Valutazione di Impatto (DPIA) per "Google Workspace for Education Fundamentals"

Sommario

Contesto - Panoramica del trattamento

Quale è il trattamento in considerazione?

La didattica digitale integrata è intesa come metodologia innovativa di insegnamento-apprendimento.
Questa modalità didattica è complementare ed integrativa rispetto alla tradizionale esperienza di scuola in presenza e può diventare indispensabile nel caso di situazioni emergenziali e/o indicazioni ministeriali.
La progettazione della didattica in modalità digitale deve tenere conto del contesto e assicurare la sostenibilità delle attività proposte e un generale livello di inclusività, evitando che i contenuti e le metodologie siano la mera trasposizione di quanto solitamente viene svolto in presenza. La Didattica Digitale Integrata e l'insegnamento da remoto comportano la fruizione di processi formativi con l'utilizzo di strumentazione informatica (personal computer, tablet, smartphone) e di tecnologie online di condivisione e di cooperazione. L'utilizzo di meccanismi di condivisione e cooperazione con l'uso di tecnologie cloud, però, comporta rischi connessi al trattamento dei dati personali dei fruitori (alunni e docenti).
Google Workspace for Education Fundamentals (precedentemente Google Suite for Education) è un pacchetto di applicazioni che consente di interagire secondo modalità collaborative anche a distanza, a beneficio della didattica. In particolare:

- Google Classroom è un servizio che consente agli insegnanti di creare una classe virtuale per gestire la comunicazione, i materiali, i compiti e le scadenze con gli studenti, direttamente online.
- Google Drive è un servizio che consente di creare, archiviare, condividere e modificare documenti direttamente online, anche in modalità collaborativa e senza necessità che sul proprio computer sia installato alcun programma, semplicemente accedendo tramite il proprio account.
- Google Meet è un'applicazione di teleconferenza che permette di svolgere lezioni e riunioni da remoto.

Per poter utilizzare queste applicazioni ad ogni studente sarà assegnata una casella di posta Gmail con un indirizzo composto dal proprio cognome e nome seguito dal nome del dominio della scuola. Gli studenti potranno utilizzare le credenziali della casella di posta assegnata per accedere alla piattaforma di e-learning di istituto e alle numerose applicazioni web utili per la didattica.
Google Workspace for Education Fundamentals (che ha sostituito G Suite for Education) costituisce un insieme di strumenti flessibili e di facile utilizzo per l'apprendimento, la collaborazione (Classroom) e la comunicazione (Gmail e Google Meet). Questa suite permette all'Istituto di usufruire di strumenti didattici ormai praticamente essenziali senza che ci sia un esborso economico.

Quali sono le responsabilità connesse al trattamento?

Il **Titolare del Trattamento**, cioè l'Istituto Scolastico, rappresentato legalmente dal Dirigente Scolastico (D.S.) in carica, riveste un ruolo di supervisione e guida anche in questa materia. Ha il compito di definire le regole di comportamento per l'utilizzo della strumentazione elettronica e di

sorvegliare sulla sua attuazione. Il Titolare deve inoltre nominare i responsabili esterni che trattano dati personali per conto dell'Istituto ai sensi dell'art. 28, comma 3 del GDPR.

Docenti. Il loro ruolo centrale nella produzione di compiti e contenuti deve essere associato ad un loro controllo nei confronti di tutte quelle attività suscettibili di violazioni della privacy. I docenti sono responsabili della documentazione accessibile ai gruppi di lavoro e vigilano sul corretto svolgimento delle operazioni. A tal fine, il Titolare si impegna ad attribuire ai docenti il compito di supervisione sulle attività didattiche su piattaforma informatica e a fornire agli stessi indicazioni sulle modalità più opportune con cui trattare i dati personali, ai fini dell'art. 2-quaterdecies del D.Lgs. 196/2003 e dell'art. 4 del Regolamento UE 2016/679.

Il **Responsabile della Protezione dei Dati (RPD/DPO)** ha il compito di fornire supporto a titolare, docenti e interessati, per tutte quelle questioni concernenti la protezione dei dati personali all'interno dell'ambito di applicazione del trattamento.

Eventuali **amministratori di sistema**: nominati dal DS quali responsabili del trattamento relativamente alla gestione dei sistemi informatici, collaborano con il DPO e il DS nel fornire consulenze e pareri relativamente allo stato delle risorse informatiche dell'amministrazione.

