Kanton Bern
Canton de Berne

Bildungs- und Kulturdirektion
Amt für Kindergarten, Volksschule und Beratung
Regelschulen Deutsch

MERKBLATT GOOGLE WORKSPACE FOR EDUCATION

1 Inhaltsverzeichnis

1 Einleitung

Dieses Merkblatt richtet sich an die verantwortlichen Stellen von Volksschulen, die das Produkt «Google Workspace for Education» als Dienstleistung nutzen wollen (Software as a Service). Es vermittelt ihnen einen groben Überblick über die Vorgehensweise, über nötige Vorabklärungen und über Massnahmen, die zu ergreifen sind, um «Google Workspace for education» möglichst datenschutzkonform zu nutzen. Namentlich berücksichtigt werden Risiken, die bei der Nutzung der Cloud für Datenbearbeitungen auftreten, sowie Massnahmen, die zu treffen sind, wenn besonders schützenswerte Personendaten bearbeitet werden.

Das Merkblatt ist eine Ergänzung zum Datenschutzlexikon des Kantons Bern.

2 Verantwortlichkeiten

Die Gemeinde trägt die alleinige Verantwortung für den Einsatz der angestrebten Infrastruktur mit Google Workspace for Education in ihrer Schule. Die kommunale Datenschutzaufsichtsstelle der Gemeinde prüft das Konzept und veranlasst unter Umständen Verbesserungen.
Die kommunale Datenschutzaufsichtsstelle kann sich mit datenschutzrechtlichen Fragen an die kantonale Datenschutzaufsichtsstelle wenden.

3 Vertragliche Ebene

Durch die Nutzung von Google Workspace for Education in der Volksschule entstehen für die verantwortlichen Behörden erhöhte Risiken im Bereich des Datenschutzes[1].

Ein wichtiges Instrument, um diese Risiken zu minimieren, ist der Educa-Rahmenvertrag, der Schweizer Recht mit Schweizer Gerichtsstand und die Wahl der Serverstandorte in der Europäischen Union oder in der Schweiz regelt.

Trotz des Rahmenvertrags verbleiben im Zusammenhang mit der Bearbeitung von besonders schützenswerten Daten und der von Google erhobenen Randdaten bestimmte Risiken. Diese können unter Umständen durch aufwendige technische Massnahmen beseitigt werden. Andere Risiken hingegen lassen sich nicht beseitigen oder allenfalls nur minimieren. Diese bleiben als sogenannte Restrisiken bestehen. Diese Restrisiken müssen ausgewiesen und der verantwortlichen Leitungsebene nachvollziehbar kommuniziert werden. Restrisiken, die die Leitungsebene als tragbar bewertet, können und müssen von dieser akzeptiert werden (Risikoakzeptanz).

Es gilt zu beachten, dass die vertraglichen Regelungen, insbesondere die Vertragsdauer, periodisch geprüft und allfällige Erneuerungen entsprechend geplant werden. Dies gilt auch für die von educa ausgehandelten Rahmenverträge.

4 Konzept

Bevor Google Workspace for Education implementiert und genutzt wird, ist ein Konzept zu erstellen, das die Inhalte der Kapitel 4.1 bis 6 regelt – insbesondere die beabsichtigte Bearbeitung von Daten und die vorgesehenen Schutzmassnahmen [2].

[1] vgl. das überarbeitete privatim-Merkblatt «Cloud-spezifische Risiken und Massnahmen»: Überarbeitetes privatim-Merkblatt «Cloud-spezifische Risiken und Massnahmen» – privatim
[2] Die Schulinformatik der PHBern unterstützt die Schulen in der Erarbeitung eines Cloudkonzepts.

Folgende Punkte sind dabei zentral:

- Nutzungsszenarien

  Welche Daten sollen für welchen Zweck auf welche Art und Weise bearbeitet werden?
- Klassifizierung der Daten

  Welchen Schutzbedarf weisen die eruierten Daten auf?
- Auswahl der geeigneten Dienste

  Mit welchen Google-Diensten will die Schule welche Nutzungsszenarien umsetzen?
- Risiken erkennen und Schutzmassnahmen treffen

  Welchen Risiken ist die Personendatenbearbeitung ausgesetzt?
  Mit welchen angemessenen Massnahmen können diese Risiken beseitigt oder zumindest minimiert werden?
- Restrisiken ausweisen

  Bestimmte Risiken verbleiben bzw. können trotz Massnahmen nicht beseitigt werden. Diese Restrisiken müssen ausgewiesen und der verantwortlichen Leitungsebene nachvollziehbar kommuniziert werden. Restrisiken, die die Leitungsebene als tragbar bewertet, können und müssen von dieser akzeptiert werden (Risikoakzeptanz).

