

(UD)

Umgang mit Daten (UD)

Ausgabe März 2019

intranet.kshp.ch/ud





Ausgangslage

In einer vermehrt digitalisierten Welt spielen Daten eine immer wichtigere Rolle. Insbesondere **personenbezogene Daten** sind ein heikles Gut: Lassen sie doch relativ einfach Rückschlüsse auf die Persönlichkeitseigenschaften zu. Als Lehrpersonen arbeiten wir täglich mit Personendaten, und deshalb ist es unerlässlich, dass wir als daten-bearbeitende Personen wissen, wie wir mit solchen Daten umgehen und diese schützen sollen.

Der vorliegende Leitfaden soll in einfachen Worten eine kleine Einführung in den Datenschutz geben und grundlegende Richtlinien für den Umgang und Schutz mit und von Personendaten definieren.

Datenschutz

Mit Datenschutz ist der Schutz der Privatsphäre und der Persönlichkeitsrechte gemeint. Die Datenschutzgesetze definieren die Rahmenbedingungen für das Bearbeiten der Personendaten. Unter Bearbeitung von Personendaten versteht man den Umgang mit Informationen (Aufzeichnungen aller Art) über Personen wie das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben oder Vernichten derselben.

Personenbezogene Daten

Personenbezogene Daten werden in zwei Kategorien eingeteilt:

- **Personendaten** sind Informationen, die sich auf eine bestimmte oder bestimmbare Person beziehen. Bestimmbar heisst, dass man mit wenig Aufwand diese Person identifizieren kann. Beispiele dafür sind Adressen, Geburtsdaten, Staatszugehörigkeit und Telefonnummern.
- **Besondere Personendaten** sind sensiblere personenbezogene Informationen, welche Rückschlüsse auf Persönlichkeitseigenschaften erlauben. Das sind z.B. Daten über religiöse oder weltanschauliche Ansichten, über die Intimsphäre, die physische und psychische Gesundheit oder die Leistung (Noten) und das Verhalten im Unterricht.

Personenbezogene Daten an der Schule

Wir Lehrpersonen arbeiten mit teils sehr sensiblen Personendaten, dies sind z.B. Daten von:

- **Schülerinnen und Schülern** – insbesondere Angaben zur Person oder zur schulischen Laufbahn aber auch Fotografien und andere Bilder von der Schülerschaft. Als besondere Personendaten gelten Informationen zu den Leistungen, zu Verhalten und Mitarbeit und zum gesundheitlichen Zustand.
- **Eltern** – insbesondere die Adressen, Telefonnummern oder Korrespondenz (bspw. E-Mails). Als besondere Personendaten gelten Informationen zum Eltern-Kinder-Verhältnis wie etwa das Sorgerecht betreffend.

Datensicherheit

Personendaten und vor allem besondere Personendaten müssen geschützt werden. Mit ein paar einfachen Grundsätzen und Einstellungen kann der Schutz dieser Daten im Wesentlichen garantiert werden. Alle Lehrpersonen werden von der Schulleitung angehalten, die folgenden Richtlinien so gut wie möglich zu beachten und umzusetzen. Anleitungen zu allen Punkten befinden sich auf dem Intranet unter ICT > Datenschutz

Einstellungen auf den persönlichen Geräten

Die folgenden Punkte gelten für die von der Schule an die Lehrpersonen abgegebenen Geräte (Laptops, iPads), sollten aber auch wenn möglich bei privat genutzten Geräten angewendet werden, wenn darauf mit Personendaten gearbeitet wird:

- Software regelmässig aktualisieren, insbesondere Betriebssysteme (Mac, Windows), Browser (Safari, Firefox, Chrome), Java und Adobe Flash Player
- Java und Adobe Flash Player, falls nicht gebraucht, deaktivieren oder deinstallieren
- Browsereinstellungen (Safari, Firefox, Chrome) für den Schutz der Privatsphäre optimieren
- Virenschutzprogramm installieren (Sophos, Avira, Avast, Intego)
- Verschlüsselung der Festplatte aktivieren (FileVault)
- Firmware-Passwort (bei Schulcomputern ist dies schon gemacht) oder BIOS-Passwort bei Windows-Geräten verwenden
- Alle zum Arbeiten wichtigen Daten regelmässig sichern. Mit Time-Machine kann ganz einfach ein Backup auf einer externen Festplatte gemacht werden



Passwörter

Passwörter tragen stark zur Datensicherheit bei und verdienen deshalb besondere Aufmerksamkeit:

- Passwörter sind nirgends zu notieren und niemandem mitzuteilen
- Starke Passwörter mit mindestens 100 Punkten auf www.passwortcheck.ch verwenden
- Passwörter sollten regelmässig geändert werden
- Es empfiehlt sich für jede Anwendung oder jeden Dienst ein anderes Passwort zu vergeben. Falls eines der Passwörter kompromittiert wurde sind somit nicht alle anderen Dienste gefährdet
- Auf <https://haveibeenpwned.com> kann überprüft werden, ob das eigene Passwort bereits auf einer Liste im Internet kursiert

Speicherung von Personendaten

Personendaten müssen immer so gespeichert werden, dass unbefugte Personen keinen Zugang erhalten können. Folgende Massnahmen sind erforderlich, um ein Mindestmass an Sicherheit gewährleisten zu können:

- Grundsätzlich gilt: Personendaten nur solange wie nötig speichern
- Clouddienste dürfen grundsätzlich nicht zum Speichern von besonderen Personendaten gebraucht werden, ausser:
- sky.kshp.ch, da die Daten an der Schule gespeichert werden
- Office365 (OneDrive) des Schulaccounts, da ein datenschutzkonformer Vertrag mit Microsoft besteht
- Personendaten auf USB-Sticks müssen immer verschlüsselt abgespeichert werden. Dies kann mit einem verschlüsselten Container gemacht werden



Kommunikation

Bei der Weitergabe von Personendaten muss zusätzliche Vorsicht gelten und es muss sicher gestellt werden, dass die Daten die richtige Person erreichen. Die folgenden Punkte beziehen sich auf die wichtigsten Kommunikationskanäle:

ProPlan

Der Fächli-Versand über ProPlan ist die sicherste Methode, um Daten auszutauschen. Insbesondere besondere Personendaten oder wichtige Dokumente müssen als «vertraulich» behandelt werden. Damit wird die Nachricht nicht per Mail versendet. Der Absender erhält lediglich den Hinweis, dass sich eine neue vertrauliche Nachricht im elektronischen Fächli befindet.

E-Mail

E-Mails gelten als nicht sichere Kommunikationsmethode, da diese unter Umständen mit genügend technischen Kenntnissen gelesen werden können. Theoretisch könnten E-Mails verschlüsselt werden, in der Praxis konnte sich dies aber nicht durchsetzen.

E-Mails werden auch regelmässig missbraucht für Erpressungen (Blackmailing, Social Engineering) oder um an Passwörter zu gelangen (Phishing). Ein paar Regeln für den Umgang mit E-Mails seien hier kurz aufgeführt:

- Unbekannten Absendern sollte grundsätzlich nicht vertraut werden, d.h. keine Anhänge und Links öffnen
- Niemals Passwörter per E-Mail übermitteln
- Schüleranfragen grundsätzlich nur an deren @kshp-Adresse beantworten.

Messaging

Mit WhatsApp ist keine datenschutzkonforme Nutzung möglich. Lehrpersonen sollten auf die schulische Nutzung verzichten. Es gibt zahlreiche Alternativen, welche die Privatsphäre der Nutzer besser schützen, wie z.B. Signal, Wire oder das Schweizer Programm Threema.



Zusammenfassung

Im Umgang mit Personendaten gibt es kein Rezept für alle Fälle. Bei Unsicherheiten sollte man sich aber in die Person, deren Daten bearbeitet werden, versetzen:

«Wie würde ich reagieren, wenn ich wüsste, dass Informationen über mich auf diese Weise gespeichert oder versendet werden?»

Zu guter Letzt: Digitale Datensicherheit bringt rein gar nichts, wenn Daten am falschen Ort ausgedruckt, Kopien liegen gelassen oder Originale auf der Kopierfläche vergessen werden.

Nützliche Links

- Website des Zürcher Datenschützers mit vielen nützlichen Tipps:
<http://www.datenschutz.zh.ch>
- Insbesondere ist die App «datenschutz.ch» zu empfehlen. Sie ist im iOS- und Android-App-Store erhältlich
- Datensicherheit für Lehrpersonen und Schulleitungen, trinationaler Leitfaden, 2015:
<https://www.lch.ch/publikationen/leitfaeden/>
- Auf dem Intranet der HoPro befinden sich Anleitungen für alle genannten Punkte:
<https://intranet.kshp.ch>
- Melde- und Anzeigestelle Informationssicherheit (MELANI) des Bundes mit aktuellen Bedrohungen und Hintergrundinformationen:
<https://www.melani.admin.ch>
- Account gehackt? Der kostenlose Service «Have I been pwned» zeigt an, ob eine Mail-Adresse, welche irgendwo als Login benutzt wird, gehackt wurde:
<https://haveibeenpwned.com>



(QD)