Google Workspace si configura come un Responsabile Esterno del Trattamento. In virtù dell'accordo (Allegato n.1) che deve essere sottoscritto dall'Istituto si riconosce la conformità degli strumenti proposti dato che con la caduta del Privacy Shield (Sentenza della Corte di Giustizia dell'Unione Europea del 16 luglio 2020, c.d. Sentenza Schrems II), ovvero lo "scudo per la privacy" fra UE e USA (meccanismo di autocertificazione per le società stabilite negli USA che intendano ricevere dati personali dall'Unione europea) l'utilizzo dei dati da parte delle aziende americane deve essere regolamentato da certificazioni e accordi particolari. Nel corso del presente documento vengono analizzate le ricadute causate dalla sentenza della Corte di Giustizia dell'Unione Europea C-311/18 (c.d. sentenza Schrems II).
Si riconosce pertanto che Google Workspace offre garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate perché il trattamento soddisfi i requisiti del GDPR e garantisca la tutela dei diritti dell'interessato.
Particolare attenzione va posta nei confronti dei fornitori di servizi cloud, ove richiesti. Si ricorda inoltre che, sulla base di quanto previsto dalla circolare AGID n. 2 del 9 aprile 2018, le Pubbliche amministrazioni possono avvalersi esclusivamente di servizi cloud abilitati (la lista aggiornata può essere trovata sul sito dell'AGID). In proposito **Workspace di Google Cloud Italy Srl** risulta essere **qualificata** dal 27-11-2019 (rinnovo qualificazione il 19/01/2023) nella tipologia **SaaS** per la categoria: Servizi per la fiscalità, Servizi demografici, Servizi interni alle PA.

Ci sono standard applicabili al trattamento?

Non risultano standard, certificazioni o codici di condotta applicabili al trattamento in esame. L'European Data Protection Board (EDPD) ha pubblicato le "Raccomandazioni 01/2020 relative alle misure che integrano gli strumenti di trasferimento al fine di garantire il rispetto del livello di protezione dei dati personali dell'UE", che specificano i comportamenti da seguire riguardo al trasferimento di dati all'estero. Si evidenzia come con la caduta del Privacy Shield l'utilizzo dei dati da parte delle aziende americane deve essere regolamentato da accordi particolari come quello riportato all'Allegato 1.

Il Ministero dell'Istruzione ha pubblicato nell'estate del 2020 le Linee Guida per la Didattica Digitale Integrata (DDI), previste dal Piano per la ripresa della scuola e passate al vaglio del Consiglio Superiore della Pubblica Istruzione (Allegato 3). Il documento contiene indicazioni operative affinché ciascun Istituto scolastico possa dotarsi di un Piano scolastico per la didattica digitale integrata che dovrà essere allegato al Piano triennale per l'offerta formativa di ciascuna scuola. Dovranno essere coinvolte tutte le componenti della comunità scolastica fornendo apposita comunicazione a docenti, famiglie e studenti sui suoi contenuti.
Pur trattandosi di un provvedimento frutto di una situazione emergenziale si ritiene che mantenga la sua valenza in considerazione della necessaria innovazione che rappresenta per la didattica.
Si ricorda inoltre che, sulla base di quanto previsto dalla circolare AGID n. 2 del 9 aprile 2018, le Pubbliche amministrazioni possono avvalersi esclusivamente di servizi cloud abilitati (la lista aggiornata può essere trovata sul sito dell'AGID). In proposito Workspace di Google Cloud Italy Srl risulta essere qualificata dal 27-11-2019 nella tipologia SaaS per la categoria: Servizi per la fiscalità, Servizi demografici, Servizi interni alle PA.
La presente DPIA viene redatta a trattamento già iniziato. L'adozione della suite con i servizi per la scuola offerti gratuitamente da Google infatti è stata un passaggio necessario per poter garantire il mantenimento di una attività didattica nel periodo emergenziale dovuto al Covid_19.
Si tenga presente anche quanto affermato dal Gruppo di lavoro congiunto Ministero dell'istruzione-Ufficio del Garante per la protezione dei dati personali, di cui al Decreto del Capo di Gabinetto prot. n. 1885 del 5 giugno 2020, nel documento "Didattica Digitale Integrata e tutela della privacy: indicazioni generali" del settembre 2020 (Allegato 7) con il fine di fornire alle istituzioni scolastiche linee di indirizzo comuni e principi generali per l'implementazione della DDI con particolare riguardo agli aspetti inerenti alla sicurezza in rete e alla tutela dei dati personali. Si veda anche il Provvedimento del 26 marzo 2020 - "Didattica a distanza: prime indicazioni" del Garante per la Privacy (Allegato 6).
In ossequio a quanto affermato da Garante e Ministero quindi in piena pandemia non è stato necessario procedere alla valutazione di impatto, ex art. 35 del GDPR, considerato che l'Istituto non effettua trattamenti di dati personali su larga scala nell'ambito dell'utilizzo del servizio on line di videoconferenza (Google Meet) nè la piattaforma Google Workspace consente il monitoraggio sistematico degli utenti. Non si ricorre comunque a nuove soluzioni tecnologiche particolarmente invasive (quali, tra le altre, quelle che comportano nuove forme di utilizzo dei dati di geolocalizzazione o biometrici).
L'Istituto ha provveduto comunque ad adottare documentazione (PDDI, regolamento, informative e guide) e le procedure volte a minimizzare i rischi per i dati personali dei soggetti interessati.