4.1 Nutzungsszenarien

Die Nutzungsszenarien für Google Workspace for Education stellen den Kern des Konzepts dar. Sie beschreiben die Bedürfnisse der Schule in Bezug auf die Digitalisierung. Sollten sich nach der Implementierung von Google Workspace for Education weitere Bedürfnisse zeigen, muss das Konzept ergänzt werden.

Die Nutzungsszenarien sollen mit allen Beteiligten Personengruppen der Schule erarbeitet werden.

Folgende Punkte sollen in der Erarbeitung berücksichtigt werden:

- Nutzungsszenario im Rahmen der gesetzlichen Aufgabenerfüllung der Schule
  - Vorgängig muss die Zweckbindung geklärt werden
    - Beispiel für eine **legitime** Zweckbindung: *«Die Lehrperson hält fest, was sie bei einer Schülerin oder einem Schüler beobachtet.»*
    - Beispiel für eine **nicht** legitime Zweckbindung:
      «Alle Lehrpersonen einer Klasse wollen über die Lernstände der Schülerinnen und Schüler in sämtlichen Fachbereichen informiert sein.»
- Involvierte Personengruppen / Betroffene festhalten
- Die daraus resultierenden Produkte/Daten

Beispiel einer Zusammenstellung von Nutzungsszenarien mit Zweckbindung (nicht abschliessend):

	Szenario	Betroffene	Produkte/Daten
1	Ergebnisse von Einzel- oder Gruppenarbeiten (kooperative Arbeitsformen) OHNE Personenbezug	Schülerinnen und Schüler, Lehrpersonen	Website, Dokument, Ton- und Videoaufnahmen
2	Durchführung von Lernkontrollen	Schülerinnen und Schüler, Lehrpersonen	Dokumente, Tabellen (Auswertung)
3	Informationen an Eltern der Klasse (Klassenlager, Schulanlässe usw. …)	Schulleitung, Lehrpersonen, Erziehungsberechtigte	Dokumente, Mail

4	Kontaktdaten der Eltern erfassen (Telefon, Mail) und der Klasse, den Lehrpersonen wie auch den Erziehungsberechtigten zugänglich machen.	Schülerinnen und Schüler, Lehrpersonen, Erziehungsberechtigte	Dokumente, Mail
5	Dokumentieren des Mitarbeitergesprächs	Schulleitung, Lehrpersonen	Dokument
6	Erstellen von Förderplänen im Bereich Integration und einfache sonderpädagogische und unterstützende Massnahmen im Regelschulangebot (MR, ehemals IBEM).[3]	Lehrpersonen, Klassenlehrperson, Erziehungsberatung, Erziehungsberechtigte	Dokumente, Mail

4.2 Klassifizierung der Daten – Bestimmung des Schutzbedarfs

Mithilfe eines Klassifizierungsprozesses ermitteln die Schulen, wie hoch der Schutzbedarf der Daten ist. Dabei werden folgende Ziele verfolgt:

- Grundlage für die Sensibilisierung bei den Nutzenden (Schulungen)
- Eruierung der zu untersuchenden Szenarien mittels einer Risikomatrix
- Eruierung des Schutzbedarfs von Daten ohne Personenbezug

Das Ampelsystem der PHBern[4] kann für die Kategorisierung von Daten eine Hilfestellung sein.

Die Produkte/Daten der einzelnen Szenarien werden analog der KRGV[5] wie folgt klassifiziert:

Schutzbedarf	Klassifizierung	Beschreibung
kein Schutzbedarf	Öffentlich	Diese Kategorie beschreibt Sachdaten wie zum Beispiel Unterrichtsmaterialien ohne Personenbezug, anonymisierte Personendaten.
normaler Schutzbedarf	Intern	In dieser Kategorie werden normale Personendaten erfasst. Beispiele: Vorname, Name, Mailadresse etc.
hoher Schutzbedarf	Vertraulich	Ein hoher Schutzbedarf besteht bei besonders schützenswerten Personendaten oder auch bei umfangreichen Sammlungen von normalen Personendaten und Persönlichkeitsprofilen. Beispiele: Krankheiten, Straftaten, Notfall-Klassenliste mit weiteren Telefonnummern und evtl. mit Informationen zu Krankheiten, Klassenübersicht mit beurteilungsrelevanten Daten. Ebenfalls können auch Sachdaten betroffen sein, die unter Berufs- oder Amtsgeheimnis stehen.

