educa.Guides

# Datenschutz

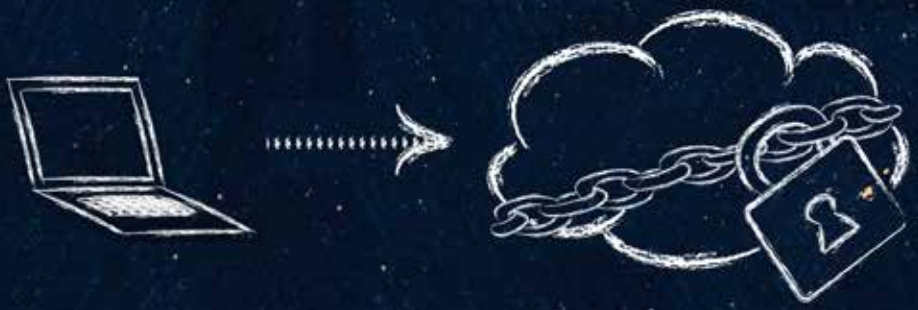
## Massnahmen betreffend Cloud Services

Merkblatt

## Impressum

Herausgeber educa.ch
Bild faithie/Shutterstock.com

© educa.ch CC BY-NC-ND (creativecommons.org)
April 2015



# 1. Datenschutz

Datenschutz ist nicht der Schutz der Daten (das wäre die Datensicherheit), sondern vielmehr der Schutz der Persönlichkeit von natürlichen und juristischen Personen vor Missbrauch der sie betreffenden Daten durch Private und Behörden. Es geht also um personenbezogene Daten und deren Schutz vor Missbrauch während der Erhebung, Verarbeitung, Nutzung und Aufbewahrung (Speicherung, Archivierung). Gleichzeitig geht es um den Schutz des Rechts auf informationelle Selbstbestimmung (jeder Mensch kann frei und selbst darüber entscheiden, wie mit seinen persönlichen Daten umgegangen wird), des Persönlichkeitsrechts und der Privatsphäre.

## 1.1 Anlaufstellen

- Anlaufstellen für Datenschutzfragen zwischen Bundesbehörden und Privaten sowie zwischen Privaten und Privaten (Lernende unter sich; Privatschule – Lernende etc.) ist der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (➔ EDÖB).
- Anlaufstellen für Datenschutzfragen zwischen kantonalen Behörden und Privaten (Schule – Lernende/Eltern/Lehrende) sind die ➔ kantonalen Datenschutzbeauftragten.

## 1.2 Basisvoraussetzungen für Cloud Computing

Die Cloud-Computing-Kundschaft in der Schweiz bleibt verantwortlich für die Einhaltung der datenschutzrechtlichen Anforderungen sowie der Geheimhaltungsvorschriften (z. B. Amtsgeheimnis). Daher ist die Beachtung folgender Punkte wichtig:

Datenschutz
- Bei Datenbearbeitung durch Dritte: Zweckbindung, Weisungsrecht, Sicherheit gewährleisten
- Beim Datenexport: Gleichwertigkeit des Datenschutzes im Ausland (EU, Safe-Harbor-Zertifizierung) oder Datenschutzvereinbarung (anerkannte Standardklauseln verwenden)
- Einbindung Subunternehmer über Cloud-Services-Anbieter

Geheimhaltung
- Spezifische Verpflichtung des Anbieters zur Einhaltung der Geheimhaltungspflicht
- Information, Einwilligung der Betroffenen bei Datenweitergabe (da Wegfall des strafrechtlichen Schutzes im Ausland)
- Verschlüsselung: möglich bei Übermittlung und bei Storage, nicht beim Processing

## 1.3 Risikobeurteilung beim Bezug von Cloud Services

Die Risikobewertung der verschiedenen Service-Modelle (IaaS, PaaS, SaaS) und Deployment-Modelle (Public, Private, Community, Hybrid Cloud) für Betrieb, Haftung, Datenschutz, Datensicherheit etc. ist unterschiedlich und hängt auch vom Schutzbedarf der Daten, Dokumente, Anwendungen, Prozesse und vom regulatorischen Umfeld ab (siehe Punkt 2 in diesem Dokument).