Dati, processi e risorse di supporto

Quali sono i dati trattati?

Google Workspace utilizza tecnologie cloud e deve quindi contenere le informazioni necessarie per identificare univocamente alunni, docenti ed eventuali altri soggetti interessati.
Per creare l'account l'Istituto fornirà nome, indirizzo email e la password dello studente. Quando uno studente utilizza i servizi di Google, quest'ultimo potrebbe raccogliere anche le informazioni basate sull'utilizzo di tali servizi, tra cui:

- informazioni sul dispositivo, ad esempio modello di hardware, versione del sistema operativo, identificatori univoci del dispositivo e informazioni relative alla rete mobile, incluso il numero di telefono (funzione disabilitata attraverso il pannello amministrativo dall'Istituto);
- informazioni di log, tra cui dettagli di come un utente ha utilizzato i servizi Google, informazioni sugli eventi del dispositivo e indirizzo IP (protocollo Internet) dell'utente (funzione disabilitata attraverso il pannello amministrativo dall'Istituto);
- informazioni sulla posizione ricavate tramite varie tecnologie, tra cui l'indirizzo IP, GPS e altri sensori (funzione disabilitata attraverso il pannello amministrativo dall'Istituto);
- numeri specifici delle applicazioni, come il numero di versione dell'applicazione; infine cookie o tecnologie analoghe utilizzate per acquisire e memorizzare le informazioni relative a un browser o dispositivo, come la lingua preferita e altre impostazioni.

Si veda in merito l'Informativa predisposta da Google (Allegato 2).

Inoltre tutta una serie di dati e informazioni prodotti da alunni e docenti nel corso dell'attività didattica potrebbero essere condivisi tra le diverse parti in causa. Tutti i soggetti devono quindi essere sensibilizzati perchè sia limitata la presenza di dati particolari, siano minimizzati i dati personali e sia evidenziato che i dati presenti nella piattaforma potranno essere oggetto di valutazione scolastica.

Periodo di conservazione: i dati di registrazione dell'account saranno trattati per la durata del corso di studi nel caso degli alunni e per la durata del contratto per i dipendenti dell'Istituto.
I dati personali raccolti in quanto parte dell'attività didattica (elaborati, registrazioni video, compiti, ecc.) saranno conservati in base ai tempi stabiliti per questo genere di attività.

Tutto il materiale prodotto dagli studenti viene conservato per la sola durata dell'anno scolastico. Esclusivamente per le prove valutative, la Circolare n° 44 del 19/12/2005 della Direzione Generale per gli archivi - "Archivi delle Istituzioni Scolastiche" prescrive la conservazione di elaborati delle prove scritte, grafiche e pratiche per almeno un anno, e la conservazione di documentazione campione un anno ogni dieci.
È possibile consultare i periodi di conservazione dei dati di Google (incluso il tempo necessario per eliminare le proprie informazioni) al link: https://policies.google.com/technologies/retention?hl=it

Qual è il ciclo di vita del trattamento dei dati (descrizione funzionale)?