Beispiel einer Klassifizierung im Konzept:

	Szenario	Betroffene	Produkte/Daten	Klassifizierung
1	Ergebnisse von Einzel- oder Gruppenarbeiten (kooperative Arbeitsformen) OHNE Personenbezug	Schülerinnen und Schüler, Lehrpersonen	Website, Dokument, Ton- und Videoaufnahmen	Öffentlich
2	Durchführung von Prüfungen/Tests inklusive Beurteilung	Schülerinnen und Schüler, Lehrpersonen	Dokumente, Tabellen (Auswertung)	Vertraulich
3	Informationen an Erziehungsberechtigte der Klasse (Klassenlager, spezielle Anlässe…)	Schulleitung, Lehrpersonen, Erziehungsberechtigte	Dokumente, Mail	Intern

[3] vgl. die VMR, https://www.belex.sites.be.ch/data/432.271.1/de/
[4] https://kibs.ch/datenschutz/ampelsystem
[5] Verordnung vom 13. März 2013 über die Klassifizierung, die Veröffentlichung und die Archivierung von Dokumenten zu Regierungsratsgeschäften (Klassifizierungsverordnung, KRGV; BSG 152.17).

4	Kontaktdaten der Erziehungsberechtigten erfassen (Telefon, Mail) und der Klasse, den Lehrpersonen wie auch den Erziehungsberechtigten zugänglich machen. Nicht im Sinne einer Liste von Krankheiten oder Allergien.	Schülerinnen und Schüler, Lehrpersonen, Erziehungsberechtigte	Dokumente, Mail	Intern
5	Liste mit Fotos und Namen der Schülerinnen und Schüler für die Lehrpersonen der Klasse	Schülerinnen und Schüler, Lehrpersonen	Dokument	Intern
6	Dokumentieren des Mitarbeitergesprächs	Schulleitung, Lehrpersonen	Dokument	Vertraulich
7	Erstellen von Förderplänen im Bereich Integration und einfache sonderpädagogische und unterstützende Massnahmen im Regelschulangebot (MR, ehemals IBEM).	Lehrpersonen, Klassenlehrperson, Erziehungsberatung, Erziehungsberechtigte	Dokumente, Mail	Vertraulich
8	Die Nutzenden vergessen ihr Passwort	Alle Nutzerinnen und Nutzer	Daten	Intern

Einzelne Produkte in Zusammenspiel mit den Szenarien der Betroffenen können unterschiedlich klassifiziert werden.

Beispiel:

	Szenario	Betroffene	Produkte	Klassifizierung
5.a	Liste mit Fotos und Namen der Schülerinnen und Schüler für die Lehrpersonen der Klasse	Schülerinnen und Schüler, Lehrpersonen	Dokument	Intern
5.b	Liste mit Fotos und Namen der Schülerinnen und Schüler für die Lehrpersonen der Klasse (Integration einer Schülerin / eines Schülers mit visuell erkennbaren Beeinträchtigungen)	Schülerinnen und Schüler, Lehrpersonen	Dokument	Vertraulich

4.3 Auswahl der Dienste

Google Workspace for Education bietet eine breite Palette von Diensten. Die Auswahl der Dienste richtet sich nach den Bedürfnissen der Schule (Kapitel 4.1). Es sollen nur Dienste genutzt werden, die vom Educa-Rahmenvertrag abgedeckt werden.

Weiter gilt zu beachten, dass Personendaten der Kategorie «*Vertraulich*» aufgrund der bestehenden Risiken in der Regel nicht mit Diensten von Google Workspace for Education bearbeitet werden sollen. Hierfür sind im Konzept andere Fachapplikationen zu berücksichtigen, die für die Bearbeitung vertraulicher Daten geeignet sind.

