STUDIO TECNICO LEGALE
CORBELLINI
Studio AG.I.COM. S.r.l.

USO SICURO DI GOOGLE WORKSPACE

PER L' AMMINISTRATORE DI PIATTAFORMA

Misure di sicurezza per contenere i rischi connessi all'utilizzo di Google Workspace for Educational

REV. 2023

Sommario

BUONE PRASSI

Il senso di questa guida è quello di fornire alcune buone prassi (best practice) per l'utilizzo in sicurezza di Google Workspace, con particolare riferimento alle criticità sollevate da alcune organizzazioni nazionali (e non) in ordine alla presunta incompatibilità di questo software con il G.D.P.R., in particolare in seguito alla sentenza della Corte di Giustizia dell'U.E. pubblicata nel 2020 e nota come "Schrems II" che ha sgomberato il campo da ogni dubbio sancendo che il regime di sicurezza dei dati garantito nel trasferimento degli stessi tra UE e USA è inadeguato e deve quindi essere integrato mediante l'adozione di idonee misure di sicurezza specifiche.

Si tratta di un problema eminentemente geo-politico, che si è aperto nel momento in cui è venuto meno l'accordo UE-USA per la gestione dei dati e che ha posto giganti come Google, prima ancora che sotto la veste di imputati, sotto quella di primi danneggiati, poiché oggi non si contesta tanto alle loro infrastrutture di essere manchevoli, quanto alla normativa statunitense di non prevedere, secondo la Corte, idonee garanzie.

BUONE PRASSI PER LA SICUREZZA DI GOOGLE WORKSPACE

La comunicazione con gli utilizzatori della piattaforma

Quando l'Istituto sceglie di adottare una piattaforma didattica come Google Workspace, non deve chiedere agli utilizzatori (docenti e allievi) alcun tipo di consenso, deve però informare gli stessi di questa circostanza.
L'informazione in questo senso viene fornita mediante l'INFORMATIVA che il nostro studio ha suggerito di adottare, in sede di iscrizione per gli allievi ed alla presa di servizio per il personale docente, che cita espressamente il fatto che i dati personali potranno entrare nella disponibilità di "*Fornitori di cui l'Istituto si avvale (gestore del registro elettronico e delle piattaforme didattiche a distanza, tecnici informatici incaricati della manutenzione, assicurazioni, agenzie di viaggio, tipografie e legatorie, fotografi e cineoperatori etc.) esclusivamente per le finalità istituzionali sopra esposte e nell'ambito di rapporti derivanti da obblighi giuridici e/o da prestazioni fornite da soggetti designati quali "responsabili del trattamento" ex art. 28 del G.D.P.R. o con cui si sono stipulati contratti contenenti clausole standard a tutela della privacy".*

Verifichi che l'Istituto abbia correttamente fornito ad inizio anno queste informative, le trova a questo link: http://www.agicomcloud.it/index.php/s/ygBuiXvLzjx9D8T identificate con il nome:

INFO ALLIEVI e

INFO PERSONALE

Oltre all'informativa scolastica, gli utilizzatori di Google Workspace dovranno disporre di altri documenti integrativi di cui è opportuno collocare i link sul sito internet istituzionale:

- Informativa fornita dalla stessa Google che si trova a questo link: https://workspace.google.com/terms/education_privacy.html

- Le informazioni sugli impegni legali assunti sempre da Google sia per i servizi principali che per quelli aggiuntivi che si trovano a questo link: https://support.google.com/a/answer/6356441

- Le informazioni sulla conformità di Google agli obblighi legali internazionali in materia di protezione dei dati che sono disponibili al link: https://cloud.google.com/terms/data-processing-addendum/

- L'informazione che i genitori possono visitare "myaccount.google.com" dopo aver eseguito l'accesso all'account Google Workspace for Education del figlio per visualizzare e gestire le informazioni personali e le impostazioni dell'account.

