Lokal DSFA

Google Workspace for Education[und

ChromeOS auf verwalteten Chromebooks]

lokale DSFA, die von Schulleitungen durchgeführt werden soll, basierend auf nationaler DSFA, DTIA und Überprüfung durch SIVON und SURF

Version 3.0 (24. Juni 2024)

KOLOPHON

DSFA und DTIA durchgeführt von	Coöperatie Samen Innoveren/Inkopen/Ict voor Onderwijs Nederland U.A.(SIVON) www.sivon.nl info@sivon.nl In SURF-Genossenschaft www.surf.nl info@surf.nl
Diejenigen, die an der Umsetzung der DSFA beteiligt sind	Datenschutzunternehmen (Den Haag) www.privacycompany.nl GreenbergTraurig (GT Law) Amsterdam www.gtlaw.com
Lokale DSFA der Autoren	Version 1.0: Ymkje Koster (Kennisnet) und Job Vos (SIVON) Version 2.0: Hans-Peter Ligthart und Job Vos (SIVON) Version 3.0: Hans-Peter Ligthart und Job Vos (SIVON)
Version	1.0: 5. August 2021 2.0: update 13 juli 2023 3.0: update 24 juni 2024

Diese DSFA nutzte die DSFA und DTIA der Privacy Company auf Google Workspace for Education, die Model DSFA von SIVON und die Model DSFA Government Version 2.0.

SIVON und Kennisnet werden vom Ministerium für Bildung, Kultur und Wissenschaft (OCW) finanziert. Diese Publikation wurde in Zusammenarbeit mit SURF und SIVON erstellt. SIVON und Kennisnet fördern die Zusammenarbeit zwischen Schulbehörden im Bereich IKT-Infrastruktur, Lernressourcen und Lernumgebungen sowie Informationssicherheit und Datenschutz (IBP). SIVON unterstützt Schulen dabei, eine sichere und zukunftsfähige digitale Bildung jetzt und in Zukunft zu realisieren und weiterzuentwickeln; Sie berät, unterstützt und fördert die Interessen der Schulen, damit diese sich auf ihre Hauptaufgabe konzentrieren können: die bestmögliche Bildung.

Inhaltsverzeichnis

1. Einführung

1.1 Allgemein

Im Jahr 2021 wurde eine Datenschutzuntersuchung zu Workspace for Education (im Jahr 2021 noch G Suite for Education genannt) durchgeführt. Die *Datenschutz-Folgenabschätzung* (DSFA) zeigte, dass mit der Nutzung von Google Workspace for Education hohe Datenschutzrisiken verbunden sind. Diese Software – zu der Programme wie Google Classroom, Google Docs und Google Meet gehören – wird auch in Schulen von [NAME BILDUNGSEINRICHTUNG] gebraucht.

SIVON und SURF, Genossenschaften von und für Bildungs- und Forschungseinrichtungen in den Niederlanden, haben als Reaktion auf die Untersuchung im Jahr 2021 Vereinbarungen mit Google getroffen,[1] um die identifizierten Datenschutzrisiken zu reduzieren. Google hat die Vereinbarung erfüllt und die erforderlichen Maßnahmen ergriffen und Änderungen an der Software vorgenommen. Diese wurden Mitte 2023 von SIVON und SURF sowie den von ihnen beauftragten externen Datenschutzexperten überprüft. Die Ergebnisse finden sich im „*Verification report Google remediation measures Workspace for Education*" von Privacy Company (vom 15. Juni 2023). Auf der Grundlage der Datenschutzfolgenabschätzung wurde im Schuljahr 2023/2024 ein *Data Transfer Impact Assessment* (DTIA) durchgeführt, und es wurden fünf neue Risiken für den Datenschutz ermittelt, die nach Rücksprache mit den zuständigen Stellen behoben wurden.

Außerdem wurde die Nutzung von ChromeOS und Chrome Browser auf von Bildungseinrichtungen verwalteten Chromebooks untersucht. Dies wird im Jahr 2023 besprochen[2] Mit Google wurden Vereinbarungen getroffen, um die festgestellten Datenschutzrisiken zu begrenzen.

Im Jahr 2024 schlossen SURF und SIVON die Konsultation mit Google ab und die von Google ergriffenen Maßnahmen wurden überprüft. Daraus sind vier (Abschluss-)Berichte entstanden:

1. Public version Updated Verification Report Workspace for Education – 17 May 2024
2. Public version DTIA Google Meet (Workspace for Education) – 11 April 2024
3. Public version New findings review Google Workspace for Education – 16 May 2024
4. Public version Verification Report Processor version Google Chrome for Education – 7 March 2024.

SIVON und SURF sind nach gründlichen Untersuchungen zu dem Schluss gekommen[3], dass Schulen Google Workspace for Education und ChromeOS und Chrome Browser auf verwalteten Chromebooks **weiterhin verwenden können**. Voraussetzung hierfür ist, dass die Schulen die von SURF und SIVON empfohlenen technischen und organisatorischen Maßnahmen befolgen. Darüber hinaus muss jede Bildungseinrichtung selbst die Ergebnisse der Untersuchungen von SURF- und SIVON in einer (lokalen) DSFA bestätigen und feststellen, dass keine zusätzlichen Risiken bestehen.

---

[1] https://sivon.nl/2021/07/akkoord-onderwijs-met-google-over-privacyrisicos/
[2] SIVON, SURF und Google einigen sich auf Nutzungsbedingungen für Google Chrome – SIVON (niederländisch)
[3] https://sivon.nl/2023/07/privacyrisicos-uit-DPIA-van-2021-google-workspace-for-education-voldoende-opgelost/

Dieser Bericht hilft Bildungseinrichtungen, die Ergebnisse der SURF- und SIVON-Untersuchungen in ihrer eigenen DSFA (von SIVON lokale DSFA genannt) zu bestätigen.

1.2 Obligatorische Umsetzung der DSFA

Um festzustellen, ob die Daten von Schülern und Mitarbeitern (personenbezogene Daten) in einer Anwendung, Software oder IT-Ressource sicher und verantwortungsvoll verwendet werden, verlangt die DSGVO die Durchführung einer Datenschutz-Folgenabschätzung (DSFA). In der DSGVO wird dies als Datenschutz-Folgenabschätzung (Data Protection Impact Assessment, DPIA) bezeichnet. Eine DSFA wird für einen Prozess, eine Anwendung oder eine Verarbeitung personenbezogener Daten durchgeführt. In der Regel handelt es sich um einen Antrag eines Anbieters(Auftragsverarbeiters). Die DSFA wird durchgeführt gemäß den Anforderungen von Art. 35 DSGVO.

Eine DSFA erfolgt durch einen für die Datenverarbeitung Verantwortlichen. Im Bildungswesen ist dies die Bildungseinrichtung (zuständige Behörde).[4]

Eine DSFA bewertet die Risiken und (möglichen) Folgen der Nutzung einer Verarbeitung für den Schutz der personenbezogenen Daten von Schülern, ihren Eltern und Mitarbeitern. Es wird festgestellt, ob die Verwendung personenbezogener Daten (Verarbeitung) ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen darstellt. Wenn die Datenschutzrisiken (zu) hoch sind, müssen Maßnahmen zur Begrenzung dieser Risiken gesucht werden. Diese werden als Abhilfemaßnahmen bezeichnet. Können die hohen Risiken nicht beseitigt werden, darf diese Verarbeitung (Anwendungsnutzung) nach der DSGVO nicht durchgeführt oder fortgeführt werden.

Das Ergebnis der DSFA ist unter anderem ein Bericht, der einen Überblick über klassifizierte Risiken für die Rechte und Freiheiten der betroffenen Personen enthält. Der Bericht listet auch die notwendigen Abhilfemaßnahmen auf. Der für die Verarbeitung Verantwortliche nimmt abschließend die DSFA an und bestimmt, welche Maßnahmen noch umgesetzt werden müssen und dass die Bildungseinrichtung die verbleibenden identifizierten Risiken akzeptiert.

Eine DSFA ist obligatorisch, wenn die Verarbeitung personenbezogener Daten – angesichts der Art, des Umfangs, des Kontexts und der Zwecke dieser Verarbeitung – voraussichtlich ein hohes Risiko für die „Rechte und Freiheiten“ (Privatsphäre) von Schülern und Mitarbeitern darstellt. Es ist auch möglich, dass die Durchführung einer DSFA nach den Vorschriften der Datenschutzaufsichtsbehörde, der niederländischen Datenschutzbehörde (AP), obligatorisch ist, die eine Liste der Verarbeitungsvorgänge veröffentlicht hat, welche die Durchführung einer DSFA erfordern.[4][5]

Für den Bildungsbereich bedeutet dies, dass eine DSFA zumindest für das Schülerbegleit[6]- und/oder -verwaltungssystem (LVS/LAS), das Personalverwaltungssystem und weit verbreitete Anwendungen mit digitalen Lernmaterialien immer obligatorisch ist.

Die Implementierung einer DSFA zu Google Workspace for Education und/oder ChromeOS und Chrome-Browsern ist obligatorisch, da die zentrale Untersuchung hohe Datenschutzrisiken gezeigt hat, die durch ergriffene Maßnahmen gemindert wurden.

---

[4] In Deutschland ist in den meisten Bundesländern die **Schulleitung** Verantwortlicher im Sinne der DSGVO

[5] In Deutschland regelt jedes Bundesland für sich, ob und für welche Verarbeitungsvorgänge eine DSFA erforderlich ist. Hinweise dazu können sich bei der zuständigen Aufsichtsbehörde oder dem Schulministerium finden.

[6] meint in den Niederlanden “ein System zur kontinuierlichen Beobachtung und Dokumentation der Lernentwicklung von Schülern”

1.3 Zentrale vs. lokale DSFA

Mit den Verhandlungen und Vereinbarungen mit Google und dem veröffentlichten Überprüfungsbericht wurden wichtige und positive Schritte unternommen, um Datenschutzrisiken bei der Nutzung von Google Workspace for Education durch den niederländischen Bildungssektor zu beseitigen. Doch die europäische Datenschutz Grundverordnung (DSGVO) schreibt vor, dass Organisationen, die (letztendlich) selbst für den Datenschutz verantwortlich sind, ihre eigenen Datenschutzuntersuchungen durchführen. Die niederländische Datenschutzaufsicht unterstützt diese Verpflichtung:

> *Schüler und Studierende haben ein verfassungsmäßiges Recht auf den Schutz ihrer personenbezogenen Daten und müssen vor Verletzungen dieses Grundrechts geschützt werden. Insbesondere Kinder haben Anspruch auf besonderen Schutz bei der Verarbeitung ihrer personenbezogenen Daten. Wenn sich nun einzelne Bildungseinrichtungen für die Nutzung eines bestimmten Produkts, Softwarepakets oder Cloud-Dienstes entscheiden, müssen diese Bildungseinrichtungen feststellen, dass diese Wahl die verfassungsmäßigen Rechte von Kindern nicht beeinträchtigt. Zu diesem Zweck müssen Bildungseinrichtungen in ihrer Eigenschaft als Verantwortlicher im Sinne der Datenschutz-Grundverordnung (DSGVO) selbst eine DSFA durchführen und eine dokumentierte Beurteilung vornehmen, ob die Nutzung von Google-Produkten sicher erfolgen kann.* [7]

Bildungseinrichtungen müssen daher selbst entscheiden, ob sie die Nutzung von Google Workspace for Education auf Basis der Datenschutz Untersuchungen von SURF und SIVON fortsetzen wollen und können (oder beginnen). Als Verantwortliche müssen Bildungseinrichtungen ihre Risikobewertung selbst vornehmen und festlegen. Die Ergebnisse der nationalen Untersuchung von SURF und SIVON können und dürfen genutzt werden. Diese DSFA wird als **zentrale DSFA** bezeichnet.

Darüber hinaus sollten Schulen prüfen, ob bei der Verwendung von Google Workspace for Education und ChromeOS auf verwalteten Chromebooks an ihren eigenen Schulen weitere Datenschutzrisiken berücksichtigt werden müssen. Diese Ergebnisse sind in Ihrer eigenen DSFA enthalten, die als **lokale DSFA** bezeichnet wird.

Die in der lokalen DSFA angewandte Methodik wird von der britischen Datenschutzbehörde ICO zur Klassifizierung von Risiken beschrieben[8]. Dazu gehört eine objektive Bewertung der Wahrscheinlichkeit und der Auswirkungen negativer Folgen (möglicher physischer, emotionaler oder materieller Schaden).