### 1.3.1 Datenschutz – Risiken

- Offenbarung, Weitergabe von Informationen an Nichtberechtigte
- Zugriff nicht autorisierter Personen
- Fehlende oder ungenügende Datensicherheit (keine Plausibilisierung, falsche Datenzuordnung, Datenverlust)
- Nicht-Verfügbarkeit von Daten bei Ausfall/Störung IT-Infrastruktur, der Telekommunikation
- Verfälschung, Zerstörung von Daten
- Kriminelle Energie: Denial of Service Attacken (DoS), Hacking, Viren, Sabotage, Datendiebstahl
- etc.

### 1.3.2 Datenschutz – Risikofolgen

- Datenverfälschung, -verlust durch Nutzende und Externe
- Verletzung von Geheimhaltungspflichten durch Lehrpersonen, Schulleitung
- Persönlichkeitsverletzungen (Lernende, Eltern, Lehrpersonen)
- Haftung der Schule für finanzielle Schäden
- Vertrauens-, Imageschaden Schule
- etc.

# 2. Schutzbedarf von Daten

Vor dem Gang in die Cloud müssen die Daten und Dokumente anhand ihres Schutzbedarfs klassifiziert werden. Der Schutzbedarf der Daten und Dokumente ist jedoch unabhängig davon, ob der Austausch physischer oder virtueller Natur ist. Die folgende Liste ist nicht abschliessend, sie soll nur eine Idee vermitteln, in welche Kategorien welche Daten und Dokumente einzuordnen sind. Die Grenzen können sich je nach Detaillierungsgrad resp. Ausführlichkeit der Informationen verschieben.

| | |
|---|---|
|  | **Sehr hoher Schutzbedarf:** *besonders schützenswerte Personendaten und Persönlichkeitsprofile*<br>Bearbeitung und Bekanntgabe nur, wenn gesetzliche Grundlage besteht oder wenn betroffene Person ausdrücklich einwilligt (Daten über religiöse, weltanschauliche, politische, gewerkschaftliche Ansichten oder Tätigkeiten; Gesundheit, Intimsphäre, Rassenzugehörigkeit, Massnahmen sozialer Hilfe, administrative oder strafrechtliche Verfolgungen und Sanktionen, Beurteilung wesentlicher Aspekte der Persönlichkeit) |
|  | **Mittlerer Schutzbedarf**: *Personendaten*<br>Bearbeiten und Bekanntgabe nur, wenn zur Erfüllung der gesetzlich umschriebenen Aufgaben notwendig oder Einwilligung durch betroffene Person (Name, Adresse etc.) |
|  | **Geringer** oder **kein Schutzbedarf** |

| Schutzbedarf | Massnahmen | Art der Dokumente |
|---|---|---|
|  | - Verschlüsseln<br>- Passwort-schutz<br>- Zugriffsrechte<br>- Digitale Signa-tur<br>- etc. | - Protokolle von Konferenzen, Elternabenden mit ge-sundheitlichen, disziplinarischen, religiösen, weltan-schaulichen, politischen etc. Informationen zu Einzel-personen<br>- Noten, Zeugnisse und Promotionsentscheide<br>- Berichte, Informationen aus Behörden, Diensten der Schulpsychologie, Sozialarbeit, Erziehungsberatung, Vormundschaft, Ausländerstatus<br>- Dispensationsentscheide<br>- Korrespondenz mit Lernenden und Eltern<br>- Personalführung, Personaldossiers, Schuladministra-tion, Lohnbuchhaltung etc.<br>- Dossiers zu Eltern und Kindern<br>- etc. |
|  | - Pseudonyme verwenden<br>- Anonymisieren oder verfrem-den<br>- Passwort-schutz<br>- Einverständnis einholen<br>- etc.<br><br>(je nach Inhalt, De-tailgrad und Ziel-gruppe) | - Arbeiten,Produktionen von Lernenden: Text, Bild, Au-dio, Video<br>- Schulwebseiten (je nach Inhalt)<br>- Handynummern auf mobilen Geräten (bei Schulreisen, Lager)<br>- Klassen- und Adresslisten<br>- etc. |
|  | - Öffentlicher Zugang<br>- Standard-Login ohne spezielle Berechtigun-gen<br><br>(je nach Inhalt, De-tailgrad und Ziel-gruppe) | - Präsentationen und Material für den Unterricht<br>- Stundenpläne und Änderungen<br>- Kalender<br>- Reservations-, Belegungspläne<br>- Veranstaltungsinformationen<br>- etc. |