BUONE PRASSI PER LA SICUREZZA DI GOOGLE WORKSPACE

I Servizi attivati e il contratto con Google

Google Workspace offre due categorie di servizi Google: **servizi principali** (come Gmail, Drive, Calendar e Classroom) forniti in base al contratto Google Workspace for Education e **servizi aggiuntivi** (come YouTube, Maps, Blogger ed il correttore ortografico avanzato) che possono essere utilizzati con gli account Google Workspace for Education, se consentito per scopi didattici, dall'amministratore di piattaforma della scuola. I Servizi aggiuntivi non fanno parte dell'offerta Google Workspace for Education e non sono quindi coperti dalle informative prima citate.

A titolo precauzionale è opportuno che vengano attivati esclusivamente i servizi principali.
Per quelli aggiuntivi invece occorre qualche precauzione in più, come ad esempio una più specifica informativa personalizzata alla quale deve seguire un esplicito consenso (come peraltro previsto dallo stesso contratto che l'Istituto ha concluso con Google).
L'Amministratore della piattaforma, in accordo con il Dirigente Scolastico, deve scegliere con cura quali Servizi aggiuntivi (ad esempio, YouTube, Maps, Blogger e il controllo ortografico avanzato) attivare/disattivare, in particolare per gli utenti minorenni.

Gli amministratori possono limitare o consentire l'accesso a servizi aggiuntivi ad una intera unità organizzativa tramite il pannello di controllo.
A tale proposito è il caso di ricordare che il Dirigente Scolastico deve nominare formalmente gli amministratori della piattaforma, fornendo loro le indicazioni in ordine a quali misure di sicurezza debbano adottare (istruzioni operative).

Troverà una lettera di nomina tipo al link: http://www.agicomcloud.it/index.php/s/ygBuiXvLzjx9D8T identificata con il nome:

NOMINA AMMINISTRATORE PIATTAFORMA DDI (GOOGLE)

In caso di dubbi è importante disporre del contenuto del contratto che l'Istituto ha concluso con Google che è disponibile a questo link: https://workspace.google.it/intl/it/terms/2013/1/premier_terms.html

Unità Organizzative e altre precauzioni

In qualità di amministratore di piattaforma, puoi gestire l'accesso degli utenti in modo cumulativo a diverse configurazioni di Google Workspace e prodotti aggiuntivi creando unità organizzative.

In questo modo è possibile raggruppare gli utenti, ad esempio distinguendo tra coloro che gestiscono dati personali/particolari (come ad esempio i docenti) e quelli che non lo fanno (gli allievi).

Dopo aver creato queste unità organizzative sarà possibile attivare o disattivare servizi e prodotti specifici senza accedere utente per utente ma facendolo per gruppi omogenei di utenti.

Come ulteriore precauzione di sicurezza, per limitare la condivisione dei dati personali, è opportuno stabilire a livello di Istituto, criteri per impedire agli utenti di includere informazioni delicate quando decidono la denominazione dei file e delle cartelle utilizzando i servizi principali di Google Workspace for Education (ad esempio, Documenti, Fogli, Presentazioni, Moduli, Drive, Gmail).

BUONE PRASSI PER LA SICUREZZA DI GOOGLE WORKSPACE

La configurazione di Google Workspace

L'amministratore di piattaforma è chiamato ad eseguire i seguenti controlli e le precisate configurazioni:

● Controlla quali app di terze parti e interne accedono ai dati di Google Workspace e verifica che sia limitato l'accesso a "Servizi Google Workspace".

● In Drive, nella sezione "Opzioni di condivisione", disattiva la condivisione di file esterni per gli studenti (o limita i file esterni condivisione per consentire solo i domini elencati) e imposta "Controllo accesso" su "Solo destinatari"

● Disattiva la chat negli editor di documenti

● In Google Meet, consenti solo a docenti e personale di creare riunioni. Gli utenti che non possono creare riunioni possono comunque partecipare alle riunioni video di Meet create da altri.

● Per tutti gli account dell'istruzione primaria e secondaria e superiore, si consiglia di evitare di utilizzare i nomi degli studenti per indirizzi e-mail e nomi utente.

● Verifica che l'accesso ai servizi avvenga effettivamente tenendo conto dell'età degli allievi.

