Dossier Datensicherheit und digitale Datenverarbeitung

Stand 20. August 2020

Inhaltsverzeichnis

1. Checkliste zu Datensicherheit und digitaler Datenverarbeitung

Für den Kanton Solothurn gilt das Informations- und Datenschutzgesetz (InfoDG) vom 21. Februar 2001 (Stand 1. Januar 2015). Im § 6 Weitere Begriffe ist beschrieben, was Personendaten und Datenbearbeitung sind.

Im Schulbereich verarbeiten Schulträger unterschiedliche Daten von Schülerinnen und Schülern, Eltern, Lehrpersonen und Schulleitungen und weiteren involvierten Personen. Die Schulträger speichern und bearbeiten Personaldossiers, Arbeiten von Schülerinnen und Schülern, Fotos oder andere Daten.

1.1. Übersicht der Datenverarbeitungsabläufe

Damit der Datenschutz und das Öffentlichkeitsprinzip gewährleistet werden können, stellen sich rechtliche und organisatorische Fragen. Die Schule entscheidet.

- Welche Daten werden zur Aufgabenerfüllung benutzt?
- Ist der Schutzbedarf definiert?
- Welche Daten dürfen veröffentlicht werden? Wer muss das Einverständnis zur Veröffentlichung geben?
- Untersteht das Dokument dem Urheberrecht?
- Sind die Zugriffsrechte geregelt, wer auf welche Daten mit Lese- oder Schreibrechten zugreifen darf?
- Welche Daten sind analog, digital oder analog und digital abgelegt?
- Ist die Informationsarchitektur mit den gespeicherten Daten, den verwendeten Systemen, den Schnittstellen und den Informationsflüssen beschrieben?
- Sind die Mitarbeitenden zu Datenschutz und Öffentlichkeitsprinzip informiert und sensibilisiert?
- Ist beim Cloudcomputing die Datensicherheit als Teil des Datenschutzes erfüllt?

⇨ Das Dokument «Landkarte zu Datenschutz und Datenverarbeitung mit Beispielen» richtet sich an Schulleitungen und Lehrpersonen. Es zeigt anhand von Beispielen, in welcher Form Personendaten verarbeitet und/oder veröffentlicht werden können.

1.2. Schutzbedarf und Risikoabschätzung

Eine wichtige Basis für die Risikoabschätzung ist die Schutzbedarfsanalyse.

Die Schutzbedarfsanalyse beurteilt die Daten nach
- Vertraulichkeit
- Verfügbarkeit
- Integrität
- Nachvollziehbarkeit

Grundsätzlich sind die Personendaten, die in der Schule bearbeitet werden, sensible Daten. Die Schutzbedarfsanalyse ist bei Anpassungen oder Neuentwicklung von IT-Anwendungen zu aktualisieren.

1.3. Informationskonzept

Die Schutzbedarfsanalyse ist die Grundlage für die Risikoanalyse und die zu treffenden Massnahmen, welche im Informationssicherheits- und Datenschutzkonzept (ISDS) festgehalten werden. Bei Anpassungen oder Neuentwicklung von IT-Anwendungen sollte eine Risikoanalyse durchgeführt werden. Besteht von den Daten her ein erhöhter Schutzbedarf, sollte das ISDS angepasst werden.

1.4. Nachweis der Datenschutzkonformität

Datenschutz gilt für Dokumente auf Papier, sowie auch für digital gespeicherte Dokumente.

- Ist das kantonale Informations- und Datenschutzdokument bekannt und umgesetzt?
- Sind die Daten in analoger und digitaler Form genügend geschützt?
- Welche Aspekte sind speziell bei der digitalen Verarbeitung, Speicherung und Archivierung zu beachten?
- Sind beim Cloudcomputing die Vertraulichkeit und die Integrität der Daten gewährleistet?
- Ist die Verfügbarkeit der Daten gewährleistet?

⇨ Das Dokument «Clouds in der Volksschule – was ist zu beachten?» richtet sich an Schulleitungen.

1.5. Meldung bei Datenschutzverletzungen/Notfallkonzept

- Besteht ein Notfallkonzept, wie bei Datenschutzverletzungen vorgegangen wird?
- Wie werden Personen, die von der Datenschutzverletzung betroffen sind, informiert?

1.6. Technische Umsetzung

⇨ Das Dokument «Datensicherheit: Allgemeine Tipps für den Schutz von Dokumenten und E-Mails» richtet sich an Schulleitungen und PICTS.

