dsb

datenschutzbeauftragte
kanton zürich

Leitfaden

G Suite Enterprise for Education

Inhalt

1	Einleitung	2
2	Rahmenverträge mit Google	2
3	Konzept	2
3.1	Art der Nutzung	3
3.2	Auswahl der Dienste und Länderauswahl	3
3.3	Auswahl und Klassifizierung der Daten	3
3.4	Informationssicherheit	4
3.4.1	Verschlüsselung besonderer Personendaten	4
3.4.2	Protokollierung	4
3.4.3	Authentifizierung und Passwörter	4
3.4.4	Rollen- und Berechtigungskonzept	5
3.4.5	Löschen	5
3.4.6	Synchronisation von Nutzerdaten	6
3.4.7	Datensicherung und Notfallplanung	6
4	Berufsgeheimnis	6
4.1	Datenzugriff mit Einwilligung	6
4.2	Verschlüsselung mit eigenem Schlüssel	6
5	E-Mail-Adressen	7
6	Schulung und Sensibilisierung	7
7	Information der Eltern	7

1 Einleitung

Dieser Leitfaden richtet sich an Bildungsinstitutionen, die G Suite Enterprise for Education nutzen. Er gibt einen Überblick über die Vorgehensweise, um einen datenschutzkonformen Einsatz zu gewährleisten.

2 Rahmenverträge mit Google

educa.ch hat mit Google einen Rahmenvertrag für die Nutzung von G Suite Enterprise for Education in den Primar- und Sekundarschulen, Schulen der Sekundarstufe II sowie der höheren Berufsbildung unterzeichnet.
Es gelten die vertraglich vereinbarten Kriterien für eine Teilnahme. Der Bezug von Lizenzen für G Suite Enterprise for Education erfolgt ausschliesslich über durch Google autorisierte Wiederverkäufer. Informationen zum Vertragsinhalt und zu den Bezugsmodalitäten können auf der Webseite von educa.ch eingesehen werden.

SWITCH hat einen Rahmenvertrag für Institutionen der universitären Hochschulen wie Universitäten, Pädagogische Hochschulen und Fachhochschulen vereinbart.
Um die Dienstleistungen unter dem SWITCH-Rahmenvertrag und somit datenschutzkonform zu nutzen, muss das Formular «G Suite Affiliate Order Form», erhältlich unter der E-Mail-Adresse procurement@switch.ch, unterzeichnet werden. Das ausgefüllte und an SWITCH retournierte Formular wird an Google weitergeleitet und der Dienst wird freigeschaltet.

Universitätsspitäler und Forschungseinrichtungen als Subdomain einer entsprechenden Hochschule können dem Rahmenvertrag ebenfalls beitreten.

Der Bezug über die Rahmenverträge ermöglicht eine datenschutzkonforme Nutzung, indem
- schweizerisches Recht anwendbar,
- ein schweizerischer Gerichtsstand zum Tragen kommt,
- der Ort der Speicherung der Daten wählbar ist (EU/Nicht-EU).

Die Rahmenverträge regeln nur die Nutzung von G Suite Enterprise for Education. Im Gegensatz dazu kann die kostenlose Version G Suite for Education nicht datenschutzkonform genutzt werden.

3 Konzept

Vor der Nutzung der Dienste ist ein Konzept zu erstellen, das insbesondere die folgenden Punkte berücksichtigt:
- die Art der Nutzung
- das auf die Art der Nutzung abgestimmte Produkt
- die Art und der Umfang der zu bearbeitenden Daten

- die Verantwortlichkeiten
- die zum Schutz der Daten umzusetzenden Massnahmen wie Zugriffe, Verschlüsselung usw.

3.1 Art der Nutzung

Bildungsinstitutionen müssen vor der Auswahl der Produkte entscheiden, zu welchen Zwecken sie die Dienste nutzen wollen und welche Aufgaben damit erledigt werden sollen. Sollen beispielsweise nur Arbeitsblätter gespeichert oder auch Hausaufgaben erledigt werden können? Es ist zu berücksichtigen, dass der Zweck die Auswahl bestimmt und nicht umgekehrt.

3.2 Auswahl der Dienste und Länderauswahl

G Suite Enterprise for Education stellt eine Reihe von Diensten zur Verfügung. Die Auswahl richtet sich nach den Bedürfnissen der Bildungsinstitution. Weitere Beschreibungen des Produkts sind hier erhältlich.

Die Vertragsbestimmungen sind nur auf die Hauptdienste von G Suite (z. B. Gmail, Google Kalender und Google Classroom) anwendbar. Die Schulen müssen festlegen, auf welche Dienste die Lernenden zugreifen können. Zu beachten ist, dass wenn über G Suite auf andere Dienste wie Youtube zugegriffen wird, wieder die allgemeinen Nutzungs- und Datenschutzbestimmungen von Google gelten.

