## Gegenstand

Die Firma Google Inc. stellt Schulen weltweit G Suite for Education kostenlos zur Nutzung bereit. Bei der G Suite for Education handelt es sich um ein komplett Cloud basiertes Office Paket mit einem integrierten Classroom Management System. G-Suite for Education ist plattformübergreifend zu nutzen. An der Schule soll die G Suite for Education eingeführt werden, um damit Unterricht in allen Jahrgangsstufen der Schule durchzuführen, Teamarbeit im Kollegium zu unterstützen und Informationen aus der Verwaltung für Lehrkräfte und Schüler bereitzustellen.

Die Datenschutz-Folgenabschätzung (DSFA) nach Art. 35 DS-GVO wird durchgeführt, da nach Ansicht der Datenschutzkonferenz “*aufgrund der Art, der Umstände und der Zwecke der Verarbeitung bei einer Online-Lernplattform in aller Regel*”[[1]](#footnote-0) von einem voraussichtlich hohem Risiko für die Rechte und Freiheiten der betroffenen natürlichen Personen (Schüler, Lehrer, Eltern) auszugehen ist. Darüber hinaus möchte auch der Schulträger über eine DSFA eine Absicherung, dass es über entsprechende Maßnahmen möglich ist, die Plattform unter Einhaltung der datenschutzrechtlichen Vorgaben der DS-GVO zu nutzen. Auf eine Schwellenwertanalyse, mit welcher festgestellt werden soll, ob die Durchführung einer DSFA notwendig ist, wird von daher verzichtet.

## An der DSFA beteiligte Personen

|  |  |  |
| --- | --- | --- |
| **Funktion** | **Name** | **Rolle** |
| Schulleitung |  | Auftraggeber der DSFA, Leitung- und Entscheidungsfunktion, kennt schulrechtliche Vorgaben zur Verarbeitung personenbezogener Daten. |
| Schulischer Administrator |  | Fachmann für schulische IT Prozesse, steht für Fragen bezüglich IT Struktur der Schule und Prozessen zur Verfügung, bereitet die DSFA weitestgehend vor. |
| Pädagogische Leitung/ Medien- beauftragter der Schule |  | Fachmann für Unterricht, kann Fragen zu pädagogischen Zielsetzungen und Abläufen auch in Bezug auf Umsetzung der Nutzung digitaler Medien beantworten und bringt das erforderliche Wissen über die beabsichtigte Verarbeitung mit ein. |
| Behördlich bestellter schulischer Datenschutz-  beauftragter |  | Hat eine beratende Funktion, vor allem im Hinblick auf die Einhaltung des geltenden Datenschutzgesetzes und datenschutzrechtlicher Belange der Schulgesetzgebung. Er informiert über die notwendigen Informationen, die ein DSFA-Bericht enthalten muss und identifiziert die betroffenen Datenkategorien. |
| Google Inc. |  | Zur Bereitstellung notwendiger Informationen bezüglich Datenverarbeitung, TOM, ... |

## Beurteilungsumfang (Scope)

Gegenstand dieser DSFA sind alle Verarbeitungsprozesse und Datenflüsse, die im Zusammenhang mit der Nutzung der G Suite for Education erforderlich sind. Betrachtet werden dabei alle Verarbeitungsprozesse, die in der Schule stattfinden, unabhängig davon, ob die Verarbeitung auf schulischen Geräten im Verwaltungs- wie im pädagogischen Netz oder auf Privatgeräten stattfindet. Verarbeitungsvorgänge, die außerhalb der Schule im privaten Bereich oder außerhalb der schulischen Netzwerkinfrastruktur stattfinden, sind nicht Gegenstand der Beurteilung. Auch die Möglichkeit, Daten lokal im pädagogischen Netz zu verarbeiten und zu speichern, ist hier nicht berücksichtigt.

Zu den betrachteten Verarbeitungstätigkeiten gehören alle, beginnend mit dem Anlegen von Benutzern, der Arbeit in der Plattform bis zum endgültigen Löschen der Benutzer.

### Systemarchitektur

Bei der Nutzung von G Suite for Education im Unterricht, für Teamarbeit und eingeschränkte Verarbeitungsvorgänge aus der Schulverwaltung sind vier große Bereiche zu betrachten:

* **Endgeräte**,
* **schulische Infrastruktur,**
* **Internetzugang** und
* die **Google Cloud Architektur**.

Diese finden ihre Entsprechung in den am Prozess beteiligten Akteuren,

* den **Betroffenen** als Nutzern (Schüler und Lehrkräfte),
* dem **schulischen IT Personal** für Administration und Support,   
  dem **Internetanbieter** und
* **Google** als Diensteanbieter für G Suite for Education.

#### Endgeräte

Die Nutzung von G Suite for Education erfolgt über verschiedene Endgeräte. Dabei ist es unerheblich, ob es sich um stationäre oder mobile Endgeräte handelt. Auch das Betriebssystem spielt aus Nutzersicht keine Rolle. Aus der Sicht des Datenschutzes ergeben sich jedoch Unterschiede aus der genutzten Systemarchitektur. Je nach Betriebssystem des Endgerätes (Windows, iOS, Chrome OS, *Android, Linux*) unterscheiden sich die Möglichkeiten, diese Geräte selbst abzusichern. Bezüglich der Sicherheit der Geräte muss zusätzlich zwischen schulischen Geräten und Privatgeräten unterschieden werden. Während schulische Geräte unter Kontrolle des schulischen Administrators stehen und dieser durch technische Maßnahmen den Schutz der Geräte sicherstellt, müssen Nutzer bei privaten Endgeräten selbst für einen ausreichenden Schutz der Geräte sorgen.

Die Tabelle gibt eine Übersicht über Kategorien von schuleigenen Endgeräten, ihre Betriebssysteme sowie Browser und Apps, die zur Nutzung der G Suite for Education in Betracht kommen.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Schulische Endgeräte** | | | | |
| **Bezeichnung** | **OS** | **Browser** | **Apps** | **genutzte Anwendungen** |
| stationäre PCs und Laptops | Windows 7/  Windows 10 | Chrome Browser, FireFox | x | * Admin Console (nur Schul Admin)   Google Core Services   * Classroom * Drive * Docs * Sheets * Slides * Forms * Drawing * Sites * Keep * Gmail * Calendar * Contacts * Groups * Talk/Hangouts * Vault * Jamboard   Additional Services[[2]](#footnote-1)   * YouTube * Maps * Earth |
| iPads | iOS 12.2 | Chrome Browser, Safari | G Suite iOS Apps:  Docs, Sheets, Slides, Drive, Keep, Photos, Mail, ... |
| Chromebooks | Chrome OS 72 | Chrome Browser | x |
| *Android Tablets* | *Android 8* | *Chrome Browser* | *Android Apps:*  *Docs, Sheets, Slides, Drive, Keep, Photos, Mail, ...* |

#### Schulische Infrastruktur

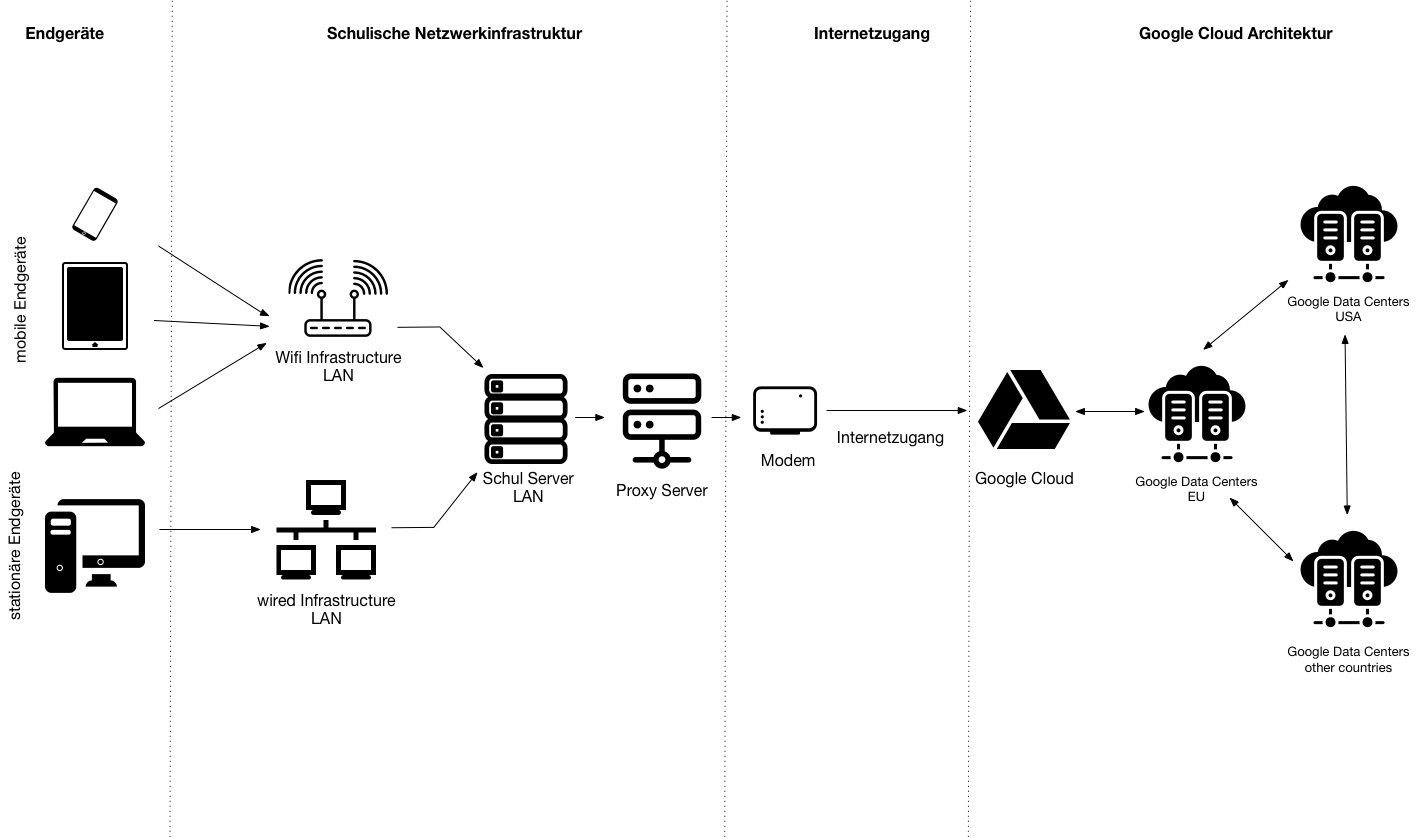
Die Schule stellt eine Netzwerk-Infrastruktur bereit, über welche stationäre und mobile Endgeräte Zugriff auf G Suite for Education erhalten. Dabei wird zwischen Ethernet und drahtlosem Netzwerk unterschieden. Während der kabelgebundene Zugang nur für schuleigene Geräte möglich ist, kann die Schule bei Bedarf auch privaten Endgeräten Zugang über das drahtlose Netzwerk gestatten. Zur schulischen Infrastruktur gehören auch Server zur lokalen Dateiablage und Server einschließlich Proxy-Server als Vermittlungsstelle zum Internet und zum Schutz des lokalen Netzwerks.

#### Internetzugang

Der schulische Zugang zum Internet erfolgt über ein vom Anbieter *XYZ* bereitgestelltes Modem mit einer Bandbreite von *X GBit/s*.

#### Google Cloud Architektur

Google stellt zur Nutzung von G Suite for Education eine Server Infrastruktur bereit, mit Standorten in Europa, den USA und anderen Ländern. Auch wenn die personenbezogenen Daten von europäischen Nutzern überwiegend auf Servern in Europa verarbeitet werden, so muss immer davon ausgegangen werden, dass zur Gewährleistung der Funktionalität von G Suite for Education personenbezogenen Daten auch außerhalb Europa verarbeitet werden.

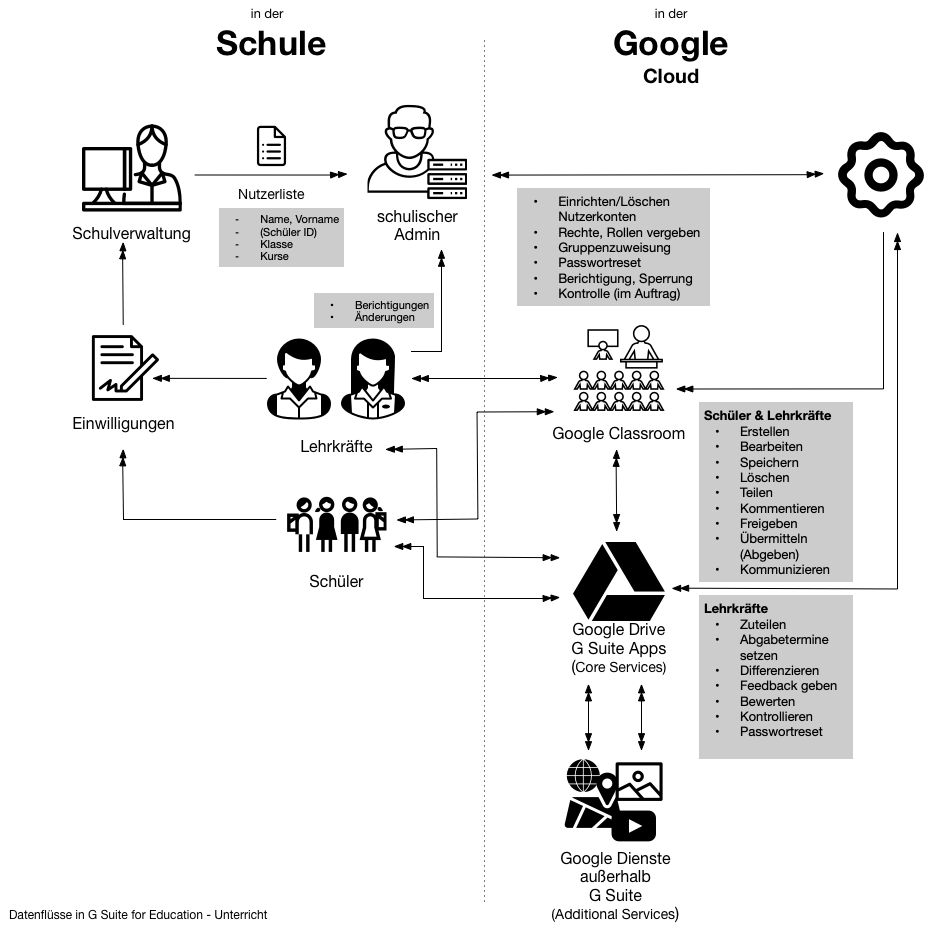


### Datenflüsse

Die Datenflüsse bei der Nutzung von G Suite for Education durch die Lehrkräfte, Schülerinnen und Schüler und die Schulverwaltung hängen von den Nutzungszwecken und den daran beteiligten Akteuren ab.

#### Unterricht

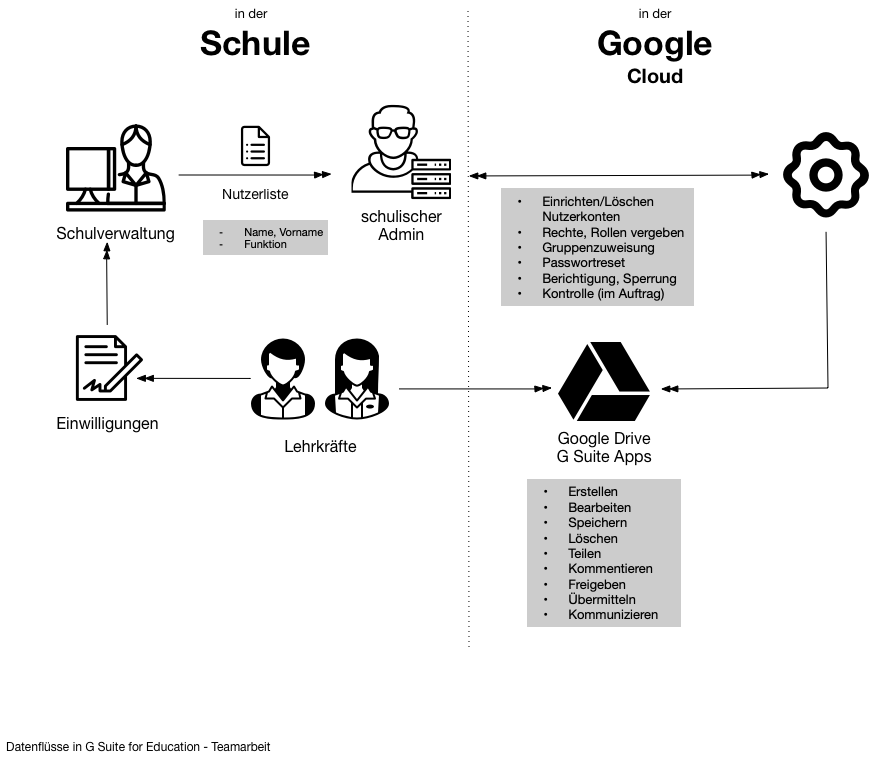
Voraussetzung für eine Nutzung der G Suite for Education durch Schülerinnen und Schüler und Lehrkräfte im Unterricht ist die Einwilligung in die dafür erforderliche Datenverarbeitung. Einwilligungen werden in der Schulverwaltung gesammelt, von wo dann Nutzerdaten in Form von Nutzerlisten an den schulischen Administrator weitergeleitet werden, um die Erstellung von Nutzerkonten zu veranlassen. Entsprechend der dabei übermittelten Informationen zu Klassen- und Kurszugehörigkeiten werden Rechte, Rollen und Gruppenzuweisungen durch den schulischen Administrator für jeden Nutzer vorgenommen.