Gli account Google Workspace for Education vengono creati e gestiti dall'Istituto Scolastico e destinati all'utilizzo da parte di studenti e docenti per lo svolgimento dell'attività didattica.
Saranno mantenuti attivi per la durata del corso di studi dell'alunno/a o nel caso dei docenti per la durata del rapporto di dipendenza/servizio.
Durante l'anno scolastico i servizi forniti da Google Workspace saranno utilizzati per svolgere le attività didattiche e affidare agli studenti esercitazioni e verifiche, che possono comportare la produzione di materiali/documenti/registrazioni contenenti dati personali. Tale materiale verrà conservato su server cloud e condiviso tra i vari membri della classe e/o del gruppo di lavoro. Alla fine della produzione dello stesso, si potrà procedere all'archiviazione del materiale da parte dei docenti interessati, che lo utilizzeranno anche per esprimere le loro valutazioni. Pertanto, la documentazione ottenuta si profila quale atto amministrativo endoprocedimentale e sarà compito del docente procedere all'archiviazione dei documenti nel momento in cui non sia più necessaria alcuna modifica da parte degli alunni. L'archiviazione dovrà essere effettuata in modo tale da rendere non accessibile la documentazione agli interessati, che potranno averne accesso o richiederne la modifica, rettifica o cancellazione solamente tramite richiesta scritta che non limiti le finalità istituzionali del trattamento, orientate al corretto svolgimento dell'attività didattica.
Per quanto riguarda la cancellazione dei dati, la Circolare n° 44 del 19/12/2005 della Direzione Generale per gli archivi - "Archivi delle Istituzioni Scolastiche" prescrive la conservazione di elaborati delle prove scritte, grafiche e pratiche per almeno un anno, e la conservazione di documentazione campione un anno ogni dieci (comunque la conservazione dei documenti sul cloud non supera l'anno scolastico, i dati in questione vengono scaricati e mantenuti all'interno della struttura scolastica).

Quali sono le risorse di supporto ai dati?

I servizi di Google Workspace possono essere utilizzati dagli interessati tramite vari tipi strumentazione informatica privata (tablet, pc e smartphone) che a loro volta possono essere basati su diversi sistemi operativi e permettere la fruizione dei servizi tramite diversi browser o applicazioni.
I servizi di Google Workspace sono servizi cloud. I server potrebbero trovarsi al di fuori dell'Unione Europea.

Principi Fondamentali

Proporzionalità e necessità

Gli scopi del trattamento sono specifici, espliciti e legittimi?

Ferma restando la dovuta predilezione per le attività scolastiche svolte in presenza, come affermato anche dal DL 11/2021 sulla scorta di quanto sostenuto dal Comitato Tecnico Scientifico nel verbale n. 34 del 12/07/2021, resta la necessità di sviluppare anche la Didattica Digitale Integrata con strumentazione e metodologie idonee in ossequio al Piano Nazionale per la Scuola Digitale, pilastro fondamentale della cd Buona Scuola (legge 107/2015). Le istituzioni scolastiche devono promuovere, all'interno dei Piani Triennali dell'Offerta Formativa e in collaborazione con il Ministero, azioni coerenti con le finalità, i principi e gli strumenti previsti nel PNSD (L. 107/2015, art. 1, commi 56 e 57 in particolare). Il PTOF dell'Istituto rappresenta quindi uno strumento importante per mettere a sistema le finalità, i principi e gli strumenti previsti nel PNSD.
Il Piano scolastico per la didattica digitale integrata deve essere approvato dal Collegio Docenti e indicare criteri e modalità di erogazione dell'attività scolastica, in modo integrato tra la consueta attività didattica in presenza e le attività didattiche a distanza, anche attraverso l'utilizzo degli strumenti digitali e in particolare di Google Workspace.

Quali sono le basi legali che rendono lecito il trattamento?

Come chiarito dal Garante nel Provvedimento del 26 marzo 2020, n. 64 (doc web n. 9300784 "Didattica a distanza: prime indicazioni"), in relazione alla attività di DDI, il trattamento dei dati personali da parte delle istituzioni scolastiche è necessario in quanto collegato all'esecuzione di un compito di interesse pubblico di cui è investita la scuola attraverso una modalità operativa prevista dalla normativa, con particolare riguardo anche alla gestione della fase di emergenza epidemiologica.
Il consenso dei genitori, che non costituisce una base giuridica idonea per il trattamento dei dati in ambito pubblico e nel contesto del rapporto di lavoro, non è richiesto perché l'attività svolta, sia pure in ambiente virtuale, rientra tra le attività istituzionalmente assegnate all'istituzione scolastica, ovvero di didattica nell'ambito degli ordinamenti scolastici vigenti. Pertanto, l'Istituto è legittimato a trattare tutti i dati personali necessari al perseguimento delle finalità collegate allo svolgimento della DDI nel rispetto dei principi previsti dalla normativa di settore. In base alle disposizioni contenute negli artt. 13 e 14 del Regolamento UE 2016/679, l'Istituto si preoccupa di informare gli interessati in merito ai trattamenti dei dati personali effettuati nell'ambito dell'erogazione dell'offerta formativa. Poiché attraverso l'utilizzo della piattaforma per l'erogazione della DDI sono trattati sia dati degli studenti che dei docenti e, in taluni casi, anche dei genitori, la Scuola fornisce a tutte queste categorie di interessati, di regola all'inizio dell'anno scolastico, anche nell'ambito di una specifica sezione dell'informativa generale o in un documento autonomo, tutte le informazioni relative a tali trattamenti.
La Scuola ha redatto un proprio Piano per la Didattica Digitale Integrata e adottato un Regolamento approvato dal Collegio Docenti e dal Consiglio d'Istituto sulla base anche delle "Linee guida per la Didattica digitale integrata" del Miur (Decreto del 6 agosto 2020) e del Piano Nazionale per la Scuola Digitale, parte integrante della legge 107/2015 (cd Buona Scuola).

