Kanton Bern
Canton de Berne

Bildungs- und Kulturdirektion
Mittelschul- und Berufsbildungsamt

Datenschutz bei der Cloudnutzung

Leitfaden für Lehrpersonen der Sekundarstufe II

Bearbeitungsdatum	30. September 2021
Version	1
Dokument Status	freigegeben
Klassifizierung	Nicht klassifiziert
Autor/-in	Projektteam unter der Leitung von Lukas Ritter, gibb
Dateiname	Leitfaden_Datenschutz_Cloudnutzung_V1_de.docx

Inhaltsverzeichnis

1. Zweck des Dokuments

Nachfolgende Beschreibungen gelten für die Klassifizierung und den Umgang mit Daten in Cloud-Diensten durch Lehrpersonen auf der Sekundarstufe II.

1.1. Ausgangslage und Ziel

1.1.1. Ausgangslage

- Das Arbeiten mit elektronischen Medien stellt erhöhte Anforderungen an die Informationssicherheit und das Datenmanagement.
- Anwendende benutzen ihre eigenen ICT-Mittel und arbeiten mit diesen Mitteln in Netzwerken ausserhalb und auch innerhalb ihrer eigenen ICT-Infrastruktur.
- Sämtliche gesetzlichen und verbindlichen Vorgaben zum Datenschutz müssen eingehalten werden.

1.1.2. Ziel

Informationen und Systeme der Schulen der Sekundarstufe II, ihrer Kund/innen, Partner/innen und dem Personal sind so behandelt, dass:

- die Vertraulichkeit dort gewahrt bleibt, wo dies erforderlich ist,
- die erforderliche Verfügbarkeit gewährleistet ist,
- die gesetzlichen und vertraglichen Verpflichtungen eingehalten sind.

1.2. Verwendete Begriffe und Abkürzungen

Begriff	Definition	Abkürzung
Bring Your Own Device	Eigenes mitgebrachtes Gerät	BYOD
information and communications technology	Englischer Begriff für jegliche Kommunikationsanwendung, darunter Radio, Fernsehen, Handys, Smartphones, Hardware und Software für Computer und Netzwerke, Satellitensysteme, sowie für die verschiedenen Dienstleistungen und Anwendungen, die damit verbunden sind.[1]	ICT

1.3. Weitere Informationen zum Thema

- Leitfaden Datenschutz in den Volksschulen des Kantons Bern[2]
- Datenschutz.ch[3] – Webauftritt des Datenschutzbeauftragten des Kantons ZH
- Educa.ch – Rahmenverträge

[1] Auszug aus Wikipedia
[2] https://www.erz.be.ch/erz/de/index/kindergarten_volksschule/kindergarten_volksschule/leitfaeden.assetref/dam/documents/ERZ/AKVB/de/09_Schulleitungen_Lehrpersonen/sl_lp_Unterlagen_datenschutz_leitfaden_d.pdf
[3] www.datenschutz.ch

2. Generelle Bedingungen

2.1. Rahmenbedingungen

Der vorliegende Leitfaden berücksichtigt nur Plattformen und Dienste, welche durch Rahmenverträge zwischen educa, der Fachagentur im Auftrag des Bundes und der Kantone, und dem/der jeweiligen Plattform-/Dienstanbieter/in abgedeckt sind. Zum aktuellen Zeitpunkt sind dies folgende privaten Anbieter/innen:

Hersteller/in	Produkt
Adobe	Creative Cloud K12
Google	G Suite for Education
Microsoft	Microsoft 365 for Education
Univention	UCS

Mit diesen privaten Anbietern hat educa Rahmenverträge abgeschlossen, welche die Voraussetzung schaffen, damit deren Produkte durch die Bildungsinstitutionen rechtskonform genutzt werden können. Dabei wird unter anderem auf folgenden Aspekt fokussiert:

- Die Vertragsbedingungen unterliegen Schweizer Gerichtsbarkeit und schaffen Grundlagen für eine rechtskonforme Nutzung.

Dadurch entsteht für die Schulen mehr Rechtssicherheit und die Risiken beim Einsatz der digitalen Dienste werden gemildert. Die Rahmenverträge befreien die Schulen allerdings nicht davor, zu prüfen, ob die darin vereinbarten Bedingungen – unter Berücksichtigung der von den Schulen geplanten Nutzung – den Anforderungen des kantonalen Rechts entspricht.[4]

2.2. Klassifizierung von Informationen

- Alle Informationseigentümer/innen sind immer verantwortlich für den Inhalt ihrer Information.
- Sie sind ebenfalls dafür zuständig, die eigenen Informationen gegenüber den Nutzenden richtig zu klassifizieren.
- Die Klassifizierung muss stufenweise entsprechend den Schutzbedürfnissen und daraus ergebenden Schutzbedingungen erfolgen.