# 3. Rollen, Rechte und Verantwortlichkeiten

Ist einmal definiert, welche Daten und Dokumente welchen Schutzbedarf benötigen, kann entschieden werden, wer diese Daten lesen, speichern, bearbeiten, archivieren und/oder löschen darf. Ausserdem ist zu entscheiden, wo (auf welchen Geräten mit welchen Sicherheitsvorkehrungen) und wie (mit welchen Applikationen) diese Bearbeitungen etc. zu erfolgen haben. Es sind Rollen, Rechte und Pflichten festzulegen, die den verschiedenen Akteuren im schulischen Kontext dann mittels Identity and Access Management (IAM) zugeordnet werden. Die Einzelheiten, sowie die Verantwortlichkeiten werden in einem Nutzungsreglement geklärt. Folgende Punkte sind zu beachten:

## 3.1 Risiken und Massnahmen

### 3.1.1 Risiken

- Zweckwidrige Nutzung
- Rechtswidrige Inhalte
- Unbefugte Offenbarung von Daten
- Unterlaufen von Sicherheitsmassnahmen
- etc.

### 3.1.2 Risikofolgen

- Verletzung Datenschutz
- Verletzung Amtsgeheimnis
- Verletzung Vertrag mit Cloud-Services-Anbieter (z. B. Hochladen von illegalen Inhalten)
- etc.

### 3.1.3 Risikominimierung durch Nutzungsreglement (Use Policy)

- Umfang der Nutzungsbefugnis (wer darf was womit?)
- Umschreibung der zulässigen Nutzungszwecke (Positivliste)
- Regelung des zulässigen Umfangs der privaten Nutzung (oder Verbot)
- Verbot unzulässiger Nutzungen (Negativliste, nicht abschliessend)
- Vorgaben bezüglich der Nutzung, wie z. B. Umgang mit Passwörtern und anderen Zugangsmitteln
- Vorgehen bei einem Schulwechsel, -austritt
- etc.

### 3.1.4 Risikominimierung durch Überwachungsreglement (Control Policy)

- Beschreibung der eingesetzten technischen Überwachungsmittel (z. B. Content Scanner, Protokollierung des Nutzerverhaltens)
- Beschreibung der Arten und der Voraussetzungen für die Auswertung von Protokollierungen (Logfiles) (anonym, pseudonym, personenbezogen)
- Massnahmen bei festgestellten Missbräuchen (Einschränkung der Nutzungsmöglichkeiten, disziplinarische, arbeitsrechtliche Sanktionen, Schadenersatzhaftung, evtl. Strafanzeige)
- Abläufe und Zuständigkeiten zur Auswertung und zur Ergreifung der erwähnten Massnahmen

## 3.2 Umsetzung

3.2.1 Empfehlungen für die schulinterne Umsetzung

- Regelung Zuständigkeiten: Abschluss von Verträgen mit Anbietern; Erlass, Durchsetzung von Reglementen; Handhabung von Datenschutzvorfällen
- Bestimmung einer datenschutzverantwortlichen Person
- Information über Nutzungsvorgaben (Reglemente)
- Sensibilisierung von Lehrpersonen, Lernenden, Eltern über mögliche Risiken und risikogerechtes Verhalten

# 4. Vertragsrisiken und Massnahmen

Sind die Punkte 2 und 3 geklärt, kann anhand des Cloud-Konzepts der Schule ein passender Cloud-Computing-Anbieter ausgesucht werden. Es ist zu empfehlen, dass dieser Prozess mit fachkundigen Personen des Bereichs Informatik und Vertragsrecht begleitet wird. Folgende Punkte sind zu beachten:

4.1.1 Anbieterkonditionen (AGB): Beurteilung der vertragsrechtlichen Risiken

- Inhalt und Qualität der Leistungen: Verfügbarkeit, Performance
- Sicherheit
- Vertragsbeendigung, Exitmanagement
- Haftung
- Rechtsanwendung, Gerichtsstand, Durchsetzung (Vollstreckung)