G Suite Enterprise for Education erlaubt eine Auswahl des Standorts zur Speicherung der Daten (EU/Non-EU). Es ist der EU-Standort zu wählen.

3.3 Auswahl und Klassifizierung der Daten

Die Bildungsinstitution muss vorgängig für jeden gewählten Dienst festlegen, welche Daten bearbeitet werden. Die Datenbearbeitung hat sich nach den Aufgaben und gesetzlichen Zwecken zu richten. Es ist sicherzustellen, dass nur die Daten bearbeitet werden, die für die jeweilige Aufgabenerfüllung und den jeweiligen Zweck notwendig sind. Ein Bearbeiten respektive Auswerten des Lernverhaltens im Sinne einer Überwachung ist beispielsweise nicht erlaubt.

Die Daten sind den folgenden Kategorien zuzuordnen, um nachfolgend die angemessenen Schutzmassnahmen bestimmen zu können:

Sachdaten	Informationen, die sich nicht auf Personen beziehen Beispiel: Arbeitsblätter
Personendaten	Informationen, die sich auf bestimmte oder bestimmbare Personen beziehen Beispiel: Name, Vorname, Adresse

Besondere Personendaten	Informationen, bei denen wegen ihrer Bedeutung, der Art ihrer Bearbeitung oder der Möglichkeit ihrer Verknüpfung mit anderen Informationen die besondere Gefahr einer Persönlichkeitsverletzung besteht Beispiel: Resultat der schulärztlichen Untersuchung, ärztliches Zeugnis

3.4 Informationssicherheit

Die Bildungsinstitution muss technische und organisatorische Massnahmen umsetzen, um die Vertraulichkeit, Integrität, Authentizität und Verfügbarkeit der Daten zu gewährleisten. Je sensibler die Daten sind, desto umfassender müssen die Informationssicherheitsmassnahmen sein. Dies gilt speziell für Informationen, die dem Berufsgeheimnis unterliegen (siehe Ziffer 4). Es sind insbesondere die folgenden Punkte zu berücksichtigen.

3.4.1 Verschlüsselung besonderer Personendaten

Sensitive, das heisst besondere Personendaten müssen verschlüsselt werden. Der Transport sowie die Speicherung der Daten sind bei G Suite Enterprise for Education bereits verschlüsselt, wobei Google über den Schlüssel verfügt. Für weitere Verschlüsselungsmöglichkeiten mit zusätzlichem Schutz siehe Ziffer 4.

Wenn Informationen den Bereich von G Suite Enterprise for Education verlassen, beispielsweise beim Versenden von E-Mails, kann ein verschlüsseltes 7-Zip-Archiv verwendet werden.

3.4.2 Protokollierung

Bei der Nutzung der Dienste können Daten über die Nutzenden und deren Aktivitäten automatisch erfasst und gespeichert werden. Man spricht von Protokollieren respektive «Loggen».
Die Protokolldaten dürfen nur bearbeitet werden, wenn dies für das Funktionieren des Systems notwendig ist. Bei Verdacht auf Missbrauch der Dienste durch die Nutzenden können Protokolldaten stichprobenweise und nach vorgängiger Information der Betroffenen ausgewertet werden.

Weitere Informationen
- Audit-Log zu Anmeldeaktivitäten

3.4.3 Authentifizierung und Passwörter

G Suite Enterprise for Education bietet grundsätzlich drei Arten der Authentifizierung:
- Verwendung der integrierten Authentifizierung
- Synchronisation des Passworts aus dem internen Active Directory zu G Suite Enterprise for Education (siehe Ziffer 3.4.6)

– Verwendung eines internen Authentifizierungsdienstes (beispielsweise Active Directory Federation Service). Weitere Informationen: Einrichtung der föderierten Einmalanmeldung (SSO) mit SAML

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

Für Administratorinnen und Administratoren oder wenn besondere Personendaten betroffen sind, ist eine Zwei-Faktor-Authentifizierung notwendig. Diese kann in G Suite Enterprise for Education aktiviert werden und ist kostenlos. Die notwendigen Schritte werden hier erläutert.

3.4.4 Rollen- und Berechtigungskonzept

Die Bildungsinstitution muss vor der Nutzung schriftlich in einem Rollen- und Berechtigungskonzept festlegen, welche Personengruppen (Lehrpersonen, Lernende, Fachpersonen, Schulpsychologinnen und Schulpsychologen, Schulpflege, Schulleitung, Administratorin oder Administrator, Kursverwaltung usw.) auf welche Dienste und welche Daten zugreifen dürfen. Das Rollen- und Berechtigungskonzept ist regelmässig zu überprüfen.
Wird «Access Approval» aktiviert, ist die verantwortliche Person im Berechtigungskonzept festzuhalten (siehe Ziffer 4.1).