[4] https://www.educa.ch/de/taetigkeiten/rahmenvertraege/informationen-fuer-schulen

2.3. Klassifizierungsstufen und Umgang mit Daten und Informationen auf Cloud-Diensten

Stufe	Kennzeichnung	Beschreibung	Speicherung	Teilen Zielgruppe	**Beispiele** (nicht abschliessend)
öffentlich	nein	Veröffentlichung auf Webseite, Cloud oder anderen Sharing-Plattformen	Mit einfacher Authentifizierung	alle	• Stundenplan, Ferienplan • Allgemeine Schulinformation • Protokoll von Fachgruppen (ohne Personendaten) • Unterrichtsvorbereitung • Arbeitsblatt (ohne Personendaten) • Kommunikation für die Öffentlichkeit (Schulanlässe etc.)
vertraulich	ja	Informationen ohne Personenbezug	Verschlüsselt und mit einfacher Authentifizierung	beteiligte und betroffene Personen	• Schulleitungsprotokoll • Kommunikation ohne psychologische oder medizinische Inhalte zu einzelnen Personen • Sitzungsprotokoll (ohne Personenbezug) • Prüfungen (nicht ausgefüllt)

Personendaten (organisatorische Informationen über eine Person)	ja	Name, Vorname, Adressen, Telefon-Nr., Geburtsdatum etc.	Verschlüsselt und mit einfacher Authentifizierung[5]	beteiligte und betroffene Personen (in der Regel Lehrpersonen der Klasse und Verwaltung)	• Klassenliste
					  ○ Telefonverzeichnis
					  ○ Absenzenliste (ohne Gründe)
					  ○ Adressliste der Klasse
					• Notenübersicht (ohne Bemerkungen zu Personen)

				beteiligte und betroffene Personen (in der Regel Klasse)	• Bild- und Tonaufnahmen (mit darin erkennbaren Personen)
				beteiligte und betroffene Personen (in der Regel Lehrpersonen und Verwaltung)	• Sitzungsprotokoll (mit allgemeinen Inhalten zu Lernenden)
Besonders schützenswerte Personendaten (private Informationen über eine Person)	ja	Gesinnungs-, Verhaltens-, Aktivitäts-, Gesundheits- sowie rechtswirksame Informationen über eine Person.	Verschlüsselt und mit 2-Faktor Authentifizierung[6]	berechtigte Personen zur Ausführung ihres Berufsauftrags	• Aktennotiz (mit Bemerkungen zu Personen) • Prüfung (ausgefüllt und bewertet) • Entschuldigung mit Begründung • Beurteilung • Arztzeugnis • Bemerkung zu Absenzen • Protokoll von MA unter Beobachtung • Gesprächsnotiz mit Lernenden • Information zum Nachteilsausgleich • Arbeitsergebnis von Lernenden • Kommunikation mit psychologischen oder medizinischen Inhalten zu einzelnen Personen

[5] Die Datenschutzaufsichtsstelle des Kantons Bern empfiehlt, Personendaten auch mit 2-Faktor Authentifizierung zu schützen.
[6] Die Datenschutzaufsichtsstelle des Kantons Bern empfiehlt, besonders schützenswerte Personendaten nicht in die Cloud auszulagern und stattdessen die dafür vorgesehenen Fachapplikationen zu benutzen.

Anhang: Hinweise & Tipps zum Umgang mit Daten

- Die Kette ist so stark wie ihr schwächstes Glied. Dazu gehören auch Endgeräte (BYOD). Darum ist es unerlässlich, dass ein Endgerät folgende Sicherheitsmerkmale aufweist:
  - Passwort Schutz bei der Anmeldung (alternativ Gesichtserkennung oder Fingerabdruckerkennung)
  - Festplatten-Verschlüsselung aktiviert (z.B. BitLocker (Windows) oder FileVault (Apple) aktivieren oder unabhängiges Tool (z.B. VeraCrypt, DiskCryptor oder 7-Zip)
  - Aktiver und aktueller Virenschutz und
  - Aktuelle Update-Version des Betriebssystems.

- Die Schule kann beim Zugriff auf ihre Cloud-Dienste die Sicherheitsmerkmale eines BYOD überprüfen. Bei Verwendung eines BYOD in der Schule muss diese Überprüfung erlaubt sein. Wenn dies nicht erlaubt wird, ist möglicherweise kein oder nur ein eingeschränkter Zugriff auf die Cloud-Dienste der Schule gewährt.

- Wird ein Arbeitsgerät von der Schule zur Verfügung gestellt, dann ist die Schul-IT für die Konfiguration der Sicherheitsmerkmale auf dem Gerät verantwortlich.

- Auch ein Handy / Mobiltelefon ist ein Computer mit Internetanschluss und Speicher. Hier gelten die gleichen Sicherheitsaspekte wie beim BYOD.

- In der Schule nie das gleiche Passwort wie privat verwenden.

- Wenn sensitive Daten aus der Cloud heruntergeladen und auf externe Speichermedien verschoben werden (USB Stick oder anderes externes physisches Speichermedium) dann sind diese Daten dort ungeschützt und es besteht die Gefahr des physischen Verlustes. Aus diesem Grund sind diese Daten dort zusätzlich mit einem Passwort zu schützen. Das kann z.B. mit dem Programm 7zip gemacht werden.

- Die Grenzen zwischen dem gesicherten Clouddienst der Schule und den ungesicherten öffentlichen Cloud-Diensten sind oft mit nur einem «Klick» überwunden.

- Es ist einfach und schnell eine Lösung auf z.B. Dropbox, Slack oder WhatsApp für die Zusammenarbeit einzurichten. Einfach und schnell ist aber nicht unbedingt der richtige Weg, wenn es um Datenschutz geht. Vor allem bei Gratisdiensten ist es oft so, dass diese gar nicht gratis sind. Man "bezahlt" mit den Daten, welche man preisgibt. Es lohnt sich diesbezüglich die AGB dieser Dienste vorher genau zu prüfen. 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 oder Threema Work).

Bern, 5. November 2021

Mittelschul- und Berufsbildungsamt

Barbara Gisi, Vorsteherin