1.4 Implementierung der lokalen DSFA

An der lokalen DSFA der [NAME BILDUNGSEINRICHTUNG] sind folgende Mitarbeiter sind beteiligt:

---

7 https://autoriteitpersoonsgegevens.nl/uploads/imported/brief_ap_privacy_in_het_onderwijs_bij_google-producten.pdf

8 https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-DPIAs/how- do-we-do-a-DPIA/#how10

- Zum Beispiel [IT-Abteilung]
- [lid IBP-Team]
- [Datenschutzbeauftragter]
- [Sicherheitsbeamter]
- [Hauptbenutzer/Benutzer]
- [Vertretung der Beteiligten]

Die lokale DSFA wurde im Zeitraum [Zeitraum] durchgeführt.

[NAME BILDUNGSEINRICHTUNG] verwendet [Google Workspace for Education Fundamental/Standard/Plus] [und ChromeOS und Chrome Browser auf verwalteten Chromebooks] für [Schüler] und [Mitarbeiter].

Die folgenden Dokumente sind integraler Bestandteil dieser lokalen DSFA:

1. Public version Updated Verification Report Workspace for Education – 17 May 2024
2. Public version DTIA Google Meet (Workspace for Education) – 11 April 2024
3. Public version New findings review Google Workspace for Education – 16 May 2024
4. Public version Verification Report Processor version Google Chrome for Education – 7 March 2024
5. Technischer Leitfaden für Google Workspace for Education v3.0 *(deutsche Version)*
6. Leitfaden für ChromeOS und Chrome Browser 2024. *(deutsche Version)*

1.5 Leseanleitung und Benutzeranweisungen lokale DSFA

Die Bildungseinrichtung kann dieses Muster für eine lokale DSFA verwenden und selbst ausfüllen. In Abschnitt 1.4 trägt die Bildungseinrichtung die Informationen über die durchgeführte lokale DSFA ein.

In Kapitel 2 (Analyse der Datenverarbeitung) legt die Leitung der Bildungseinrichtung fest, für welche Zwecke die Produkte Google Workspace for Education und/oder ChromeOS verwendet werden.

In Kapitel 3 (Risikoanalyse) werden die auf nationaler Ebene festgestellten Datenschutzrisiken erörtert und bewertet. Etwaige zusätzliche Risiken und Maßnahmen können von der Bildungseinrichtung hinzugefügt werden.

In Kapitel 4 („Abschließende Schlussfolgerung“) wird festgestellt, ob die Risiken für den Schutz der Privatsphäre auf der Grundlage der lokalen DSFA ausreichend gemindert wurden, einschließlich der Abwägungen und der getroffenen und noch zu treffenden Maßnahmen.

In Kapitel 5 legt die Schulleitung die Ergebnisse der DSFA selbst in einer Erklärung fest.

Die Anlagen 1 und 2 enthalten eine Übersicht über die zu treffenden technischen Maßnahmen.

In diesem Modell sind die Teile, die von der Bildungseinrichtung auszufüllen sind, gelb unterlegt. Es wird von der Verwendung von Google Workspace for Education ausgegangen. Eine große Anzahl von Bildungseinrichtungen verwendet auch ChromeOS und den Chrome-Browser auf verwalteten Chromebooks. Für jeden Abschnitt sollten daher die gelb unterlegten Texte gewählt werden, um den Text anzupassen, falls die Bildungseinrichtung ChromeOS verwendet oder nicht.

2. Analyse der Datenverarbeitung

In diesem Abschnitt legt die Leitung der Bildungseinrichtung fest, wie Google Workspace for Education und/oder ChromeOS und Chrome Browser auf verwalteten Chromebooks innerhalb der eigenen Organisation verwendet werden. Die landesweite DSFA und DTIA konzentrieren sich auf den Einsatz von Google-Produkten im Bildungswesen als Office-Paket, zusätzlich zur bestehenden IT-Infrastruktur, IT-Ressourcen und eingesetzten Anwendungen wie dem Schüler- und Personalverwaltungssystem.

2.1 Die Beteiligten

Die zentrale DSFA sowie die lokale DSFA untersuchen die Folgen für die Rechte und Freiheiten der betroffenen Personen durch die Verarbeitung ihrer personenbezogenen Daten in Google Workspace for Education – nach Anwendung von Risikominderungsmaßnahmen. Bei den beteiligten Personen handelt es sich um Schüler und/oder Mitarbeiter der Bildungseinrichtung.

Bei Schülern der Primar- und Sekundarstufe gelten besondere Risiken für minderjährige Nutzer der Google Workspace for Education-Dienste. Im aktualisierten DSFA-Bericht 2021[9] findet sich hierzu eine Beschreibung (ab Seite 31). Nach der DSGVO sind Minderjährige in den Niederlanden Kinder unter 16 Jahren. Die niederländische Aufsichtsbehörde (AP) hat die personenbezogenen Daten dieser Minderjährigen als „sensible personenbezogene Daten“ eingestuft.[10] Von diesen Schülern kann nicht erwartet werden, dass sie eigenständig Datenschutzmaßnahmen ergreifen, und sie haben auch nicht die Möglichkeit, die Erlaubnis zur Nutzung von Schuleinrichtungen zu erteilen oder zu verweigern (dies liegt bei ihren gesetzlichen Vertretern/Eltern/Erziehungsberechtigten). Der AP verlangt, dass Bildungseinrichtungen das Risiko für minderjährige Schüler im DSFA ausdrücklich berücksichtigen.

Die Betroffenen sind [Schüler und/oder Mitarbeiter]. [Beschreibung der Nutzung durch die Betroffenen.]

Für Schüler betrifft dies die Altersgruppen:

	Altersspanne	Besondere Risiken
☐	6 – 9 Jahre	In dieser Altersgruppe lernen die Kinder lesen und schreiben und beginnen, Informations- und Kommunikationstechnologien zu nutzen. Jüngere Kinder (4-6 Jahre) können bereits mit dem Google-Ökosystem in Berührung kommen, wenn die Lehrkraft YouTube-Clips an der Tafel im Klassenzimmer zeigt. Sowohl zu Hause als auch in Bildungseinrichtungen sehen sich Kinder viele YouTube-Clips an, sogar schon in sehr jungem Alter. Die Nutzung konzentriert sich auf Klicks auf vertraute und angebotene Icons und Bilder, da nicht alle NutzerInnen in der Lage sind, richtig zu lesen und zu verstehen, worauf sie klicken.
☐	9 – 12 Jahre	Diese Altersgruppe wurde als eigene Kategorie definiert, weil Kinder in diesem Alter anfangen, selbst Smartphones zu benutzen. Sie

[9] https://sivon.nl/wp-content/uploads/2022/07/Update-DPIA-report-Google-Workspace-for-Education-2-augustus-2021.pdf

[10] Anders als in den Niederlanden werden die personenbezogenen Daten von Minderjährigen in Deutschland nicht pauschal als "sensible Daten" eingestuft.

		teilen ihr Leben und ihre Welt miteinander und mit der Außenwelt, ohne sich der Gefahren/Risiken bewusst zu sein. In diesem Alter loggen sich die Kinder ein und klicken los, meist ohne zu wissen, was sie da tun. Sie achten nicht auf die Art des Umfelds, in dem sie arbeiten (pädagogisch oder kommerziell).
☐	12-16 Jahre	Im Alter von 12 Jahren kommen die Kinder in weiterführende Schulen. Die Nutzung von Informationstechnologien ist normal. Sie haben in der Regel ihre eigenen Smartphones und verknüpfen ihre Schulkonten mit ihren privaten Konten. In diesem Alter lesen die Kinder in der Regel die Nutzungsbedingungen und Erklärungen zum Datenschutz nicht sorgfältig. Die Nutzung ist zielgerichtet: Sie klicken einfach auf jeder grünen Schaltfläche auf jeder Website auf Ja, ohne Rücksicht auf die Folgen der Standardeinstellungen. Gleichzeitig ist der Druck durch Gleichaltrige sehr groß, alle Arten von sozialen Medien mit stark datenschutzverletzenden Funktionen zu nutzen.

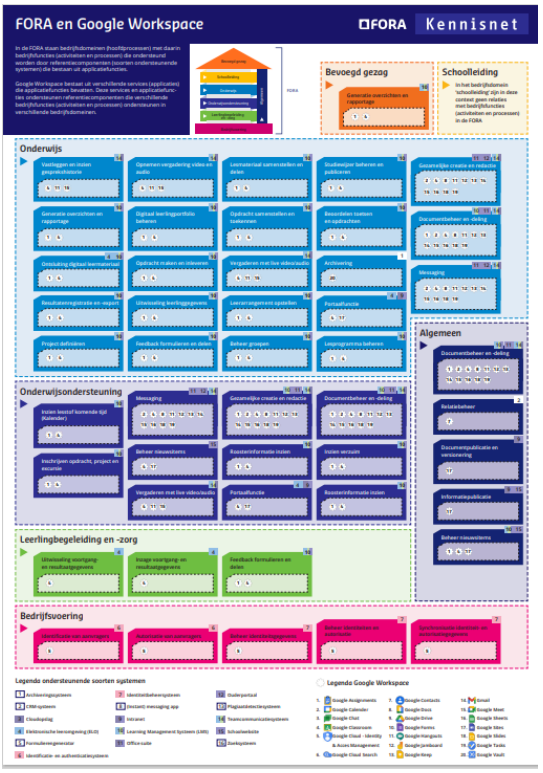
Erläuterung: Google hat in Google Workspace for Education eine spezielle K-12-Einstellung entwickelt, die für Schüler bis 18 Jahre gedacht ist. Indem sie sich als K-12 identifizieren, profitieren Schulen und Universitäten von den datenschutzfreundlichsten Einstellungen in Google Workspace for Education. Google hat bestätigt, dass es keine Altersüberprüfung (für die Einrichtung) durchführt: Universitäten und Berufsbildungseinrichtungen können und sollten auch die K-12-Einstellungen wählen, um von diesen datenschutzfreundlichen Einstellungen zu profitieren. Die Wahl der K-12-Einstellungen reicht jedoch nicht aus: Nur die kostenpflichtigen Versionen von Workspace for Education bieten den erforderlichen, zentral durchsetzbaren Datenschutz, der die besonderen Datenschutzrisiken für Minderjährige berücksichtigt.[11]

2.2 Prozesse und Nutzung von Google Workspace for Education

Grundlage für diese Analyse sind Prozessbeschreibungen, die auf den im FORA beschriebenen Geschäftsfunktionen basieren[12].

[11] Das ist auch zu empfehlen, wenn man den Schutzbedarf der Daten von Kindern und Jugendlichen unter 16 Jahren nicht als “besonders sensibel” einstuft.

[12] 8733_Figure_Applications_Google_Workspace-FORA_FASE_2_-_2022_01.pdf (wikixl.nl)



Google Workspace for Education wird verwendet für/als:

Archivierungssystem, CRM-System, Cloud-Speicher, Digitale Lernumgebung (ELO), Formulargenerator, Identifikations- und Authentifizierungssystem, Identitätsmanagementsystem, (Instant-) Messaging-App, Intranet, Learning Management System (LMS), Office-Suite, Elternportal, Plagiatserkennungssystem, Teamkommunikationssystem (einschließlich Videokonferenzen und Chat), Schulwebsite, Suchsystem

Die folgenden Teile von Google Workspace for Education werden verwendet:

1. Google Assignments
2. Google Calendar
3. Google Chat
4. Google Classroom
5. Google Cloud - Identity & Access Management
6. Google Cloud Search
7. Google Contacts
8. Google Docs
9. Google Drive
10. Google Forms
11. Google Hangouts
12. Google Jamboard
13. Google Keep
14. Gmail
15. Google Meet
16. Google Sheets
17. Google Sites
18. Google Slides
19. Google Tasks
20. Google Vault

2.3 Zwecke der Verarbeitung personenbezogener Daten

Die nachstehende Tabelle übernimmt die Tätigkeiten des Unternehmens aus der FORA. Die Tätigkeiten können auch als Zwecke betrachtet werden, wie sie in der DSGVO genannt werden. Bitte geben Sie für jede Tätigkeit/jeden Zweck an, ob sie in Ihrer Bildungseinrichtung anwendbar sind.