Beispiel einer Dienstauswahl im Konzept:

Datenklassifizierung	**gewählte Dienst**

öffentlich & intern	Google Workspace for Education Google Docs, Google Tabellen, Google Präsentationen, Drive, Meet, Chat, Kalender, Kontakte, Classroom
vertraulich	Beurteilungsapplikation Kanton Bern[6] Lehreroffice, Tresorit, Protonmail, Klapp, Threema, Scolaris und andere (Vorabkontrolle durch Gemeinde nötig)

4.4 Risiken erkennen und Schutzmassnahmen treffen

Die Nutzungsszenarien und die daraus resultierenden Produkte/Daten werden unter Berücksichtigung der Klassifizierung auf Risiken hin untersucht. Szenarien mit Produkten/Daten der Kategorie «*Öffentlich*» müssen nicht überprüft werden.
Beim der Kategorie «*Vertraulich*» sind erhöhte Anforderungen an den Schutz der Vertraulichkeit der Daten zu stellen und in der Risikoabwägung zu berücksichtigen.

Die folgende Risikomatrix verdeutlicht, welche Risiken durch zusätzliche Schutzmassnahmen zu minimieren sind. Die Ziffern der Achse «Eintrittswahrscheinlichkeit» werden mit den Ziffern «Auswirkung / Schadensausmass» multipliziert. Die Ergebnisse können in der Regel wie folgt gelesen werden:

- 1 und 2: Keine Massnahmen
- 3 – 6: Technische und organisatorische Massnahmen.
- 8 – 16: Wahl einer spezifischen Fachapplikation oder weitergehende technische und schulorganisatorische Massnahmen.

Eintrittswahrscheinlichkeit					
	4 sicher	4	8	12	16
	3 sehr wahrscheinlich	3	6	9	12
	2 wahrscheinlich	2	4	6	8
	1 unwahrschienlich	1	2	3	4
		1 unwesentlich	**2 geringfügig**	**3 kritisch**	**4 katastrophal**
	Auswirkung / Schadensausmass				

[6] https://www.beurteilung.apps.be.ch/beurteilung/SetLanguage.do

Beispiele von häufig eintretenden Risiken mit verschiedenen Schutzmassnahmen:

	Szenario/Risiko	Schadensausmass	Eintrittswahrscheinlichkeit	Risiko	Schutzmassnahmen (verschiedene Beispiele aus Sicht der Schule)
2.a	Durchführung von Produkten/Lernkontrollen inklusive Beurteilung (Prädikat/Benotung). Die Prüfungsresultate werden in der Schule publik.	2	3	6	Die Lehrpersonen werden dahingehend geschult, die einzelne Beurteilung nicht im gleichen Dokument zu vermerken, sondern diese in der entsprechenden Fachapplikation zu dokumentieren.
2.b	Dokumentation prognostische Beurteilungen/Einschätzungen. Würden solche Beurteilungen bekannt, könnte das den Betroffenen nachhaltig schaden, zum Beispiel im Zusammenhang mit der Berufswahl.	3	3	9	Das Konzept der Schule sieht vor, dass diese vertraulichen Daten nur in der spezifischen Fachapplikation bearbeitet werden dürfen. Die Sensibilisierung/Schulung hierzu ist in [(Referenzen anfügen] ausgewiesen. Die Fachapplikation wird mit einer Zwei-Faktor-Authentifizierung betrieben.
7.a	Förderpläne im Bereich Integration und einfache sonderpädagogische und unterstützende Massnahmen (MR, ehemals IBEM) werden erstellt und in Google Docs / Drive gespeichert. Administratoren von Google Workspace können auf diese Daten zugreifen. Behördenzugriffe seitens der USA (Cloudact) sind aufgrund von fehlenden Kontrollmöglichkeiten nicht überprüfbar.	3	4	12	Die Förderpläne werden in einem anderen Textverarbeitungsprogramm als Google Docs auf dem Computer der Lehrperson erstellt und unter Umständen in der spezifischen Fachapplikation gespeichert.
7.b	Diese Förderpläne werden per Mail der Schulleitung oder auch den Erziehungsberechtigten zugestellt. Die Gefahr einer fälschlich eingegebenen Mailadresse ist gross. Der Schaden für die betroffene Person kann unter Umständen gross sein (Mobbing, Cybermobbing).	3	4	12	Entweder: Mailinhalte und Anhänge an externe Mailadressen werden verschlüsselt. Das Passwort wird über einen zweiten Kanal übermittelt. Zusätzlich wird eine digitale Signatur eingesetzt (S/MIME). Oder: Für die Übermittlung dieser Inhalte per Mail wird ein separater Maildienst mit zusätzlicher Verschlüsselung eingesetzt. Beispiel: Protonmail. Dieser Maildienst wird mit einer Zwei-Faktor Authentifizierung betrieben. Oder: Dateien werden nur als Link auf einem dritten, sicheren Server mittels separatem Passwort freigegeben. Beispiel: Proton Drive oder Tresorit / Tresorit Send
8	Die Nutzenden vergessen ihr Passwort. Eine Administratorin/ein Administrator kann jederzeit die Passwörter der Nutzerinnen und Nutzer zurücksetzen und sich potenziell auch Zugang zu den Daten verschaffen. Passwortlisten bergen die Gefahr, dass Konten gehackt werden.	2	3	6	Die Admin-Rolle ist im Rollen- und Berechtigungskonzept verankert. Eine zusätzliche Vereinbarung regelt die Rechte und Pflichten. Die Nutzerinnen und Nutzer erhalten ein Default-Passwort und müssen dieses bei der nächsten Anmeldung erneuern.