Im Unterricht fließen Daten zwischen den Mitgliedern eines Classrooms über den Classroom selbst, Google Drive oder andere Apps der G Suite for Education, sei es durch Freigaben oder über Kommunikationsmöglichkeiten wie Chat (z.B. innerhalb eines Google Docs), Kommentare bzw. Feedback oder E-Mail.

#### Teamarbeit

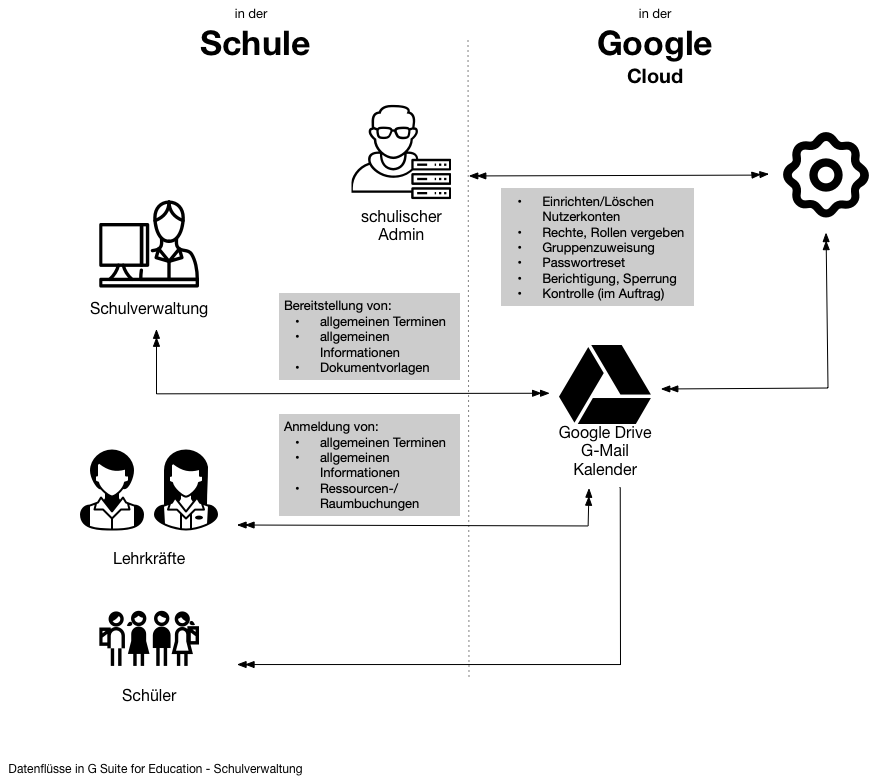
Wird G Suite for Education auch im Unterricht genutzt und nicht nur zur Teamarbeit im Kollegium, sind die Datenflüsse, welche durch das Einwilligungsverfahren und die Übermittlung von Nutzerdaten der Lehrkräfte an den schulischen Administrator zur Einrichtung von Nutzerkonten entstehen, identisch zu den im Diagramm “Datenflüsse in G Suite for Education - Unterricht” abgebildeten.



Datenflüsse finden zwischen den Lehrkräften statt bei der Erstellung von Inhalten und der Bereitstellung für das Kollegium, dem kollaborativen Arbeiten, dem Austausch von Informationen im Zusammenhang mit der Erstellung von Inhalten und der Kommunikation dazu über E-Mail, Chat innerhalb eines Google Docs oder über Kommentare. Informationen mit Personenbezug entstehen auch bei der Pflege gemeinsamer Kalender.

#### Schulverwaltung

Die Darstellung der Datenflüsse bei einer Nutzung von G Suite for Education für eingegrenzte Verarbeitungsprozesse in der Schulverwaltung geht davon aus, dass zumindest eine Nutzung für Unterricht erfolgt und Einwilligungen vorliegen. Die durch das Einwilligungsverfahren bedingten Datenflüssen sind deshalb hier nicht noch einmal berücksichtigt.



## Überblick

### Geplante Verarbeitung

Die G Suite for Education soll in der Schule zur Nutzung im Unterricht, zur Teamarbeit im Kollegium, zur Abbildung von organisatorischen Prozessen innerhalb der Schule und zur Bereitstellung von Informationen und Unterlagen durch die Schulverwaltung genutzt werden. Anders als die für Privatleute verfügbare G Suite, die jeder Nutzer automatisch mit einer Anmeldung für Gmail erhält, handelt es sich bei der G Suite for Education um eine speziell für den Bildungsbereich angebotene Version mit zusätzlichen Funktionen in der Verwaltung und speziell angepassten Datenschutzrichtlinien, mit denen Google dem besonderen Schutzbedarf von Kindern und Jugendlichen und den daraus resultierenden gesetzlichen Verpflichtungen nachkommt.

#### Unterricht

Im Unterricht soll G Suite auf der einen Seite durch Lehrkräfte zur Steuerung des Unterrichts genutzt werden, indem sie Aufgaben austeilen, Informationen und Materialien bereitstellen und Abgabetermine setzen, sie Umfragen erstellen und informelle Tests durchführen. Zur Unterstützung der Schüler sollen Lehrkräfte die Möglichkeiten der Plattform nutzen, Feedback zu geben. Schüler nutzen die Plattform, um Lernprozesse aktiv zu gestalten, Aufgabenstellung zu bearbeiten, Informationen zusammenzutragen, Lernprodukte zu erstellen, innerhalb der Plattform zu kommunizieren und kollaborativ zu arbeiten. Als Portfolioinstrument dient die Plattform auch als Sammlung von Lernprodukten der Schüler.

#### Teamarbeit

Dem Kollegium soll G Suite als Plattform für Teamarbeit und Kommunikation dienen, um gemeinsam Unterrichtsmaterialien, Unterrichtsreihenplanungen und schulinterne Lehrpläne zu erstellen und zu teilen.

#### Schulverwaltung

Für die Schulverwaltung soll G Suite eine Plattform bieten, über welche allgemeine Informationen einfach und effizient an Lehrkräfte und Schüler weitergegeben werden können und Vorlagen für Dokumentation und Information bereitgestellt werden.

#### Organisation

Über die Kalender der Plattform sollen Termine geplant, abgestimmt und bekannt gemacht werden. Dazu gehören allgemeine, öffentliche Termine der Schule, sowie interne Termine, Klassenarbeitstermine, Ressourcenbuchungen und ähnliche.

### Zuständigkeiten für die Verarbeitung

#### Verantwortlicher

Die Schule bzw. Schulleitung ist bei der Nutzung von G Suite entsprechend Abs. 3 *RdErl. d. Ministeriums für Schule und Bildung v. 19.01.2018 - 222-2.06.08.03.01-17491[[3]](#footnote-2)* speichernde Stelle im Sinne des DSG NRW. Die Schulleitung als Verantwortlicher. Gemäß §2 Abs. 3 VO-DV I[[4]](#footnote-3) ist die Schule berechtigt “*unter Beachtung der Voraussetzung des § 11 DSG NRW die Datensicherheit gewährleistende und zuverlässige Institutionen mit der Verarbeitung ihrer Daten zu beauftragen. Die Datenverarbeitung im Auftrag ist nur zulässig nach Weisung der Schule oder der Schulaufsichtsbehörden und ausschließlich für deren Zwecke.*”

Die Schule erhebt und verarbeitet personenbezogene Daten der Beteiligten. Sie ist für die Rechtmäßigkeit der Verarbeitung von personenbezogenen Daten von Schülern und Lehrkräften der Schule in G Suite verantwortlich, sorgt für eine datenschutzrechtliche Information der Betroffenen und holt

#### Auftragsverarbeiter

Google Ireland, als europäische Tochter von Google LLC, tritt gegenüber der Schule als Auftragsverarbeiter entsprechend Art. 28 DS-GVO auf und verarbeitet personenbezogene Daten von Schülerinnen und Schülern sowie Lehrkräften nach Weisung der Schule.

#### Normen oder Standards der Verarbeitung

Google -

* **C5 Testat** (Testat des BSI)[[5]](#footnote-4) [[6]](#footnote-5),
* **ISO 27001**[[7]](#footnote-6) [[8]](#footnote-7) (Informationssicherheit, orientiert sich am IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik (BSI))
* **ISO 27018**[[9]](#footnote-8) [[10]](#footnote-9), (Datenschutz in der Cloud)
* **ISO 27017**[[11]](#footnote-10) [[12]](#footnote-11) (internationale Norm zur Absicherung von Cloud-Services, Informationssicherheit in der Cloud, orientiert sich am IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik (BSI))
* **SOC 2[[13]](#footnote-12), SOC 3[[14]](#footnote-13)**
* **EU-US Privacy Shield**[[15]](#footnote-14) [[16]](#footnote-15) (entspricht in der Funktion quasi einem Angemessenheitsbeschluss)
* **EU Model Contract Clauses**[[17]](#footnote-16) [[18]](#footnote-17) (EU Standardvertragsklauseln)
* Auch wenn in Europa rechtlich nicht bindend - US Gesetze und Selbstverpflichtung (die Google aber trotzdem auch außerhalb der USA einhält)
  + **COPPA** (Children’s Online Privacy Protection Act of 1998)[[19]](#footnote-18)
  + **FERPA** (Family Educational Rights and Privacy Act)[[20]](#footnote-19)
  + **Student Privacy Pledge** des Future of Privacy Forum (FPF)

Eine Übersicht über alle Standards, Vorgaben und Zertifikate, welche Google mit seinen Cloud Diensten weltweit erfüllt, siehe auch <https://cloud.google.com/security/compliance/#/> . Auf europäische Vorgaben begrenzt <https://cloud.google.com/security/compliance/#/regions=Europe>

## Daten, Prozesse und Unterstützung

### Verarbeitete Daten

#### Kategorien von personenbezogenen Daten

Bei der Nutzung von G-Suite for Education gilt an der Schule der Grundsatz der Datenminimierung. Trotzdem fallen bei der Nutzung personenbezogene Daten an.

* **Benutzerkennung/ Login Daten**
* **Benutzer-Organisationsdaten** (z.B. Rollen, Rechte, Gruppenmitgliedschaften, Klassenzugehörigkeit, Aufnahmedatum im System, …)
* **Inhalte & Kommunikation des Benutzers** (z.B. Texte, Tabelle, Präsentationen, Zeichnungen, Kommentare, Kommunikationsinhalte, E-Mails, Kalendereinträge, Fotos, Audio, Video, Browserverlauf, …)
* **Metadaten zu** **Inhalte & Kommunikation des Benutzers** (z.B. Erstelldatum, Änderungsdatum, Versionen, Freigaben, Mitarbeiter, Bearbeitungsverlauf, Kommunikation: Empfänger, Absender, Datum Versand, Empfang, gelesen, ungelesen, Verlauf)
* **Unterrichtsdaten** (z.B. zugewiesene Aufgaben, Termine, Abgabedatum, Versäumnisse, Kommentare, Feedback der Lehrkraft, Abfragen: Anzahl beantwortete Fragen, Richtige, Falsche, nicht beantwortet, Anzahl Wiederholungen)
* **Technische Nutzungsdaten** (Google): (z.B. Login mit Datum, Zeit, Ort, IP, Gerät, OS, genutzte Applikationen, Fehlermeldungen, …)

#### Speicherdauer

Grundsätzlich werden die personenbezogenen Daten eines Nutzers nur bis zum Ende der Schulzugehörigkeit gespeichert oder bis der Nutzer sie selbst löscht. Bis ein Löschprozess durch Google umgesetzt ist, einschließlich der Löschung aus Backups, vergehen bis zu 180 Tage. Die Speicherdauer von personenbezogenen Daten hängt allerdings auch davon ab, wem eine Datei gehört bzw. wer sie geteilt hat. Beiträge eines Nutzers an einer geteilten Datei eines anderen Nutzers bleiben solange gespeichert, bis die Daten dieses Nutzers gelöscht werden. Solange bleiben Inhalte und Kommentare in kollaborativ bearbeiteten Materialien bzw. E-Mails und Nachrichten an einen anderen Nutzer bei diesem bestehen. Dieses gilt im Falle von Schülern auch für Materialien, die von Lehrkräften als Aufgaben ausgeteilt und eingesammelt/ zurückgegeben wurden. Da sie der Lehrkraft gehören, bleiben sie weiterhin bestehen, auch wenn der Schüler als Nutzer bereits aus dem System gelöscht wurde. Lehrkräfte löschen Schülermaterialien spätestens ein Jahr nachdem sie diese zuletzt unterrichtet haben, gerechnet ab dem Ende des Kalenderjahres. Alle im Zusammenhang mit der Bearbeitung einer Datei entstehenden Metadaten (z.B. Erstellungsdatum, Versionen, Mitarbeiter, Bearbeitungsverlauf, Speicherort, Format, …) bleiben solange gespeichert wie auch die Datei selbst.

#### Zugriffsberechtigte Personen

Sämtliche Daten im Verzeichnis eines Benutzers sind im Standard auf privat eingestellt. Das bedeutet, nur der Benutzer selbst kann sie einsehen.

##### Zugriff durch Schüler und Lehrkräfte

Schüler und Lehrkräfte können auf sämtliche von ihnen selbst erstellten Inhalte, E-Mails und Nachrichten zugreifen. Außerdem erhalten sie Zugriff auf alle mit ihnen geteilten Inhalte und an sie übermittelten E-Mails, Nachrichten und Inhalte.

##### Zugriff durch den schulischen Administrator

Der schulische Administrator hat vollen Zugriff auf alle Daten in der G Suite for Education Instanz der Schule. Ein Zugriff auf das private Verzeichnis eine Benutzers und dessen Inhalte sowie auf von einem Benutzer verschickte E-Mails und Nachrichten erfolgt durch den schulischen Administrator jedoch nur, wenn ein begründeter Verdacht auf einen Verstoß gegen die Nutzungsvereinbarung besteht. Der schulische Administrator darf hierbei jedoch nur auf Weisung und im Beisein der Schulleitung (Vier-Augen-Prinzip) auf die persönlichen Daten des Benutzers zugreifen, nachdem der Benutzer darüber zuvor informiert wurde.

##### Zugriff durch Systemadministratoren von Google

kann auf sämtliche Daten zugreifen, wenn

* es zur Durchsetzung der geltenden Nutzungsbedingungen, einschließlich der Untersuchung möglicher Verstöße erforderlich ist
* es darum geht, Betrug, Sicherheits- oder technische Probleme aufzudecken, zu verhindern oder anderweitig zu beheben.
* es Schutz vor Schäden an den Rechten, dem Eigentum oder der Sicherheit von Google, seinen Nutzern oder der Öffentlichkeit geht, soweit dies gesetzlich vorgeschrieben oder zulässig ist.

Ein Zugriff unter den beschriebenen Voraussetzungen durch Google erfolgt, indem der schulische Administrator einem zuvor benannten Google Mitarbeiter einen vorübergehenden Testzugang mit Administratorrechten einrichtet. Dieses Testadminstratorkonto darf nur zur Behebung des Problems genutzt werden.

#### Empfänger von personenbezogenen Daten

Personenbezogene Daten von Benutzern der schulischen Instanz von G Suite for Education verbleiben grundsätzlich innerhalb dieser Instanz und werden nur dem Rechte- und Rollenkonzept entsprechend anderen Benutzern als dem Eigentümer der Daten zugänglich gemacht. Empfänger von personenbezogenen Daten eines Benutzers sind alle Personen innerhalb der Schule, denen dieser sie übermittelt oder mit denen er sie teilt. Bei Benutzern, welche die Berechtigung haben, E-Mail und Nachrichten auch an Personen außerhalb der Schule zu übermitteln und mit diesen Personen auch Inhalte teilen können, können auch Personen außerhalb der Schule Empfänger von personenbezogenen Daten sein.