> Negli Istituti di Istruzione Superiore, di default, gli account degli studenti sono designati come appartenenti a persone con più di 18 anni, mentre negli Istituti del primo ciclo come minori di 18 anni, puoi però apportare delle personalizzazioni se ritieni che l'età configurata non sia appropriata.

A titolo esemplificativo, non è concesso l'accesso da parte dei minori di anni 18 a questi servizi:

- Youtube
- Search
- Google Play
- Google Maps e Google Harth
- Google Photos

● Verifica che la cronologia delle posizioni sia disattivata (opzione di default) per tutti gli utenti
(Dalla console di amministrazione, vai ad Applicazioni > Servizi Google aggiuntivi > Cronologia delle posizioni ed accertati che sia disattivata)

● Verifica che la cronologia di youtube (se hai attivato il servizio) sia disattivata. Per le scuole del I ciclo è disattivata per impostazione predefinita.
(Dalla Console di amministrazione, vai ad Applicazioni > Altre Google servizi > YouTube ed accertati che sia disattivata)

● Di default non sono presenti annunci pubblicitari in Google Workspace for Education così come Google non raccoglie né utilizza i dati degli allievi per scopi pubblicitari.
Inoltre, gli utenti di Workspace for Education non visualizzano gli annunci quando eseguono delle ricerche su Google ma solo dopo aver eseguito l'accesso ai loro account Google Workspace for

Education. Si rammenta invece che alcuni dei servizi aggiuntivi di Google (es. Blogger e YouTube) mostrano annunci agli studenti, ancorché non personalizzati.
Nei domini dell'istruzione superiore invece, è abilitata la possibilità che i singoli utenti ricevano avvisi pubblicitari, occorre che gli stessi siano istruiti sulla disattivazione di questa impostazione dalla pagina Gestione attività, poiché l'opzione non è modificabile dall'amministratore.

- Ricorda che hai la possibilità di attivare/disattivare l'accesso al WEB ed alle APP degli allievi.
  L'Amministratore deve valutare con il Dirigente Scolastico se attivare o meno questa funzione.
  (Dalla Console di amministrazione, vai ad App > Servizi Google aggiuntivi > Attività web e app, per impostazione predefinita, per gli account degli istituti del I ciclo il parametro è disattivato e non è modificabile dall'utente finale. Quando il servizio è attivato, gli utenti finali hanno la possibilità di attivarlo/disattivarlo a loro piacimento).

  L'accesso al WEB tramite Chrome, comporta la possibilità di sincronizzare la navigazione, i segnalibri, la cronologia, le password e altre impostazioni degli utenti nei loro account Google e consente agli utenti di accedere a queste impostazioni in ogni momento e su qualsiasi dispositivo sincronizzato.
  Per i domini Google Workspace EDU, la sincronizzazione di Chrome è un servizio principale.
  A titolo precauzionale è auspicabile che tale possibilità di sincronizzazione venga disattivata.

- Il controllo ortografico di base avviene in locale, mentre quello avanzato si basa su cloud e invia il testo digitato dagli utenti a Google. Per impostazione predefinita, il controllo avanzato è attivato per tutti gli utenti. E' auspicabile disabilitare il controllo ortografico avanzato (salvo che non lo si voglia adottare per la correzione di testi del tutto privi di dati personali), dal menu Chrome del singolo utente facendo clic su Preferenze > Avanzate > Lingue.
  Importante rammentare che il controllo ortografico avanzato non è parte dei servizi di base di Google Workspace for Educational ma di quelli avanzati per i quali è necessario richiedere il consenso.

Nelle pagine che seguono è disponibile l'Appendice 1 al documento "Google Workspace for Education data protection implementation guide" che è disponibile a questo link:
https://services.google.com/fh/files/misc/google_workspace_edu_data_protection_implementation_guide.pdf e che costituisce la guida per la configurazione in sicurezza della piattaforma.

Informazioni di contatto

Per qualsiasi informazione o approfondimento :

LUCA CORBELLINI
DATA PROTECTION OFFICER
SPECIALISTA IN INFORMATICA GIURIDICA

Tel. 02-90601324
Fax 02-700527180
dpo@agicomstudio.it

Informazioni sulla società

Studio AG.I.COM. S.r.l. unipersonale
Via XXV Aprile, 12 – 20070 SAN ZENONE AL LAMBRO (MI)
Tel. 02-90601324
Fax 02-700527180
www.agicomstudio.it

STUDIO TECNICO LEGALE
CORBELLINI
Studio AG.I.COM. S.r.l.