I dati raccolti sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati (minimizzazione dei dati)?

La segreteria dell'Istituto crea gli account Google utilizzando i dati minimi necessari e si occupa della loro eliminazione al termine del ciclo di studi o del contratto di servizio per quanto riguarda i dipendenti.
L'Istituto deve predisporre le proprie informative in materia di trattamento dati personali e dare evidenza di quelle di Google Workspace per poter sensibilizzare al massimo gli interessati in merito alla pubblicazione e condivisione di dati personali. Tutti i soggetti coinvolti nell'attività didattica sono tenuti al rispetto del Piano scolastico per la DDI e al Regolamento.

I dati sono esatti e aggiornati?

La segreteria dell'Istituto garantisce massima attenzione nel caricamento dei dati di studenti e docenti.
I dati personali contenuti nel materiale prodotto durante l'attività didattica corrispondono a quanto caricatom dagli interessati, fatte salve modifiche, volute o accidentali, intervenute nei processi di collaborazione o condivisione dei documenti.

Qual è il periodo di conservazione dei dati?

I dati utilizzati per la creazione dell'account sono conservati per la durata del corso di studi nel caso degli alunni e per la durata del contratto di servizio/dipendenza nel caso dei docenti.
La conservazione dei dati relativi all'attività didattica è necessaria per un periodo strettamente necessario allo svolgimento dell'attività formativa. I dati verranno poi archiviati dal docente (anche attraverso una apposita funzionalità proposta dal servizio, ove presente), e la documentazione prodotta verrà resa inaccessibile agli interessati, salvo richiesta scritta di accesso o cancellazione degli interessati.
Nel caso in cui gli elaborati debbano essere oggetto di valutazione, l'archiviazione deve essere mantenuta per almeno un anno dalla produzione, a meno che non ci si trovi nei casi particolari previsti dalla Circolare n° 44 del 19/12/2005 della Direzione Generale per gli archivi - "Archivi delle Istituzioni Scolastiche" che prescrive la conservazione di documentazione campione un anno ogni dieci. Bisogna distinguere i due casi:

- dati ed elaborati non soggetti a valutazione: non hanno necessità di essere conservati per eventuali verifiche o controlli per cui devono essere cancellati nel momento in cui termina l'attività formativa svolta. Di norma tali dati vanno cancellati alla fine dell'anno scolastico a meno che l'attività programmata si svolga su più anni scolastici ed è necessario per essa operare qualche forma di trattamento anche sui dati raccolti gli anni precedenti;
- dati ed elaborati soggetti a valutazione: i dati verranno scaricati e conservati presso la struttura scolastica con le stesse modalità della didattica tradizionale.

Misure a tutela dei diritti degli interessati

Come sono informati del trattamento gli interessati?

Gli interessati vengono informati del trattamento precedentemente all'inizio dello stesso, tramite

somministrazione di informativa ex Art. 13 del Reg. UE 206/679. L'informativa deve essere somministrata a docenti, alunni e genitori degli stessi tramite registro elettronico o altra modalità ritenuta idonea.
L'Istituto darà massima evidenza tramite pubblicazione sul proprio sito istituzionale (possibilmente in una sezione dedicata) anche delle informative prodotte da Google in merito ai prodotti/servizi adottati, del Piano scolastico e del Regolamento di Didattica Digitale Integrata.

Ove applicabile: come si ottiene il consenso degli interessati?