2. Landkarte zu Datenschutz und Datenverarbeitung mit Beispielen

	Mitarbeitende	Schülerinnen und Schüler Eltern	Speicherung	E-Mail-Versand
Personendaten	– geschäftliche Personenangaben (z.B. Kontaktdaten einer Schulleitung) – geschäftliches Foto eines Mitarbeitenden	– Adressdaten zur gegenseitigen Kontaktaufnahme (Rundtelefon, SMS) – Aufsatz mit Namen einer bestimmbaren Person – Foto mit erkennbaren Gesichtern ohne eindeutige Namen	– interne Dateiablage – clientseitig verschlüsselte Public-Cloud – Gerichtsstand Schweiz – Speicherort Schweiz – Speicherort Europa mit educa-Microsoft-Rahmenvertrag	Personendaten von einzelnen Personen unverschlüsselt möglich
besonders schützenswerte Personendaten	Personalakten – Mitarbeiterbeurteilung – Arztzeugnisse – Arbeitszeiterfassungen – weitere	– Beurteilungen – Zeugnisse – Berichte – Schulausschluss – medizinische Daten – laufende Abklärungen – Portfolio – Aufsatz mit besonders schützenswerten Personendaten, z.B. mit Name und Krankheit einer Person – Foto mit erkennbaren Gesichtern und Namen	– interne Dateiablage – clientseitig verschlüsselte Public-Cloud mit Schlüssel beim Schulträger – Gerichtsstand Schweiz – Speicherort Schweiz	verschlüsselt

§ 6 des kantonalen Informations- und Datenschutzgesetzes (InfoDG)

3. Clouds in der Volksschule – was ist zu beachten?

3.1. Ausgangslage

In der Broschüre «Informatische Bildung – Regelstandards für die Volksschule» von 2015 ist der Referenzrahmen informatische Bildung mit sieben didaktischen Handlungsfeldern enthalten. Die Umsetzung in den Schulen erfolgt seit dem Schuljahr 2017/2018 flächendeckend. Neben den pädagogischen Aspekten enthält die Broschüre auch Empfehlungen zu technischen Aspekten. Diese sind:

- 1:1-Computing und Bring Your Own Device (BYOD) nutzen
- für immer heterogenere Infrastruktur bereit sein
- leistungsfähige Bandbreiten und professionelle Netzwerke einrichten
- Cloud-Computing angemessen einsetzen
- professionellen technischen und pädagogischen Support sicherstellen

3.2. Cloud-Computing

ENISA (European Network and Information Security Agency) definiert Cloud-Computing folgendermassen: «Cloud-Computing ist ein Modell, das es erlaubt, bei Bedarf jederzeit und überall bequem über ein Netz auf einen geteilten Pool von konfigurierbaren Rechnerressourcen (z. B. Netze, Server, Speichersysteme, Anwendungen und Dienste) zuzugreifen, die schnell und mit minimalem Managementaufwand oder geringer Serviceproviderinteraktion zur Verfügung gestellt werden können.»

Es gibt verschiedene Service-Modelle:

- IaaS (Infrastructure as a Service) = Infrastruktur wie beispielsweise Datenspeicher, Rechenleistung
- PaaS (Platform as a Service) = Plattform mit verschiedensten Dienstleistungen
- SaaS (Software as a Service) = Software, Anwendungen, Apps

Beim Cloud-Computing werden Daten via Browser übertragen und an anderen Orten gespeichert. Datenschutz und Datensicherheit sind, neben weiteren Aspekten, zentral.

3.3. Privatim – die schweizerischen Datenschutzbeauftragten

Privatim hat drei Merkblätter zu Cloud-Computing herausgegeben:

- privatim – die schweizerischen Datenschutzbeauftragten: «Merkblatt – Cloud Computing» V 1.0/Juli 2013
- privatim – die schweizerischen Datenschutzbeauftragen: «Merkblatt – Cloud Computing im Schulbereich», V 1.0/Oktober 2013
- privatim – die schweizerischen Datenschutzbeauftragten: «Merkblatt – Cloud-spezifische Risiken und Massnahmen», V 2.1/17.12.2019

Diese Merkblätter sind bei der Nutzung von Cloud-Computing zu beachten.