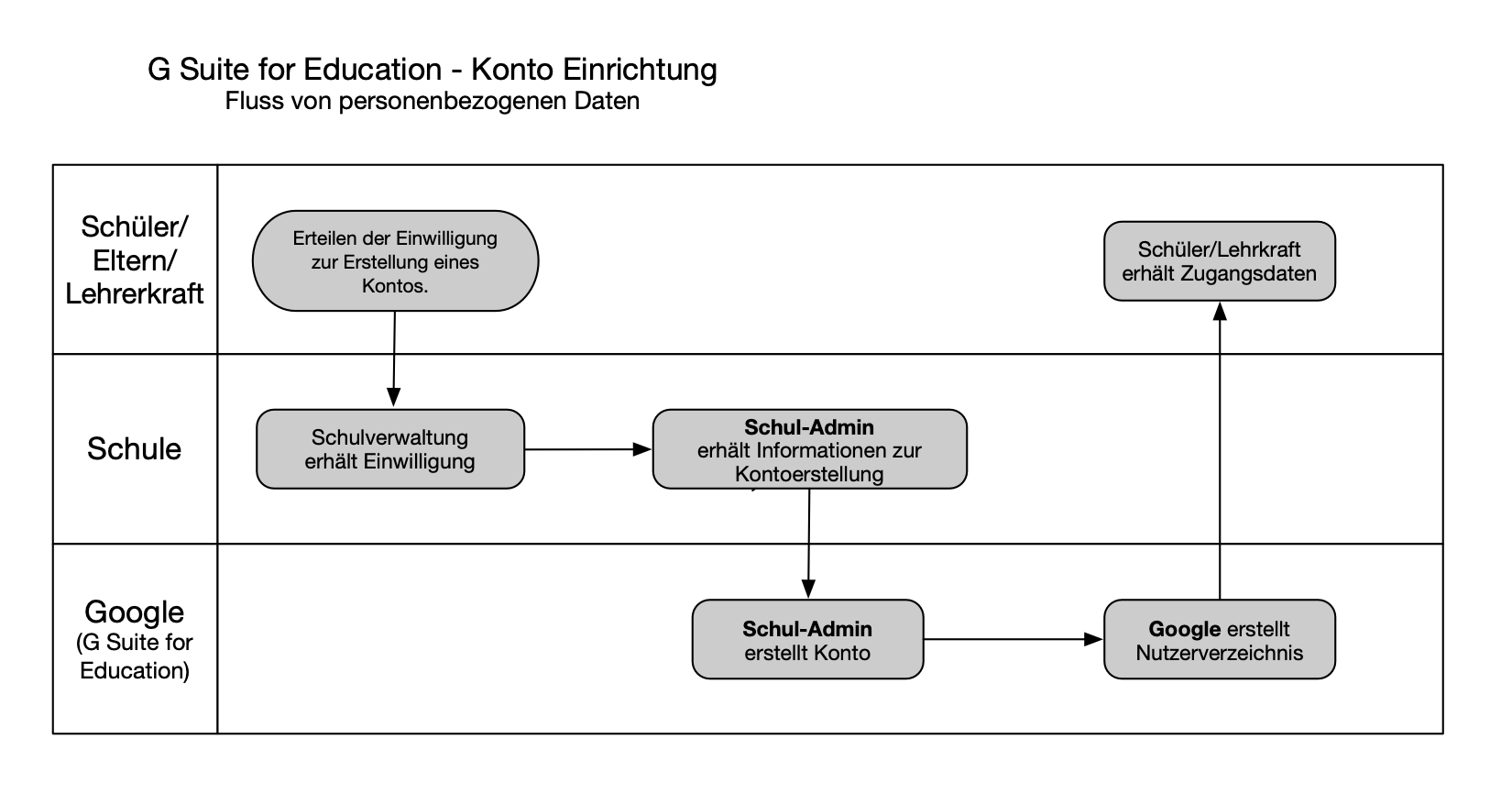
Bei Verstößen gegen die Nutzungsvereinbarung, die Nutzungsbedingungen von Google, das Urheberrecht oder andere rechtliche Vorgaben kann es erforderlich werden, Inhalte und Informationen von Benutzern an Dritte außerhalb der Schule weiterzugeben.

Google kann sämtliche Daten eines Benutzers an Dritte weitergeben, wenn

* Google eine zusätzliche Zustimmung des Nutzers zur Weitergabe personenbezogener Daten eingeholt hat; oder
* durch Gesetze oder andere Rechtsvorschriften dazu verpflichtet ist.

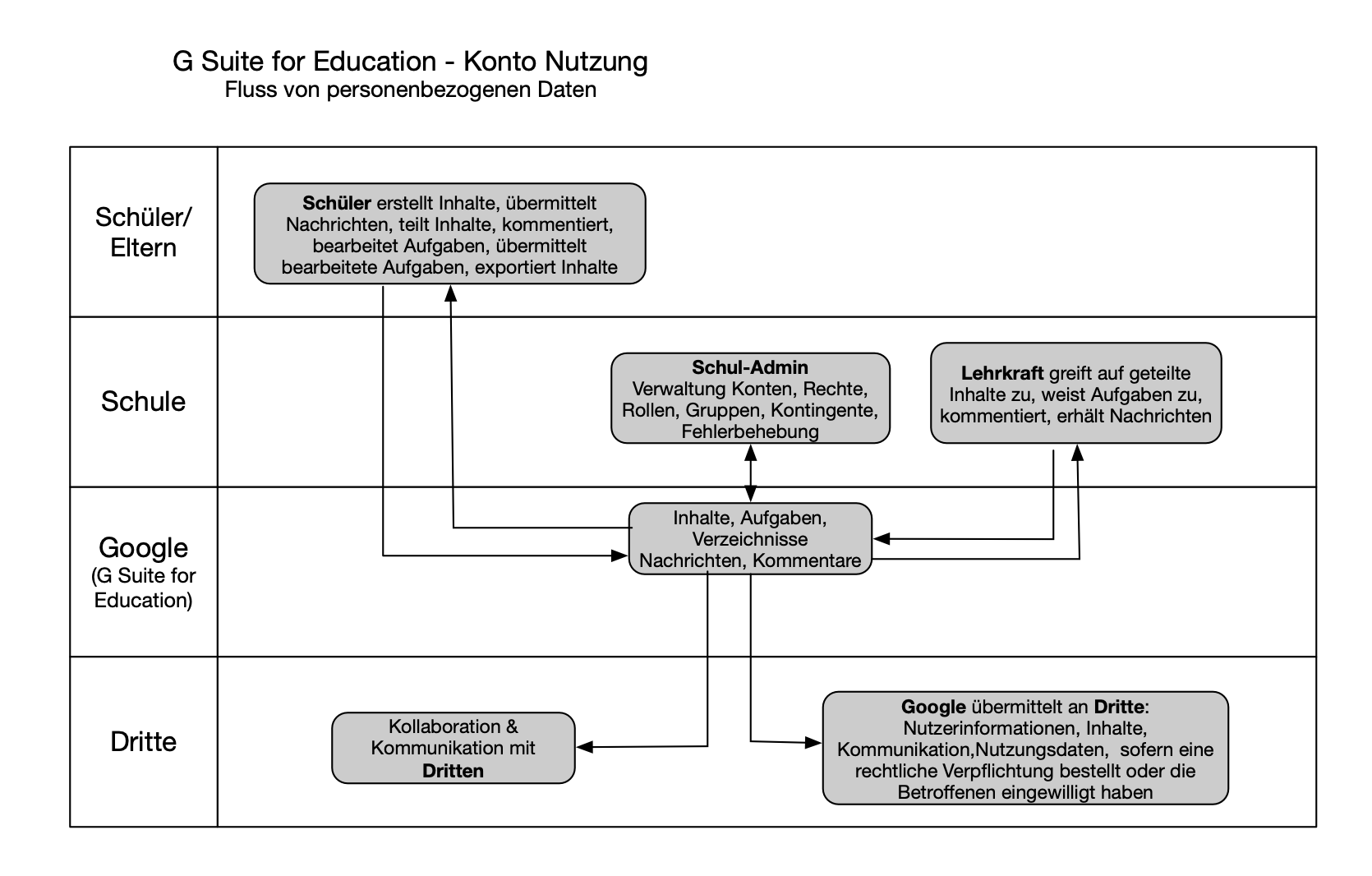
### Daten und Prozesse

#### Einrichtung eines Kontos in G Suite for Education



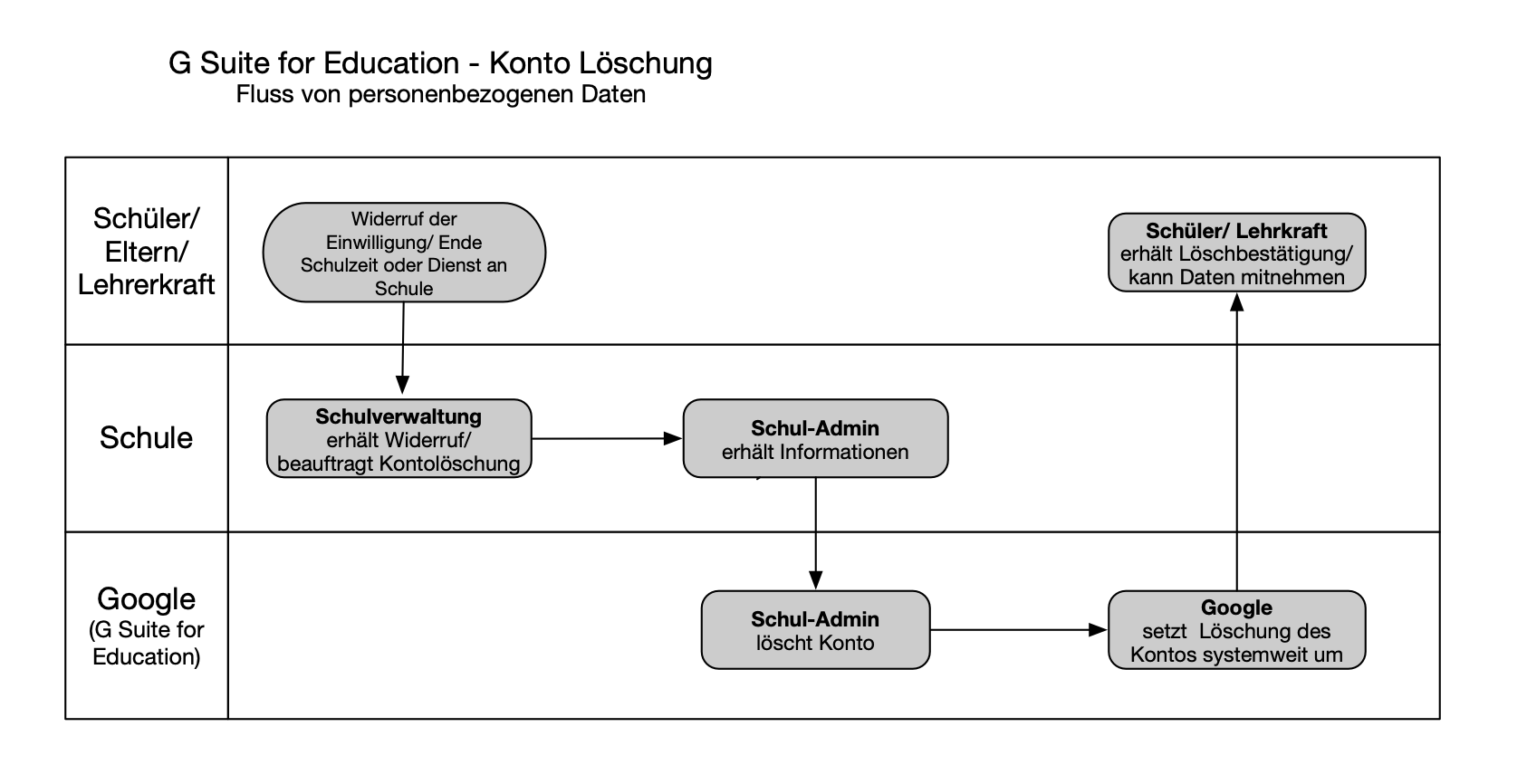
* Schulverwaltung übermittelt auf Weisung der Schulleitung Nutzerdaten an den Schul-Admin zur Einrichtung eines Nutzerkontos.
* Schul-Admin erstellt in G Suite for Education das Nutzerkonto samt Rollen, Rechten und Gruppenzugehörigkeiten.
* Google erstellt automatisiert entsprechende Verzeichnisse und Gruppen und stellt entsprechend Apps und Ressourcen für den Nutzer bereit.
* Nutzer erhält von Google Zugangsdaten zum Erstlogin an hinterlegte E-Mail Adresse.  
  [alternativ - Nutzer erhält von Schulverwaltung Zugangsdaten zum Erstlogin.]
* Schul-Admin kontrolliert Passwortsicherheit über Funktionen der Admin Console.

#### Nutzung eines Kontos in G Suite for Education



* Schüler erstellen Inhalte, laden Inhalte hoch, erhalten Aufgaben zugewiesen, bearbeiten Aufgaben, greifen auf geteilte Inhalte zu, kommentieren, kommunizieren, exportieren Inhalte - innerhalb der Institution [und mit Dritten außerhalb der Institution in kooperativen Projekten mit Externen]
* Lehrkräfte weisen Aufgaben zu, teilen Inhalte, greifen auf geteilte Inhalte zu, kommunizieren, geben Feedback, exportieren Inhalte, resetten Passworte [auf Anfrage durch Schüler]
* Schul-Admin behebt Fehler, passt Rechte an, …
* Google legt automatisiert Backups an, logt Nutzeraktivitäten im Zusammenhang der Erstellung von Inhalten, Bearbeitung von Aufgaben, Kommunikation usw.
* Google übermittelt Nutzerdaten (Inhalte und Nutzungsdaten) an Dritte, sofern eine rechtliche Verpflichtung vorliegt oder der Nutzer eingewilligt hat.

#### Löschung eines Kontos in G Suite for Education



* Endet die Schulzeit eines Schülers, die Dienstzeit einer Lehrkraft an der Schule oder widerspricht ein Nutzer der Verarbeitung von personenbezogenen Daten gegenüber der Schulleitung, beauftragt die Schulverwaltung auf Weisung der Schulleitung den Schul-Admin mit der Löschung des Nutzerkontos.
* Schul-Admin leitet die Löschung des Nutzerkontos ein.
* Google setzt automatisiert eine systemweite Löschung des Nutzerkontos um, einschließlich der Löschung aus Backups.
* Google informiert den Nutzer über die eingeleitete Kontolöschung und gibt Hinweis auf Möglichkeit zur Datenmitnahme.  
  [alternativ - informiert Schule über die eingeleitete Kontolöschung die Möglichkeit einer Datenmitnahme innerhalb einer vorgegeben Frist.]

## Akteure und betroffene Personen

Welche Akteure hier in Frage kommen, hängt auch von der Schule und vom geplanten Einsatz der Plattform ab. Es geht um die Akteure wie auch die Betroffenen.

|  |  |
| --- | --- |
| **Name** | **Vertreten durch** |
| **Akteure** | |
| Schule | Schulleitung, schulischer Administrator |
| Google | Auftragsverarbeiter, Betreiber der Plattform G Suite for Education |
| Schulträger/ IT Dienstleister[[21]](#footnote-20) | Auftragsverarbeiter |
| **Betroffene** | |
| Schüler | Schülervertretung, Elternpflegschaft, Schulkonferenz |
| Lehrkräfte | Lehrerrat oder eventuell örtlicher Personalrat, Schulkonferenz |
| Eltern[[22]](#footnote-21) | Elternpflegschaft, Schulkonferenz |
| Schulverwaltung[[23]](#footnote-22) | Betriebsrat  (der städtischen/ kommunalen Verwaltung bei Schulen in öffentlicher Trägerschaft) |

## Verhältnismäßigkeit und Notwendigkeit der Verarbeitung

### Definition und Rechtmäßigkeit der Verarbeitungszwecke

Durch die Schule werden in G Suite for Education personenbezogene Daten von Schülern und Lehrkräften zur **Durchführung von Unterricht** entsprechend §3 Abs. 1 Satz 1[[24]](#footnote-23) und §120 Abs. 1 SchulG NRW verarbeitet. Zur Durchführung von Unterricht gehört auch die Bereitstellung geeigneter Medien. G Suite for Education ist eine digitale online Plattform, welche zur Durchführung von Unterricht genutzt werden kann, als gemeinsame Arbeitsplattform und als Classroom Management zur Ablaufsteuerung und Organisation des Unterrichts. Zu den Zielen des Unterrichts gehört auch die Schulung des sicheren, kreativen und verantwortungsvollen Umgangs mit Medien in Orientierung an den im Medienkompetenzrahmen NRW[[25]](#footnote-24) festgelegten Kompetenzbereichen. G Suite for Education stellt dafür eine ideale Plattform bereit.

Da es sich dabei um eine digitale und online-basierte Plattform handelt, ist zur Arbeit damit auch die Verarbeitung von weiteren, durch das SchulG NRW nicht legitimierten personenbezogenen Daten erforderlich. Dieses sind Daten, welche für den technischen Betrieb und zur Bereitstellung der Funktionalitäten innerhalb von G Suite for Education und der zugrundeliegenden Cloud Infrastruktur erforderlich sind, zur Gewährleistung ihrer Sicherheit und zur Optimierung und Weiterentwicklung der verschiedenen Dienste von G Suite for Education. Ein Teil dieser Verarbeitungsprozesse ergibt sich zusätzlich aus rechtlichen Verpflichtungen, welchen Google als Diensteanbieter nach europäischem und internationalem Recht unterliegt.

### Rechtsgrundlagen der Verarbeitung

Für die zu bewertenden Verarbeitungsvorgänge liegen die folgenden Rechtsgrundlagen vor.