Haupttätigkeit	Tätigkeit/-zweck	Bitte kreuzen Sie an, ob dies auf die Bildungseinrichtung zutrifft
Zusammenarbeit und Kommunikation mit Mitarbeitern und extern	Dokumentenverwaltung und -freigabe	☐
	Mitteilung von Neuigkeiten und Updates	☐
	Gezielte Kommunikation	☐
	Verwaltung von Beziehungen und Außenbeziehungen	☐
	Verwaltung von Referenzinformationen (z. B. Standardlisten mit Codes für Abteilungen, Standorte, Kostenstellen usw.)	☐
Zusammenarbeit und Kommunikation mit den Eltern	Klassenweite Elternkommunikation	☐
	Elternkommunikation, schülerspezifisch	☐
Die Schüler arbeiten zusammen und kommunizieren	Information der Schüler über logistische Angelegenheiten	☐
	Anmeldung für Projekte und Exkursionen	☐
	Unterstützung der Zusammenarbeit bei Projekten von Schülerinnen und Schülern	☐
Bildungsunterstützung: Eintritt, Durchlauf, Austritt	Gruppen- und Klassenverwaltung	☐
Bildungsvorbereitung	Entwicklung der Ausbildung	☐
	Entwicklung von Material	☐
	Planung und Terminierung	☐
Pädagogische Umsetzung	Durchführung des Unterrichts	☐
	(Zugang zu) Bereitstellung von Lernmaterial	☐
	Testdurchführung	☐
Bildungsevaluation	Bewertung	☐

	Registrierung der Ergebnisse	☐
	Feedback-Rückmeldung	☐
Angemessene Bildung	Fortschritts- und Ergebnisanzeige	☐
IT-Unterstützung	Authentifizierung und Autorisierung	☐
	Identitäten verwalten	☐
	IT- Service-Verwaltung (Geräteverwaltung)	☐
Informationssicherheit und Datenschutz	Umsetzung von Sicherheitsmaßnahmen (Protokollierung und Überwachung)	☐
Umsetzung und Aufrechterhaltung der digitalen Zugänglichkeit	Sicherstellen, dass Anwendungen auf verschiedenen Gerätetypen leicht zugänglich sind.	☐
Weitere Geschäftsfunktionen/Zwecke, nämlich:		
	…	☐
	…	☐

Bei anderen als den oben beschriebenen Nutzungen können Datenschutzrisiken bestehen, die im Rahmen der nationalen DSFA und DTIA nicht untersucht wurden.

2.4 personenbezogene Daten

Um ein Konto in Google Workspace for Education und ChromeOS und Chromebrowser auf verwalteten Chromebooks einzurichten, wird nur ein begrenzter Satz von Daten der betroffenen Person (Schüler, Mitarbeiter) benötigt: Vorname, Nachname, Passwort und Schul-E-Mail-Adresse. Es ist hier nicht notwendig, den echten Vor- und Nachnamen der betroffenen Person zu verwenden. Es wird empfohlen, keinen Namen in die E-Mail-Adresse aufzunehmen.

Im Hinblick auf die Nutzung von ChromeOS und Chrome-Browser auf verwalteten Chromebooks wird das Geräte- und Identitätsmanagement innerhalb von Google Workspace for Education verwendet. Es sind keine zusätzlichen Daten erforderlich. Für die Verwaltung von Chromebooks ist jedoch eine spezielle Lizenz erforderlich (für die gesamte Lebensdauer des Geräts): Chrome Education Upgrade.

Wenn eine betroffene Person die Dienste von Google Workspace for Education nutzt, werden Nutzungsdaten (Metadaten) generiert. Durch die Nutzung der von SIVON und SURF mit Google ausgehandelten Verträge[13] und die Anwendung der im *Handbuch für technische Maßnahmen (v3.0 – 2024)* wurde die Erhebung und Verarbeitung dieser Nutzungsdaten auf das erforderliche Minimum beschränkt.

[13] Diese sollten den Stand Oktober 2024 allgemein verfügbaren Verträgen entsprechen.

Wenn Ihre Bildungseinrichtung andere personenbezogene Daten innerhalb von Google Workspace for Education verarbeitet (z. B. in Google Docs, Spreadsheet oder Gmail erfasste personenbezogene Daten), geben Sie dies bitte unten an. Im Zusammenhang mit dem Gebot der Datenminimierung begründen Sie, warum diese personenbezogenen Daten verarbeitet werden.

Geben Sie unten nach Art der betroffenen Person an, welche personenbezogenen Daten von Ihrer Bildungseinrichtung in Google Workspace verarbeitet werden.

Persönliche Daten in Google Workspace for Education		
Betroffene Person(en) (Schüler, Mitarbeiter, Eltern, andere Beteiligte)	**Verarbeitete personenbezogene Daten**	**Motivation**
Schüler, Mitarbeiter	(Fiktiver) Vorname	Diese Informationen werden benötigt, um ein Konto in Google Workspace for Education zu erstellen
	(Fiktiver) Nachname	
	Passwort	
	E-Mail-Adresse (Schule)	
Schüler, Mitarbeiter	Diagnosedaten wie Protokoll- und Überwachungsdaten, Metadaten	*Siehe nationale DSFA- und DTIA-Berichte Google Workspace for Education und Verification Report ChromeOS*
	IP-Adresse	
	Benutzer personenbezogener Daten (*Kundendaten*) in Dateien	
…	Weitere personenbezogene Daten, nämlich: … … …	…

2.5 Beurteilung der Rechtmäßigkeit

Bitte geben Sie unten für jede auf Sie zutreffende Haupttätigkeit an::

- was die Rechtsgrundlage für die Verarbeitung in diesem Prozess ist.
- ob das Gebot der Datenminimierung erfüllt ist (es werden nicht mehr personenbezogene Daten verarbeitet als nötig). Berücksichtigen Sie auch die spezifischen Risiken und Maßnahmen bei der Verarbeitung personenbezogener Daten von Kindern unter 16 Jahren in Google Workspace for Education.
- ob das Transparenzgebot erfüllt ist. Sind die betroffenen Personen ausreichend über die Verarbeitung ihrer personenbezogenen Daten und die ihnen zustehenden Rechte informiert?

*Wenn Sie Google Workspace for Education **nicht** für eine oder mehrere der genannten Haupttätigkeiten verwenden (siehe Tabelle in Abschnitt 2.2), dann löschen Sie die entsprechende(n) Tabelle(n) unten.*

Haupttätigkeit	Beurteilung der Rechtmäßigkeit	
Mitarbeiter arbeiten zusammen und kommunizieren	Rechtsgrundlage	Ausführung einer Vereinbarung (z.B. eines Arbeitsvertrags/ § Schulgesetz)
	Datenminimierung	Ja/Nein Erläuterung:
	Transparenz	Ja/Nein Die Beteiligten wurden wie folgt informiert:

Haupttätigkeit	Beurteilung der Rechtmäßigkeit	
Zusammenarbeit und Kommunikation nach außen	Rechtsgrundlage	• Ausführung eines Vertrags (z. B. Kauf- oder Abtretungsvertrag) • Wahrnehmung öffentlicher Aufgaben (Kommunikation mit Behörden) • Berechtigtes Interesse (weitere externe Kontakte)
	Datenminimierung	Ja/Nein Erläuterung:
	Transparenz	Ja/Nein Die Beteiligten wurden wie folgt informiert:

Haupttätigkeit	Beurteilung der Rechtmäßigkeit	
Zusammenarbeit und Kommunikation mit den Eltern	Rechtsgrundlage	Wahrnehmung öffentlicher Aufgaben (u.a. § 11 WPO, § 23b WVO, § 20 WEV, Schulpflichtgesetz)
	Datenminimierung	Ja/Nein Erläuterung:
	Transparenz	Ja/Nein Die Beteiligten wurden wie folgt informiert:

Haupttätigkeit	Beurteilung der Rechtmäßigkeit	
Zusammenarbeit und Kommunikation zwischen Schülern	Rechtsgrundlage	Wahrnehmung einer öffentlichen Aufgabe (Art. 8 WPO, Art. 2 WVO, Art. 9 WEC)
	Datenminimierung	Ja/Nein Erläuterung:

	Transparenz	Ja/Nein Die Beteiligten wurden wie folgt informiert:

Haupttätigkeit	Beurteilung der Rechtmäßigkeit	
Bildungsunterstützung: Eintritt, Durchlauf, Austritt	Rechtsgrundlage	Gesetzliche Verpflichtung (Artikel 40b WPO, Artikel 27b WVO, Artikel 42a WEC)
	Datenminimierung	Ja/Nein Erläuterung:
	Transparenz	Ja/Nein Die Beteiligten wurden wie folgt informiert:

Haupttätigkeit	Beurteilung der Rechtmäßigkeit	
Vorbereitung auf den Unterricht	Rechtsgrundlage	Wahrnehmung einer öffentlichen Aufgabe (Art. 8 WPO, Art. 2 WVO, Art. 9 WEC)
	Datenminimierung	Ja/Nein Erläuterung:
	Transparenz	Ja/Nein Die Beteiligten wurden wie folgt informiert:

Haupttätigkeit	Beurteilung der Rechtmäßigkeit	
Angemessene Bildung	Rechtsgrundlage	Wahrnehmung einer öffentlichen Aufgabe (Art. 8 und 18a WPO, Art. 2 und 17a WVO, Art. 9 und 28a WPO)
	Datenminimierung	Ja/Nein Erläuterung:
	Transparenz	Ja/Nein Die Beteiligten wurden wie folgt informiert:

Haupttätigkeit	Beurteilung der Rechtmäßigkeit	
IT-Support	Rechtsgrundlage	Berechtigtes Interesse, nämlich Sicherheit und Kontinuität des Geschäftsbetriebs der Bildungseinrichtung
	Datenminimierung	Ja/Nein

		Erläuterung:
	Transparenz	Ja/Nein Die Beteiligten wurden wie folgt informiert:

Haupttätigkeit	**Beurteilung der Rechtmäßigkeit**	
Informationssicherheit und Datenschutz	Rechtsgrundlage	Berechtigtes Interesse, nämlich Sicherheit und Kontinuität des Geschäftsbetriebs der Bildungseinrichtung
	Datenminimierung	Ja/Nein Erläuterung:
	Transparenz	Ja/Nein Die Beteiligten wurden wie folgt informiert:

Haupttätigkeit	**Beurteilung der Rechtmäßigkeit**	
Umsetzung und Bewahrung der digitalen Barrierefreiheit	Rechtsgrundlage	Berechtigtes Interesse, nämlich Sicherheit und Kontinuität des Geschäftsbetriebs der Bildungseinrichtung
	Datenminimierung	Ja/Nein Erläuterung:
	Transparenz	Ja/Nein Die Beteiligten wurden wie folgt informiert:

Haupttätigkeit **von Prozessen**	**Beurteilung der Rechtmäßigkeit**	
Anderer Zweck, nämlich:** **<Beschreibung des Verarbeitungszwecks>**	Rechtsgrundlage	<Grundlage, Gesetz, Verordnung>
	Datenminimierung	Ja/Nein Erläuterung: …
	Transparenz	Ja/Nein Die Beteiligten wurden wie folgt informiert: …

** Wenn Ihre Bildungseinrichtung Google Workspace for Education für mehrere „andere“ Zwecke nutzt, kopieren Sie diese Tabelle und geben Sie Ihre anderen, eigenen Zwecke ein.

3. Risikoanalyse

Um eine Risikoanalyse durchzuführen, nehmen Sie die für Google zentral ermittelten Risiken und Maßnahmen zur Kenntnis. Anschließend führen Sie eine Bestandsaufnahme der Umsetzung der zentral festgelegten Abhilfemaßnahmen, die von Bildungseinrichtungen ergriffen werden müssen, durch. Analysieren Sie gegebenenfalls Ihre einrichtungsspezifischen Risiken und etwaige Abhilfemaßnahmen (die in der DSFA und der DTIA nicht berücksichtigt werden). Anschließend stellen Sie fest, ob die identifizierten Datenschutzrisiken durch die getroffenen Maßnahmen hinreichend begrenzt, d.h. gemindert werden.

3.1 Nationale Risiken und Abhilfemaßnahmen

3.1.1 Google Workspace for Education

Die DSFA 2021 identifizierte hohe Datenschutzrisiken. Diese wurden nach Absprachen zwischen SIVON und SURF mit Google reduziert, indem Google technische Maßnahmen ergriffen hat und die Bildungseinrichtungen organisatorische und technische Maßnahmen ergreifen.

Die Risiken und Maßnahmen sind im Bericht „Public version Updated Verification Report Workspace for Education – 17. Mai 2024“ beschrieben. Die Bildungseinrichtung hat den Inhalt dieses Berichts zur Kenntnis genommen. Der „Technische Leitfaden für Google Workspace for Education v3.0“ beschreibt, ob und wie die identifizierten Risiken gemindert werden können.