4.1.2 Vereinbarung und Verhandlung der Qualität der Leistungen

- Inhalt (Service Descriptions), relevant auch bei Standard-Services
- Verantwortungsbereiche des Kunden
- Service Level Agreements zur Absicherung Qualität: Definition Service Levels (Verfügbarkeiten, Antwortzeiten); Messung, Reporting der Service Levels; Service Credits, Penalties; Ansprechpartner, Hotline

4.1.3 Prüfung der Security-Bestimmungen, Verfügbarkeit, Datensicherheit verhandeln, vereinbaren

- User-Authentifizierung und User-Deaktivierung
- Zugriffsschutz: Zugriffsmethoden, -rechte; Schutz der Infrastruktur, Applikationen und Daten gegen externe Angriffe; Identity Access Management
- Business Continuity Management (Backup, Restore und Desaster Recovery)
- Zertifizierung des Service Anbieters, z. B. ISO 27001; Befolgung internationaler Standards

4.1.4 Ausgestaltung Vertragsbeendigung, Exitmanagements (je nach Service-Modell)

- Feste (Mindest-)Vertragsdauer
- Kündigungsfristen, -termine
- Zugriff auf und Herausgabe von Daten
- Löschung von Daten (nicht nur Deaktivierung)
- Migrationsunterstützung durch Service Anbieter

4.1.5 Verhandeln einer risikokonformen Haftungsregelung, Risikotoleranz evaluieren

- Haftungsausschlüsse, -beschränkungen analysieren: gesetzeskonform, risikogerecht?
- Beurteilung Haftungsklausel: Schadenspotential, Risiko des Schadenseintritts, eigenes Haftungsrisiko gegenüber Dritten, Versicherungsdeckung des Service-Anbieters?
- Subunternehmer-Risiko: Subunternehmer des Anbieters bekannt?

4.1.6 Regelung des Umgangs mit Personendaten mit dem Anbieter ➔ Vorgaben privatim

- Gegenstand und Umfang der Datenbearbeitung
- Verantwortung (wer ist wofür verantwortlich?)
- Zweckbindung (Daten dürfen nur für die Zwecke der Schule bearbeitet werden)
- Geheimhaltungsverpflichtungen (primär Amtsgeheimnis)

- Rechte der Betroffenen (Auskunftsrecht und Durchsetzung des Rechts auf Berichtigung, Löschung müssen vertraglich garantiert werden)
- Kontrollmöglichkeit der Schule oder externer Prüfstellen (z. B. Audits)
- Informationssicherheitsmassnahmen (für die Gewährleistung der Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit)
- Unterauftragsverhältnisse (Offenlegung derselben und Änderung nur mit Bewilligung der Schule)
- Bearbeitung im Ausland: entweder gleichwertiges Datenschutzniveau oder es sind zusätzliche Massnahmen zu vereinbaren
- Orte der Datenbearbeitung (Orte sind bekannt, Ortswechsel wird gemeldet und durch Schule bewilligt)
- Anwendbarkeit von Schweizer Recht (Rechtswahl)
- Gerichtsstand in der Schweiz

# 5. Auszüge gesetzlicher Grundlagen

**Geschütze Daten (DSG Art. 3)**

- Personendaten: Daten einer bestimmten oder bestimmbaren natürlichen oder juristischen Person;
- Besonders schützenswerte Personendaten sind Daten über:
  1. die religiösen, weltanschaulichen, politischen oder gewerkschaftlichen Ansichten oder Tätigkeiten,
  2. die Gesundheit, die Intimsphäre oder die Rassenzugehörigkeit,
  3. Massnahmen der sozialen Hilfe,
  4. administrative oder strafrechtliche Verfolgungen und Sanktionen
- Persönlichkeitsprofile natürlicher Personen: Beurteilung wesentlicher Aspekte der Persönlichkeit

**Grundsätze der Datenbearbeitung (DSG Art. 4)**

- **rechtmässig**: nur auf gesetzlicher Grundlage
- **verhältnismässig**: nur soweit und solange als notwendig
- **zweckgebunden**: keine nachträgliche Zweckänderung
- **erkennbar**: keine heimliche Datensammlung
- **transparent**: Auskunftspflicht über die Datenbearbeitung

**Richtigkeit der Daten (DSG Art. 5)**

Wer Personendaten bearbeitet, hat sich über deren Richtigkeit zu vergewissern. Er hat alle angemessenen Massnahmen zu treffen, damit die Daten berichtigt oder vernichtet werden, die im Hinblick auf den Zweck ihrer Beschaffung oder Bearbeitung unrichtig oder unvollständig sind.