3.4.5 Löschen

Das Löschen der Dokumente ist analog der Papierversion vorzunehmen. Lehrpersonen oder andere für die Löschung Verantwortliche können selbst löschen oder die Lernenden beauftragen, entsprechende Verzeichnisse oder Dokumente nach den für die jeweilige Institution geltenden Fristen zu löschen oder auf andere Speichermedien zu übertragen.

Daten von Lernenden oder Lehrpersonen, die ihr Konto nicht mehr nutzen, müssen gelöscht werden.

Die Löschung der Protokolldaten erfolgt automatisiert. Die Speicherfrist beträgt für die meisten Protokolldaten 180 Tage. Ausnahmen sind folgende Berichte:

– In E-Mail-Protokollen suchen (30 Tage)
– Über die API abgerufene Nutzungsdaten von Entitäten (30 Tage)
– Über die API abgerufene Nutzungsdaten von Kunden/Nutzern (15 Monate)

Weitere Informationen

– Datenaufbewahrung und Zeitverzögerungen – Wie lange werden Daten gespeichert?

3.4.6 Synchronisation von Nutzerdaten

Für verschiedene Zwecke, beispielsweise für eine effiziente Benutzererstellung, können Nutzerdaten mit G Suite Enterprise for Education synchronisiert werden (zum Beispiel Benutzernamen, E-Mail-Adresse usw.). Bei einer Synchronisation sind grundsätzlich nur diej Nutzerdaten zu übermitteln, die für die Benutzung von G Suite Enterprise for Education nötig sind. Im Synchronisationsdienst ist eine entsprechende Filterung vorzunehmen.

Weitere Informationen
- Informationen zu Google Cloud Directory Sync
- Daten einer Bildungsinstitution mit G Suite Enterprise for Education synchronisieren

3.4.7 Datensicherung und Notfallplanung

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

4 Berufsgeheimnis

Informationen unter dem Berufsgeheimnis wie schulärztliche Daten geniessen neben dem datenschutzrechtlichen auch einen strafrechtlichen Schutz. Dritte sollten keine, oder nur unter besonderen Voraussetzungen, Kenntnis dieser Daten erhalten, weshalb zusätzlich zu den in Ziffer 3 aufgeführten Massnahmen die folgenden Punkte zu berücksichtigen sind.

4.1 Datenzugriff mit Einwilligung

Bei der Nutzung von G Suite Enterprise for Education-Diensten ist eine Grundverschlüsselung für den Transport und die Speicherung implementiert. Google verfügt jedoch über den Schlüssel. Deshalb muss der Access-Approval-Prozess aktiviert werden. Dadurch wird sichergestellt, dass Google in Supportfällen nur auf explizite Anfrage und nach expliziter Einwilligung der Administratorin respektive des Administrators auf die Daten zugreifen kann.

Die für diesen Prozess verantwortliche Person ist im Rollen- und Berechtigungskonzept festzuhalten.

4.2 Verschlüsselung mit eigenem Schlüssel

Institutionen, die über eine gewisse Grösse oder eine geeignete IT-Infrastruktur verfügen, können für die Daten in G Suite Enterprise for Education einen eigenen Schlüssel implementieren.
Dieser Schlüssel wird in einem Schlüsseltresor (Cloud Key Management Service (KMS)) durch Google verwaltet. Aus diesem Grund muss zusätzlich der Access-Approval-Prozess aktiviert werden (siehe Ziffer 4.1). Die verwendeten Passphrasen und Schlüsselpaare sind sicher zu generieren und aufzubewahren.

5 E-Mail-Adressen

Müssen E-Mail-Adressen vergeben werden, sollten abgekürzte Namen oder Pseudonyme verwendet werden. Pseudonyme erschweren den Missbrauch der Konten durch Dritte.

6 Schulung und Sensibilisierung

Alle Personen, die mit diesen Diensten Daten bearbeiten, müssen instruiert werden, wie jeder Dienst rechtmässig genutzt werden kann. Weiter sind Lernende über die Art des Bearbeitens durch die jeweilige Institution zu informieren.

7 Information der Eltern

Im Sinne der Transparenz sind die Eltern im Rahmen der Volksschule über diese neue Art der Datenbearbeitung insbesondere über die folgenden Punkte zu informieren:

- Ob G Suite Enterprise for Education unter dem Rahmenvertrag von educa.ch genutzt wird
- Welche Dienste genutzt werden
- Welche Daten damit bearbeitet werden
- Welche Bedingungen für die Lernenden ausserhalb des Schulbetriebs gelten

Einerseits sind im Internet Rückschlüsse auf Lernende möglich, beispielsweise durch E-Mail-Adressen, welche den Namen mit der Schule verbinden, andererseits nutzen Lernende das Internet für die Schule auch zu Hause.

V 1.0 / April 2020

dsb

datenschutzbeauftragte
kanton zürich

Datenschutzbeauftragte
des Kantons Zürich
Postfach, 8090 Zürich

Telefon 043 259 39 99
datenschutz@dsb.zh.ch

www.datenschutz.ch
twitter.com/dsb_zh