen Anforderungen nicht erfüllt sind, wie Dropbox und Google Drive, können nur für das Bearbeiten von nicht sensitiven Daten eingesetzt werden. Ausgetauscht werden können beispielsweise Unterrichtsmaterialien, Arbeitsblätter und Fotos. Aufsätze, in denen persönliche Erlebnisse beschrieben werden, dürfen nicht mit diesen Produkten bearbeitet werden. Zu berücksichtigen ist weiter, dass gewisse Dienste verlangen, Daten über sich bekannt zu geben. Werden beispielsweise E-Mail-Adressen mit dem Namen verknüpft, sollte die Schule die Lernenden darüber informieren und bei Bedenken Pseudonyme für die E-Mail-Adressen verwenden.

Vor der Inanspruchnahme eines Produkts oder der Vergabe einer Datenbearbeitung an einen Dritten ist abzuklären, welche Daten dadurch bekannt gegeben werden und ob dies mit den rechtlichen Anforderungen vereinbar ist. Insbesondere bei der Auslagerung von besonders sensitiven Daten wie Gesundheitsdaten, aber auch bereits bei Personendaten wie Name und Adresse sind genaue Abklärungen zu treffen und Massnahmen zum Schutz der Daten umzusetzen. Die Massnahmen richten sich nach der Art der Informationen (Sachdaten, Personendaten, besonders schützenswerte Personendaten), nach der Art des Bearbeitens (Informatikleistung, Datenbearbeitung durch Dritte, Inanspruchnahme einer anderen Dienstleistung) und nach dem

Umfang. Je höher die durch eine solche Auslagerung entstehenden Risiken sind, desto umfassender sind die Massnahmen. Besonders schützenswerte Personendaten, die zur Weitergabe an Drittpersonen den geschützten Bereich der Schulsysteme verlassen, müssen verschlüsselt werden.

Weitere Informationen können dem Merkblatt der Konferenz der Schweizerischen Datenschutzbeauftragten privatim entnommen werden:

https://www.privatim.ch/wp-content/uploads/2019/12/privatim-Cloud-Papier_v2_1_20191217.pdf

7 Daten auf persönlichen PCs, Laptops, externen Laufwerken und Datenträgern

Vor der Entsorgung von PCs, Laptops und anderen Datenträgern sind die Daten fachgerecht zu löschen, so dass Rekonstruktionen nicht mehr möglich sind.

8 Inkrafttreten

1. September 2021

Amt für Mittel- und Hochschulen
Der Amtschef



Urs Schwager