#### Beauftragung von Google

Nach §2 Abs. 3 VO-DV I dürfen Schulen “die Datensicherheit gewährleistende und zuverlässige Institutionen mit der Verarbeitung ihrer Daten der personenbezogenen Daten von Schülerinnen und Schülern beauftragen. Entsprechendes gilt nach §3 VO-DV II auch für die Verarbeitung von personenbezogenen Daten von Lehrkräften. Voraussetzung für die rechtmäßige Beauftragung durch die Schule ist dass dieses nach §3 VO-DV II Satz 2 bzw. §2 Abs. 3 VO-DV I Satz 2 ausschließlich auf Weisung der Schule und nur für deren Zwecke erfolgt. Dazu ist der Abschluss eine Vertrages zur Auftragsverarbeitung nach §52 DSG NRW (neu) bzw. Art. 28 DS-GVO erforderlich. Auch wenn Google mit Sitz in Irland einen Standort innerhalb der EU hat, handelt es sich um ein US Unternehmen und die Verarbeitung von personenbezogenen Daten aus der Schule ist nicht auf EU Server begrenzt. Entsprechend wird nach Art. 28 DS-GVO ein anderes Rechtsinstrument nach Unionsrecht, welches “*den Auftragsverarbeiter in Bezug auf den Verantwortlichen bindet und in dem Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte des Verantwortlichen festgelegt sind*.”[[26]](#footnote-25) Entsprechende vertragliche Regelungen finden sich in:

* G Suite for Education-Vereinbarung (online)[[27]](#footnote-26)
* Data Processing Amendment to G Suite[[28]](#footnote-27) (dort 10.2 EU Standardvertragsklauseln)
* Standard Contractual Clauses (processors)[[29]](#footnote-28)

Die verschiedenen Vertragsbestandteile werden einmal bei Anmeldung für die G Suite for Education abgeschlossen und dann innerhalb der Google Admin Console nach Anmeldung ergänzt.

Bei der Nutzung von G Suite for Education ist zu berücksichtigen, dass die personenbezogenen Daten der Betroffenen auch auf Servern in den USA verarbeitet werden können. Für die USA liegt kein Angemessenheitsbeschluss der Kommission im Sinne von Art. 44 DS-GVO vor. Eine Absicherung erfolgt hier durch die oben aufgeführten Standard Contractual Clauses nach Art. 46 Abs. 2 lit. d DS-GVO und die Zeichnung des EU-US Privacy Shield durch Google, welcher der Anwendung der Regelungen aus Art. 45 DS-GVO entspricht.

#### Einpflegen der Nutzerdaten

Grundsätzlich wäre es möglich, einen Teil der zur Nutzung von G Suite for Education erforderlichen Nutzerdaten wie Name, Klasse, Rolle auf der Grundlage von Art. 6 Abs. 1 lit. e DS-GVO in die Plattform einzupflegen, da die Erhebung und Verarbeitung dieser Daten für Schüler durch §120 Abs. 1 Satz 1 SchulG NRW und §4 Abs. 2 VO-DV I legitimiert ist und für Lehrkräfte nach §121 Abs. 1 Satz 1 und §5 Abs. 1 VO-DV II.

#### Nutzung der G Suite for Education

Die Nutzung der G Suite for Education durch **Schülerinnen und Schüler** ist nur auf der Grundlage einer Einwilligung nach Art. 6 Abs. 1 lit. a DS-GVO möglich, da die bei der Nutzung der Plattform verarbeiteten personenbezogenen Daten, soweit sie über Name, Klasse und Rolle hinausgehen, nicht durch §120 Abs. 1 Satz 1 SchulG NRW und §4 Abs. 2 VO-DV I legitimiert sind und so §120 Abs. 2 Satz 2 gilt: “*Andere Daten dürfen nur mit Einwilligung der Betroffenen erhoben werden.*”

Die Nutzung der G Suite for Education durch **Lehrkräfte** ist nur auf der Grundlage einer Einwilligung nach Art. 6 Abs. 1 lit. a DS-GVO möglich, da die bei der Nutzung der Plattform verarbeiteten personenbezogenen Daten, soweit sie über Name, Klasse und Rolle hinausgehen, nicht durch §121 Abs. 1 Satz 1 und §5 Abs. 1 VO-DV II legitimiert sind und so §121 Abs. 1 Satz 5 gilt: “*Andere Daten dürfen nur mit Einwilligung der Betroffenen erhoben werden.*”

Eine Einwilligung durch das Schulverwaltungspersonal entfällt, da für diese Personen ein gesonderter nicht personalisierter gemeinsamer Verwaltungs-Account erstellt wird.

### Erforderlichkeit, Relevanz und Beschränkung der erhobenen Daten auf das für die Datenverarbeitung Notwendige

#### Anmeldung/ Nutzerverwaltung

Wie der Unterricht im analogen Raum nicht ohne personenbezogene Daten ablaufen kann, so ist auch für die Nutzung digitaler Medien im Unterricht ein Minimum an personenbezogenen Daten erforderlich. Die Anmeldung selbst an der Plattform braucht keine für den Betreiber persönlich identifizierbaren Daten, da die Schule den Zugriff regelt, indem sie die Nutzerkonten anlegt. Damit die am Unterricht beteiligten Personen sich innerhalb von G Suite for Education zur Kommunikation und Kollaboration, zur Zuteilung von Aufgaben und zur Zuordnung von Arbeitsergebnissen untereinander erkennen können, ist ein Minimum an personenbezogenen Daten erforderlich. Innerhalb einer Klasse wäre es vielleicht noch vorstellbar, dass Mitglieder der Lerngruppe sich die Pseudonyme ihre Mitschüler merken. Von Lehrkräften, die oft mehrere hundert Schüler in einem Schuljahr unterrichten, kann dieses nicht erwartet werden. Da es allen Beteiligten die Arbeit in G Suite for Education erleichtert, ist zumindest ein Teil des Namens als **Benutzername**, den alle sehen können, erforderlich. Um Verwechslungen durch Namensgleichheiten zu vermeiden, reicht ein Namensteil nicht aus. Da die Ansprache in Schule primär über Vornamen erfolgt, sollte der Benutzername zumindest aus dem Vornamen und einem Teil des Nachnamens bestehen. Besser noch wäre der gesamte Name. Zur Vergabe von Rollen und Rechten in G Suite for Education ist es auch erforderlich, anzugeben ob der Benutzer **Schüler** oder **Lehrer** ist. Die **Klassen- bzw. Kurszugehörigkeit** ist zur Zuordnung zu Gruppen innerhalb der Plattform erforderlich. Mit Gruppenzugehörigkeit können Prozesse gesteuert werden, wie beispielsweise die finale Löschung von Nutzern am Ende der Schulzeit, ohne diesen Vorgang bei jedem Nutzer einzeln vornehmen zu müssen. Mit der Anmeldung in der schulischen Instanz von G Suite for Education wird dem Schüler dort auch das Merkmal Schulzugehörigkeit zugewiesen. Weitere personenbezogenen Daten (Individualdaten), wie Geburtsdatum, Adresse, Religion und ähnlich sind für die Nutzungszwecke nicht erforderlich.

#### Unterricht

Im Unterricht entstehen personenbezogene Daten durch die Nutzung der Funktionen von G Suite for Education. Ein Teil davon entspricht denen, die auch im Unterricht ohne digitale Medien anfallen.

##### Lernprodukte der Schüler

Auch der Unterricht ohne digitale Medien besteht zu einem großen Teil aus der Produktion von Inhalten, egal ob diese in mündlicher oder schriftlicher Form erfolgen oder aus anderen Handlungsformen resultieren. Wird eine digitale Plattform wie G Suite for Education genutzt, ist dieses nicht anders. Es erfolgt dann mittels der Möglichkeiten der Plattform.

##### Qualität der von Schülern produzierten Inhalte

Arbeiten Schülerinnen und Schüler in G Suite for Education, so haben die von ihnen dabei produzierten Inhalte unvermeidlich verschiedene Qualitäten, die Aufschluss darüber geben können, wie intensiv sich jemand mit einem Thema bzw. Aufgabenstellung auseinandergesetzt hat, wie kompetent der Umgang mit bestimmten Inhalten ist, wie die Beherrschung der Sprache ist, der Rechtschreibung usw..

##### Feedback

Entsprechend der Qualität der von Schülern produzierten Inhalte fällt der Feedback der Lehrkraft und eventuell auch von Mitschülern aus. Während die Inhalte der Schüler für sich genommen noch relativ neutral sind, so ist Feedback, welches dazu gegeben wird, ein Indikator bezüglich der Qualität der produzierten Inhalte, egal ob dieses ein Lob ist, ein Hinweis auf einen Fehler oder ein Verbesserungsvorschlag. Die Möglichkeit, Feedback zu geben, ist eine Stärke von G Suite for Education und für Schüler beim Erwerb von Kompetenzen unverzichtbar. Über schnelles und gezieltes Feedback können Lehrkräfte Schüler im Sinne von Formative Assessment zu richtigen Lösungswegen für bei der Auseinandersetzung mit einer Problemstellung führen. Die Feedbackmöglichkeiten über Kommentare erlauben es, Schülern wesentlich mehr Rückmeldung zu geben als im herkömmlichen Unterricht.

##### Bewertung

Die eindeutigste Aussage über die Qualität eines von Schülern produzierten Inhaltes ist die Bewertung in Form von Noten, da diese die Inhalte an einem Erwartungshorizont messen und vergleichbar machen.

##### Persönliche Meinungen, Vorlieben, Gesinnungen

Je nach Aufgabenstellung können im Unterricht auch Inhalte entstehen, welche in welchen persönliche Meinungen, Vorlieben, Gesinnungen und ähnlich zum Ausdruck gebracht werden. Inhalte von produzierten Medien können sehr persönlich sein.

##### Digitale Abbildungen

Bei digitalen Medien wie Fotos, Videos oder Audioaufzeichnungen können zudem weitere personenbezogene Daten entstehen wie Abbildungen von Personen oder Aufzeichnungen der Stimme oder Kombinationen davon.

#### Betrieb der Plattform

##### Administration durch die Schule

Zur Nutzung von G Suite for Education nimmt die Schule Einstellungen an der Plattform, die mit den Zwecken zusammenhängen, für welche sie genutzt wird, die Strukturen der schulischen Organisation von Unterricht digital abbilden und Anpassungen für verschiedene Altersgruppen von Schülern darstellen, die mit Daten- und Jugendschutz zusammenhängen. Durch Zuweisung zu Gruppen, welche so mit bestimmten Rechten und Einschränkungen versehen sind, werden auch entsprechende Merkmale auf die Schüler übertragen.

##### Nutzung durch Schüler und Lehrkräfte

Während der Nutzung von G Suite for Education fallen über die von den Nutzern produzierten Inhalte zahlreiche weitere Daten an, die mit den einzelnen Nutzern verknüpft, personenbezogene oder zumindest personenbeziehbare Daten darstellen:

* Daten von Erstellung und Veränderung von Inhalten
* Versionierung/ Bearbeitungsverlauf
* Dokument- bzw. Dateiinhaltsmetadaten z.B. Schriftarten, Wortzahl, Verknüpfungen zu anderen Inhalten, Gliederung, ...
* Speicherung mit Speicherort und weiteren Metadaten
* Kommentare/ Feedback & Chat im gleichen Dokument
* Verzeichnisstrukturen in Google Drive
* geteilt mit
* Mitarbeit durch
* Freigabe durch/ Aufgabe erhalten ...
* Abgabe/ Erledigt
* angezeigte Rechtschreib- und Grammatikfehler
* Browserverlauf
* Sucheingaben
* je nach Sicherheitseinstellung Anzeige von Logins mit neuen Geräten

##### Betrieb durch Google

Google gibt an, für den Betrieb von G Suite for Education von Nutzern folgende Informationen zu sammeln. Google macht dabei keinen Unterschied, ob der Zugriff auf die Plattform von einem schulischen Gerät aus erfolgt oder von einem privaten Endgerät oder wo der Zugriff erfolgt. Beim Zugriff über Privatgeräte erhebt Google Daten, die einen Personenbezug über das Gerät ermöglichen könnten.

Mit einer Nutzung außerhalb der Schule könnte ein Personenbezug durch Standortdaten möglich werden, unabhängig davon ob es sich um ein Privatgerät oder ein Schulgerät handelt. Sind derartige Nutzungsszenarien geplant, müssen diese Formen der Datenerhebung durch Google zumindest in Teilen in Kauf genommen werden, da hier berechtigte Interessen von Seiten des Anbieters bestehen, wie zuvor beschrieben.

* Geräteinformationen, wie z. B. Hardwaremodell, Betriebssystemversion, eindeutige Gerätekennungen und Mobilfunkinformationen einschließlich der Telefonnummer des Benutzers (nur bei Nutzung eines entsprechenden Gerätes, z.B. eines privaten Smartphones);
* Protokollinformationen, einschließlich Details darüber, wie ein Benutzer unseren Dienst genutzt hat, Geräteereignisinformationen und die Internetprotokoll-(IP)-Adresse des Benutzers;
* Standortinformationen, die durch verschiedene Technologien wie IP-Adresse, GPS und andere Sensoren bestimmt werden;
* eindeutige Anwendungsnummern, wie z.B. die Versionsnummer der Anwendung; und
* Cookies oder ähnliche Technologien, die verwendet werden, um Informationen über einen Browser oder ein Gerät zu sammeln und zu speichern, wie beispielsweise die bevorzugte Sprache und andere Einstellungen.

Diese Daten werden gesammelt nach Angaben von Google in der G Suite for Education Privacy Notice[[30]](#footnote-29), um die sogenannten Core Services bereitstellen zu können, nicht jedoch, um Anzeigen dagegen zu schalten. Google gibt an, die in den Core Services und anderen Google Diensten gesammelten Informationen von Nutzern aus der Schule zu nutzen, um diese Dienste bereitzustellen, zu warten, zu schützen und zu verbessern, neue zu entwickeln und Google selbst und die Nutzer von Google Diensten zu schützen.

## Maßnahmen zum Schutz der Persönlichkeitsrechte der betroffenen Personen

### Information der Betroffenen Personen über die Verarbeitung

Vor der Nutzung der G Suite for Education werden Schüler und ihre Eltern und Lehrkräfte entsprechend Art. 13 DS-GVO über die geplante Verarbeitung ihrer personenbezogenen Daten informiert (siehe Anlage 2). Bei erwachsenen Schülern werden nur die Schüler selbst informiert. Lehrkräfte werden im Rahmen einer Lehrerkonferenz über die Plattform und die damit verbundenen datenschutzrechtlichen Implikationen umfassend aufgeklärt, da es bei der Nutzung von G Suite for Education nicht nur um ihre eigenen Daten geht, sondern auch um die der überwiegend minderjährigen Schülerinnen und Schüler. Bei dieser Veranstaltung klärt die Schule auch darüber auf, welche Maßnahmen von Seite der Schule getroffen werden, um die Sicherheit und den Schutz der personenbezogenen Daten aller Nutzer der Schule zu gewährleisten. Entsprechende Informationen werden Schülern und ihren Erziehungsberechtigten im Rahmen von Klassen- oder Stufen-Pflegschaftssitzungen gegeben. Alle Beteiligten erhalten außerdem mit der Einwilligung in die Nutzungsvereinbarung und der datenschutzrechtlichen Einwilligung umfangreiche Informationen entsprechend Art. 13 DS-GVO in schriftlicher Form. Um Papier zu sparen, werden die Informationen leicht zugänglich auf der Homepage der Schule hinterlegt. Sie finden sich außerdem auch in G Suite for Education an verschiedenen Stellen, so etwa in jedem Classroom. Auf Wunsch können Betroffene die Informationen zur Datenverarbeitung und die Nutzungsvereinbarung auch in gedruckter Form, unentgeltlich im Sekretariat der Schule enthalten.

### Einholen der Einwilligung der betroffenen Personen

Da die Verarbeitung von personenbezogenen Daten in G Suite for Education eine Einwilligung der Betroffenen voraussetzt, wird ein Zugang erst dann angelegt bzw. freigeschaltet, wenn eine schriftliche Einwilligung der Betroffenen vorliegt.

* Bei Schülerinnen und Schülern vor Vollendung des 16. Lebensjahres ist eine Einwilligung der Erziehungsberechtigten erforderlich.
* Bei Schülerinnen und Schülern ab Vollendung des 16. Lebensjahres ist die Einwilligung der Erziehungsberechtigten sowie der Schülerinnen und Schüler erforderlich.

Die Einwilligung in die Verarbeitung von personenbezogenen Daten ist mit einer Einwilligung in die Nutzungsvereinbarung gekoppelt. Da letztere ein wesentlicher Bestandteil des Sicherheitskonzeptes bei der Nutzung von G Suite for Education ist, wird ein Zugang nur dann angelegt bzw. freigeschaltet, wenn die Einwilligung in beide vorliegt.