**Grenzüberschreitende Bekanntgabe (DSG Art. 6)**

[1] Personendaten dürfen nicht ins Ausland bekannt gegeben werden, wenn dadurch die Persönlichkeit der betroffenen Personen schwerwiegend gefährdet würde, namentlich weil eine Gesetzgebung fehlt, die einen angemessenen Schutz gewährleistet.
[2] Fehlt eine Gesetzgebung, die einen angemessenen Schutz gewährleistet, so können Personendaten ins Ausland nur bekannt gegeben werden, wenn:
a. hinreichende Garantien, insbesondere durch Vertrag, einen angemessenen Schutz im Ausland gewährleisten;

**Datensicherheit (DSG Art. 7)**

Personendaten müssen durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden.

**Informationssicherheit (Beispiel: IDG § 8 Kanton BS)**

[1] Das öffentliche Organ schützt Informationen durch angemessene organisatorische und technische Massnahmen.

[2] Die Massnahmen richten sich nach den folgenden Schutzzielen:

a) Informationen dürfen nicht unrechtmässig zur Kenntnis gelangen (Vertraulichkeit);

b) Informationen müssen richtig und vollständig sein (Integrität);

c) Informationen müssen bei Bedarf vorhanden sein (Verfügbarkeit);

d) Informationsbearbeitungen müssen einer Person zugerechnet werden können (Zurechenbarkeit);

e) Veränderungen von Informationen müssen erkennbar und nachvollziehbar sein (Nachvollziehbarkeit).

[3] Die zu treffenden Massnahmen richten sich nach der Art der Information, nach Art und Zweck der Verwendung und nach dem jeweiligen Stand der Technik.

**Datenbearbeitung durch Dritte (DSG Art. 10a)**

[1] Das Bearbeiten von Personendaten kann durch Vereinbarung oder Gesetz Dritten übertragen werden, wenn:

a. die Daten nur so bearbeitet werden, wie der Auftraggeber selbst es tun dürfte; und

b. keine gesetzliche oder vertragliche Geheimhaltungspflicht es verbietet.

[2] Der Auftraggeber muss sich insbesondere vergewissern, dass der Dritte die Datensicherheit gewährleistet.

**Rechte der Betroffenen (DSG Art. 5, 8, 15, 20, 25)**

- Auskunftsrecht / Einsichtnahme
- Berichtigung unrichtiger Daten
- Vernichtung / Löschung unrechtmässig erlangter oder nicht mehr benötigter Daten
- Sperrung der unberechtigten Bekanntgabe an Dritte
- Bestreitungsvermerk wenn Richtigkeit/Unrichtigkeit nicht erwiesen
- Unterlassung unberechtigter Bearbeitungen
- Schadenersatz / Genugtuung / Publikation Urteil

**Amtsgeheimnis: Art. 320 Strafgesetzbuch**

[1] Wer ein Geheimnis offenbart, das ihm in seiner Eigenschaft als Mitglied einer Behörde oder als Beamter anvertraut worden ist, oder das er in seiner amtlichen oder dienstlichen Stellung wahrgenommen hat, wird mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft. Die Verletzung des Amtsgeheimnisses ist auch nach Beendigung des amtlichen oder dienstlichen Verhältnisses strafbar.

[2] Der Täter ist nicht strafbar, wenn er das Geheimnis mit schriftlicher Einwilligung seiner vorgesetzten Behörde geoffenbart hat.

educa.ch
Schweizer Medieninstitut für Bildung und Kultur
Erlachstrasse 21 | Postfach 612 | CH-3000 Bern 9

Telefon: +41 (0)31 300 55 00
info@educa.ch | www.educa.ch