Tabelle 1: Anfängliche hohe Risiken, die im DSFA-Update identifiziert wurden, von Google vereinbarte Maßnahmen und Überprüfungsergebnisse

Nein.	Risiko	Vereinbarte Schadensbegrenzungsmaßnahme Google	Sachlicher Maßstab
1, 2	**Fehlende Zweckbindung Kunden- und Servicedaten**	Google verarbeitet personenbezogene Kundendaten und Diagnosedaten (einschließlich Kontodaten) ausschließlich als Auftragsverarbeiter, und zwar für drei Zwecke, wenn dies erforderlich ist: *1. Bereitstellung, Wartung und Verbesserung der Dienste und technischen Supportleistungen (TSS), die der Kunde abonniert hat;* *2. Sicherheitsbedrohungen, Risiken, Fehler und andere Anomalien identifizieren, berbeiten und beheben* 3. *Entwicklung, Bereitstellung und Installation von Updates für die Dienste, die der Kunde abonniert hat (einschließlich neuer Funktionen im Zusammenhang mit den Diensten, die der Kunde abonniert hat).*	Risikobegrenzung durch vertragliche Maßnahmen im Privacy Amendment.
		Google verarbeitet keine personenbezogenen Kundendaten und/oder Servicedaten für Werbezwecke oder für Profilerstellung, Datenanalyse und Marktforschung.	Risikobegrenzung durch vertragliche Maßnahmen im Privacy Amendment.
		7 identifizierte Zwecke, für die Google als unabhängiger Verantwortlicher für die Datenverarbeitung Diagnosedaten weiterverarbeiten darf.	* **Bemerkung**: Google schreibt in der GCPN-Nachtrag, dass es Servicedaten verwenden kann, um Empfehlungen für verwandte Produkte zu geben (d. h.

		1. Abrechnungs- und Kontoverwaltung sowie Verwaltung der Kundenbeziehungen und des damit verbundenen Schriftverkehrs mit Kunden und Kunden-Administratoren; 2. Verbesserung und Optimierung der Leistung und Kernfunktionalität der Zugänglichkeit, des Datenschutzes, der Sicherheit und der Effizienz der IT-Infrastruktur der Cloud-Dienste und des TSS[14]; 3. interne Berichterstattung, Finanzberichterstattung, Umsatzplanung, Kapazitätsplanung und Prognose-Modellierung (einschließlich Produktstrategie); 4. Erkennung, Verhinderung und Schutz vor Missbrauch (z. B. automatisches Scannen nach Übereinstimmungen mit CSAM-Kennungen, Scannen nach Viren und Scannen zur Erkennung von Verstößen gegen die AUP[15]); 5. die Verarbeitung personenbezogener Daten in Support-Tickets und Support-Anfragen (einschließlich der Korrespondenz mit Kunden und Kunden-Administratoren sowie aller Anhänge), die von Administratoren an Google gesendet werden; 6. Feedback erhalten und nutzen; und 7. Einhaltung gesetzlicher Verpflichtungen. Zur Verdeutlichung: **Die Bearbeitung von TSS-Daten ist eine Verarbeitungstätigkeit.**. Google wird sicherstellen, **dass andere Zwecke in den Google Cloud-Datenschutzhinweisen nicht für die Nutzung von Workspace durch niederländische Schulen und Universitäten[16] gelten**. Was das Scannen von Inhalten auf Material über sexuellen Kindesmissbrauch (CSAM) und die Meldung von „Treffern“ an die NCMEC betrifft, so wird Google die geltenden rechtlichen Richtlinien des EDPB einhalten.	Produkte, die der Kunde nicht abonniert hat), was nach dem Privacy Amendment nicht zulässig ist. Geringes Risiko, da die Bedingungen in dem Privacy Amendment Vorrang vor den Informationen von Google haben.
		Google versichert, dass maschinelles Lernen zur inhaltlichen Verbesserung der von der Rechtschreib- und Grammatikprüfung gesammelten Daten auf die eigene Domain des Kunden beschränkt ist.	Google schreibt in seinem Datenschutz-Umsetzungs-Leitfaden für Workspace for Education: „*Es ist wichtig zu betonen, dass Ihre Kundendaten nicht verwendet werden, um die Rechtschreib- und*

[14] steht für Technical Support Services; https://cloud.google.com/terms/tssg
[15] steht für Acceptable Use Policy; https://cloud.google.com/terms/aup?hl=de
[16] Sollte so auch für Schulen in D gelten

			Grammatikdienste für die Konten anderer Kunden zu verbessern.“
		Aufnahme der Definition der Anonymisierung im Privacy Amendment gemäß den WP29-Richtlinien für Anonymisierungstechniken[17].	Risikobegrenzung durch vertragliche Maßnahmen im Privacy Amendment.
		Der Rahmenvertrag legt fest, wie Google mit Geheimhaltungsverfügungen (Gag Orders) umgeht, wenn es aufgefordert wird, Inhalts- und Diagnosedaten an Strafverfolgungsbehörden weiterzugeben.	Im Privacy Amendment und Informationen im öffentlichen Whitepaper.
		Google setzt die Standardeinstellung für die Anzeigenpersonalisierung bei neuen Endnutzern auf Aus (relevant für die Nutzung von Zusätzlichen Diensten).	Korrigieren Sie die Standardeinstellung in Workspace for Education für neue Benutzer.
3, 4, 7[18]	**Mangelnde Transparenz bezüglich Kunden- und Service Daten**	Google wird ein Inspektionstool entwickeln, das Administratoren den Zugang zu Telemetriedaten ermöglicht, einschließlich der Nutzung von Funktionen	Google hat ein Diagnostic Information Tool (DIT) entwickelt, das Telemetrieereignisse (die auch Inhaltsdaten enthalten können) anzeigt. Der Zugriffszeitraum umfasst aufgrund der langen Wiederherstellungszeit nur die letzten 24 Stunden. Darüber hinaus können niederländische Administratoren ältere Telemetriedaten anfordern, wenn eine betroffene Person Zugang beantragt.
		Google wird einen Hilfeartikel veröffentlichen, in dem die Kategorien und Zwecke der Verarbeitung von Diagnosedaten (einschließlich der von Cloud-Servern gesammelten Daten und Android-Telemetrieereignisse (Atome)) detailliert beschrieben werden.	Google hat einen Neue Erklärungsseite über das DIT und den Inhalt der Telemetriedaten veröffentlicht. Auf dieser Seite finden Sie eine allgemeine Beschreibung der Aufbewahrungsfristen. "*Wir bewahren die meisten Arten von Servicedaten für einen festen Zeitraum von bis zu 180 Tagen auf.* (..) *In der Praxis werden Diagnosedaten für kürzere Zeiträume von 30 bis 63 Tagen aufbewahrt.* Google verweist zudem auf seine Google Cloud-Datenschutzerklärung. Dies beschreibt die drei Kriterien, die Google verwendet, um Dienstdaten für längere Zeiträume aufzubewahren. Diese sind: 1. *Sicherheit, Verhinderung von Betrug und Missbrauch,* 2. *Einhaltung gesetzlicher oder behördlicher Vorschriften und*

[17] Gemeint sind die Leitlinien der Artikel-29-Datenschutzgruppe; siehe https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_de.pdf

[18] Die Risiken waren: Mangelnde Transparenz von Kundendaten, Mangelnde Transparenz von Diagnosedaten, Mangelnde Kontrolle Dritter/Verarbeiter.

			3. *Einhaltung von steuerlichen, buchhalterischen oder finanziellen Vorschriften*
		Google hat bestätigt, dass alle Unterauftragsverarbeiter, die Diagnosedaten verarbeiten, auch Kundendaten verarbeiten und daher bereits in der Liste der Unterauftragsverarbeiter für Kundendaten aufgeführt sind. Google wird Einzelheiten zu seinen Unterauftragsverarbeitern, insbesondere für Diagnosedaten, bereitstellen. Google wird Folgendes angeben o vollständiger Name des Unternehmens, o relevante(r) Dienst(e), o Ort(e), an dem die Daten verarbeitet werden, o Tätigkeit (d. h. was macht der Unterauftragsverarbeiter, o ob der Unterauftragsverarbeiter Dienstdaten in temporären, persönlichen und/oder archivierten Protokollen verarbeitet.	Google hat die Informationen über seine Unterauftragsverarbeiter und verbundenen Unternehmen erweitert, welche personenbezogenen Daten sie zu welchen Zwecken einsehen können. Die Liste der Unterauftragsverarbeiter umfasst Unternehmen und verbundene Unternehmen in zwei Drittstaatenlisten. Google hat SURF und SIVON die vereinbarten zusätzlichen Informationen über die Unterauftragsverarbeiter zur Verfügung gestellt und mit der DTIA zusammengearbeitet, um die Risiken der Übermittlung in Drittländer zu bewerten. Die DTIA kommt zu dem Schluss, dass keine hohen Übertragungsrisiken für personenbezogene Daten über Meet bestehen, vorausgesetzt, dass Schulen (**i**) eine kostenpflichtige Version von Workspace verwenden und (**ii**) sich dafür entscheiden, Inhaltsdaten in der EU zu speichern. Wenn sie besondere Kategorien von Daten über Meet austauschen möchten, müssen sie (**iii**) eine clientseitige Verschlüsselung anwenden, um das Risiko eines unbefugten Zugriffs auf diese Daten in Drittländern auszuschließen.
		Google zeigt das Profilbild eines Endnutzers[19] auf der Landing Page für alle Workspace Core Services (sowohl Web als auch Mobilgeräte). Dieses Bild verschwindet, wenn der Endnutzer die datenschutzgeschützten Workspace-Dienste verlässt. Google verpflichtet sich, reguläre Workspace-Konten automatisch abzumelden, wenn sie deaktivierte *Zusätzliche Dienste* besuchen, und eine Warnung für K-12-Nutzer anzuzeigen.	Google hat die vereinbarten Maßnahmen umgesetzt. Wann *Zusätzliche Dienste* in einer K-12-Umgebung deaktiviert sind, zeigt Google den Endnutzern eine Warnung an, wenn sie versuchen, auf diese deaktivierten Dienste zuzugreifen.
		Google wird alle relevanten rechtlichen Informationen über das Google Workspace-Konto in einem Hinweis für Endnutzer dauerhaft zur Verfügung stellen.	Das Pop-up wurde verbessert und personalisiert. Relevante rechtliche Informationen sind nicht ständig über das Login- oder Google-Kontomenü verfügbar. Google hat sich verpflichtet, bis zum **[Datum**

[19] Gemeint ist das kleine kreisrunde Bild mit Initialen oder Avatar oben rechts

			vertraulich][20] bestimmte Änderungen an der Benutzeroberfläche vorzunehmen.
		Google wird eine domänenweite Takeout-Funktion auf der Ebene der einzelnen Nutzer/Organisationseinheiten entwickeln.	Google hat Informationen zum organisatorischen Datenexport veröffentlicht unter https://support.google.com/a/answer/12940323 und https://support.google.com/a/answer/100458 Die Daten müssen in die Google Cloud Platform (GCP) exportiert werden. Google hat sichergestellt, dass der Administrator die („Verarbeiter"-) Bedingungen aus dem Cloud Data Processing Addendum akzeptieren muss. Für diesen Anwendungsfall ist GCP kein Workspace-*Zusätzlicher Dienst*.
		Google gibt eine neue Warnung an Endnutzer im Feedback-Formular aus, keine sensiblen Daten an Google weiterzugeben	Google zeigt ein Popup mit einer Warnung an.
		Google wird die Erklärung für Administratoren im Datenschutz-Implementierungsleitfaden verbessern, dass Google Kontodaten als Auftragsverarbeiter verarbeitet, wenn das Google-Konto in den Wichtigen Diensten (*Core Services*) verwendet wird.	Google bietet eine Erklärung.
		Google wird die Verfügbarkeit von Administrator-Audit-Protokollen auf alle Kerndienste ausweiten.	Google stellt viele weitere Audit-Protokolle zur Verfügung, die mit dem Abhilfeplan übereinstimmen - soweit getestet.
5, 6	**Keine Rechtsgrundlage für Google und Schulen/ Universitäten + Fehlende Datenschutzkontrollen**	In Bezug auf die (gesonderte) Rechtsgrundlage für das Auslesen von Cookie- und Telemetriedaten von Endnutzergeräten, wie sie in der ePrivacy-Richtlinie definiert ist, wird Google die regulatorischen Vorgaben befolgen.	Google erklärt die Notwendigkeit, Inhaltsdaten in Rechtschreib- und Grammatik-Telemetrieereignisse einzubeziehen, in einem separaten Thema auf der Seite neue DIT-Informationsseite, unter *Rechtschreib- und Grammatikvorschläge*. Es ist wahrscheinlich, dass diese Datenerhebung gemäß der niederländischen Ausnahmeregelung für die analytische Einwilligung von der Einwilligung ausgenommen ist.[21]
		Google erklärt sich vertraglich damit einverstanden, dass die Zustimmung des Endnutzers nicht als Grund für die Weitergabe von Dienstedaten an Dritte gilt, wenn die Dienste dieser Parteien vom	Im Datenschutzzusatz (*Privacy-Amendement*) enthalten.