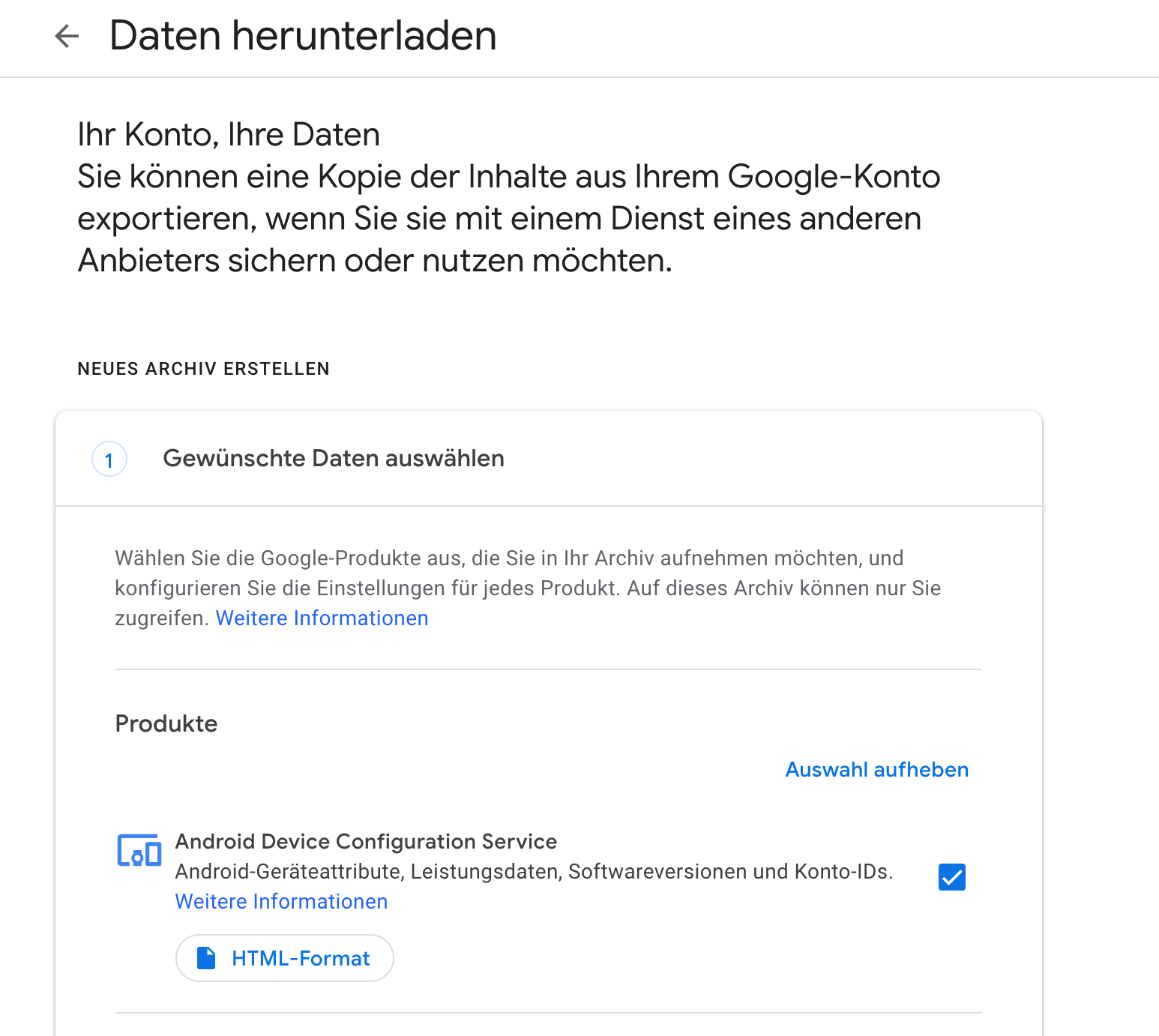
### Ausübung des Betroffenenrechtes auf Auskunft und Datenübertragbarkeit

G Suite for Education besitzt eine Funktion, die es Nutzern ermöglicht, selbst ein Einblick in die Verarbeitung der sie betreffenden personenbezogenen Daten zu erhalten.

Noch sehr viel einfacher ist es, das Recht auf Datenübertragbarkeit auszuüben. Hier gibt es im Bereich der Kontoeinstellungen eine Funktion, über welche sämtliche die eigene Person betreffenden personenbezogenen Daten exportiert und heruntergeladen werden können.

#### Daten herunterladen

Unter Daten herunterladen[[31]](#footnote-30) können Nutzer ihre sämtlichen bei Google gespeicherten personenbezogenen Daten oder auch nur Teile von herunterladen.



### Ausübung des Betroffenenrechtes auf Berichtigung und Löschung (Recht auf Vergessenwerden)

Schülerinnen und Schüler sowie Lehrkräfte können ihre Rechte auf Berichtigung ausüben, indem sie zum einen selbst erkannte Fehler korrigieren, wo dies mittels ihrer eigenen Benutzerrechte möglichst ist. In Fällen, wo solches nicht möglich ist, können sie sich an den schulischen Administrator wenden.

Bezüglich des Rechtes auf Löschung haben alle Nutzer die Möglichkeit, eine Löschung einzelner Google Dienste mit sämtlichen zugehörigen Daten innerhalb ihrer Kontoeinstellungen einzuleiten. Sollte es hierbei Schwierigkeiten geben, können Sie sich an den schulischen Administrator wenden. Dieser ist auch Ansprechpartner, wenn es um das Recht auf Vergessenwerden geht. Eine Löschung des gesamten schulischen Kontos ist nur über den schulischen Administrator möglich und setzt einen Widerruf der Einwilligung oder einen Widerspruch in die Verarbeitung voraus.

Kontaktinformationen des schulischen Administrators:

[**Name des schulischen Administrators, E-Mail des schulischen Administrators**]

### Ausübung des Betroffenenrechtes auf Einschränkung oder Widerspruch der Verarbeitung

Alle Nutzer der schulischen Instanz von G Suite for Education können von ihrem Recht auf Einschränkung oder Widerspruch der Verarbeitung Gebrauch machen. Sie richten derartige Einsprüche direkt an die Schulleitung als Verantwortlicher für die Datenverarbeitung in der Schule.

Kontaktinformationen der Schulleitung:

[**Name der Schulleitung, E-Mail der Schulleitung, Telefon, Postanschrift**]

### Vertragliche Regelungen der Verpflichtungen des Auftragsverarbeiters

Die vertraglichen Regelungen bezüglich der Verpflichtungen von Google als Auftragsverarbeiter gegenüber der Schule als Verantwortliche Stelle sind sämtlich in von Google bereitgestellten Vertragsunterlagen beschrieben. Dort finden sich auch entsprechende Regelungen bezüglich Unterauftragsverarbeitern von Google, deren Verträge mit Google den gleichen Regelungen unterliegen wie die, welche durch die Schule mit Google abgeschlossen werden (siehe dazu *11. Subprocessors* in *Data Processing Amendment to G Suite*[[32]](#footnote-31)). Informationen zu den beauftragten Unterauftragsverarbeitern von Google finden sich in *G Suite Agreement and/or Complementary Product Agreement - Subprocessors*[[33]](#footnote-32).

### Schutz der Daten bei Datenübermittlung in Länder außerhalb der Europäischen Union

Da die Cloud Services von Google nicht nur auf Server innerhalb der Europäischen Union stattfinden, sondern auch auf Servern in den USA und anderen Ländern[[34]](#footnote-33), finden entsprechende Datenübermittlungen statt.

Google hat, wie bereits unter [Normen oder Standards der Verarbeitung](#_l4fi65diy47w) beschrieben den **EU-US Privacy Shield**[[35]](#footnote-34) [[36]](#footnote-35) gezeichnet und bietet darüber hinaus die **EU Model Contract Clauses**[[37]](#footnote-36) [[38]](#footnote-37) (EU Standardvertragsklauseln) an, die Bestandteil des Vertrags mit Google zur Nutzung der G Suite for Education sind. Letztere gelten auch für Server Standorte außerhalb der USA, in Asien und Südamerika (siehe *Data Processing Amendment to G Suite*[[39]](#footnote-38)).

## Maßnahmen zur Datensicherheit

### Maßnahmen der Schule

#### Sensibilisierungsmaßnahmen

Datenschutz und Datensicherheit, verantwortungsvolles Handeln in G Suite for Education und datensparsame Nutzung sind Thema regelmäßig durchgeführter Schulungen in den Klassen und Lerngruppen sowie im Kollegium. Alle Schüler und Lehrkräfte der Schule, die Nutzer der G Suite for Education sind, müssen einmal im Jahr an einer solchen Schulung teilnehmen. Die Durchführung der Schulungen wird entsprechend in Klassen- und Kursbüchern sowie Protokollen von Lehrerkonferenzen oder Dienstbesprechungen dokumentiert. Vor der ersten Nutzung von G Suite for Education erfolgt eine Einweisung unter besonderer Berücksichtigung datenschutzrechtlicher Aspekte, die deutlich umfangreicher ist die jährlichen Schulungen. Die in den darauffolgenden Jahren durchgeführten Wiederholungen dienen der Auffrischung und fallen kürzer aus.

Sollte es zu Zwischenfällen mit missbräuchlicher Nutzung kommen, welche ein Verstoß gegen die Nutzungsvereinbarung darstellen, wird mit den betreffenden Personen eine anlassbezogene Schulung durchgeführt, bevor sie die Plattform wieder benutzen dürfen.

#### Nutzungsvereinbarung

Die Nutzungsvereinbarung (Anhang 1), in welche jeder Nutzer einwilligen muss, bevor ein Benutzerkonto erstellt und freigeschaltet wird, gibt Nutzungs- und Verhaltensregeln vor, welche sicherstellen sollen, dass G Suite for Education von Schülern und Lehrkräften verantwortungsvoll genutzt wird, so dass das eigene Recht auf informationelle Selbstbestimmung sowie das aller anderen Nutzer aus der Schule gewahrt bleibt. Um Nutzern die Möglichkeit zu geben, sich die Nutzungsvereinbarung immer zu vergegenwärtigen, ist sie nicht nur auf der Schulhomepage hinterlegt, sondern auch innerhalb von G Suite for Education überall leicht zugänglich. Sie findet sich so beispielsweise im Infobereich eines jeden Classrooms als PDF hinterlegt.

#### Datenminimierung

Zur Erstellung eines Benutzerkontos in G Suite for Education werden nur die minimal erforderlichen personenbezogenen Daten angelegt. Zur Datenminimierung gehört auch die Beschränkung des Anmeldenamen auf ein Pseudonym (siehe [Pseudonymisierung](#_vuk0x8p37y3w)). Über die Nutzungsvereinbarung (Anlage 1) verpflichten sich Benutzer auf eine datensparsame Nutzung der Plattform.

#### Logische Zugriffskontrolle

Ein Rechte- und Rollenkonzept gewährleistet, dass die verschiedenen Gruppen von Nutzern in G Suite for Education nur auf die personenbezogenen Daten anderer Nutzer Zugriff haben, die für ihre Funktion erforderlich sind. Lehrkräfte können so nur personenbezogene Daten der Schüler sehen, welche in ihren Lerngruppen sind und dabei auch nur die Daten, welche unmittelbar mit ihrem Unterricht in der Lerngruppe zu tun haben. Schüler sehen nur ihre eigenen Daten und bei Freigabe durch Lehrkräfte oder Mitschüler Daten, welche diese Personen ihn explizit offenbaren.

Das Rechte- und Rollenkonzept ist an Benutzerprofile gekoppelt, die aus der Zugehörigkeit zu Gruppen ableiten. Zum Schutz jüngerer Schülerinnen und Schüler sind die Rechte dieser Gruppe eingeschränkter als die der älteren Schüler.

##### Benutzerprofile, Rollen und Rechte

|  |  |  |
| --- | --- | --- |
| **Gruppenname** | **Rolle** | **Merkmale des Benutzerprofils, Rechte** |
| Schüler bis Klasse 8 | Schüler | * Gmail Versand nur innerhalb der Schule möglich. * Inhalte in Google Drive sind im Standard auf privat gesetzt. * Freigabe von Inhalten aus Google Drive nur innerhalb der Schule möglich. * Beschränkung der verfügbaren Google Apps. |
| Schüler ab Klasse 9 | Schüler | * Gmail Versand uneingeschränkt möglich. * Inhalte in Google Drive sind im Standard auf privat gesetzt. * Freigabe von Inhalten aus Google Drive uneingeschränkt möglich. * Vollständige Google Apps Suite. |
| Lehrkräfte | Lehrer | * Gmail Versand uneingeschränkt möglich. * Inhalte in Google Drive sind im Standard auf privat gesetzt. * Freigabe von Inhalten aus Google Drive uneingeschränkt möglich. * Vollständige Google Apps Suite. * Können Classrooms erstellen und Schüler einladen. * Können Passwörter von Schülern zurücksetzen * Können Team Drives einrichten und verwalten. |
| Schulleitung | Admin | * Administrator Rechte (Zugriff auf die Google Admin Console, Zugriff mit eingeschränkten Rechten.) |
| Schulverwaltung (ein allgemeiner, nicht persönlicher Verwaltungs-Account steht zur Verfügung) | Verwaltung | * Gmail Versand nur innerhalb der Schule möglich. * Freigabe von Inhalten aus Google Drive nur innerhalb der Schule möglich. * Beschränkung der verfügbaren Google Apps (Drive, Docs, Sheets, Gmail, Calendar, Contacts). |
| schulische Administratoren | Admin | * Zugriff auf die Google Admin Console, Zugriff mit eingeschränkten Rechten für schulinterne Verwaltung von Nutzern, Gruppen, ... |
| IT Mitarbeiter Schulträger/ Dienstleister | Admin | * Zugriff auf die Google Admin Console, Vollzugriff mit allen Rechten |

##### Authentifizierungsmethoden

Um die individuellen Accounts vor unbefugtem Zugriff zu schützen, werden über die Admin Console der G Suite for Education Regeln vorgegeben, die in Abhängigkeit von der Funktion der Benutzer und den damit verbundenen Rechten die Stärke der Schutzmechanismen regeln. Bei jüngeren Schülern sind die Vorgaben etwas abgeschwächt, um möglichen Schwierigkeiten bei der Authentifizierung durch eine zu große Komplexität der Vorgaben vorzubeugen. Benutzern mit umfangreichsten Berechtigungen im System sind die strengsten Sicherheitsregeln zur Authentifizierung vorgegeben.

|  |  |
| --- | --- |
| **Gruppenname** | **Vorgaben zur Authentifizierung** |
| Schüler bis Klasse 8 | **Passwort**, 6-20 Zeichen, Regel für starke Passwörter (Buchstaben, Zahlen und Sonderzeichen müssen verwendet werden), keine Verwendung für andere Logins, unbegrenzt gültig |
| Schüler ab Klasse 9 | **Passwort**, 8-100 Zeichen, Regel für starke Passwörter (Buchstaben, Zahlen und Sonderzeichen müssen verwendet werden), keine Verwendung für andere Logins, unbegrenzt gültig |
| Lehrkräfte | **Passwort**, 8-100 Zeichen, Regel für starke Passwörter (Buchstaben, Zahlen und Sonderzeichen müssen verwendet werden), keine Verwendung für andere Logins, unbegrenzt gültig  **Zwei Faktor Authentifizierung** (**2FA**) über USB Dongle, SMS, Authenticator, OTP verpflichtend |
| Schulleitung | **Passwort**, 12-100 Zeichen, Regel für starke Passwörter (Buchstaben, Zahlen und Sonderzeichen müssen verwendet werden), keine Verwendung für andere Logins, unbegrenzt gültig  **Zwei Faktor Authentifizierung** (**2FA**) über USB Dongle, Authenticator, OTP verpflichtend, (kein SMS!) |
| Schulverwaltung (ein allgemeiner, nicht persönlicher Verwaltungs-Account steht zur Verfügung) | **Passwort**, 8-100 Zeichen, Regel für starke Passwörter (Buchstaben, Zahlen und Sonderzeichen müssen verwendet werden), keine Verwendung für andere Logins, unbegrenzt gültig |
| schulischer Administrator | Passwort, 12-100 Zeichen, Regel für starke Passwörter (Buchstaben, Zahlen und Sonderzeichen müssen verwendet werden), keine Verwendung für andere Logins, unbegrenzt gültig  **Zwei Faktor Authentifizierung** (**2FA**) über USB Dongle, Authenticator, OTP verpflichtend, (kein SMS!) |
| IT Mitarbeiter Schulträger/ Dienstleister |

#### Pseudonymisierung

Die Benutzerverwaltung unterscheidet zwischen dem **Benutzernamen** und dem **Anmeldenamen**. Der Benutzername enthält den realen Namen (Klarname) des Benutzers und ist für die Identifikation des Schülers durch betreuende Lehrer erforderlich. Der Anmeldename wird bei der Anmeldung an G Suite for Education verwendet und ist nicht mit dem Benutzernamen identisch. Auch im Sinne der Datenminimierung wird hier ein Pseudonym genutzt. Der Anmeldename besteht bei G Suite for Education aus einer E-Mail Adresse. Diese wird aus einem Namenskürzel und der Schüler-Identnummer aus der Schulverwaltung gebildet. Die Anmeldung mit Pseudonymen soll den Missbrauch des Kontos durch Dritte deutlich erschweren. Eine Verknüpfung zwischen Schüler-Identnummer mit dem Namen ist für Dritte ohne Zugriff auf die Schulverwaltungssoftware oder den Aktenbestand im Schulsekretariat nicht möglich.

#### Weitere technische und organisatorische Maßnahmen

##### Sicherheit schulischer Endgeräte und IT Infrastruktur

Die schulische IT wird durch das Supportpersonal immer auf dem aktuellen Stand gehalten, so dass bei Windows Systemen alle Betriebsystem- und Sicherheitsupdates eingespielt sind. Entsprechendes gilt für Software zum Schutz vor Viren, Trojanern und anderer Malware.

Dem Stand der Technik entsprechend sind die Geräte durch Verschlüsselung der Festplatte vor unberechtigten Zugriffen geschützt.

In der Schule genutzte Endgeräte wie iPads und Chromebooks werden unter Nutzung der vom jeweiligen OS bereitgestellten Sicherheitsmechanismen auf größtmögliche Sicherheit eingerichtet.