4.5 Restrisiken ausweisen

Auch wenn die aufgeführten Massnahmen umgesetzt werden, können Risiken verbleiben (Restrisiken). Zurzeit sind die meisten Restrisiken in fehlenden Kontrollmechanismen auszumachen.
Diese Restrisiken müssen ausgewiesen und der verantwortlichen Leitungsebene nachvollziehbar kommuniziert werden. Restrisiken, die die Leitungsebene als tragbar bewertet, können und müssen von dieser akzeptiert werden (Risikoakzeptanz).

Beispiele
Vertragsgebundene Restrisiken:

- Fehlende Überprüfbarkeit der Zugriffe auf die Daten durch Google bzw. Subunternehmen von Google.
- Fehlende Überprüfbarkeit der Zugriffe durch amerikanische Sicherheitsbehörden (Cloud Act).
- Die verantwortliche Behörde kann nicht überprüfen, ob Personendaten, die für eine Zwei-Faktor-Authentifizierung verwendet werden (Name, Vorname, Geschäftliche Mail, unter Umständen private Handynummer) auch wirklich nach der vertraglich festgelegten Dauer der Speicherung unwiderruflich gelöscht werden.
- Die verantwortliche Behörde kann die Zusammenarbeit von Google mit Subunternehmen durch den Rahmenvertrag von Educa nicht ausschliessen.
- Erfassung der Nutzenden mit Vor- und Nachnamen. Diese Personendaten bergen das Risiko des Profilings.
- Fehlende Kontrollmöglichkeiten der vertraglich geregelten Nicht-Nutzung von Diagnosedaten seitens Google
- Einseitige Vertragsanpassungen durch Google.

Schulorganisatorische Restrisiken:

- Die Passwörter von Schülerinnen und Schülern im Zyklus 1 werden durch die verantwortliche Lehrperson der Klasse verwaltet
- Rückmeldungen zu Arbeiten von Schülerinnen und Schülern im selben Dokument können als formative Beurteilung interpretiert werden.

4.6 Verschlüsselung

Bei der Nutzung von Google Workspace for Education ist standardmässig die Übertragung sowie die Speicherung der Daten verschlüsselt («data in transit» und «data at rest»). Google verfügt über den entsprechenden Schlüssel und kann damit grundsätzlich auf die in der Cloud verschlüsselt hinterlegten Daten zugreifen. Während des eigentlichen Bearbeitungsvorganges der Daten in der Cloud («data in process») sind diese nicht verschlüsselt.

Das Risiko der unbefugten Dateneinsicht durch Mitarbeitende von Google (bzw. von Mitarbeitenden entsprechender Subunternehmen) kann grundsätzlich durch die Aktivierung von Access Approval oder durch die Verwendung eines eigenen behördenseitigen Schlüssels (zum Beispiel bei der Bearbeitung von vertraulichen Daten) minimiert werden. Access Approval kann in der Google Workspace for Education Plus aktiviert werden. Google verpflichtet sich damit, den Schlüssel nur mit der ausdrücklichen Zustimmung der Behörde zu verwenden. Die verantwortliche Person der Schule, die die entsprechende Zustimmung erteilen darf, muss im Rollen- und Berechtigungskonzept festgehalten werden.
Damit ist aber immer noch nicht ausgeschlossen, dass US-Behörden via Cloud Act Zugriff auf gespeicherte Daten haben können.