Il consenso non costituisce una base giuridica idonea per il trattamento dei dati e quindi non è richiesto perché l'attività didattica svolta, sia pure in ambiente virtuale, rientra tra le finalità istituzionali della Scuola.

Come fanno gli interessati a esercitare i loro diritti di accesso e di portabilità dei dati?

Gli interessati possono sempre rivolgersi ai contatti presenti nell'informativa per l'esercizio dei propri diritti.

Come fanno gli interessati a esercitare i loro diritti di rettifica e di cancellazione (diritto all'oblio)?

Gli interessati possono sempre rivolgersi ai contatti presenti nell'informativa per l'esercizio dei propri diritti.

Come fanno gli interessati a esercitare i loro diritti di limitazione e di opposizione?

Gli interessati possono sempre rivolgersi ai contatti presenti nell'informativa per l'esercizio dei propri diritti.

Gli obblighi dei responsabili del trattamento sono definiti con chiarezza e disciplinati da un contratto?

Google Workspace si configura come un Responsabile Esterno del Trattamento in virtù dell'accordo (Allegato n.1) che deve essere sottoscritto dall'Istituto. Si riconosce la conformità degli strumenti proposti dato che con la caduta del Privacy Shield, ovvero lo "scudo per la privacy" fra UE e USA (meccanismo di autocertificazione per le società stabilite negli USA che intendano ricevere dati personali dall'Unione europea) l'utilizzo dei dati da parte delle aziende americane deve essere regolamentato da certificazioni e accordi particolari. Si riconosce pertanto che Google Workspace offre garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate perché il trattamento soddisfi i requisiti del GDPR e garantisca la tutela dei diritti dell'interessato.
Il contratto d'uso di Google Workspace, visualizzato e accettato in forma elettronica, descrive l'ambito delle rispettive responsabilità e specifica gli obblighi per le parti.

In caso di trasferimento di dati al di fuori dell'Unione europea, i dati godono di una protezione equivalente?

I servizi previsti si basano sull'uso di server che possono anche essere localizzati in territori extra Unione Europea. Questo fatto ha delle criticità in relazione alla sentenza C.311/18 (Schrems II) con la quale la Corte di Giustizia ha dichiarato l'invalidità della decisione di adeguatezza Privacy Shield e che ha indotto Google stessa ad individuare nelle clausole contrattuali standard la base legale del

trattamento. Cadendo quindi la valutazione di conformità a priori garantita dal Privacy Schield l'Istituto è consapevole che deve verificare che le clausole contrattuali costituiscano una garanzia sufficiente per la tipologia di dati trattati.
Dall'analisi condotta, riteniamo di poter affermare che il livello di protezione garantito è adeguato alla tipologia dei dati trattati limitata a quelli strettamente necessari al perseguimento delle finalità didattiche.
Si precisa che a seguito della sentenza Schrems II, intervenuta a luglio del 2020, l'Istituto scolastico ha valutato le possibili alternative all'uso della piattaforma Google G Suite (oggi Workspace for Education Fundamentals) adottata per garantire la didattica in periodo emergenziale in attuazione del dpcm dell'8 marzo 2020.
Le possibilità attualmente disponibili però non permettono di garantire gli stessi servizi (creazione di caselle mail illimitate, drive illimitato, ecc.) offerti da Google Worspace for Education Fundamentals alle stesse condizioni economiche.

Rischi: Misure esistenti o pianificate

Crittografia

I dati sono trattati tramite l'utilizzo di meccanismi di conservazione e comunicazione cifrati, ai fini di garantire la minimizzazione del rischio di acceso agli stessi.

Controllo degli accessi logici

L'accesso alle funzionalità della piattaforma Google Workspace for Education Fundamentals deve essere regolato da un sistema di attivazione di account con permessi specifici, protetti da password, attivabili e disattivabili dall'amministratore del software (il D.S. o un suo delegato).

Archiviazione

Tutta la documentazione relativa all'attività Istituzionale dell'Amministrazione è regolata dalla normativa vigente in materia di archiviazione nella pubblica amministrazione, contenente indicazioni specifiche per la pubblica istruzione.

Minimizzazione dei dati

I dati vengono trattati e archiviati in forma minima, per quanto previsto dalla normativa vigente. I dati sensibili devono essere limitati a quelli strettamente necessari.