3.4. Kriterienkatalog für Cloudlösungen des Bildungsraums Nordwestschweiz

Die Arbeitsgruppe informatische Bildung/ICT Schulen des Bildungsraums Nordwestschweiz hat einen Kriterienkatalog für Cloudkriterien als Entscheidungshilfe für Schulleitungen und ICT-Verantwortliche entwickelt. Der Kriterienkatalog und der zu Office365 ausgefüllte Kriterienkatalog sind auf der Webseite des Bildungsraum Nordwestschweiz aufgeschaltet unter https://www.bildungsraum-nw.ch/dokumente.

3.5. Anforderungen an Cloud-Computing

Für die Schulen ist wichtig, dass die Schülerinnen und Schüler, die Lehrpersonen, die Schulleitung

und die Schulverwaltung jederzeit, ortsunabhängig und mit unterschiedlichen Geräten auf Daten zugreifen und diese bearbeiten können.

Cloudplattformen

Eine Cloudplattform kann einzelne oder mehrere Cloud-Dienste anbieten:

- Dateiablage
- E-Mail-Services
- Agenda
- Aufgaben
- Kollaborationsmöglichkeiten
- Lernplattformen

Daten

Eine Schule speichert und verarbeitet Personendaten von Schülerinnen und Schülern, Eltern und Mitarbeitenden. Zu den Personendaten gehören beispielsweise Adresslisten, Arbeiten von Schülerinnen und Schülern, Mitarbeiterbeurteilungen und Zeugnisdaten. Informations- und Datenschutzgesetz vom 21.02.2001 (Stand 01.01.2015) beschreibt den Umgang mit Personendaten.

Welches sind die Anforderungen von den Schulen her an Cloudpattformen?
Die Daten sind

- gemäss rechtlichen Vorgaben bearbeitet und gespeichert
- an einem sicheren Ort gespeichert
- gemäss Anforderungen verfügbar
- ortsunabhängig bearbeitbar
- einfach nutzbar
- von unterschiedlichen Geräten her bearbeitbar
- mit unterschiedlichen Betriebssystemen bearbeitbar
- einfach mit lokalen Daten synchronisierbar
- mit anderen teilbar

Anforderungen an die Datensicherheit

Ein Teil des Datenschutzes ist die Datensicherheit. Zur Datensicherheit gehören:

Merkmale	Umsetzung
gesicherte Verbindungen	Können die Daten mit einer sicheren Verbindung übertragen werden?
verschlüsselte Datenspeicherung	Wie können die Daten verschlüsselt werden? Ist der Schlüssel beim Kunden gespeichert?
regelmässige Backups und Recovery-Möglichkeit	Wie oft wird ein Backup gemacht? Gibt es eine Recovery-Möglichkeit?
redundant gespeicherte Daten an einem anderen Speicherort	Sind die Daten an einem zweiten Speicherort gesichert?
Berechtigungskonzept	Ist ein klares Rollen- und Rechtekonzept vorhanden? Kann die Cloudlösung das Konzept abbilden?
Authentifizierung	Wie werden Benutzerinnen und Benutzer überprüft?
Schutz vor ausserordentlichen Ereignissen	Welchen Schutz bietet die Cloudfirma bei Stromausfall oder anderen Ereignissen?
Schutz der Daten vor Missbrauch durch Mitarbeitende von Rechenzentren	Wie wird der Schutz der Daten vor Missbrauch durch Mitarbeitende gewährleistet?
Schutz der Daten, auch wenn der Provider die Daten bei einer anderen Firma speichert (Subkontrakt)	Vergibt der Cloudanbieter Aufträge an weitere Firmen? Sind Subkontrakte im Vertrag geregelt?
Schutz der Daten im Konkursfall eines Datenproviders	Nicht alle Risiken können mit Prävention und Verträgen abgesichert werden.

Verträge mit Cloudanbietern

- Welche Daten mit welchem Schutzbedarf werden in der Cloud gespeichert? Der Schutzbedarf der Daten bestimmt, ob und mit welchen Sicherheitsvorkehrungen die Daten in einer Cloud gespeichert werden.
- Erfüllt der Cloudanbieter die Anforderungen des Datenschutzes?
- Welche Punkte sollte ein Cloud-Dienstleistungsvertrag regeln?
  - Dienstleistungen
  - Betrieb mit Verfügbarkeit, Datenschutz, Datensicherheit, Backups
  - Wartung und Aktualisierung der Systeme
  - Support mit Bereitschafts- und Antwortzeiten
  - Verschlüsselung der Daten bei Übertragung und Speicherung
  - Information der Kundinnen und Kunden bei Umstellungen oder Systemausfällen
  - Standort der gespeicherten Daten
  - Recht, Gerichtsstand
  - Vorgehen bei Vertragsauflösung
  - Kosten