Appendix 1: Privacy control mapping

This privacy control mapping provides a convenient way to assess what you need to support requirements from various privacy regulations when using Google Workspace for Education. Please note this is not an exhaustive list of all privacy controls, but is intended as a general high-level mapping. We recommend that you consult with a legal expert to obtain guidance on the specific requirements applicable to your organization, as this guide does not constitute legal advice.

Data controller considerations

Typical privacy controls	Customer responsibility	Google Workspace for Education supporting functionality
Understanding the organization and its context	The organization shall determine its role as a Personally Identifiable Information (PII) controller and/or a PII processor to identify the appropriate requirements (regulatory, etc.) for processing Customer Personal Data.	See the roles and responsibilities when processing Customer Data in section 5 of the Google Workspace for Education Data Processing Amendment.
Determine when consent is to be obtained and record consent	The customer should understand legal or regulatory requirements for obtaining consent from individuals prior to processing Customer Personal Data, and record the consent when needed.	Google does not provide support for gaining and recording user consent for all of your activities. When users sign in to the organization managed Google Account you created, they receive a notice explaining how their data is collected and can be accessed by their admin.
Identify lawful basis and document purpose	The customer should understand any requirements related to the lawful basis of processing, such as whether consent must first be collected. The customer should document the purpose for which Customer Personal Data is processed.	Google does not provide support for gathering the lawful basis of processing for all of your activities. To learn about the processing activities Google performs for you, and the purposes of that processing, see the Google Workspace for Education Agreement and Data Processing Amendment.
Contracts with PII processors	The customer should ensure that their contracts with processors include requirements for aiding with any relevant legal or regulatory obligations related to processing and protecting	As your data processor, Google will assist you in ensuring compliance with your obligations (taking into account the nature of the processing of Customer Personal Data and the information available to Google) in accordance with the Data

	Customer Personal Data.	Processing Amendment. See Section 7.1.4 (security assistance), 9.2.2 (data subject rights assistance), and 8.1 (DPIA assistance) for more information.
Limit collection and processing	The customer should understand requirements around limits on collection and processing of Customer Personal Data (e.g., that the collection and processing should be limited to what is needed for the specified purpose).	To learn about the processing activities Google performs for you, and the purposes of that processing, see the Google Workspace for Education Agreement and Data Processing Amendment.
Records related to processing PII	The customer should maintain all necessary and required records related to processing Customer Personal Data.	Google Workspace for Education provides audit logs to give you visibility on the data access and help you answer such questions as, *Who did what, where did they do it, and when did they do it?* Available audit logs include admin activity logs (admin audit log), security logs (login, SAML, and access transparency), and user services and account logs (email log search and Drive audit log). To learn more about audit logs, see available audit logs. The general retention time for audit logs is 6 months (for details, see Data retention and lag times). You can customize what you review for any audit log in your Google Admin console by filtering by user or activity, organization unit, or date. You can also set up alerts for certain activities.

Organizational data protection policy and assessment

Typical privacy controls	Customer responsibility	Google Workspace for Education supporting functionality
Independent review of information security	The customer shall apply an information security risk assessment process to identify risks associated with the loss of confidentiality, integrity, and availability. This may include internal or external audits, or other measures for assessing the security of processing. Where the customer is dependent on another	You are responsible for your use of the services and your storage of any copies of Customer Data outside of Google systems or Google's subprocessors' systems. Google undergoes an increasing amount of independent third-party audits on a regular basis. For each one, an independent auditor examines our data

