Informationssicherheit und Datenschutz

Merkblatt zu wichtigen Punkten

Die **gesetzliche Grundlage** für den grundsätzlichen Umgang mit Personendaten an der Schule bildet das [Gesetz über die Information und den Datenschutz (IDG)](http://www.zhlex.zh.ch/Erlass.html?Open&Ordnr=170.4)[[1]](#footnote-2) des Kantons Zürich aus dem Jahr 2007. Alle Mitarbeitenden der Schule stellen sicher, dass sie die Bestimmungen im Schulalltag einhalten. Mittels Merkblättern und Weisungen werden die gesetzlichen Bestimmungen konkretisiert.

Sowohl **analoge wie digitale Informationen** (Daten), die an einer Schule beschafft, gespeichert oder anderweitig bearbeitet werden, müssen geschützt werden. Dazu werden technische und organisatorische Massnahmen zur Informationssicherheit ergriffen, wie beispielswiese regelmässige Backups. Personendaten und besondere Personendaten erfordern während des ganzen Zyklus (von der Beschaffung bis zur Vernichtung) meist höhere Schutzmassnahmen als andere Informationen wie Sachdaten.



# Wichtige Grundsätze für den Schulalltag

## Erhebung und Bearbeitung von Personendaten

* **Zweckbindung** Personendaten dürfen nur für den Zweck bearbeitet werden, für den sie erhoben wurden, also bestimmt sind. Das Notfallblatt für das Klassenlager beispielsweise darf nur im Lager verwendet und muss anschliessend vernichtet werden. Die Daten dürfen auch nicht elektronisch für später abgelegt werden.
* **Verhältnismässigkeit** Personendaten dürfen nur verhältnismässig bearbeitet werden, also soweit es für den Zweck geeignet, erforderlich und angemessen ist.
* **Aufbewahrung** Personendaten dürfen (u.a. wegen Zweckbindung und Verhältnismässigkeit) nur so lange aufbewahrt werden, wie es für den Zweck notwendig ist. Am Beispiel von oben nur während dem Klassenlager.
* **Vernichtung** Nach dieser Frist sind die Daten entweder zu archivieren oder zu vernichten.
* **Datensparsamkeit** Es sollen nur notwendige Daten erhoben und bearbeitet werden.

Diese Grundsätze bedeuten auch, dass keine Daten auf Vorrat erhoben oder gespeichert werden sollen.

## Datensicherheit

* **Zugriffsschutz** Informationen müssen vor unbefugtem Zugriff geschützt werden. So sind beispielsweise sichere Passwörter und verschlüsselte Speichermedien zu verwenden und im Teamzimmer keine Informationen über SuS auszutauschen.
* **Verfügbarkeit** Informationen müssen bei Bedarf vorhanden sein. So ist beispielsweise durch Back-ups sicherzustellen, dass Notenlisten verfügbar sind, wenn Zeugnisse erstellt werden müssen.
* **Integrität** Informationen sollen nicht unberechtigt oder unbeabsichtigt verändert werden. So ist beispielsweise durch die Umsetzung eines Berechtigungskonzepts sicherzustellen, dass unbefugte Personen nicht Dokumente löschen können.
* **Zurechenbarkeit** Die Bearbeitung von Informationen muss einer Person zugerechnet werden können.

## Weitergabe von Daten

* **Vertraulichkeit** Daten dürfen nur an berechtigte Personen weitergegeben werden. So soll beispielsweise der Verteiler im E-Mail immer genau geprüft werden. Es sind die gesetzlichen Grundlagen für die Weitergabe zu prüfen.
* **Informationspflicht** Betroffene Personen müssen informiert werden, wenn ihre Daten weitergegeben werden. Dies gilt auch, wenn Daten an den SPD oder andere Stellen weitergegeben werden.

## Rechte der Betroffenen

* **Auskunftsrecht** Betroffene haben das Recht zu erfahren, welche Daten über sie gespeichert sind. Eltern können somit Auskunft über die erfassten Informationen zu ihnen selbst und zu den Kindern verlangen, bei denen sie das Sorgerecht haben. Einträge zu den SuS sind daher so zu erfassen, dass sie jederzeit den Eltern gezeigt werden können.
* **Berichtigungsrecht** Betroffene können die Berichtigung oder Vernichtung unrichtiger Daten verlangen.

## Umgang mit besonderen Personendaten

Daten zur Gesundheit, Religion oder Massnahmen der Sozialhilfe sind als besondere Personendaten besonders zu schützen. Es sind besondere Massnahmen bei der Speicherung und bei der Übertragung erforderlich, beispielsweise Versand mit einem sicheren E-Mail-Dienst (z.B. Inca-Mail), Zugriffschutz mittels Multifaktor-Authentifizierung oder eine Speicherung in einer CH-Cloud mit den entsprechenden Schutzmassnahmen (z.B. Verschlüsselung).

# Praktische Tipps

* **Interne Schulungen** Um sich weiterzubilden, kann man an schulinternen Schulungen zum Datenschutz teilnehmen oder sich selbst mit der [Lernumgebung Schule des DSB Zürich](https://lerne.datenschutz.ch/schule/)[[2]](#footnote-3) weiterbilden.
* **Sichere Passwörter** Mit dem [Passwortcheck](https://www.passwortcheck.ch/)[[3]](#footnote-4) können die Passwörter sicher überprüft werden.
* **Ansprechpartner** Bei Fragen kann man sich an die/den Datenschutzberaterin/Datenschutzberater der Schule wenden.

# Und falls doch einmal etwas passieren sollte – Meldepflicht

«Das verantwortliche öffentliche Organ meldet … unverzüglich die unbefugte Bearbeitung oder den Verlust von Personendaten, wenn die Grundrechte der betroffenen Person gefährdet sind.» (§ 12)

Falls doch ein Vorfall passiert, hat eine interne Meldung an die für den Datenschutz beauftragte Personen zu erfolgen. Diese meldet den Fall je nach Tragweite an die Datenschutzbeauftragte des Kantons.

Weitere Informationen sind auf der [Webseite der Datenschutzbeauftragten](https://datenschutz.ch/datenschutz-in-oeffentlichen-organen/informationssicherheit)[[4]](#footnote-5) des Kantons Zürich zu finden.

1. <http://www.zhlex.zh.ch/Erlass.html?Open&Ordnr=170.4> [↑](#footnote-ref-2)
2. [https://lerne.datenschutz.ch/schule](https://lerne.datenschutz.ch/schule/) [↑](#footnote-ref-3)
3. [https://www.passwortcheck.ch](https://www.passwortcheck.ch/) [↑](#footnote-ref-4)
4. <https://datenschutz.ch/datenschutz-in-oeffentlichen-organen/informationssicherheit> [↑](#footnote-ref-5)