[20] Inwieweit diese Zusage Googles bereits in der Breite umgesetzt ist, müsste man austesten.

[21] Was es genau mit dieser niederländischen Ausnahmegenehmigung auf sich hat, müsste in der DPIA von privacy company nachzulesen sein - ob diese Ausnahme auf D übertragbar ist, wäre zu klären.

		Kunden deaktiviert werden (einschließlich Google als Dritter für zusätzliche Dienste).	
		Google meldet Workspace-Endnutzer automatisch ab, wenn sie auf (**aktivierte**) Zusätzliche Dienste zugreifen.	Administratoren können den Zugriff auf alle *Zusätzlichen Dienste* deaktivieren.
		Google fungiert als Datenverarbeiter für die Diagnosedaten und die Bereitstellung von Support, nicht jedoch für die Feedback-Daten. Den Schulen wird empfohlen, ihre Mitarbeiter davor zu warnen, Feedback zu verwenden.	Google ist ein Datenverarbeiter für die Bereitstellung von TSS gemäß der Datenschutzänderung, kann aber auch Supportdaten als Datenverantwortlicher *weiterverarbeiten*. Sowohl die Verarbeitung von Feedback-Daten als auch die Weiterverarbeitung von Support-Daten sind vereinbarte legitime Geschäftszwecke.
		Administratoren können die Verwendung von *Zusätzlichen Diensten* verbieten, wenn sie mit einem Workspace Enterprise-Konto angemeldet sind.	Admins können den Zugriff auf alle *Zusätzlichen Dienste* deaktivieren.
8	**Kein Zugriff für die Beteiligten**	Google wird ein individuelles TakeOut-Tool entwickeln	Google bietet 3 verschiedene Tools für Administratoren und Endnutzer an, um persönliche Daten zu exportieren (Data Export, Google Vault und Google Takeout). Diese Tools konzentrieren sich auf Inhaltsdaten, mit einigen Aktivitätsprotokollen (*Daten, die den Benutzern gehören*). Diese Self-Service-Tools bieten nicht Zugriff auf alle Dienstdaten, aber Administratoren können Diagnose- und Telemetriedaten exportieren und Endnutzer können das DSAR-Formular[22] von Google verwenden, um Zugang zu personenbezogenen Daten zu beantragen, die Google als für die Datenverarbeitung Verantwortlicher verarbeitet.
		Google bietet keinen individualisierten Zugang zu Diagnosedaten, Telemetriedaten und Webserver-Zugriffsprotokollen/ Cookie-Daten (Google nennt diese Daten Dienstdaten). Administratoren können einige Diagnosedaten sammeln, indem sie erweiterte Audit-Protokolle exportieren und individuelle Nutzerdaten anfordern. Das DIT erlaubt nur den Zugriff auf die letzten 24 Stunden.	Administratoren müssen BigQuery verwenden, um Audit- Logs zu exportieren. Google hat sichergestellt, dass der Administrator die („Verarbeiter“-) Bedingungen des Google Cloud Processing (GCP) Addendum akzeptieren muss. Für diesen Anwendungsfall ist GCP kein Workspace *Zusätzlicher Dienst*. Google ermöglicht es Superadministratoren auch, den Zugriff auf historische Telemetriedaten zu beantragen.

[22] DSAR = data subject access request = Antrag auf Auskunft gem. Art. 15 DSGVO

		Google wird Einzelheiten darüber veröffentlichen, warum es generell keinen Zugriff auf Telemetriedaten, Website-Daten und personenbezogene Daten aus den SIEM-Sicherheitsprotokollen von Google gewähren kann. Google hat bestätigt, dass es jede Anfrage gemäß Artikel 15 DSGVO prüfen wird (d. h. keine standardmäßige Ablehnung).	Neue Erklärung veröffentlicht unter *Informationen, die nicht als Antwort auf eine Zugriffsanfrage bereitgestellt werden*.
		Das Design des DSAR-Formulars von Google ist nicht benutzerfreundlich: Nutzer wissen nicht, welche Kategorien von Daten Google verarbeitet.	Schulen und Universitäten können die Erläuterungen in diesem Bericht nutzen, um Mitarbeitern und Schülern dabei zu helfen, Zugriff auf alle ihre persönlichen Daten anzufordern, und zwar über Self-Service-Tools, über ihre Verwaltung und über Das Auskunftsantragsformular von Google.
9	**Übermittlung personenbezogener Daten in die USA + mangelnde Kontrolle über Unterauftragsverarbeiter**		Die Risiken der Übermittlung der sechs Kategorien personenbezogener Daten werden im separaten DTIA bewertet. Die DTIA kommt zu dem Schluss, dass bei der Übermittlung personenbezogener Daten über Meet keine größeren Risiken bestehen, wenn **(i)** Schulen eine kostenpflichtige Version von Workspace verwenden und **(ii)** sich dafür entscheiden, Inhaltsdaten in der EU zu speichern. Wenn sie besondere Kategorien von Daten über Meet austauschen möchten, müssen sie **(iii)** eine Client-Seitige Verschlüsselung (CSE) anwenden, um das Risiko eines unbefugten Zugriffs auf diese Daten in 7 Drittländern auszuschließen.

3.1.2 Folgenabschätzung für die Datenübertragung (DTIA)

Die im Jahr 2021 durchgeführte DSFA stellte fest, dass personenbezogene Daten mit den Vereinigten Staaten ausgetauscht werden. Hierzu wurde ein sogenanntes Data Transfer Impact Assessment (DTIA) durchgeführt. Dabei werden die Datenschutzrisiken einer Datenübermittlung in Länder außerhalb des Europäischen Wirtschaftsraums (EWR) untersucht. Das DTIA – einschließlich der Umsetzung daraus resultierender Maßnahmen – wird im Jahr 2024 abgeschlossen sein. Die DTIA ist im Bericht „Öffentliche Version DTIA Google Meet (Workspace for Education) – 11. April 2024“ enthalten. Der „Technische Leitfaden für Google Workspace for Education v3.0“ beschreibt, ob und wie die im DTIA identifizierten Risiken begrenzt werden können.

Öffentliche Version DTIA Google Meet (Workspace for Education) – 11. April 2024:

Inhaltsdaten (content data)

In Anbetracht der oben genannten und der geltenden Datenschutzgesetze ist die Übertragung sensibler und besonderer Kategorien von Daten (besondere personenbezogene Daten) ohne clientseitige Verschlüsselung:	nicht erlaubt

Im Hinblick auf das Vorstehende und das geltende Datenschutzrecht ist die Übermittlung gewöhnlicher personenbezogener Daten: erlaubt

Kontodaten (account data)

Im Sinne der obigen Ausführungen und der geltenden Datenschutzvorschriften ist die Übermittlung: erlaubt

Supportdaten (support data)

Im Sinne der der obigen Ausführungen und der geltenden Datenschutzvorschriften ist die Übermittlung: erlaubt

Diagnosedaten (diagnostic data)

Im Sinne der der obigen Ausführungen und der geltenden Datenschutzvorschriften ist die Übermittlung: erlaubt

Sicherheitsdaten, AGB (security data, T&S)

Im Sinne der der obigen Ausführungen und der geltenden Datenschutzvorschriften ist die Übermittlung: erlaubt

Website-Daten (website data)

Im Sinne der der obigen Ausführungen und der geltenden Datenschutzvorschriften ist die Übermittlung: erlaubt

3.1.3 Neue Erkenntnisse Google Workspace for Education

Im Rahmen der Umsetzung der DSFA und der Überwachung der von Google ergriffenen Maßnahmen traten im Jahr 2023 fünf neue Datenschutzrisiken auf. SIVON und SURF haben sich diesbezüglich auch mit Google beraten, um diese neuen Risiken zu begrenzen. Die Risiken und die ergriffenen Maßnahmen werden im Bericht „Public version New findings review Google Workspace for Education – 16. Mai 2024“ beschrieben. Der „Technische Leitfaden für Google Workspace for Education v3.0“ beschreibt, ob und wie die identifizierten Risiken gemindert werden können.

Tabelle 1: (potenziell) hohe Risiken, Erkenntnisse, Google-Maßnahmen und empfohlene Maßnahmen für Schulen/Universitäten

Ursprüngliche(s) Risiko(s)	Erkenntnisse	Von Google ergriffene Maßnahme	Empfohlene Maßnahme für Schulen und Universitäten
Fehlende Zweckbindung	Google kann Endnutzern in den Wichtigen Diensten (Core	Google hat bestätigt, dass K-12-Nutzern keine	Schulen und Universitäten müssen in ihrem Tenant die K-12-Einstellung

Kundendaten und Diagnosedaten	Services) Umfragen anzeigen.	Umfragen angezeigt werden.	wählen, auch wenn ihre Benutzer 18+ sind. Google hat bestätigt, dass das tatsächliche Alter von Nutzern im Bildungsbereich nicht überprüft wird.
Fehlende Zweckbindung Kundendaten **Keine Rechtsgrundlage für Google und Schulen/Universitäten** **Standardmäßig kein Datenschutz**	Einführung von *intelligenten Funktionen* wie Smart Compose, die maschinelles Lernen nutzen. Die Rolle von Google ist unklar/nicht dokumentiert. Nutzer werden dazu gedrängt, Dienste zu aktivieren.	*Intelligente Funktionen* sind für Domains in Europa standardmäßig deaktiviert, aber die Nutzer können sie dennoch aktivieren. Google hat sich bereit erklärt, alle Inhalts- und Diagnosedaten von Smart Features im Rahmen der Rolle des Auftragsverarbeiters zu verarbeiten (abgesehen von begrenzten vereinbarten legitimen Geschäftszwecken), und die Ergebnisse verbleiben in der Domäne des Kunden.	
Keine Rechtsgrundlage für Google und Schulen/Universitäten **Fehlende Datenschutzkontrollen**	Verwendung des multifunktionalen NID-Cookies bei der Anmeldung bei einem Workspace-Konto und beim Aufrufen der Google Cloud Privacy Notice.	Google hat SURF und SIVON darüber informiert, dass das in der Workspace-Umgebung oder beim Nachschlagen der Google Cloud Privacy Notice (GCPN)[23] gesetzte NID-Cookie nicht für Werbezwecke verwendet wird.Bei der Abmeldung müssen die Nutzer der Verwendung des NID-Cookies und anderer nicht wesentlicher Cookies für Werbung auf Google-Websites und auf Websites Dritter mit	-

[23] Google Cloud Datenschutzerklärung

		Google-Werbung zustimmen. Google hat den Text des Cookie-Banners auf der GCPN-Seite verbessert, um darauf hinzuweisen, dass die GCPN-Seite keine Cookies für Werbung verwendet.	
Mangelnde Transparenz	Google erfasst Inhaltsdaten von Rechtschreibprüfungen in Telemetrieereignissen und direkt identifizierbare personenbezogene Daten (Name/E-Mail-Adresse). Die Aufbewahrungsdauer dieser Ereignisse ist unbekannt.	Google hat erklärt und am 9. Juni 2023 eine Erklärung veröffentlicht, warum die Erhebung dieser Daten erforderlich ist und dass die Aufbewahrungsfrist 30 Tage beträgt.	-
Keine Rechtsgrundlage für Google und Schulen/Universitäten	Neue Leitlinien des EDSA zu hohen Risiken beim CSAM-Scannen.	Google bestätigte, dass es nur nach **bekannten** CSAM scannt und kein maschinelles Lernen/keine KI verwendet.	-

3.1.4 ChromeOS und Chrome Browser auf verwalteten Chromebooks

Die DSFA 2021 ergab, dass mit der Verwendung von ChromeOS und dem Chrome-Browser auf Chromebooks (die von Schülern und/oder Mitarbeitern verwendet werden) auch Datenschutzrisiken verbunden sind. SIVON und SURF haben eine Untersuchung dieser hohen Datenschutzrisiken eingeleitet. Nach Rücksprache zwischen SIVON und SURF mit Google wurden diese Risiken gemindert, indem Google technische Maßnahmen ergriff und einen speziellen Data Processor Mode" (Auftragsverarbeiter Version) von ChromeOS für niederländische Bildungseinrichtungen verfügbar gemacht hat.[24] Die Ergebnisse der Untersuchung sind im Bericht „Public version Verification Report Processor version Google Chrome for Education – 7. März 2024“ enthalten. Das „Google-Handbuch ChromeOS und Chrome Browser. 2024“ beschreibt, ob und wie die identifizierten Risiken eingegrenzt werden können.