	organization or third party for all or part of the processing, they should collect information about such assessments performed by them.	centers, infrastructure, and operations. Regular audits are conducted to certify our compliance with the auditing standards ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, ISO/IEC 27701, and SOC 2. For a list of compliance certifications, see the Google Cloud Compliance resource center. Based on your contract terms with Google as a Google Workspace for Education customer, Google may allow you—or an independent auditor appointed by you—to conduct audits (including inspections) to verify Google's compliance with its obligations, in accordance with section 7.5 (Reviews and Audits of Compliance) in the Data Processing Amendment.
Data protection impact assessment (DPIA)	The customer should be aware of requirements for completing a data protection impact assessment (when they should be performed, what needs to be included in the assessment, and who should perform the assessment, etc.).	As your data processor, Google will assist you in ensuring compliance with its obligations around data protection impact assessment (taking into account the nature of the processing and the information available to Google) in accordance with section 8 of the Data Processing Amendment.
Determining the scope of the information security management system	As part of any overall security or privacy program that a customer may have, they should include the processing of Customer Personal Data and requirements relating to it. Policies for system development and design should include guidance for the organization's PII processing, based on obligations to PII principals and/or any applicable legislation and/or regulation and the types of processing performed by the organization.	Google does not provide support for its customers' internal process. At least annually, consider creating privacy policies and associated training materials to disseminate to users and privacy groups across your organization. Google offers Professional Services options for educating users on cloud security and privacy, including but not limited to a Google Workspace Security Assessment.
Information security policies	The customer should augment any existing information security policies to include protection of	Google does not provide support for its customers' internal process.

	Customer Personal Data, including policies necessary for compliance with any applicable legislation. The customer should determine and assign responsibility for providing relevant training related to protecting Customer Personal Data.	Consider developing an org-wide security and privacy assessment and authorization policy that defines the procedures and implementation requirements of organization privacy assessments, privacy controls, and authorization controls.
Organization of Information Security Customer consideration	The customer should, within their organization, define responsibilities for security and protection of Customer Personal Data. This may include establishing specific roles to oversee privacy-related matters, including a Data Protection Officer (DPO). Appropriate training and management support should be provided to support these roles.	Google does not provide support for its customer internal process. Consider appointing one or more persons responsible for developing, implementing, maintaining, and monitoring an organization-wide governance and privacy program, to ensure compliance with all applicable laws and regulations regarding the processing of PII (Personally Identifiable Information). You can designate your data protection officer and EU representative in the Google Admin console at **Account Settings > Legal and Compliance**. Google has designated a DPO for Google LLC and its subsidiaries, to cover data processing subject to various privacy regulations.
Classification of information	The customer should explicitly consider their use of PII as part of a data classification scheme.	Google does not provide support for its customers' internal process. Your information classification system should explicitly consider your use of PII as part of the scheme that you implement. Considering PII within the overall classification system is integral to understanding what type or special categories of PII that you process, where such PII is stored, and the systems through which it can flow. Your data classification scheme should describe how you classify data, depending on its sensitivity and identifiability. Data owners are responsible for determining the

		appropriate data classification based on who requires access and for what purposes, the potential risks and harm if the data is subject to unauthorized access, as well as the general context of the data.
Management of information security incidents	The customer should have processes for determining when a Customer Personal Data breach has occurred. The customer should understand and document their responsibilities during a data breach or security incident involving Customer Personal Data. Responsibilities may include notifying required parties, communications with processors or other third-parties, and responsibilities within the customer's organization.	We recommend that you establish an incident response policy for your organization, including procedures to facilitate and implement incident response controls, and that you create security groups for your organization's incident response teams and authorities. We also recommend that you develop an incident response test plan, procedures, checklists, requirements and benchmarks for success. Consider specifying classes of incidents that should be recognized by your organization, and outline the associated actions to take in response to such incidents. Consider also defining the specific actions that should be taken by authorized personnel in the event of an incident, such as steps for managing information spills, cybersecurity vulnerabilities, and attacks. Additionally, take advantage of capabilities in Google Workspace for Education to scan and quarantine email content, block phishing attempts, and set restrictions on attachments. You can also use data loss prevention (DLP) to inspect, classify, and de-identify sensitive data to help restrict exposure. See Prevent data loss using DLP for Drive, Scan your email traffic using DLP rules, and DLP whitepaper. As a Google customer, Google will notify you promptly after becoming aware of a Data Incident, and promptly take reasonable steps to minimize harm and secure Customer Data. See our commitment in section 7.2 (Data Incident) of the Data Processing