Weiter sind auf dem Markt Lösungen für Datenspeicherung oder für Mail mit stärksten Sicherheitstechnologien verfügbar. Wichtig hierzu sind Abklärungen, ob es sich um eine Firma mit Gerichtsstand Schweiz und Serverstandort Europäische Union/Schweiz handelt und wie sich die Benutzerfreundlichkeit im Schulumfeld gestaltet.

4.7 Protokollierung

Bei der Nutzung von Google Workspace for Education können Daten über die Nutzenden und deren Aktivitäten automatisch erfasst und gespeichert werden (Log-Daten).

Diese Log-Daten dürfen aber nur unter bestimmten Voraussetzungen ausgewertet werden (vgl. kantonale Randdatenverordnung RDV):

- Technische Probleme der Infrastruktur
- Missbrauchsverdacht:
    - Eine hinreichende schriftliche Begründung des konkreten Missbrauchsverdachts oder
    - Ein erwiesener Missbrauch.
    - Eine schriftliche Information der betroffenen Person

Da die automatisierte Übermittlung von Daten an Google nicht unterbunden werden kann, sind diese bei den Restrisiken zu vermerken (siehe 4.5).

4.8 Authentifizierung und Passwörter

Für Administratorinnen und Administratoren ist eine Zwei-Faktor-Authentifizierung notwendig. Diese kann in Google Workspace for Education aktiviert werden und ist kostenlos.
Für Lehrpersonen wird die Zwei-Faktoren-Authentifizierung empfohlen. Der Verzicht auf eine Zwei-Faktoren-Authentifizierung (Anmeldung mit einem einzigen Single-Faktor) birgt ein hohes Risiko, da damit eine unrechtmässige Übernahme des Kontos durch eine andere Person ermöglicht wird.

Google Workspace for Education bietet grundsätzlich zwei Arten der Authentifizierung:

- Verwendung der integrierten Google-Authentifizierung
- Verwendung eines Authentifizierungsdienstes. Weitere Informationen: Einrichtung der föderierten Einmalanmeldung (SSO) mit SAML

Die Art der Authentifizierung ist im Rahmen einer Risikoanalyse zu bestimmen. Dabei sind Zweck und Umfang der Datenbearbeitung sowie die Art der bearbeiteten Daten zu berücksichtigen.

4.9 Rollen- und Berechtigungen

Die erteilten Rollen- und Berechtigungen sind jährlich zu prüfen. Jede Person soll nur auf diejenigen Daten zugreifen können, die sie auch tatsächlich benötigt.

4.10 Erfassen der Nutzerinnen und Nutzer

Google bearbeitet nicht nur die innerhalb der Cloud-Dienste übermittelten Personendaten (also insbesondere Inhaltsdaten), sondern auch von den Nutzerinnen und Nutzer selbst bzw. von ihren Diensten generierte Daten über die Nutzerinnen und Nutzer (zum Beispiel Rand-, Telemetrie- oder Protokollierungsdaten). Diese zusätzlichen Personendaten sind mit der gleichen Sorgfalt zu behandeln wie die Daten, die zur eigentlichen Aufgabenerfüllung bearbeitet werden.

Folglich ist auch bei der Erfassung der Nutzerinnen und Nutzer darauf zu achten, dass nur die nötigsten Angaben erfasst werden (Datensparsamkeit).
Sollten die Daten explizit mit der integrierten Google-Authentifizierung erfasst werden, sind ausser der Namen keine weiteren Attribute zu erfassen.

Bei Bedenken oder auf Wunsch soll eine Pseudonomysierung angeboten werden.

4.11 Synchronisation von Nutzerdaten

Das Google Directory kann mit einem Microsoft Active Directory- oder einem LDAP-Server synchronisiert werden. Nur zwingend nötige Nutzerdaten sollen übermittelt werden.
Auch bei einem Einsatz eines Identitätsproviders (IdP) sollen nur zwingend nötige Attribute übermittelt werden.

Beispiel: Der Einsatz von einem Google Directory als IdP für die Anbindung an edulog.

Weitere Informationen:

- Informationen zu Google Cloud Directory Sync

4.12 Löschen

Das Löschen der Daten kann analog physischer Daten betrachtet werden. Es gelten die Aufbewahrungspflichten des Kantons Bern. Daten, die nicht mehr benötigt werden, müssen gelöscht werden. Die Nutzerinnen und Nutzer sollen die Möglichkeit erhalten, ihre Daten vor der Löschung auf ein anderes Speichermedium zu transferieren.