Das schulische Netz ist nach außen durch Sicherheitsmaßnahmen wie Firewall, Proxyfilter und ähnlich geschützt.

### Maßnahmen Googles

Google trifft umfangreiche technische und organisatorische Maßnahmen, um Schutz und Sicherheit der personenbezogenen Daten der Benutzer von G Suite for Education vor internen und externen, menschlichen und nichtmenschlichen Risikoquellen zu schützen. Diese Maßnahmen sind umfangreich dokumentiert.

#### EU Model Contract Clauses

(EU Standard Vertrags Klauseln**[[40]](#footnote-39)**)

Appendix 2 - Technische und organisatorische Maßnahmen bezüglich der

* **Server Farmen** (z.B. geographische Verteilung der Infrastruktur auf verschiedene Orte, Redundanz, abgesicherte Energieversorgung, sichere Server Betriebssysteme)
* **Netzwerk & Übermittlung** (z.B. private Hochgeschwindigkeitsverbindungen über Kabel, diverse Schutzschirme zur Abwehr von Angriffen von außen, Systeme zur Erkennung von Eindringlingen, Reaktionspläne für Zwischenfälle, Verschlüsselungstechnologien)
* **Zugangsschutz** (z.B. durch technische Überwachung der Serverstandorte, Sicherheitspersonal, Sicherheitsschleusen usw.)
* **Zugriffsschutz** (z.B. durch Schutz durch Überwachung innerhalb der Anlagen und Rechte- und Rollenkonzepte für das Personal
* **Datenspeicherung, Datentrennung und Authentifizierung**
* **Sichere Löschung** von Festplatten, die wiederverwendet werden, und **Zerstörung** für Festplatten, die ausgemustert werden
* **Sicherheitsmaßnahmen Personal** (z.B. gründliche Schulung, Absolvierung von Sicherheitstrainings und Zertifizierung, Unterzeichnung von Verschwiegenheitsvereinbarungen)
* **Sicherheit bei Unterauftragsverarbeitern** (z.B. durch einen Audit der Sicherheitsmaßnahmen bevor eine Beauftragung zustande kommt, Abschluss von entsprechenden Verträgen, welche Sicherheit, Vertraulichkeit und Schutz der im Auftrag verarbeiteten personenbezogenen Daten garantieren)
* **Datenschutzbeauftragter** - das für Sicherheit zuständige Team bei Google ist unter <https://support.google.com/a/contact/googlecloud_dpr> erreichbar (mit Login von der Admin Console aus).

## Modellierung der Risikoquellen

|  |
| --- |
| Die **Quellen des Risikos** für die Rechte und Freiheiten natürlicher Personen müssen identifiziert werden. Insbesondere ist zu bestimmen, **welche Personen** motiviert sein könnten, die Verarbeitungsvorgänge und die hierin verarbeiteten Daten in unrechtmäßiger Weise zu nutzen, und welches ihre **Beweggründe** und **möglichen Ziele** sein können. Anhand dessen können die damit zusammenhängenden **Eintrittswahrscheinlichkeiten** ermittelt werden. |

### Interne menschliche Quellen:

**Unbeabsichtigtes Handeln:**

* individuelle oder strukturelle Fehler

**Vorsätzliches Handeln:**

* Schaden für den Betroffenen wird entweder billigend in Kauf genommen oder wird vom Verursacher beabsichtigt und stellt Ziel der Handlung dar

### Externe menschliche Quellen:

**Unbeabsichtigtes Handeln:**

* individuelle oder strukturelle Fehler

**Vorsätzliches Handeln:**

* Angreifer oder Verursacher außerhalb der verantwortlichen Stelle mit dem Ziel der Schädigung des Unternehmens oder der Betroffenen

### Nichtmenschliche Quelle:

**Intern/extern:**

* Systemfehler (Software/Hardware) führen zu Verlust, Veränderung oder missbräuchlicher Verwendung personenbezogener Daten

### Mögliche Risikoquellen

Welche Risikoquellen sind beim Einsatz von G Suite for Education vorstellbar?

#### Interne menschliche Quellen

* Schüler
* Lehrkräfte
* Schulischer Administrator
* Schulverwaltungsmitarbeiter
* Schulleitung

#### Externe menschliche Quellen

* Schüler, die selbst keine Benutzer sind
* Lehrkräfte
* Freunde
* Familienmitglieder
* ehemalige Schüler
* ehemalige Lehrkräfte
* ehemalige schulische Administratoren
* Cyberkriminelle (Hacker/Schadsoftware)
* staatliche Institutionen (Nachrichtendienste)
* staatliche Institutionen (Strafverfolgung)
* Google Mitarbeiter
* Mitarbeiter möglicher Subunternehmer von Google

#### Nichtmenschliche Quelle (intern/extern):

* Softwarefehler
* Hardwaredefekte (physikalisch)
* Umwelteinflüsse (Naturgewalt)

Tabelle mit den wichtigsten in Frage kommenden Risikoquellen und Motivation zur Modellierung der Risikoquellen.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Art der Quelle** | **Extern/ Intern** | **Unbeabsichtigt/ Vorsätzlich** | **Akteur/ Risikoquelle** | **Motivation falls vorsätzlich** | **Verarbeitungs- grundsatz Art. 5 DS-GVO** |
| menschlich | intern | unbeabsichtigt | * Schüler, * Lehrkräfte, * schulischer Administrator * Schulverwaltung * Schulleitung   Bedienfehler, Verarbeitung von sensiblen Daten in G Suite for Education (*Leistungsdaten, Gutachten, Angaben zum Sozialverhalten, Informationen zu eth. Herkunft, Politik, Religion, Sexualleben, Gesundheit, etc*.) |  | Integrität und Vertraulichkeit, Rechtmäßigkeit,  Datenminimierung |
| vorsätzlich | * Schüler, * Lehrkräfte * schulischer Administrator * Schulverwaltung * Schulleitung   Weitergabe Zugangsdaten an Mitschüler/ Kollegen/ Freunde/ Verwandte | anderen einen Gefallen tun, helfen wollen | Integrität und Vertraulichkeit |
| * Schüler * Lehrkräfte   Manipulation eigener Daten/ fremder Daten/ Accounts durch Diebstahl von fremdem Passwort/ Missbrauch von Benutzerrechten | anderen schaden, sich selbst Vorteile verschaffen | Rechtmäßigkeit |
|
| * Schulleitung   Missbrauch von Nutzerdaten zur Kontrolle des Arbeits- und Leistungsverhaltens von Lehrkräften |
| * schulischer Administrator   Missbrauch von Administratorrechten |
| * Schüler * Lehrkräfte   *nicht Nutzer von G Suite for Education* Manipulation fremder Daten/ Accounts durch Diebstahl von fremdem Passwort | anderen schaden | Integrität und Vertraulichkeit |
|
| * Schüler * Lehrkräfte   Koppelung des schulischen Accounts mit anderen privaten Accounts | sich selbst Vorteile verschaffen | Integrität und Vertraulichkeit |
| **Art der Quelle** | **Extern/ Intern** | **Unbeabsichtigt/ Vorsätzlich** | **Akteur/ Risikoquelle** | **Motivation falls vorsätzlich** | **Verarbeitungs- grundsatz Art. 5 DS-GVO** |
|  | extern | vorsätzlich | * ehemalige Schüler * ehemalige Lehrkräfte * ehemaliger schulischer Administrator * ehemalige Schulleitung * ehemalige Schulverwaltung   Manipulation des eigenen ehemaligen Accounts/ fremder Daten/ Accounts durch noch gültigen eigenen Zugang/ durch Diebstahl von fremdem Passwort | anderen schaden, sich selbst Vorteile verschaffen | Integrität und Vertraulichkeit |
| menschlich | * Cyberkriminelle   Diebstahl Zugangsdaten durch Schadsoftware auf Endgeräten/ durch social Engineering/ Hacking | Datendiebstahl, sich selbst Vorteile verschaffen, Spaß, ... | Integrität und Vertraulichkeit |
| * Google Mitarbeiter/ Contractors * Mitarbeiter von möglichen Subunternehmern | Datendiebstahl, sich selbst Vorteile verschaffen ... | Integrität und Vertraulichkeit |
| * Google   Profilerstellung für Werbeanzeigen | Monetarisierung von Daten | Rechtmäßigkeit,  Zweckbindung |
| * Google   Änderung der Geschäftsbedingungen |
| * Deutsche Ermittlungsbehörden   Zugriff im Rahmen einer Ermittlung | Aufklärung eines Verbrechens | Integrität und Vertraulichkeit,  Rechtmäßigkeit |
| * Inlandsgeheimdienst BND | geheimdienstliche Ermittlungen | Integrität und Vertraulichkeit,  Rechtmäßigkeit |
| * CIA * andere US-amerikanische Ermittlungsbehörden   Zugriff im Rahmen einer Ermittlung im Rahmen des Cloud Act | Aufklärung eines Verbrechens | Integrität und Vertraulichkeit,  Rechtmäßigkeit |
| * Auslandsgeheimdienste | Spionage | Integrität und Vertraulichkeit,  Rechtmäßigkeit |
| * Gesetzesänderungen in den USA oder der EU | veränderte politische Lage/ Regierungswechsel | Integrität und Vertraulichkeit,  Rechtmäßigkeit |
| Nicht menschlich | intern | unbeabsichtigt | * Softwarefehler * Hardwaredefekt (physikalisch) |  | Integrität und Vertraulichkeit |
| extern | * Netzstörungen * Umwelteinflüsse (Naturgewalt) |  | Integrität und Vertraulichkeit |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

## Risikobeurteilung (Risikoanalyse)

Im Folgenden wird, aufbauend auf den vorherigen Schritten, bestimmt, ob in Bezug auf die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung von personenbezogenen Daten in G Suite for Education ein hohes Risiko für die Rechte und Freiheiten der Benutzer, Schüler und Lehrkräften, besteht.

Die Risiken werden hinsichtlich der Schwere des Schadens und der Eintrittswahrscheinlichkeit beschrieben. Die Risikobeurteilung orientiert sich an den Vorgaben der ISO 31000[[41]](#footnote-40). Die Die Risikobeurteilung besteht dabei aus

* der **Risikoidentifikation (I.)** - *Risikobeschreibung samt Risikoquelle sowie der dazugehörige Verarbeitungsgrundsatz nach Art 5 DS-GVO* (siehe vorheriger Abschnitt)
* der **Risikoanalyse (II.)** - *möglicher Schaden, die Schadenskategorie gem. ErwGr. 75, die Eintrittswahrscheinlichkeit und die Schwere des Schadens*
* der **Risikobewertung (III.)** - *Ergebnis der Risikobewertung*

### Schadenskategorien nach ErwGr. 75 DS-GVO

Erwägungsgrund 75[[42]](#footnote-41) führt eine Reihe von möglichen Risiken für die Rechte und Freiheiten natürlicher Personen auf, zu welchen Schüler und Lehrkräfte zählen.

* Diskriminierung
* Rufschädigung
* Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden personenbezogenen Daten
* andere wirtschaftliche oder gesellschaftliche Nachteile (z.B. Verlust einer zugesagten Ausbildungsstelle, Disziplinarstrafe, Bußgeld, zivilrechtliche Strafe, …)
* Profilbildung durch Bewertung persönlicher Aspekte (Vorlieben, Interessen, Meinungen, Aufenthaltsort, Ortswechsel, etc.)
* Profilbildung durch Bewertung von schulischen Leistungen, Arbeitsverhalten, Zuverlässigkeit, ...
* Unbefugten Aufhebung der Pseudonymisierung
* Verarbeitung von sensiblen Daten (Eth. Herkunft, Politik, Religion, Sexualleben, Gesundheit, etc.)
* Hinderung der Kontrolle der Betroffenen über eigene Daten



Matrix zur Risikobewertung

### Schwere und Eintrittswahrscheinlichkeit

#### Einstufungen zur Bewertung der Schwere des Risikos/ Schadens

Die Schwere eines möglichen Schadens muss in jedem Einzelfall insbesondere unter Berücksichtigung von Art, Umfang, Umständen und Zwecken der Verarbeitung bestimmt werden (ErwGr. 76).

* geringfügig - kleine Unannehmlichkeit
* überschaubar - größere Unannehmlichkeit
* substantiell - wesentliche Folgen
* groß - wesentliche und/ oder irreversible Folgen

#### Einstufung zur Bewertung der Eintrittswahrscheinlichkeit

Die Eintrittswahrscheinlichkeit eines Risikos beschreibt, mit welcher Wahrscheinlichkeit ein bestimmtes Ereignis (das selbst auch ein Schaden sein kann) eintritt **und** mit welcher weiteren Wahrscheinlichkeit es zu Folgeschäden kommen kann.

* geringfügig - fast unmöglich/ nicht vorstellbar
* überschaubar - mit gewissem Aufwand machbar (schwierig)
* substantiell - mit geringem Aufwand machbar
* groß - einfach machbar

### Risikobewertung

#### Unrechtmäßiger Zugriff auf Daten

|  |  |
| --- | --- |
| **(A) Unrechtmäßiger Zugriff auf Daten** | |
| mögliche wesentlichen **Auswirkungen** für die betroffenen Personen, wenn es Risiko eintritt | **Hinderung an der Kontrolle über eigene Daten** (durch Passwortänderung), **Profilbildung** aus den Nutzungsdaten und Inhalten/ aus schulischen Leistungen, Arbeitsverhalten, Zuverlässigkeit usw., **Rufschädigung** durch Veröffentlichung von persönlichen Inhalten |
| **Hauptbedrohungen**, die zu dem Risiko führen könnten | * unangemessener Gebrauch * Manipulation * Beschädigung * Veränderung * Verlust |
| mögliche **Risikoquellen** | **nichtmenschlich**  **intern:** Sicherheitslücke, Schadsoftware,  **menschlich:** *(durch Weitergabe von Zugangsdaten an Dritte, durch Diebstahl von Zugangsdaten, Machtmissbrauch)* **Intern:** Mitschüler, Lehrkräfte, schulischer Admin, Schulleitung **extern:** Cyberkriminelle, Geheimdienste, ehemalige Schüler und Lehrkräfte, Mitschüler ohne G Suite Account, Freunde, Familienmitglieder, (ausländische Nachrichtendienste, US Ermittlungsbehörden) |
| identifizierte **Maßnahmen**, die zur Bewältigung des Risikos beitragen | **Schule:** Nutzungsvereinbarung, Sensibilisierung, Einweisung vor Erstbenutzung, Pseudonymisierung der Anmeldedaten, Passwortregeln, bei Lehrkräften und Funktionsträgern 2FA, abgestuftes Rechtekonzept, Kontrolle Passwort-Komplexität durch Schul-Admin über Funktion Admin Console  **Google:** Redundanz der gespeicherten Daten, Aufzeichnung des Bearbeitungsverlaufs bei jeder Datei, Nachverfolgbarkeit von Aktionen in Benutzerkonten über Log-Dateien |
| **Risikoschweregrad**, insbesondere hinsichtlich der möglichen Auswirkungen und geplanten Maßnahmen | **(3)** - die Folgen eines unrechtmäßigen Zugriffs könnten Auswirkungen mit wesentlichen Folgen haben, vor allem, wenn es dadurch zu einem Missbrauch der Daten kommt. Schäden an Daten und der Zugang zum eigenen Konto sind reparabel, können aber zu größeren Unannehmlichkeiten führen. |
| **Eintrittswahrscheinlichkeit** des Risikos insbesondere hinsichtlich der Bedrohungen, Risikoquellen und geplanten Maßnahmen | (**1**) - für **externe** - Cyberkriminelle - durch die technischen Maßnahmen auf Seiten von Google kaum machbar (*bisher sind keine Fälle bekannt geworden, dass Externe Zugriff auf Daten erhalten haben*) - Google/ Subunternehmer von Google - nicht zu erwarten, da Google sich hier recht gut absichert durch technische und organisatorische Maßnahmen. Eine Veränderung der Geschäftsbedingungen, die einen Zugriff Googles auf die Daten zuließen, müsste vorher angekündigt werden.  (**2**) - für interne und externe durch leichtsinniges Handeln der Betroffenen, z.B. Passwortweitergabe oder Social Engineering mit einem gewissen Aufwand machbar |