Beispiel der Firma anykey IT AG:
- Allgemeine Geschäftsbedingungen, April 2015
- Datenschutz, April 2020

4. Datensicherheit: Allgemeine Tipps für den Schutz von Dokumenten und E-Mails

Es gelten folgende Grundsätze:

- Sichere Passwörter verwenden und diese an einem sicheren Ort aufbewahren. Es gibt Anwendungen, bei denen man die Passwörter nicht wiederherstellen kann und damit auch nicht mehr auf die Daten zugreifen kann.
- Beim Versand von verschlüsselten oder mit Passwort geschützten Dokumenten, das Passwort mit einem anderen Medium mitteilen, beispielsweise mündlich oder per SMS.
- Für den Versand von E-Mails empfiehlt sich eine Secure-Mail-Lösung.
- Einrichten und Support der Anwendungen durch eine IT-Fachperson.

Was	Wie	Tool	Eigenschaften	Bemerkungen
Passwörter sicher aufbewahren	Sichere Aufbewahrung von Passwörtern	https://keypass.info/	Open Source	Geht das Hauptpasswort verloren, kann man nicht mehr auf die anderen Passwörter zugreifen.
Zwei-Faktor-Authentifizierung anwenden	Neben dem Passwort braucht es eine weitere Komponente, wie beispielsweise einen weiteren PIN-Code oder ein Smartphone.	– Authy – Free OTP		
Datei-Archive verschlüsseln	Verschlüsselung mit einem Passwort	– 7-Zip	Open Source	Verschlüsseltes Archiv und Passwort dazu mit zwei verschiedenen Medien übertragen (mündlich oder per SMS).

Was	Wie	Tool	Eigenschaften	Bemerkungen
E-Mails versenden	Secure-Mail verwenden	– PrivaSphere – Inca-Mail von der Post – Proton-Mail – Pretty Good Privacy (PGP): GnuPG		Ein Secure-Mail sollte verwendet werden. IT-Fachperson
Daten mit Webtransfer übertragen	Sind die Dokumente zu gross als E-Mail-Anhang ist die Übertragung mit Webtransfer möglich.	– We Transfer	US-Firma	nur Sachdaten, Daten mit 7-Zip verschlüsseln
Daten auf mobilen Geräten oder USB-Sticks	Zur Verschlüsselung	– Veracrypt		IT-Fachperson
Clouddaten verschlüsseln	Sichere Verschlüsselungssoftware	– Boxcryptor – Cryptomator		IT-Fachperson

Die Aufstellung zeigt als Beispiele Software-Lösungen auf (Stand August 2019)

5. Link-Zusammenstellung Informations- und Datenschutzunterlagen

5.1. Rechtliche Grundlagen Kanton Solothurn

- Informations- und Datenschutzgesetz vom 21.02.2001 (Stand 01.01.2015)
- Informations- und Datenschutzverordnung vom 10.12.2001 (Stand 01.07.2004)

5.2. Kantonale Merkblätter zu Information und Datenschutz Kanton Solothurn

- Merkblatt: Fotos auf den Webseiten von Schulen, Juli 2015/aktualisiert 2018
- Merkblatt - Ihre Rechte nach dem Informations- und Datenschutzgesetz
- Merkblatt – Datenschutz an der solothurnischen Volksschule

5.3. Dokumente von Privatim

- privatim – die schweizerischen Datenschutzbeauftragten: «Merkblatt – Cloud Computing» V 1.0/Juli 2013
- privatim – die schweizerischen Datenschutzbeauftragen: «Merkblatt – Cloud Computing im Schulbereich», V 1.0/Oktober 2013
- privatim – die schweizerischen Datenschutzbeauftragten: «Merkblatt – Cloud-spezifische Risiken und Massnahmen», V 2.1/Dezember 2019

5.4. Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter EDÖB

- Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter EDÖB: «Datenschutz Informationsdossier», ohne Datum

5.5. Bildungsraum Nordwestschweiz

- Kriterienkatalog für Cloudlösungen
- Kriterienkatalog für Cloudlösungen – Office 365 Education

5.6. Beispiel Firma anykey IT AG

- Allgemeine Geschäftsbedingungen, April 2015
- Datenschutz, April 2020