Die Löschung der Protokolldaten erfolgt automatisiert. Die Speicherfristen betragen für die meisten Protokolldaten 180 Tage.

Weitere Informationen:

- Datenaufbewahrung und Zeitverzögerungen – Wie lange werden Daten gespeichert?

4.13 Datensicherung und Notfallplanung

Die Anforderungen in Bezug auf die Verfügbarkeit von Google Workspace for Education sind zu definieren. Bei Bedarf sind entsprechende Massnahmen zur Datensicherung und Notfallplanung zu implementieren.

4.14 Diagnosedaten

Wird Google Workspace for Education eingesetzt, werden möglicherweise Daten an Google übermittelt.

Da die Administratorinnen und Administratoren keine Möglichkeit haben, Massnahmen betreffend Diagnosedaten zu treffen, bleibt nur, das Restrisiko auszuweisen.

5 Informationen der betroffenen Personen

Nutzerinnen und Nutzer sind über den geplanten Einsatz von Google Workspace for Education in der Schule im Vorfeld zu informieren. Dabei sind die wichtigsten Risiken und die getroffenen Schutzmassnahmen offenzulegen.

Die Nutzerinnen und Nutzer erhalten eine Zusammenstellung, welche Dienste von Google Workspace for Education in der Schule genutzt und wie sie eingesetzt werden.

Die Schulinformatik der PHBern bietet hierzu einen für jede Schule konfigurierbaren Ampelflyer an[7].

Beispiel eines Ampelflyers:

5.1 Schulung und Sensibilisierung

Die Schulungen zur Infrastruktur sowie die Sensibilisierung in datenschutzrelevanten Anwendungsbereichen soll beginnen, sobald die Infrastruktur implementiert ist und genutzt wird.

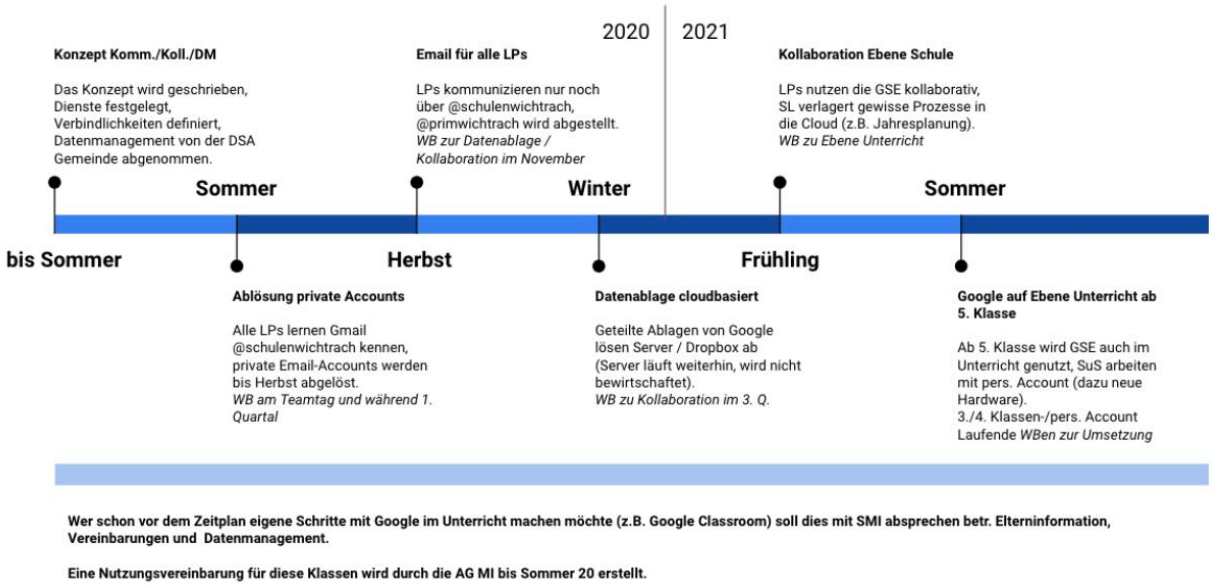
5.1.1 Lehrpersonen

Die Weisungen zum Umgang mit Daten in der Schule ergänzen die technischen Schutzmassnahmen (Vgl. 4.4 *Beispiele*).
Schulen sind mit starken Fluktuationen im Lehrpersonalbereich konfrontiert. Hier gilt es sicherzustellen, dass neue Lehrpersonen unkompliziert und schnell die wichtigsten Informationen zur Nutzung der Schulhausinfrastruktur erhalten.
Auch hierzu dient der konfigurierbare Ampelflyer der Schulinformatik der PHBern.