Lotta contro il malware

Il sistema scolastico è protetto da malware con modalità di protezione sia hardware che software (firewall e antivirus). Si ritiene opportuno fornire agli utilizzatori (docenti e alunni) delle linee guida sull'utilizzo sicuro delle risorse elettroniche e digitali, che includano le istruzioni per una efficace lotta al malware.

Backup

I sistemi di didattica da remoto utilizzati per il trattamento devono essere provvisti di una modalità di backup.

Manutenzione

Viene effettuata regolare manutenzione dei sistemi hardware scolastici. Il responsabile del trattamento garantisce inoltre il corretto funzionamento del software cloud di didattica da remoto. Si ritiene opportuno fornire agli utilizzatori (docenti e alunni) delle linee guida sull'utilizzo sicuro delle risorse elettroniche e digitali.

Contratto con il responsabile del trattamento

I responsabili del trattamento vengono nominati tali tramite la stipula di un contratto, ai sensi degli artt. 28 e 29 del Reg. Ue 679/2016.

Politica di tutela della privacy

L'Istituto, in collaborazione con il DPO, ha messo in atto una serie di misure orientate all'adeguamento della stessa alla normativa vigente. I dipendenti sono stati autorizzati al trattamento ai sensi dell'Art. 2- quaterdecies del D.Lgs. 196/2003, per l'esercizio delle loro funzioni.

Gestire gli incidenti di sicurezza e le violazioni dei dati personali

L'Istituto ha adottato una procedura per la gestione dei Data Breach.

Gestione del personale

Formazione specifica degli interessati. Gli interessati devono essere informati e istruiti riguardo alle modalità di utilizzo dei software per limitare i rischi per la sicurezza e la privacy.

Rischio - Accesso illegittimo ai dati

Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare?

Furto d'identità, Reati informatici, Uso improprio di dati personali, Ripercussioni sulla Didattica, Violazione di Norma di Legge, Danno Reputazionale, Richieste di Risarcimento

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Mancata formazione, Sottovalutazione del Rischio, Comportamento negligente, Attività Fraudolenta

Quali sono le fonti di rischio?

Virus informatici, Attacchi Hacker, Errore umano, Malfunzionamento, Incidente/sinistro, Interruzione alimentazione elettrica

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Crittografia, Minimizzazione dei dati, Politica di tutela della privacy, Lotta contro il malware, Controllo degli accessi logici, Backup, Archiviazione, Manutenzione, Gestione del personale, Contratto con il responsabile del trattamento, Gestire gli incidenti di sicurezza e le violazioni dei dati personali

Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?

Trascurabile, Trascurabile per quanto concerne il trattamento dati di docenti e alunni. Limitato per quanto concerne i dati dell'utente amministratore della piattaforma.

Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

Limitata, Essendo la maggior parte degli utenti costituita da minorenni si ritiene essere possibile che si concretizzino delle minacce ai dati personali dello studente in questione per mancata consapevolezza.

Rischio - Modifiche indesiderate dei dati

Quali sarebbero i principali impatti sugli interessati se il rischio si dovesse concretizzare?

Uso improprio di dati personali, Valutazioni Errate, Ripercussioni sulla Didattica, Danno Reputazionale

Quali sono le principali minacce che potrebbero consentire la concretizzazione del rischio?

Comportamento negligente, Mancata formazione, Sottovalutazione del Rischio

Quali sono le fonti di rischio?

Errore umano, Malfunzionamento, Incidente/sinistro, Attacchi Hacker

Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?

Crittografia, Minimizzazione dei dati, Backup, Gestione del personale, Politica di tutela della privacy, Controllo degli accessi logici

Come stimereste la gravità del rischio, in particolare alla luce degli impatti potenziali e delle misure pianificate?

Trascurabile, Trascurabile per quanto concerne il trattamento dati di docenti e alunni. Limitato per quanto concerne i dati dell'utente amministratore della piattaforma.

Come stimereste la probabilità del rischio, specialmente con riguardo a minacce, fonti di rischio e misure pianificate?

Trascurabile, Essendo la maggior parte degli utenti costituita da minorenni si ritiene essere possibile che si concretizzino delle minacce ai dati personali dello studente in questione per mancata consapevolezza.

Rischio - Perdita di dati

Quali potrebbero essere gli impatti principali sugli interessati se il rischio dovesse concretizzarsi?

Ripercussioni sulla Didattica, Valutazioni Errate, Danno Reputazionale

Quali sono le principali minacce che potrebbero consentire la materializzazione del rischio?

Sottovalutazione del Rischio, Mancata formazione, Comportamento negligente, Attività Fraudolenta

Quali sono le fonti di rischio?