Tabelle 1: Kombinierte Ergebnisse der Erstinspektion und dieses Verifizierungsberichts

Thema	Empfohlene Abhilfemaßnahmen für Schulen	Von Google ergriffene Abhilfemaßnahmen

[24] Die spezielle Version von ChromeOS und Chrome Browser steht seit Oktober 2024 auch in Deutschland zur Verfügung

DSAR-Ergebnisse unvollständig (Antrag der betroffenen Personen auf Einsichtnahme)	Blockieren Sie weiterhin den Zugriff auf den Chrome Web Store und den Google Play Store.	Verpflichtung zu einer individuellen Bewertung jedes DSAR
	Benutzen Sie die Richtlinien von SIVON um Schüler darüber zu informieren, wie sie Zugriff bei der Schule und bei Google beantragen können.	Google ist Auftragsverarbeiter für das Domain-weite Takeout-Tool für Administratoren
		Google ist Auftragsverarbeiter für das individuelle Endnutzer Takeout-Tool
		Google hat in vielen verschiedenen Hilfeartikeln für jeden Chrome-Dienst eine Dokumentation darüber veröffentlicht, welche Diagnose-/Telemetriedaten die wesentlichen Chrome-Dienste sammeln, sofern sie überhaupt benutzer- oder gerätebezogene Daten erfassen. Die Hilfeartikel sind über Hyperlinks in der Liste der wesentlichen und optionalen Chrome-Dienste zugänglich.
		Google hat weitere Informationen zum Speichern von Chrome-Daten in einem Hilfeartikel zur Aufbewahrung von Workspace-Daten veröffentlicht.
		Google hat einen Service Data Downloader für Administratoren entwickelt
DSAR-Ablehnung unzureichend erklärt	Verwenden Sie die verfügbaren Administrator-Ereignisprotokolle, um auf persönliche Daten zuzugreifen.	Das verwaltete ChromeOS umfasst Dienste für den Zugriff auf die Daten, wie den Service Data Downloader und das Diagnostic Information Tool (DIT, ein für Workspace entwickelter Telemetriedaten-Viewer).
		Google hat eine verbesserte Erklärung veröffentlicht warum der Zugriff auf einige personenbezogene Daten möglicherweise verweigert wird.
		Google hat Dokumentation veröffentlicht über welche Kategorien personenbezogener Daten, bezogen auf welchen Dienst, in den Ereignisprotokollen für Administratoren verfügbar sind.
Fehlende Zweckbindung	Deaktivieren Sie weiterhin Workspace *Zusätzlich Dienste.*	Google ist zum Datenverarbeiter für die Takeout-Tools für Administratoren und Endnutzer geworden.

bezüglich der Daten im Takeout-Tool		
Fehlende Zweckbindung für ChromeOS und Browser	Melden Sie sich für die neue ChromeOS- und Browser-Auftragsverarbeiter-Vereinbarung an.	Der Auftragsverarbeitungsvertrag für das verwaltete ChromeOS und den Browser enthält zwei erschöpfende Listen von Zwecken: für Google als Auftragsverarbeiter und für die vereinbarte Weiterverarbeitung durch Google als für die Verarbeitung Verantwortlicher für seine legitimen Geschäftszwecke.
	Aktivieren Sie nicht die *optionalen Chrome-Dienste*, für die Google weiterhin als Verantwortlicher fungiert (für Neukunden bereits deaktiviert).	
	Wählen Sie die K-12-Einstellung (auch Universitäten), um die Verarbeitung für kommerzielle Zwecke zu blockieren, wie z. B. die Erstellung von Gruppenprofilen in der Privacy Sandbox und die Standardpräsentation von Umfragen.	
Fehlende Zweckbindung für die Synchronisation von Daten außerhalb von Workspace for Education	Obwohl die fehlende Zweckbeschränkung behoben wurde, wird Schulen aufgrund der Übertragungsrisiken weiterhin davon abgeraten, Chrome Sync zu aktivieren, wenn Nutzern die Nutzung von Google-Konten für private Zwecke gestattet ist.	Auf der Grundlage des Auftragsverarbeitungsvertrags für das verwaltete ChromeOS und den Browser ist Google ein Datenverarbeiter für Chrome Sync, sowohl für Inhalts- als auch für Diagnosedaten (getrennt von Workspace for Education, wo Sync bereits ein Auftragsverarbeitungs-Dienst ist).
Fehlende Zweckbindung (verwalteter) Play Store und Chrome Webstore	Deaktivieren Sie den Zugriff für alle *Zusätzlichen Dienste* in Workspace, einschließlich des (verwalteten) Play Store und des Chrome Webstore. Wenn Schulen den Schülern die Nutzung ausgewählter erlaubter Apps ermöglichen möchten, müssen sie diese Apps über ihr eigenes Netzwerk verteilen. Für Browsererweiterungen können sie die Option „Installation erzwingen“ anwenden, ohne dass Benutzer den Chrome-Webstore besuchen müssen.	Google hat keine Maßnahmen angekündigt.
Kein rechtlich oder sachlich stichhaltig begründeter Grund für die Übermittlung	Unterzeichnen Sie die neue Auftragsverarbeitungsvereinbarung und wenden Sie alle Maßnahmen zur	Google ist zum Datenverarbeiter für das verwaltete ChromeOS und den Browser geworden. Niederländische Bildungskunden verlassen sich auf

personenbezogener Daten in die USA	Datenminimierung an aktualisierte Richtlinien von SIVON inklusive aller Schritte im Handbuch.	geeignete Transfermechanismen gemäß Kapitel V DSGVO.
	Deaktivieren Sie SafeSites mit einer Registrierungseinstellung (erwägen Sie die Verwendung eines Filters eines Drittanbieters).	Google reagierte nicht auf die Anfrage, lokale Filterung zuzulassen, anstatt URLs mit den IP-Adressen in die USA weiterzuleiten.
	Schulen sollten alle datenschutzfreundlichen Einstellungen zentral durchsetzen, einschließlich der Sperrung des Zugriffs auf google.com und youtube.com, indem sie entweder die Verwendung eines Proxyservers erzwingen, um die Funktionalität im lokalen Netzwerk zu blockieren, oder durch manuelle URL-Blockierungsoptionen in der Verwaltungskonsole.	Google bietet zentrale Verwaltungsoptionen für den Gastmodus auf verwalteten Chromebooks, einschließlich der Blockierung von Cookies von Drittanbietern.
	Schulen werden (immer noch) davon abgeraten, Chrome Sync zu aktivieren, wenn Nutzer Google-Konten für private Zwecke verwenden dürfen, einschließlich privater E-Mails und privatem Surfverhalten, bei dem besondere Datenkategorien offengelegt werden könnten – aufgrund des Risikos eines unbefugten Zugriffs durch Regierungsbehörden in 7 Drittstaaten.	Google übermittelt personenbezogene Daten in 7 Drittländer. Niederländische Bildungskunden verlassen sich auf entsprechende Übertragungsmechanismen gemäß Kapitel V DSGVO. Aus der für Google Workspace Meet durchgeführten DTIA geht hervor, dass die Übertragung besonderer Datenkategorien ein hohes Risiko birgt, wenn Schulen diese Daten nicht mit einem lokal gespeicherten Schlüssel verschlüsseln können.
	Deaktivieren Sie Sync, indem Sie die Richtlinie *SyncDisabled* auf true setzen, oder stellen Sie sicher, dass die Studenten eine selbst verwaltete lokale Passphrase zur Verschlüsselung der Sync-Daten verwenden.	Google hat noch keine Richtlinien für Administratoren entwickelt, um die Verwendung der Chrome Sync-Datenverschlüsselung mit lokal gespeicherten Schlüsseln auf den Geräten der Endnutzer zentral durchzusetzen.
Datenschutzfeindliche Standardeinstellungen	Behalten Sie nach Möglichkeit die empfohlenen datenschutzfreundlichen Einstellungen bei.	Privacy Sandbox-Testversionen sind für Benutzer unter 18 Jahren deaktiviert.
		Google hat nicht auf die Aufforderung reagiert, die Funktionen zum Schutz vor Tracking im Chrome-Browser zu verbessern, wenn Cookies von Drittanbietern blockiert sind, das

		DNT-Signal[25] aktiviert ist und das Vorladen von Websites deaktiviert ist. Zum Beispiel durch die Blockierung des Datenverkehrs zu Google-Diensten, bei denen Google nicht als Datenverarbeiter fungiert (wie Analytics und Schriftarten). Google erklärt, dass Administratoren Richtlinien verwenden können, um Cookies und Javascript von Drittanbietern, einschließlich Google, einzuschränken.
	Deaktivieren Sie die Privacy Sandbox für alle Benutzer (bereits deaktiviert, wenn Schulen dem Rat folgen und die K-12-Einstellung wählen).	Google hat Administratoren im Rahmen der Privacy Sandbox in der Auftragsverarbeiterversion von verwaltetem ChromeOS die Kontrolle über das Blockieren der Personalisierung und Messung von Werbung gegeben.
Mangelnde Transparenz	Deaktivieren Sie den Zugriff auf den (verwalteten) Play Store und Chrome Webstore.	Google hat keine Maßnahmen angekündigt.

3.1.5 Transparenz durch Bildungseinrichtung

Ein wichtiger Teil der DSFA ist Transparenz: Die betroffenen Personen (Schüler, deren Eltern und Mitarbeiter) müssen wissen, wie und welche personenbezogenen Daten von Google verwendet werden. Google stellt den betroffenen Personen hierzu weitere Informationen zur Verfügung. Für Workspace for Education-Benutzer im niederländischen Bildungswesen steht eine separate Seite zur Verfügung[26]. Für die Bildungseinrichtung ist es wichtig, die Beteiligten auch über die Ergebnisse der DSFA zu informieren. SIVON hat Musterbriefe für Schüler (und deren Eltern, wenn der Schüler jünger als 16 Jahre alt ist) erstellt.[27], Personal[28] sowie das GRM und der Aufsichtsrat[29].

SIVON hat eine ergänzende Erklärung zur Transparenz und Datenverarbeitung innerhalb von Google Workspace for Education für Administratoren (Verwalter), Datenschutzbeauftragte und Beauftragte für den Datenschutz erstellt[30] Diese Informationen geben unter anderem Einblick in die verschiedenen verfügbaren Tools, um Einblick in die verschiedenen personenbezogenen Daten zu erhalten, die Google verarbeitet.

3.1.6 Empfehlungen Google-Sicherheitsmaßnahmen

Der sichere und verantwortungsvolle Umgang mit persönlichen Daten erfordert auch die richtigen Sicherheitseinstellungen. SIVON hat in Zusammenarbeit mit Google eine Reihe von *Empfehlungen* für

[25] Do not Track
[26] https://services.google.com/fh/files/misc/gcpnaddendum_jan_23_nl.pdf
[27] https://sivon.nl/voorbeeldbrief-google-workspace-ouders-verzorgers/
[28] https://sivon.nl/voorbeeldbrief-google-workspace-leerkrachten-en-docenten/
[29] https://sivon.nl/voorbeeldbrief-mr-en-rvt/
[30] https://sivon.nl/uitleg-transparantie-gegevensverwerkingen-google-workspace-for-education/

Sicherheitseinstellungen[31] für Google Workspace for Education erarbeitet. Erwägen Sie die Verwendung dieser empfohlenen Einstellungen.

3.2 Lokale DSFA

3.2.1 Ermittlung zentraler Risiken und Maßnahmen zur Risikominderung

[NAME BILDUNGSEINRICHTUNG] hat die oben aufgeführten zentral identifizierten Risiken und Minderungsmaßnahmen berücksichtigt und legt diese in der Risikobewertung für die eigene Organisation fest. Das Urteil lautet, dass die Risiken für die (weitere) Nutzung von Google Workspace for Education und/oder ChromeOS und Chrome Browser auf verwalteten Chromebooks [ausreichend/unzureichend] gemindert werden.