Die Erfahrungen der Schulinformatik der PHBern haben gezeigt, dass eine kontinuierliche Weiterbildung der Lehrpersonen zur Infrastruktur (zum Beispiel durch die Spezialistinnnen und Spezialisten Medien und Informatik, SMI) nachhaltiger ist als eine einmalige Schulung durch eine externe Firma.
Zur Entlastung der SMI-Lehrperson können Schulen zentrale Abläufe oder auch Sensibilisierungsthemen in Form von Dokumenten oder Videos zur Verfügung stellen.

[7] www.kibs.ch

Beispiel einer Planung zur Einführung von Google Workspace for Education über 1 Jahr



5.1.2 Schülerinnen und Schüler

Die Schulung der Schülerinnen und Schüler kann im Konzept Medien und Informatik der Schule unter den Anwendungskompetenzen des Modullehrplans Medien und Informatik subsumiert werden.

6 Eltern

Eltern sollen über den geplanten Einsatz von Google Workspace for Education frühzeitig (vor der Implementierung) informiert werden.

6.1 Information der Eltern

Die Information der Eltern soll auf mehreren Kanälen erfolgen. Einerseits sollen alle Konzepte zur Infrastruktur und zu Medien und Informatik im Unterricht (Vgl. Empfehlungen[8]) transparent und frei zugänglich sein. Andererseits sollen Eltern auch die Möglichkeit erhalten, Fragen zu stellen und Bedenken zu äussern.

6.1.1 Dokumente

- Konzept Medien und Informatik (Konzept aus Empfehlungen des Kantons Bern) [9]– Beispiele für dessen Inhalt:
  - Unterricht und Unterrichtsentwicklung
  - Personalentwicklung
  - Kollaboration und Kommunikation
  - Datenmanagement und Rechtliches
  - Technik und Finanzierung
- Konzept zur Cloud-Infrastruktur / Cloudkonzept (Konzept gefordert aus diesem Merkblatt)

[8] https://www.lp-sl.bkd.be.ch/content/dam/lp-sl_bkd/dokumente/de/startseite/themen/medien-und-informatik/medien-informatik-empfehlungen-d.pdf
[9] Unterstützung bietet kibs.ch, Schulinformatik PHBern

6.1.2 Veranstaltung

Eine an die Eltern gerichtete Veranstaltung – bevor die Infrastruktur implementiert wird –, ist ein wichtiger Bestandteil in der Kommunikation zur Personendatenbearbeitung der Schule/Gemeinde.

Nebst den allgemeinen Informationen zur Infrastruktur soll auch die Unterrichtsebene (Modullehrplan Medien und Informatik) beleuchtet werden. Idealerweise nehmen an dieser Veranstaltung alle Beteiligten der Konzeptarbeiten teil (Gemeinde, kommunale Datenschutzaufsichtsstelle, Schulleitung, SMI, Lehrpersonen, evtl. Firmen und/oder PHBern).

Die Veranstaltung kann so dazu beitragen, dass Bedenken oder Wünsche aufgenommen respektive erfüllt werden.

6.1.3 Kenntnisnahme

Wurde Google Workspace for Education gemäss diesem Merkblatt implementiert, kann davon ausgegangen werden, dass die Erziehungsberechtigten die Umsetzung zur Kenntnis genommen haben.

7 Anhänge

7.1 Dienste unter dem Rahmenvertrag

Die Vertragsbestimmungen im Rahmenvertrag von Educa mit Google sind nur auf die Hauptdienste von Workspace for Education Plus anwendbar.

Die Hauptdienste sind einsehbar unter:
https://workspace.google.com/intl/de/terms/user_features.html

Die wichtigsten Hauptdienste für eine Schule sind (Auswahl):

- Cloud Identity-Dienste für das Nutzer und Nutzerinnen Management
- Gmail
- Google Kalender
- Google Cloud Search
- Google Classroom
- Google Kontakte
- Google Docs mit Google Docs, Google Tabellen, Google Präsentationen, Google Formulare
- Google Drive
- Google Groups
- Google Hangouts, Chat und Meet
- Google Sites
- Google Vault