#### Unerwünschte Veränderung von Daten

|  |  |
| --- | --- |
| **(B)** **Unerwünschte Veränderung von Daten** | |
| mögliche wesentlichen **Auswirkungen** für die betroffenen Personen, wenn es Risiko eintritt | **Schüler:** schlechtere Bewertung, Rufschädigung, disziplinarische Konsequenzen, strafrechtliche Konsequenzen; (vorübergehende) Sperrung des Zugriffs auf die Plattform  **Lehrkräfte:** Rufschädigung, materielle Schäden durch disziplinarische Konsequenzen, strafrechtliche Konsequenzen; (vorübergehende) Sperrung des Zugriffs auf die Plattform |
| **Hauptbedrohungen**, die zu dem Risiko führen könnten | **Weitergabe von Zugangsdaten an Dritte, Diebstahl von Zugangsdaten → Manipulation der Daten durch Dritte**  **Schüler:** manipulierte Arbeitsmaterialien, Beiträge, E-Mails mit schädlichem, beleidigendem oder diskriminierendem Inhalt werden innerhalb der Schule oder aus der Schule versandt; Kommentare mit beleidigendem oder diskriminierendem Inhalt werden gegenüber Mitschülern oder Lehrkräften in Dokumenten gemacht  **Lehrkräfte:** verlieren Arbeitsergebnisse, Bewertungsgrundlagen; E-Mails mit schädlichem, beleidigendem oder diskriminierendem Inhalt werden innerhalb der Schule oder aus der Schule versandt; Kommentare mit beleidigendem oder diskriminierendem Inhalt oder fachlich unzutreffenden Inhalten werden gegenüber Schülern oder Kollegen in Dokumenten gemacht |
| mögliche **Risikoquellen** | **nichtmenschlich**  **intern:** Softwarefehler, Technikversagen  **menschlich:**  **Intern:** Mitschüler, Lehrkräfte, schulischer Admin **extern:** Cyberkriminelle, ehemalige Schüler und Lehrkräfte, Mitschüler ohne G Suite Account, Freunde, Familienmitglieder |
| identifizierte **Maßnahmen**, die zur Bewältigung des Risikos beitragen | **Schule:** Nutzungsvereinbarung, Sensibilisierung, Einweisung vor Erstbenutzung, Pseudonymisierung der Anmeldedaten, Passwortregeln, bei Lehrkräften und Funktionsträgern 2FA, Sperrung von Nutzerkonten, sobald Nutzer aus der Schule ausgeschieden sind  **Google:** Redundanz der gespeicherten Daten, Aufzeichnung des Bearbeitungsverlaufs bei jeder Datei, Nachverfolgbarkeit von Aktionen in Benutzerkonten über Log-Dateien |
| **Risikoschweregrad**, insbesondere hinsichtlich der möglichen Auswirkungen und geplanten Maßnahmen | **(3)** - bis nachgewiesen ist, dass beispielsweise E-Mails und Kommentare nicht von den Betroffenen verfasst wurden, können die Auswirkungen wesentliche Folgen haben. |
| **Eintrittswahrscheinlichkeit** des Risikos insbesondere hinsichtlich der Bedrohungen, Risikoquellen und geplanten Maßnahmen | (**1**) - für **externe** - Cyberkriminelle - durch die technischen Maßnahmen auf Seiten von Google kaum machbar (*bisher sind keine Fälle bekannt geworden, dass Externe Zugriff auf Daten erhalten haben*)  (**2**) - für interne und externe durch leichtsinniges Handeln der Betroffenen, z.B. Passwortweitergabe oder Social Engineering mit einem gewissen Aufwand machbar |

#### Datenverlust

|  |  |
| --- | --- |
| **(C) Datenverlust** | |
| mögliche wesentlichen **Auswirkungen** für die betroffenen Personen, wenn es Risiko eintritt | **Schüler:** verlieren Arbeitsergebnisse, E-Portfolio - mit Folgen wie eventuell Probleme, eine gute Note zu erlangen, schlechtere Bewertung, Rufschädigung  **Lehrkräfte:** verlieren Arbeitsergebnisse, Bewertungsgrundlagen - mit Folgen wie Rufschädigung (Glaubwürdigkeit, wenn es um Begründung von Noten geht.), Arbeitszeit durch verlorene Arbeitsmaterialien |
| **Hauptbedrohungen**, die zu dem Risiko führen könnten | physische Zerstörung der Daten |
| mögliche **Risikoquellen** | **nichtmenschlich**  **extern:** Naturkatastrophen  **intern:** Softwarefehler, Technikversagen  **menschlich**  **extern:** Cyberkriminelle, Anschläge  **intern:** Sabotage, Manipulation der Daten |
| identifizierte **Maßnahmen**, die zur Bewältigung des Risikos beitragen | **Google:** verschiedene Serverstandorte, Redundanz der gespeicherten Daten, abgesicherte Stromversorgung, sicheres Serverbetriebssystem, Zugangsschutz, Zugriffsschutz, |
| **Risikoschweregrad**, insbesondere hinsichtlich der möglichen Auswirkungen und geplanten Maßnahmen | **(2)** - durch einen zumindest vorübergehenden Datenverlust könnte es bei den Betroffenen zu Ängsten und Sorgen kommen. |
| **Eintrittswahrscheinlichkeit** des Risikos insbesondere hinsichtlich der Bedrohungen, Risikoquellen und geplanten Maßnahmen | **(1)** - durch die vielfältigen technischen und organisatorischen Maßnahmen durch Google sehr geringe Wahrscheinlichkeit, dass Daten unwiederbringlich verloren gehen können. |

#### 

### Ergebnis der Risikobewertung

### 

**A** Unrechtmäßiger Zugriff auf Daten

**B** Unerwünschte Veränderung von Daten

**C** Datenverlust

### Auswertung

Die Modellierung der verschiedenen Risiken, welche für Schülerinnen und Schüler und Lehrkräfte als Nutzer von G Suite for Education entstehen können, zeigt vor allem eines deutlich. Weder nichtmenschliche Quellen stellen das größte Risiko dar, egal ob intern oder extern, noch sind es externe menschliche Quellen. Das größte Risiko geht stattdessen von internen menschlichen Quellen aus, den Nutzern selbst. Auch wenn die Wahrscheinlichkeit für einen durch einen Nutzer in der Schule verursachten Risikofall eher gering ist, so kann das Ausmaß des für die Betroffenen entstehenden Schadens substanziell sein. Ob der Schaden dauerhafter Natur ist oder vorübergehend, hängt einmal davon ab, ob die betroffenen Daten durch technische Maßnahmen, welche Verfügbarkeit und Integrität der Daten garantieren sollen, wieder in ihren Ausgangszustand hergestellt werden können, und welcher Natur der Schaden für die betroffene Person ist, der aus einer Manipulation oder Offenlegung von personenbezogenen Daten gegenüber Dritten entstanden ist.

Von den drei unter Berücksichtigung bestehender oder geplanter Maßnahmen bewerteten Datenschutzrisiken werden zwei, Unrechtmäßiger Zugriff auf Daten und Unerwünschte Veränderung von Daten, ganz erheblich durch Fehler der Nutzer ursächlich bedingt. Die Sicherheit eines G Suite for Education Benutzerkontos ist in großem Maße von der Absicherung der Konten selbst bestimmt. Das meint an erster Stelle die Authentifizierung der Benutzer. Gerade bei Schülern kommt es aus Erfahrung immer wieder einmal vor, dass sie ihre Zugangsdaten Mitschülern verraten, besten Freunden oder Familienmitgliedern. Das kann Folgen haben, da die Person, welche über die Zugangsdaten einen Kontos verfügt, auch alle damit verbunden Rechte hat. Auch wenn diese durch logischen Zugriffskontrollen auf die für die Rolle erforderlichen Rechte beschränkt sind, kann so einiger Schaden verursacht werden.

Mögliche Risiken, die von Geheimdiensten, egal ob inländische oder ausländische, sind wie bei jeder vergleichbaren Plattform, ausgehen können, wenn diese sich Zugang verschaffen, ist mangels ausreichender Informationen nicht kalkulierbar. Gleiches gilt für die Schadensschwere, die durch einen solchen Zugriff für einzelne Benutzer verursacht werden könnte. Aus diesem Grund sind solche Szenarien in dieser DSFA nicht in die Risikobeurteilung eingeflossen. Wenn die Möglichkeit des Zugriffs durch Geheimdienste ein Ausschlusskriterium für eine Plattform darstellt, dann gilt dieses für jede Plattform, die mit dem Internet verbunden ist und dadurch angreifbar ist.

Auch bezüglich der Risiken durch Zugriffe US amerikanischer Ermittlungsbehörden lässt sich keine belastbare Abschätzung vornehmen. Die Risiken dürften sich nicht wesentlich unterscheiden hinsichtlich der rechtlichen Grundlage, auf welcher sie erfolgen (Cloud-Act oder im Rahmen von Rechtshilfeabkommen in Strafsachen (engl. Mutual Legal Assistance Treaty – MLAT)). Der einzige Unterschied ist der, dass die Betroffenen bei Zugriffen ohne den Weg über das Rechtshilfeabkommen möglicherweise nie davon erfahren. Die mögliche Schwere eines Schadens durch einen solchen Zugriff wird sehr stark vom einzelnen Fall abhängen und ist auch von daher nicht verallgemeinerbar zu abzuschätzen.

## Abhilfemaßnahmen

Da die Sicherheit des Zugangs zum Konto das größte Risiko darstellt, sollten Abhilfemaßnahmen darauf abzielen, eben dieses Risiko zu reduzieren. Dieses kann durch technische wie organisatorische Maßnahmen erfolgen. Technische Maßnahmen sollten es Nutzern auf der einen Seite erleichtern, ein Mehr an Sicherheit zu gewinnen, und es ihnen gleichzeitig erschweren, durch unsicheres Handeln die Sicherheit ihres Kontos zu kompromittieren. Organisatorische Maßnahmen sollen durch Sensibilisierung und Regelvorgaben die Benutzer dabei unterstützen, riskantes Verhalten zu vermeiden.

#### 2FA für alle Nutzer ermöglichen

Die Schule hat bisher nur geplant, eine Zwei Faktor Authentifizierung für Nutzer vorzuschreiben, welche über umfangreichere Rechte in der Plattform verfügen. Dieses sind die Lehrkräfte, die Schulleitung und der schulische Administrator. Um das Risiko noch einmal deutlich zu reduzieren sollten auch Schülerinnen und Schüler die Möglichkeit erhalten, ihren Zugang über eine doppelte Authentifizierung abzusichern. Dieses verhindert zwar nicht, dass Schüler ihr Passwort aus Gefälligkeit an andere weitergeben, doch es erschwert die Weitergabe, da das Passwort alleine ohne den zweiten Faktor nicht genutzt werden kann. Die Schülerin bzw. Schüler müsste der anderen Person also auch noch bei der zweiten Authentifizierung behilflich sein oder ihr den zweiten Faktor übergeben, wenn es sich um ein Hardware Dongle handelt. In der einfachsten Form ist die Zwei Faktor Authentifizierung mit einem Smartphone und einer Authenticator App umzusetzen. Ein solches führen Schülerinnen und Schüler in der Regel mit sich.

#### Sichere Passwörter für alle Nutzer erzwingen

Die Google Admin Konsole bietet Möglichkeiten, die Sicherheitsvorgaben für Passwörter zu verschärfen. Eine Option ist das Erzwingen von sicheren Passwörtern (siehe hierzu *Passworteinstellungen der Nutzer verwalten[[43]](#footnote-42)*). Wie sicher Passwörter sind können Administratoren in der Admin Konsole überprüfen. Dort prüft ein Algorithmus die Passwörter auf Länge und Stärke und zeigt durch farbige Markierung und Symbole an, ob ein Passwort sicher ist oder nicht. Stellt ein Administrator fest, dass ein Nutzer ein nicht ausreichend starkes Passwort nutzt, sollte er diesen darauf aufmerksam machen.

#### (Keine) regelmäßige Änderung der Passwörter

In der Google Admin Konsole lässt sich auch eine Ablauffrist für Passwörter einstellen. Dieses soll die Sicherheit erhöhen. Man geht aktuell jedoch davon aus, dass der Zuwachs an Sicherheit vernachlässigbar ist. Häufiger passiert es, dass ist nach der Änderung des Passwortes zu Problemen für den Nutzer kommt, weil er die Änderung vergessen hat. Nutzer haben jedoch immer die Möglichkeit, von sich aus ihr Passwort zu ändern.

#### Thema sichere Passwörter bei Schulung

Sichere Passwörter und die sichere Verwahrung von Passwörtern sind ein wichtiges Thema und sollten Thema bei der Einführung Schulung für neue Nutzer der G Suite for Education sein. Lernen sollten Schülerinnen und Schüler und auch Lehrkräfte so, was ein sicheres Passwort ausmacht und wie man ein solches Passwort einfach erstellen kann. Außerdem sollten mit den Nutzern auch Passwortmanager thematisiert werden. Einen solchen könnten sich die Schüler beispielsweise auf ihrem Smartphone installieren (siehe hierzu *Starkes Passwort erstellen und für mehr Kontosicherheit sorgen[[44]](#footnote-43)*).

##### Datenschutzeinstellungen im Benutzerkonto

Bei der Bereitstellung der G Suite for Education sollten die schulischen Nutzer sowie Erziehungsberechtigten über verschiedenen Datenschutzeinstellungen im Benutzerkonto informiert werden, die es ihnen ermöglichen, eigenständig zu entscheiden, wie Informationen in Google-Diensten verwendet werden. Abhängig von den von der Schule aktivierten Einstellungen können Benutzer die verschiedenen in den Datenschutzbestimmungen beschriebenen Kontrollen, wie z.B. die Google-Aktivitäts-Steuerung, verwenden, um ihre Privatsphäre und Informationen zu verwalten. In der Einführungsschulung sollten die Kontrollmöglichkeiten, den Nutzern ausführlich erklärt werden.

#### Wiederherstellungs E-Mail

Wenn die Schule eigene schulische E-Mail-Adressen hat und jeder Schülerin und jeder Schüler sowie alle Lehrkräfte über eine solche E-Mail-Adresse verfügt, sollte diese zur Absicherung des Benutzerkontos genutzt werden. Kommt es zu verdächtigen Kontoaktivitäten, kann das System die Nutzer hierüber mittels dieser E-Mail-Adresse informieren und ihnen die Möglichkeit geben, die Aktivitäten zu überprüfen und gegebenenfalls Maßnahmen zu ergreifen. Nutzer können diese Option eigenständig aktivieren und ihre private E-Mail-Adresse eingeben und sollten deshalb bei der Schulung für neue Nutzer über mögliche Risiken diesbezüglich aufgeklärt werden.

#### Sitzungsdauer für Web Apps begrenzen

Wird G Suite for Education auf Endgeräten genutzt, die von verschiedenen Benutzern verwendet werden, so wäre eine mögliche Maßnahme, die Sicherheit der Benutzerkonten zu erhöhen, indem Sitzungsdauer für im Browser genutzte Core Services (Classroom, Docs, Drive, …) begrenzt wird. Dieses kann in der Google Admin Konsole festgelegt werden. Möglich ist hierbei 1 Stunde, 4 Stunden, 8 Stunden, 12 Stunden, ..... Nach Ablauf der Sitzungsdauer muss das Passwort erneut eingegeben werden. Eine solche Begrenzung kann beispielsweise am Lehrer PC im Computerraum sehr sinnvoll sein, wenn sich Lehrkräfte dort mit einem Benutzerpasswort am Rechner anmelden. Sollten Sie vergessen, sich abzumelden, oder dieses Passwort gelangt in falsche Hände, besteht die Chance, dass die Sitzung bereits abgelaufen ist und ein Zugriff auf das Benutzerkonto in der G Suite for Education damit nicht mehr möglich ist.

#### ID Management System nutzen

Es empfiehlt sich, das ID und Access Management über ein zentrales Identity Management System zu steuern. So kann die Schule den Serverstandort bestimmen und behält die komplette Kontrolle über Identitäten und Berechtigungen, die einzelnen Personen in der Schule zugeordnet sind. Damit wird das Konzept der Datenminimierung bei der Nutzung von G Suite for Education unterstützt, da die Identität der Nutzer nicht mehr bei Google selbst hinterlegt wird. Dadurch kann eine direkte Anmeldung an G Suite for Education für Dritte erschwert werden. Ein eigenes Identity Management System ist einer Nutzung von G Suite for Education für Single Sign-on an anderen Plattformen grundsätzlich vorzuziehen, da auch damit zusätzliche personenbezogene Daten der Nutzer aus Google gehalten werden.

#### Eindeutige Vorgaben für Lehrkräfte

Damit für alle Lehrkräfte klar ist, welche personenbezogenen Daten auf gar keinen Fall in G Suite for Education verarbeitet werden dürfen, sollte zur Hilfe eine Anweisung ausgegeben werden, welche eine Positivliste von zulässigen Daten enthält und eine Negativliste von nicht zulässigen Daten.

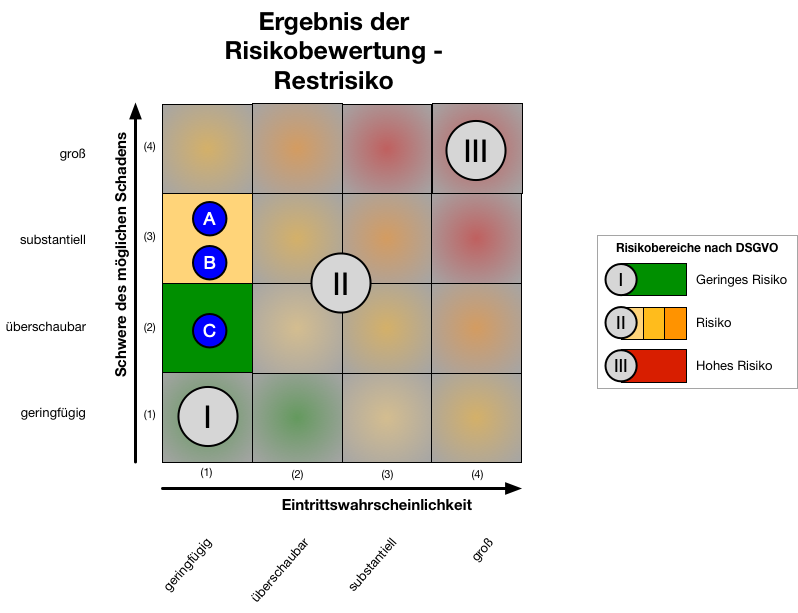
Lehrkräfte können wie alle Nutzer, für die ein Dokument freigegeben wurde, im Bearbeitungsverlauf sehen, wann ein Nutzer an dem Dokument gearbeitet hat. Ebenso können Lehrkräfte im Classroom sehen, an welchem Datum und zu welcher Uhrzeit Aufgaben abgegeben wurden. Diese “Nutzungsdaten” dürfen nur genutzt werden, soweit diese zur Wahrnehmung schulischer Aufgaben erforderlich sind[[45]](#footnote-44), etwa um zu kontrollieren, ob ein Abgabetermin eingehalten wurde, oder um einen Bearbeitungsverlauf zu besprechen. Entsprechende Regelungen sollten dafür in die Nutzungsvereinbarung für Lehrkräfte aufgenommen werden.