Reichen die von Google und der Bildungseinrichtung ergriffenen und noch zu ergreifenden Maßnahmen aus, um die hohen Risiken für Ihre Bildungseinrichtung zu beseitigen?	**Ja/Nein**
Diese Beurteilung basiert auf folgenden Dokumenten:	
1. Public version Updated Verification Report Workspace for Education – 17. Mai 2024	
2. Public version DTIA Google Meet (Workspace for Education – 11. April 2024	
3. Public version New findings review Google Workspace for Education – 16. Mai 2024	
4. Public version Verification Report Processor version Google Chrome for Education – 7 March 2024	
5. Technischer Leitfaden für Google Workspace for Education v3.0	
6. Leitfaden für ChromeOS und Chrome Browser 2024.	

** Diese Dokumente finden Sie auf den Websites von SIVO In SURF.*

Wenn die Antwort auf die obige Frage „Nein“ lautet, zieht [NAME DER BILDUNGSEINRICHTUNG] Folgendes in Bezug auf die Risiken für die Privatsphäre und zusätzliche Abhilfemaßnahmen in Betracht: [Erwägung].

3.2.2 Umsetzung zentral festgelegter Maßnahmen

Bildungseinrichtungen müssen zunächst: *Workspace for Education (Online)-Vereinbarung (Änderungen der Vereinbarung (gesendet am 9. August 2021)* Akzeptieren Sie die von SURF und SIVON ausgehandelten. Darüber hinaus in der *Technisches Maßnahmenhandbuch (August 2021)* beschreibt die Maßnahmen, die eine Bildungseinrichtung selbst ergreifen muss, um die festgestellten hohen Risiken zu beseitigen. Wenn [NAME BILDUNGSEINRICHTUNG]die geänderte Vereinbarung (noch) nicht akzeptiert und (noch) nicht alle diese

[31] https://sivon.nl/wp-content/uploads/2022/06/Beveiliging-Google-Workspace.pdf

Maßnahmen umgesetzt hat, bleiben hohe Restrisiken bei der Nutzung von Google Workspace for Education bestehen..

Das Technische Handbuch für Google Workspace for Education v3.0 und ChromeOS sowie das Handbuch für Chrome Browser 2024 enthalten Einstellungen, die Bildungseinrichtungen selbst implementieren müssen, um Datenschutzrisiken zu mindern. „ANHANG 1: Maßnahmen zu Google Workspace for Education“ und „ANHANG 2: Maßnahmen zu ChromeOS und Chrome Browser auf verwalteten Chromebooks“ enthalten einen Überblick über die zu ergreifenden Maßnahmen.

Geben Sie im Folgenden an, welche Maßnahmen Ihre Bildungseinrichtung (noch) nicht umgesetzt hat, wie die Planung für die Umsetzung der Maßnahme aussieht, oder begründen Sie, warum Ihre Bildungseinrichtung beschlossen hat, die Maßnahme nicht umzusetzen. Beschreiben Sie schließlich die Restrisiken, die mit der (noch) nicht erfolgten Umsetzung der Maßnahme verbunden sind.

Wurden die im *Technischen Leitfaden für Google Workspace for Education v3.0* beschriebenen Maßnahmen, die für Ihre Bildungseinrichtung gelten, umgesetzt?				**Ja/Nein***
Wurden die im ChromeOS- und Chrome-Browser-Handbuch beschriebenen Maßnahmen, die für Ihre Bildungseinrichtung gelten, umgesetzt?				**Ja/Nein***
Wenn die Antwort „Nein“ lautet, dann füllen Sie bitte die folgende Tabelle aus.				
Beschreibung der nicht bzw. noch nicht umgesetzten Maßnahme:	Wird die Maßnahme noch umgesetzt?	In welchem Zeitraum wurde die Maßnahme umgesetzt?	Es wurde beschlossen, die Maßnahme nicht umzusetzen, weil:	Beschreibung des Restrisikos mit Risikoklassifizierung (niedrig, mittel, hoch)
…	Ja/Nein*	Für <Datum>	…	…
…	Ja/Nein*	Für <Datum>	…	…

* Streichen Sie, was nicht zutrifft.

3.2.4 Organisationsspezifische Risikobewertung und Maßnahmen

Der nächste Schritt besteht darin, festzustellen, ob die Nutzung von Workspace for Education durch Ihre Bildungseinrichtung weitere Risiken für den Datenschutz birgt. Dabei handelt es sich um Risiken, die nicht in der zentralen DSFA und DTIA identifiziert wurden oder werden können, sondern nur von der Bildungseinrichtung selbst. Der Grund dafür ist, dass jede Bildungseinrichtung Google Workspace for Education anders nutzt. Eine Bildungseinrichtung nutzt es vielleicht nur für die gemeinsame Nutzung digitaler Lernmaterialien oder den Online-Unterricht, während eine andere es auch für die Aufbewahrung von Unterlagen verwendet.

Bestehen daher angesichts der Zwecke, für die Google Workspace for Education in Ihrer Bildungseinrichtung verwendet wird, der personenbezogenen Daten, die verarbeitet werden, und der Art und Weise, wie diese Verarbeitungen technisch und organisatorisch eingebettet sind, andere Risiken als die in Abschnitt 3.1 beschriebenen Risiken und Maßnahmen? Um dies festzustellen, können Sie zum Beispiel die MAPGOOD-Methode anwenden. Jedes Element in MAPGOOD birgt bestimmte Risiken, zum Beispiel:

- Mensch
  - Unwissenheit, Schlamperei
  - nicht vorschriftsmäßig arbeiten
  - Betrug, Sabotage
- Hardware
  - veraltet, fehlerhafte Funktion
  - Stromausfall
- Software
  - Design-/Programmierfehler
  - keine aktuellen Updates
- Daten
  - unzugänglich
  - für Unbefugte zugänglich
  - verloren gehen
- Organisation
  - unklare Aufgaben, Befugnisse
  - fehlende Verhaltenskodizes
- Umfeld
  - unzureichend gesicherte Räumlichkeiten
  - Naturkatastrophe
- Dienstleistungen
  - keine guten Vereinbarungen mit Anbietern
  - Anbieter geht in Konkurs

Durch die Einteilung von Datenschutzrisiken in diese Kategorien werden mögliche Maßnahmen bereits im Vorfeld einsortiert. Eine Bedrohung in der Kategorie „Mensch“ erfordert beispielsweise häufig Sensibilisierungs- oder Schulungsmaßnahmen.

Nach der Risikoermittlung beurteilen Sie, ob die Risiken durch bestehende oder neue Maßnahmen gemindert werden können. Dies wird als Risikominderung bezeichnet. Das Risiko wird nach Anwendung der Risikominderungsmaßnahmen als Restrisiko bezeichnet.

Anschließend gilt es festzustellen, wie groß die festgestellten Risiken sind. Dies wird als Klassifizierung eines Risikos bezeichnet. Dabei wird die Wahrscheinlichkeit des Eintretens einer Bedrohung mit der Auswirkung bzw. dem verursachten Schaden multipliziert. Wir gehen von einer Skala von 3 aus; auf diese Weise kann die Einstufung des Risikos Werte zwischen 1 und 9 annehmen.

Das Risiko – für die betroffene Person – wird anhand der folgenden Klassifizierung und Berechnung beurteilt:

Chance (Wahrscheinlichkeit) X Auswirkung (Schwere) –/- die risikomindernden Maßnahmen = Restrisiko

Risiko	geringe Eintritts-wahrscheinlichkeit (1)	mittlere Eintritts-wahrscheinlichkeit (2)	hohe Eintritts-wahrscheinlichkeit (3)

große Schadens-Auswirkungen (3)	normales Risiko (Punktzahl: 3)	hohes Risiko (Punktzahl: 6)	(sehr) hohes Risiko (Punktzahl: 9)
mittlere Schadens-Auswirkungen (2)	geringes Risiko (Punktzahl: 2)	normales Risiko (Punktzahl: 4)	hohes Risiko (Punktzahl: 6)
geringe Schadens-Auswirkungen (1)	Sehr geringes Risiko (Punktzahl: 1)	geringes Risiko (Punktzahl: 2)	normales Risiko (Punktzahl: 3)

Eine Restrisikobewertung von 1 und 2 bedeutet ein geringes Risiko, eine Bewertung von 3 oder 4 ein mittleres und eine Bewertung von 6 oder 9 ein hohes Risiko. Bei der Ermittlung eines durchschnittlichen Risikos muss berücksichtigt werden, ob sich das Risiko kurz- oder längerfristig zu einem hohen Datenschutzrisiko entwickeln könnte.

Die nachstehende Tabelle beschreibt organisationsspezifische Risiken, die Sie in Ihrer Bildungseinrichtung identifiziert haben, einschließlich der Maßnahmen zur Risikominderung und der Einstufung des Restrisikos. Es handelt sich also um Risiken und Maßnahmen, die nicht zentral identifiziert und beraten wurden.

Sollten Sie in Ziffer 2.4 bei der Beurteilung der Rechtmäßigkeit der Verarbeitung festgestellt haben, dass die Anforderungen an Datenminimierung und Transparenz nicht (vollständig) erfüllt sind, nehmen Sie auch diese Risiken und Maßnahmen in die nachstehende Tabelle auf.

Organisationsbeschreibung spezifisches Risiko	**Mildernde Maßnahme(n)**	**In welchem Zeitraum wurde die Maßnahme umgesetzt?**	**Risikoklassifizierung (niedrig, mittel, hoch) bereits Umsetzungsmaßnahme (Restrisiko)**
…	…	…	…
…	…	…	…
…	…	…	…

4. Schlussfolgerung und Entscheidung

4.1 Festlegung der Risikobewertung und Maßnahmen

Auf der Grundlage der im Rahmen der zentralen DSFA, der DTIA Google Workspace for Education und ChromeOS sowie des Chrome-Browsers auf den Chromebooks der Administratoren durchgeführten Untersuchung kommt [NAME BILDUNGSEINRICHTUNG] zu dem Schluss, dass die Auswirkungen auf die Rechte und Freiheiten dieser betroffenen Personen durch die Verarbeitung personenbezogener Daten von Schülern und Mitarbeitern - nach Anwendung risikomindernder Maßnahmen - in [unzureichendem/ausreichendem] Maße unter Kontrolle sind. Die in Kapitel 3 genannten (Rest-)Risiken werden akzeptiert. Diese Schlussfolgerung wird sich ändern, wenn die nachfolgend genannten risikomindernden Maßnahmen durch oder im Namen der Leitung (zuständige Behörde) nicht oder unzureichend umgesetzt werden.

Die getroffenen und noch zu treffenden Maßnahmen, Schutzmaßnahmen, Sicherheitsvorkehrungen und Vorkehrungen, die innerhalb von [Google Workspace for Education und ChromeOS **und/oder** Chrome-Browser auf Administrator Chromebooks] den Schutz personenbezogener Daten gewährleisten, sind [unzureichend/ausreichend] darauf ausgerichtet, die Risiken für die Rechte und Freiheiten der betroffenen Personen zu mindern.

Es wurden [keine/hohe] Risiken für die Rechte und Freiheiten der betroffenen Personen identifiziert, die zu einer 'vorherigen Konsultation' bei der Datenschutzbehörde führen müssen, wie in Artikel 36 DSGVO beschrieben.

4.2 Risikomindernde Maßnahmen für Bildungseinrichtungen

Bei dieser Bewertung wurde eine Reihe von Maßnahmen ermittelt, die ergriffen werden müssen, um die in der (zentralen und lokalen) DSFA und der DTIA ermittelten Risiken für den Datenschutz zu mindern. Es handelt sich dabei um die nachstehend aufgeführten Maßnahmen, für deren Umsetzung die Leitung (zuständige Behörde) als für die Datenverarbeitung Verantwortlicher zuständig ist.

[NAME BILDUNGSEINRICHTUNG] hat folgende Maßnahmen ergriffen oder plant dies:

1. Befolgen Sie die Empfehlungen im technischen Leitfaden für Google Workspace for Education v3.0 (siehe Anhang 1).
2. [ChromeOS und Chrome Browser auf verwalteten Chromebooks: Befolgen Sie die Empfehlungen im Leitfaden zu ChromeOS und Chrome Browser 2024, siehe Anhang 2.]
3. Gute Nutzungshinweise für Administratoren und Benutzer (in der Schule), um Missbrauch oder Sicherheitsvorfälle zu verhindern. Für Administratoren, verwenden Sie die zusätzlichen Erklärungen[32] von SIVON über Transparenz und Datenverarbeitung innerhalb von Google Workspace for Education.
4. Erwerben Sie eine kostenpflichtige Lizenz für Google Workspace for Education aufgrund der erforderlichen zusätzlichen Funktionen für die Datenspeicherung innerhalb der EU (DTIA) und zusätzlicher Sicherheitsoptionen.
5. Richten Sie die korrekten Berechtigungen in Google Workspace for Education ein. Sorgen Sie dabei für eine Funktionstrennung, bei der im Falle der Berechtigungsvergabe das Vier-Augen-Prinzip für Administratorfunktionen angewendet wird. Bei Konten von Schülern muss die K-12-Funktion gewählt werden, wodurch die Konten als (K-12) Schülerkonten gekennzeichnet werden."