		Amendment. See also our data incident response process.
Information backup	The customer should have a policy that addresses the requirements for backup, recovery, and restoration of PII (which can be part of an overall information backup policy) and any further requirements (e.g., contractual and/or legal requirements) for the erasure of PII contained in information held for backup requirements.	We recommend that you develop a contingency plan for your organization that defines the procedures and implementation requirements for contingency planning controls across your organization. We also recommend that you identify key contingency personnel, roles, and responsibilities across organizational elements. Additionally, highlight the mission-essential and business-essential information system operations within your organization. Outline recovery time objectives (RTO) and recovery point objectives (RPO) for resuming essential operations once the contingency plan has been activated. Document critical information systems and associated software. Identify any additional security-related information, and provide guidance and requirements for storing backup copies of critical system components and data. Google owns and operates data centers all over the world, helping to keep the internet humming 24/7 and providing redundancies and resilience to our customers. You can also deploy additional backup and sync from your local files to Google Drive.

Data protection & security settings

Typical privacy controls	Customer responsibility	Google Workspace for Education supporting functionality
User access management (including user access provisioning, and management of privileged access)	The customer should be aware of which responsibilities they have for access control within the service they are using, and	We recommend that you develop an org-wide access control policy for information system accounts in the cloud. We recommend that you define the

	manage those responsibilities appropriately, using the tools available.	parameters and procedures by which your organization will create, enable, modify, disable, and remove information from system accounts. The Google Admin console provides you with centralized administration, which makes setup and management more efficient. You can protect your organization with security analytics and best practice recommendations within the security center. You can use Cloud Identity and Access Management (IAM) to assign roles and permissions to administrative groups, using the methodology of least privilege and separation of duties. Learn how to add Cloud Identity to your Google Workspace Account.
Secure log-on procedures	The customer should provide the capability for secure log-on procedures for any user accounts under its control.	As a Google Workspace for Education customer, you can use integrated Cloud Identity features to manage users and set up security options like 2-step verification and security keys. With 2-step verification, you add an extra layer of security to Google Workspace for Education accounts by requiring users to enter a verification code in addition to their username and password when they sign in. The Security Key is an enhancement for 2-step verification. Google, working with the FIDO Alliance standards organization, developed the Security Key — an actual physical key used to access your organization managed Google Account. It sends an encrypted signature rather than a code, and helps ensure that your login cannot be phished. For details, see How to use a security key for 2-Step Verification. For additional user authentication/authorization features, see the Google Cloud Security and

		Compliance Whitepaper.
Event logging and protection	The customer should understand the capabilities for logging provided by the system and utilize such capabilities to ensure that they can log actions related to Customer Personal Data that they deem necessary. A process should be put in place to review event logs using continuous, automated monitoring and alerting processes, or else manually where such review should be performed with a specified, documented periodicity, to identify irregularities and propose remediation efforts.	Google Workspace for Education provides audit logs to help you answer such questions as, *Who did what, where did they do it, and when did they do it?* Available audit logs include admin activity logs (admin audit log), security logs (login, SAML, and Access Transparency), and user services and account logs (email log search and Drive audit log). To learn more about audit logs, see Available audit logs. The general retention time for audit logs is 6 months (for details, see Data retention and lag times). You can customize what you review for any audit log in your Google Admin console by filtering by user or activity, organizational unit, or date. You can also set up alerts for certain activities.
Encryption	The customer should determine which data may need to be encrypted, and whether the service they are utilizing offers this capability. The customer should utilize encryption as needed, using the tools available to them.	Google Workspace for Education Customer Data is encrypted in transit, at rest, and on backup media. Encryption is an important piece of the Google Workspace for Education security strategy, helping to protect your emails, chats, Google Drive files, and other data. Additional details on how data is protected at rest, in transit, and on backup media, and details on encryption key management can be found in our Google Workspace Encryption Whitepaper. As an admin, if your organization needs additional encryption on outgoing email, you can set up rules to require outgoing messages to be signed and encrypted using Secure/Multipurpose Internet Mail Extensions (S/MIME). This helps to ensure appropriate security, confidentiality, and integrity of Customer Personal Data.