#### Sicherheitsmaßnahmen bei Nutzung mit Apps auf mobilen Endgeräten

Wird G Suite for Education in der Schule mit mobilen Endgeräten genutzt, aus denen keine separaten Nutzer eingerichtet sind, stellt die Nutzung von Apps wie Google Docs, Google Classroom und anderen ein Sicherheitsrisiko dar, weil Nutzer häufig vergessen, sich an diesen Apps bzw. am System abzumelden. Dieses ist, verglichen mit einer Abmeldung aus dem Browser (Web App) deutlich aufwendiger. Werden beispielsweise iPads genutzt und dieses ohne shared iPads, so sollte aus Sicherheitsgründen auf die Installation der Apps verzichtet werden. Gleiches gilt auch für Android Tablets oder Chromebooks (auf denen Apps installiert werden können).

## Restrisikoanalyse

Die beschriebenen Maßnahmen, welche vor allem darauf abzielen, riskantes Nutzerverhalten zu unterbinden, sollten dazu führen, dass die Eintrittswahrscheinlichkeit noch einmal ein Stück abgesenkt werden kann. Nach dem Prinzip der Datenminimierung ist eine Beschränkung der in G Suite for Education verarbeiteten Daten auf die für den Unterrichtszweck unbedingt erforderlichen beabsichtigt. Von daher ist an dieser Stelle keine weitere Verbesserung mehr möglich, ohne eine sinnvolle Nutzung der Plattform zur Durchführung von Unterricht unmöglich zu machen.



## Nachweis über DS-GVO Konformität

Die geplante Nutzung von G Suite for Education durch die Schule zur Durchführung von Unterricht und zur Teamarbeit im Kollegium sollte durch die Beschränkung der in der Plattform verarbeiteten personenbezogenen Daten auf das erforderliche Minimum und die getroffenen Maßnahmen zur Eingrenzung des durch Nutzer selbst verursachten Risikos wie auch durch die umfangreichen technischen und organisatorischen Maßnahmen auf Seiten von Google unter Berücksichtigung aller Vorgaben der DS-GVO möglich sein.

Anders als von der Datenschutzkonferenz angenommen, ist bei einer Nutzung von G Suite for Education nicht einem voraussichtlich hohem Risiko für die Rechte und Freiheiten der betroffenen natürlichen Personen (Schüler, Lehrer, Eltern) auszugehen, wenn die Plattform wie im von der Schule geplanten Nutzungszenario eingesetzt wird. Eine Umsetzung der vorgeschlagenen Abhilfemaßnahmen sollte die bestehenden Risiken weiter reduzieren können. Die Wirksamkeit der bestehenden und geplanten Maßnahmen zur Datensicherheit sollten nach dem ersten oder zweiten Jahr der Einführung von G Suite for Education auf ihre Wirksamkeit hin überprüft und die Bewertung der Risiken entsprechend angepasst werden.

## Anlagen

* **Anlage 1** - Nutzungsvereinbarung zur G Suite for Education
* **Anlage 2** - Datenschutzerklärung zur G Suite for Education
* **Anlage 3** - Übersicht der verschiedenen Quellen
* [**Anlage 4** - Stellungnahmen der Mitbestimmungsgremien im Rahmen von Art. 35 Abs. 9 DS-GVO zu Risiken und möglichen Schäden]

#### Anlage 3

Übersicht der verschiedenen Quellen, die bei der Erstellung dieser DSFA referenziert wurden.

##### Google

* [G Suite for Education - Privacy & Security Center](https://edu.google.com/training-support/privacy-security/?modal_active=none)
* [Hauptdienste und zusätzliche Dienste für G Suite for Education](https://support.google.com/a/answer/6356441?hl=de)
* [G Suite: Zusammenfassung der Dienste (Core Services)](https://gsuite.google.com/intl/de/terms/user_features.html) (ausführliche Auflistung)
* [Data Processing Amendment to G Suite and/or Complementary Product Agreement (Version 2.1)](https://gsuite.google.com/intl/de/terms/dpa_terms.html)
* [Compliance amendments for G Suite and Cloud Identity](https://support.google.com/a/answer/2888485?hl=en)
* [G Suite for Education-Vereinbarung (online)](https://gsuite.google.com/intl/de/terms/education_terms.html)
* [G Suite - Standard Contractual Clauses (processors)](https://gsuite.google.com/terms/mcc_terms.html)
* [G Suite Agreement and/or Complementary Product Agreement - Subprocessors](https://gsuite.google.com/intl/en/terms/subprocessors.html)
* [Data center locations](https://www.google.com/about/datacenters/inside/locations/index.html)
* [G Suite for Education Privacy Notice](https://gsuite.google.com/terms/education_privacy.html)
* [Starkes Passwort erstellen und für mehr Kontosicherheit sorgen](https://support.google.com/accounts/answer/32040?hl=de)
* [Passworteinstellungen der Nutzer verwalten](https://support.google.com/a/answer/139399?hl=de)
* [Datenlöschung auf der Google Cloud Platform](https://cloud.google.com/security/deletion/?hl=de) (lässt sich auf G Suite übertragen)

##### Andere

* [Kurzpapier Nr. 18: Risiko für die Rechte und Freiheiten natürlicher Personen](https://www.datenschutzzentrum.de/artikel/1225-Kurzpapier-Nr.-18-Risiko-fuer-die-Rechte-und-Freiheiten-natuerlicher-Personen.html)
* [Art. 5 DSGVO Grundsätze für die Verarbeitung personenbezogener Daten](https://dsgvo-gesetz.de/art-5-dsgvo/)
* [Risk Assessment & Datenschutz-Folgenabschätzung, Leitfaden](https://www.bitkom.org/Bitkom/Publikationen/Risk-Assessment-Datenschutz-Folgenabschaetzung.html); Bitcom
* [Privacy Impact Assessment for School District No. 61 (Greater Victoria) and School District No. 63 (Saanich) Google Apps for Education PIA](https://www.sd61.bc.ca/wp-content/uploads/sites/91/2018/09/GSuite-PIA-SD61_63.pdf)
* [Dossier IV: Datenschutz-Folgenabschätzung](https://stiftungdatenschutz.org/fileadmin/Redaktion/Dossiers_Infoplattform/DSGVO-Info-Dossier_IV___Datenschutzfolgenabschaetzung_AR.pdf), Stiftung Datenschutz
* [Orientierungshilfe\_Online-Lernplattformen\_2018.pdf](https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/content-downloads/OH%20Lernplattformen.pdf)
* [GDD-Praxishilfe DS-GVO XIV](https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_14.pdf) - Die Datenschutz-Folgenabschätzung
* [Kurzpapier Nr. 5 - Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO](https://www.lda.bayern.de/media/dsk_kpnr_5_dsfa.pdf), DSK
* [Durchführung einer Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO in Anlehnung an die ISO/IEC 29134](https://www.lda.bayern.de/media/03_dsfa_fallbeispiel_baylda_iso29134.pdf), Musterbeispiel, Bayerisches Landesamt für Datenschutzaufsicht
* [Standard Datenschutz Modell](https://www.datenschutzkonferenz-online.de/media/ah/201804_ah_sdm.pdf) - V.1.1 – Erprobungsfassung , April 2018
* [Software zur Datenschutz-Folgenabschätzung (PIA-Tool)](https://www.datenschutz-bayern.de/technik/pia-tool.html.de) (Windows)

1. "Orientierungshilfe für Online- Lernplattformen im Schulunterricht ...." <https://www.bildungsserver.de/onlineressource.html?onlineressourcen_id=57564>. Accessed 13 May. 2019. [↑](#footnote-ref-0)
2. "Hauptdienste und zusätzliche Dienste für G Suite for ... - Google Support." <https://support.google.com/a/answer/6356441?hl=de>. Accessed 28 Apr. 2019. [↑](#footnote-ref-1)
3. "Dienstanweisung für die automatisierte Verarbeitung." <https://www.schulministerium.nrw.de/docs/Recht/Datenschutz/DienstanweisungRdErl.pdf>. Accessed 24 Apr. 2019. [↑](#footnote-ref-2)
4. "VO-DV I." <https://www.schulministerium.nrw.de/docs/Recht/Schulrecht/Verordnungen/VO-DV_I.pdf>. Accessed 24 Apr. 2019. [↑](#footnote-ref-3)
5. "Cloud Computing Compliance Controls Catalog (C5) | Google Cloud." <https://cloud.google.com/security/compliance/bsi-c5/>. Accessed 26 Apr. 2019. [↑](#footnote-ref-4)
6. "Google Cloud jetzt mit C5-Testat | Google Cloud Blog." 18 Sep. 2018, <https://cloud.google.com/blog/products/identity-security/google-cloud-completes-bsi-c5-audit-de>. Accessed 26 Apr. 2019. [↑](#footnote-ref-5)
7. "ISO 27001 - Compliance | Google Cloud." <https://cloud.google.com/security/compliance/iso-27001/>. Accessed 24 Apr. 2019. [↑](#footnote-ref-6)
8. "EYCP Certificate Template - Google services." <https://services.google.com/fh/files/misc/gsuite_iso27001_fall_2018.pdf>. Accessed 24 Apr. 2019. [↑](#footnote-ref-7)
9. "ISO 27018 - Compliance | Google Cloud." <https://cloud.google.com/security/compliance/iso-27018/>. Accessed 24 Apr. 2019. [↑](#footnote-ref-8)
10. "EYCP Certificate Template - Google services." <https://services.google.com/fh/files/misc/gsuite_iso27018_fall2018.pdf>. Accessed 24 Apr. 2019. [↑](#footnote-ref-9)
11. "ISO 27017 - Compliance | Google Cloud." <https://cloud.google.com/security/compliance/iso-27017/>. Accessed 24 Apr. 2019. [↑](#footnote-ref-10)
12. "EYCP Certificate Template - Google services." <https://services.google.com/fh/files/misc/gsuite_iso27017_fall2018.pdf>. Accessed 24 Apr. 2019. [↑](#footnote-ref-11)
13. "SOC 2 - Compliance | Google Cloud." <https://cloud.google.com/security/compliance/soc-2/>. Accessed 27 Apr. 2019. [↑](#footnote-ref-12)
14. "SOC 3 - Compliance | Google Cloud." <https://cloud.google.com/security/compliance/soc-3/>. Accessed 27 Apr. 2019. [↑](#footnote-ref-13)
15. "Google - Privacy Shield." <https://www.privacyshield.gov/participant?id=a2zt000000001L5AAI>. Accessed 24 Apr. 2019. [↑](#footnote-ref-14)
16. "Privacy Shield - Compliance | Google Cloud." <https://cloud.google.com/security/compliance/privacy-shield/>. Accessed 24 Apr. 2019. [↑](#footnote-ref-15)
17. "G Suite Terms of Service – G Suite - Google." <https://gsuite.google.com/terms/mcc_terms.html>. Accessed 24 Apr. 2019. [↑](#footnote-ref-16)
18. "EU Model Contract Clauses - Compliance | Google Cloud." <https://cloud.google.com/security/compliance/eu-mcc/>. Accessed 24 Apr. 2019. [↑](#footnote-ref-17)
19. "COPPA - Compliance | Google Cloud." <https://cloud.google.com/security/compliance/coppa/>. Accessed 26 Apr. 2019. [↑](#footnote-ref-18)
20. "FERPA - Compliance | Google Cloud." <https://cloud.google.com/security/compliance/ferpa/>. Accessed 26 Apr. 2019. [↑](#footnote-ref-19)
21. Wenn der Schulträger/ IT Dienstleister Administrationsaufgaben für die Schule übernimmt. [↑](#footnote-ref-20)
22. Kommt eventuell in Frage, wenn auch die Eltern einen Zugang zur G Suite for Education erhalten sollen. [↑](#footnote-ref-21)
23. Falls diese mit personalisierten Konten Zugang erhält. [↑](#footnote-ref-22)
24. “(1) Die Schule gestaltet den Unterricht, die Erziehung und das Schulleben im Rahmen der Rechts- und Verwaltungsvorschriften in eigener Verantwortung.” [↑](#footnote-ref-23)
25. "Medienkompetenzrahmen NRW." <https://medienkompetenzrahmen.nrw.de/>. Accessed 27 Apr. 2019. [↑](#footnote-ref-24)
26. "Art. 28 DSGVO – Auftragsverarbeiter | Datenschutz-Grundverordnung ...." <https://dsgvo-gesetz.de/art-28-dsgvo/>. Accessed 27 Apr. 2019. [↑](#footnote-ref-25)
27. "Nutzungsbedingungen für G Suite – G Suite - Google." <https://gsuite.google.com/intl/de/terms/education_terms.html>. Accessed 27 Apr. 2019. [↑](#footnote-ref-26)
28. "G Suite Terms of Service – G Suite - Google." <https://gsuite.google.com/terms/dpa_terms.html>. Accessed 27 Apr. 2019. [↑](#footnote-ref-27)
29. "G Suite Terms of Service – G Suite - Google." <https://gsuite.google.com/terms/mcc_terms.html>. Accessed 27 Apr. 2019. [↑](#footnote-ref-28)
30. "G Suite for Education Privacy Notice - Google." <https://gsuite.google.com/terms/education_privacy.html>. Accessed 27 Apr. 2019. [↑](#footnote-ref-29)
31. "Anmelden – Google Konten - Google Takeout." <https://takeout.google.com/?utm_source=pp&hl=de>. Accessed 18 May. 2019. [↑](#footnote-ref-30)
32. "G Suite Terms of Service – G Suite - Google." <https://gsuite.google.com/terms/dpa_terms.html>. Accessed 28 Apr. 2019. [↑](#footnote-ref-31)
33. "G Suite Terms of Service – G Suite - Google." <https://gsuite.google.com/terms/subprocessors.html>. Accessed 28 Apr. 2019. [↑](#footnote-ref-32)
34. "Data center locations – Data Centers – Google." <https://www.google.com/corporate/datacenter/locations.html>. Accessed 28 Apr. 2019. [↑](#footnote-ref-33)
35. "Google - Privacy Shield." <https://www.privacyshield.gov/participant?id=a2zt000000001L5AAI>. Accessed 24 Apr. 2019. [↑](#footnote-ref-34)
36. "Privacy Shield - Compliance | Google Cloud." <https://cloud.google.com/security/compliance/privacy-shield/>. Accessed 24 Apr. 2019. [↑](#footnote-ref-35)
37. "G Suite Terms of Service – G Suite - Google." <https://gsuite.google.com/terms/mcc_terms.html>. Accessed 24 Apr. 2019. [↑](#footnote-ref-36)
38. "EU Model Contract Clauses - Compliance | Google Cloud." <https://cloud.google.com/security/compliance/eu-mcc/>. Accessed 24 Apr. 2019. [↑](#footnote-ref-37)
39. "G Suite Terms of Service – G Suite - Google." <https://gsuite.google.com/terms/dpa_terms.html>. Accessed 28 Apr. 2019. [↑](#footnote-ref-38)
40. "G Suite Terms of Service – G Suite - Google." <https://gsuite.google.com/terms/mcc_terms.html>. Accessed 28 Apr. 2019. [↑](#footnote-ref-39)
41. "ISO 31000 – Wikipedia." <https://de.wikipedia.org/wiki/ISO_31000>. Accessed 27 Apr. 2019. [↑](#footnote-ref-40)
42. "Erwägungsgrund 75 - Risiken für die Rechte und Freiheiten ...." <https://dsgvo-gesetz.de/erwaegungsgruende/nr-75/>. Accessed 27 Apr. 2019. [↑](#footnote-ref-41)
43. "Passworteinstellungen der Nutzer verwalten - G ... - Google Support." <https://support.google.com/a/answer/139399?hl=de>. Accessed 29 Apr. 2019. [↑](#footnote-ref-42)
44. "Starkes Passwort erstellen und für mehr ... - Google Support." <https://support.google.com/accounts/answer/32040?hl=de>. Accessed 29 Apr. 2019. [↑](#footnote-ref-43)
45. "Orientierungshilfe Online-Lernplattform im Schulunterricht." S. 8; Kapitel 6.1.3 Nutzungsdaten <https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/Orientierungshilfe%20Online-Lernplattform%20im%20Schulunterricht%20-%20Stand%2004-2018.pdf>. Accessed 30 Apr. 2019. [↑](#footnote-ref-44)