[32] https://sivon.nl/uitleg-transparantie-gegevensverwerkingen-google-workspace-for-education/

6. Information der Beteiligten über die Ergebnisse der DSFA und die (möglichen) Folgen für ihre Rechte und Freiheiten. Nutzen Sie hierfür die Musterbriefe von SIVON für Schüler und Eltern[33], Mitarbeiter[34] und die Mitbestimmungsgremien (z.B. Schulkonferenz)[35] [36].
7. Erwägen Sie die Übernahme der empfohlenen Sicherheitseinstellungen für Google Workspace, wie in diesem Handbuch beschrieben[37].
8. [Falls zutreffend: Ergreifen Sie die technischen und organisatorischen Maßnahmen, die sich aus Ihrer eigenen lokalen Risikobewertung ergeben: [Beschreibung der Maßnahmen].

Die unter den Nummern [Zahl] aufgeführten Punkte müssen bis zum [Datum] umgesetzt werden.

4.3 Empfehlungen des Datenschutzbeauftragten und Beteiligten

Hinweis an den Datenschutzbeauftragten
Notieren Sie die Ratschläge des Datenschutzbeauftragten unten.
…

Beratung der Beteiligten
Wurden die Schulkonferenz/ Mitbestimmungsgremien der Schule oder andere Betroffene bei der Durchführung der Datenschutz-Folgenabschätzung (DSFA) konsultiert, oder wurde die (Entwurfsfassung der) DSFA mit den Betroffenen mitgeteilt? Falls nein, beschreiben Sie unten, warum nicht. Falls ja, beschreiben Sie unten den Input der Betroffenen.
…

DSFA-Revision
Wann wird der DSFA-Bericht überarbeitet oder neu bewertet? *Hinweis: Wiederholen Sie die DSFA alle drei Jahre oder bei größeren Änderungen an Verfahren oder Systemen*
…

[33] https://sivon.nl/voorbeeldbrief-google-workspace-ouders-verzorgers/
[34] https://sivon.nl/voorbeeldbrief-google-workspace-leerkrachten-en-docenten/
[35] https://sivon.nl/voorbeeldbrief-mr-en-rvt/
[36] In den niederländischen Original geht es hier um einen “Gemeinsamer Mitbestimmungsrat” und “Aufsichtsrat” der Schule
[37] https://sivon.nl/wp-content/uploads/2022/06/Beveiliging-Google-Workspace.pdf

5. ERKLÄRUNG DER BILDUNGSEINRICHTUNG

Basierend auf der Untersuchung, die im Rahmen der zentralen Datenschutz-Folgenabschätzung (DSFA) und Datentransfer-Folgenabschätzung (DTIA) sowie der lokalen DSFA durchgeführt wurde, sind die Auswirkungen auf die Rechte und Freiheiten der betroffenen Personen durch die Verarbeitung personenbezogener Daten von Schülern und Mitarbeitern in Google Workspace for Education [und ChromeOS sowie Chrome-Browser auf verwalteten Chromebooks] - nach Anwendung risikomindernder Maßnahmen - in [unzureichendem/ausreichendem] Maße unter Kontrolle.

Diese Schlussfolgerung ist bzw. wird eine andere sein, wenn die in dieser lokalen DSFA genannten Maßnahmen nicht oder nicht ausreichend umgesetzt werden.

Die Maßnahmen, Schutzmaßnahmen, Sicherheitsmaßnahmen und -mechanismen, die ergriffen wurden und werden, um den Schutz personenbezogener Daten innerhalb von Google Workspace for Education zu gewährleisten, sind [unzureichend/ausreichend] darauf ausgerichtet, die Risiken für die Rechte und Freiheiten der betroffenen Personen zu mindern.

Es wurden [keine/hohe] Risiken für die Rechte und Freiheiten der betroffenen Personen identifiziert, die zu einer 'vorherigen Konsultation' bei der Datenschutzbehörde führen müssen, wie in Artikel 36 DSGVO beschrieben.

Die Schulleitung von [NAME BILDUNGSEINRICHTUNG] erklärt unter Berücksichtigung der Schlussfolgerungen und Empfehlungen hiermit:

- den Inhalt dieser organisationsspezifischen DSFA zur Kenntnis genommen zu haben;
- von der durch SIVON und SURF durchgeführten zentralen DSFA, Datentransfer-Folgenabschätzung (DTIA) und Untersuchung zu ChromeOS und Chrome-Browser sowie den von ihnen erzielten Verhandlungsergebnissen Kenntnis genommen zu haben;
- die in diesem Bericht aufgeführten (Rest-)Risiken zu akzeptieren;
- der Umsetzung der im Bericht genannten Maßnahmen zuzustimmen;
- den Auftrag zur Durchführung der empfohlenen Maßnahmen zur Kontrolle und Steuerung von Risiken innerhalb der dafür genannten Fristen zu erteilen;
- diese DSFA nach einem Zeitraum von <Monaten/ Jahren> oder früher, falls erforderlich, überprüfen zu lassen;
- eine vorherige Konsultation bei der Datenschutzbehörde einzureichen / nicht einzureichen;
- das DSFA-Team zu entlassen.

UND BESCHLIESST - NACH ERNEUTER PRÜFUNG - DIE NUTZUNG VON [GOOGLE WORKSPACE FOR EDUCATION UND/ODER CHROMEOS UND CHROME-BROWSER AUF VERWALTETEN CHROMEBOOKS] [FORTZUSETZEN/NICHT FORTZUSETZEN]."

Name der Bildungseinrichtung:

Name des/der Schulleiter(in):

Ort:

Datum:

Unterschrift:

ANHANG 1: Google Workspace for Education-Maßnahmen

Technischer Leitfaden für Google Workspace for Education v3.0			
Für.	**Beschreibung**	Durchgeführte Aktion J/N	Planung
Allgemeine Hinweise und Informationen			
2.4	Übermittlung personenbezogener Daten in Drittländer: Bitte informieren Sie sich auf dieser Seite über die Unterauftragsverarbeiter von Google: https://workspace.google.com/terms/subprocessors.html (engl.)		
2.5	Informationen zum Datenschutz finden Sie hier: https://www.google.com/chrome/privacy/whitepaper.html (deutsch)[38] https://services.google.com/fh/files/misc/google_workspace_edu_data_protection_implementation_guide.pdf (englisch) Erläuterung der Transparenz der Datenverarbeitung in Google Workspace for Education durch SIVON: https://sivon.nl/uitleg-transparantie-gegevensverwerkingen-google-workspace-for-education/ (niederländisch)		
2.6	Geltungsbereich Google Workspace for Education: Im Rahmen der Vereinbarung mit Google ist nur die Nutzung von "*Core Services*" zulässig. Bei der Nutzung anderer, zusätzlicher Dienste ist Google und nicht die Bildungseinrichtung verantwortlich. https://workspace.google.com/intl/de/terms/user_features/ (deutsch) Zusätzliche Google-Dienste deaktivieren: https://support.google.com/a/answer/181865#zippy=%2Cservices-aan--of-uitzetten-voor-gebruikers (deutsch)[39]		
Maßnahmenübersicht			
3.2	Maßnahmen bezüglich Benutzerkonten		
3.3	Maßnahmen zur Datenminimierung in Produkten und Funktionalitäten		
3.4	Individuelle Maßnahmen und Anleitungen		
Aktivierung der zentralen Verwaltungsoptionen			
4.1	Stellen Sie Chromebooks und Chrome-Browser unter Verwaltung		
4.2	Chromebooks in die Verwaltung aufnehmen		
4.3	Mit Chromebook verwaltete Gastsitzung		
4.4	Chrome-Browser verwalten		
4.5	Einstellungen am Betriebssystem per Gruppenrichtlinie		
Einstellungen in der Admin-Console			
5.1	Einrichten von Google Workspace als K-12		

[38] unten auf Seite Sprache auf Deutsch einstellen
[39] unten auf Seite Sprache einstellen

5.2	Benutzernamen in E-Mail-Adressen (Pseudonymisierungshinweis)		
5.3	Benutzerprofile		
5.4	Speicherung von geografischen Standortdaten		
5.5	Zusätzliche Google-Dienste (Additional Services)		
5.6	Google Workspace Marketplace-Apps		
5.7	Neue Google-Produkte		
5.8	Rechtschreibprüfung und Rechtschreibprüfungs-Webdienst		
5.9	Deaktivieren Sie die Chrome-Synchronisierung		
5.10	Deaktivieren Sie die automatische Übersetzung von Websites		
5.11	Deaktivieren Sie die Geolokalisierung		
5.12	Erlauben Sie kein Benutzer-Feedback		
5.13	Berichtsstatistiken: ausschalten		
5.14	Neuer Tab		
5.15	Search suggested service (omnibox)		
5.16	Anmeldung bei sekundären Konten		
5.17	Cookie-Richtlinie		
5.18	Systemberichte über besuchte Seiten		
5.19	Chrome Cleanup		
Individuelle Einstellungen und Anleitungen			
6.1	Personalisierung von Werbung (wenn die K-12-Einstellung nicht aktiviert ist)		
6.2	Einbettung von YouTube-Videos		
6.3	Verwendung des Chrome-Browsers		
Benutzen Sie Google nicht als Suchmaschine			
7.1	Verwenden Sie einen Werbe- und/oder Tracking Blocker		
7.2	Verwenden Sie keine datenschutzrelevanten Informationen in Datei- und Ordnernamen (Benutzeranweisungen).		
Folgenabschätzung für die Datenübertragung (DTIA)			
8.1	Data Regions. *Bitte beachten Sie: Dies ist in der kostenlosen Version von Google Workspace for Education Basic nicht möglich, es ist eine kostenpflichtige Lizenz erforderlich*		
8.2	Erwägen Sie die Anwendung der clientseitigen Verschlüsselung		
Sicherheitseinstellungen			
	Erwägen Sie die Verwendung der von Google empfohlenen Sicherheitseinstellungen: https://sivon.nl/wp-content/uploads/2022/06/Beveiliging-Google-Workspace.pdf (niederländisch - deutsche Übersetzung liegt vor)		

Erläuterung zu „Compliance“ oder „Explain“ (Erklärung zur Abweichung vom Rat): Eine Begründung finden Sie in Abschnitt 3.2.2.

ANHANG 2: Maßnahmen für ChromeOS und Chrome Browser auf verwalteten Chromebooks

Handbuch zu Google ChromeOS und Chrome Browser 2024			
Kapitel	**Beschreibung**	Durchgeführte Aktion J/N	Planung
2	**ChromeOS-Verarbeitungsvertrag abschließen (Datenprozessormodus)**		
3	**Kaufen Sie das Chrome Education-Upgrade für Chromebooks (für die Lebensdauer jedes Chromebooks)**		
4	**Datenschutzeinstellungen für ChromeOS und Chrome-Browser**		
	„Optionale Dienste“ deaktivieren		
	Verwenden Sie immer die K-12-Einstellungen		
	Deaktivieren Sie den Chrome Web Store		
	Schalten Sie Google Play aus		
	Deaktivieren Sie die personalisierte Werbung. Für K-12 ist dies der Standardwert		
	Senden Sie keinen „Absturzbericht“ an Google		
	Erwägen Sie, „Sichere Websites“ zu deaktivieren und eine andere Filterfunktion zu implementieren		
5	**Endbenutzereinstellungen**		
	Schalten Sie die Privacy Sandbox aus.		
	Anzeigenthemen deaktivieren		
	Von Websites vorgeschlagene Anzeigen deaktivieren		
	Anzeigenmessung deaktivieren		
	Verwenden Sie die Chrome-Sync-Verschlüsselung		
6	**Verwenden Sie datenschutzfreundliche Browsereinstellungen**		
	Deaktivieren Sie „Do Not Track“ und deaktivieren Sie das Vorladen der Website		

Erläuterung zu „Compliance“ oder „Explain“ (Erklärung zur Abweichung vom Rat): Eine Begründung finden Sie in Abschnitt 3.2.2.