Records of countries and organizations to which PII might be transferred	The customer should understand, and be able to provide to the individual, the countries to which Customer Personal Data is or may be transferred. Where a third-party/processor may perform this transfer, the customer should obtain this information from the processor.	Google owns and operates data centers around the world to keep its products running 24 hours a day, 7 days a week. For more details, see Discover our data center locations. You can choose to store your data in a specific geographic location (the United States or Europe) by using a data region policy. This service provides fine-grained control of the geographical location for storage of email messages, documents, and other Google Workspace for Education content. Please review our data regions product offering carefully and consult with legal counsel to make your own assessment as to whether it meets your specific compliance or business needs.
Records of PII disclosure to third parties	The customer shall record disclosures of PII to third parties, including what PII has been disclosed, to whom and when. This may include disclosures to law enforcement, etc. Where a third-party/processor discloses the data, the customer should ensure that they maintain the appropriate records and obtain them as necessary.	Google and its affiliates use a range of *subprocessors* to assist with the provision of its services. For details, see our disclosure of Google Workspace subprocessors. As an admin, we recommend that you evaluate the use of third-party applications. You have the option to disable users from installing third-party applications, such as Google Drive apps and Google Docs add-ons. We recommend that you review the security documentation provided by third-party developers, as well as the applicable data processing terms, before using any such third-party applications with Google Drive and Google Docs. If Google receives a government data request for Cloud Customer Data, it is Google's policy to direct the government to request such data directly from the Cloud customer. We have a team that reviews and evaluates each request we receive to make sure it satisfies legal requirements. When compelled to produce data, Google promptly notifies

		customers before any information is disclosed, unless such notification is prohibited by law or except in emergency situations involving a threat to life. Google will, to the extent allowed by law and by the terms of the request, comply with a customer's reasonable requests regarding its efforts to oppose a request. Detailed information is available in our Transparency Report and Google Cloud Government Requests Whitepaper.
Determining data subjects' rights and enabling exercise (including access, correction, erasure, export)	The customer should understand requirements around the rights of individuals related to the processing of their Customer Personal Data. These rights may include things such as access, correction, erasure, and export. Where the customer uses a third-party system, they should determine which (if any) parts of the system provide tools related to enabling individuals to exercise their rights (e.g., to access their data). Where the system provides such capabilities, the customer should utilize them as necessary.	As a Google Workspace for Education Administrator, you can use the Google Admin console to help you fulfill potential obligations related to Data Subject Requests (DSRs). Google Workspace for Education provides functions for both Google Workspace for Education admins and data subjects to access and export customer personal data from Google products directly. Google Workspace for Education admins can use the Data Export tool to export organization level data, and use Google Vault for targeted user-based searches and export. Data subjects (users) can use the Google Takeout interface to directly access and export customer personal data by themselves. For instructions, see the Google Workspace Data Subject Requests Guide.

Retention and deletion	The organization that processes PII should ensure that, based on the relevant jurisdiction, it disposes of PII after a specified period.	As an admin, Google will follow your instructions to delete the relevant Customer Data from Google's systems. Admins can manage user accounts through the Google Admin console, including deleting an account or removing customer personal data from mobile devices and products. If your organization is required to preserve data for a period of time, you can configure Vault to retain it even if users delete messages and files, and then empty their trash. For instructions on deletion settings, see the Google Workspace Data Subject Requests Guide. See our commitment for data deletion in section 6 (Data Deletion) of the Data Processing Amendment. Please check out Google Cloud Privacy Notice for the deletion and retention of service data.
Endpoint management	The customer should ensure that the use of mobile devices does not lead to a compromise of PII.	As an admin using Google endpoint management, you can make your organization's data more secure across your users' mobile devices, desktops, laptops, and other endpoints. With basic management, you can set up basic passcode enforcement, mobile reports, hijacking protection, remote account wipe, and device audits and alerts. With advanced management, you get additional security and privacy features such as strong password enforcement, the blocking of compromised devices, device approval, and more. For more details and to choose the proper device management version, see Compare mobile management features. See also Set up basic mobile device management and Set up advanced mobile management.