Attacchi Hacker, Incidente/sinistro, Errore umano, Virus informatici, Malfunzionamento, Interruzione alimentazione elettrica

Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?

Backup, Archiviazione, Crittografia, Minimizzazione dei dati, Gestire gli incidenti di sicurezza e le violazioni dei dati personali, Politica di tutela della privacy, Controllo degli accessi logici, Lotta contro il malware, Manutenzione, Contratto con il responsabile del trattamento, Gestione del personale

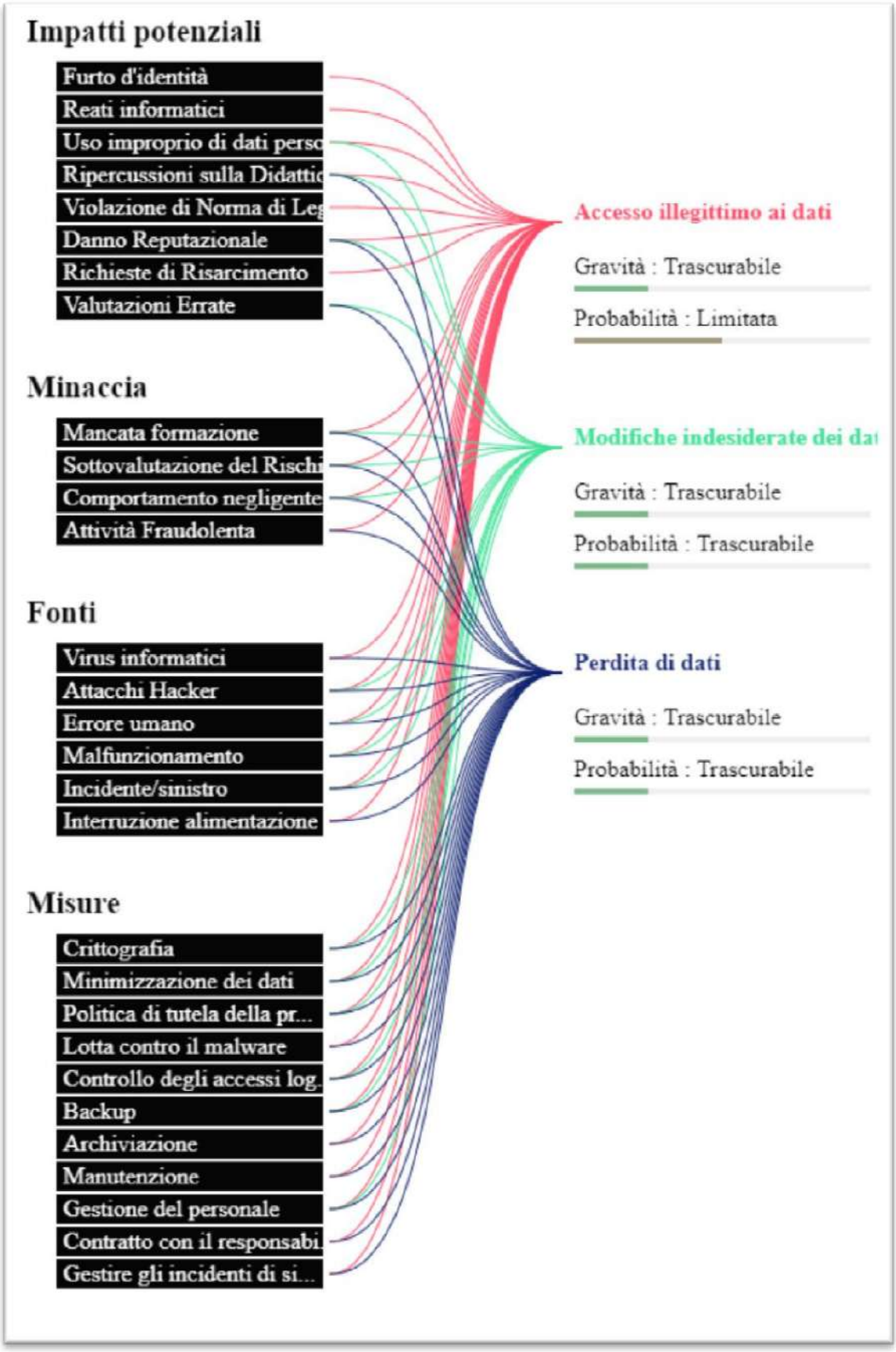
Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?

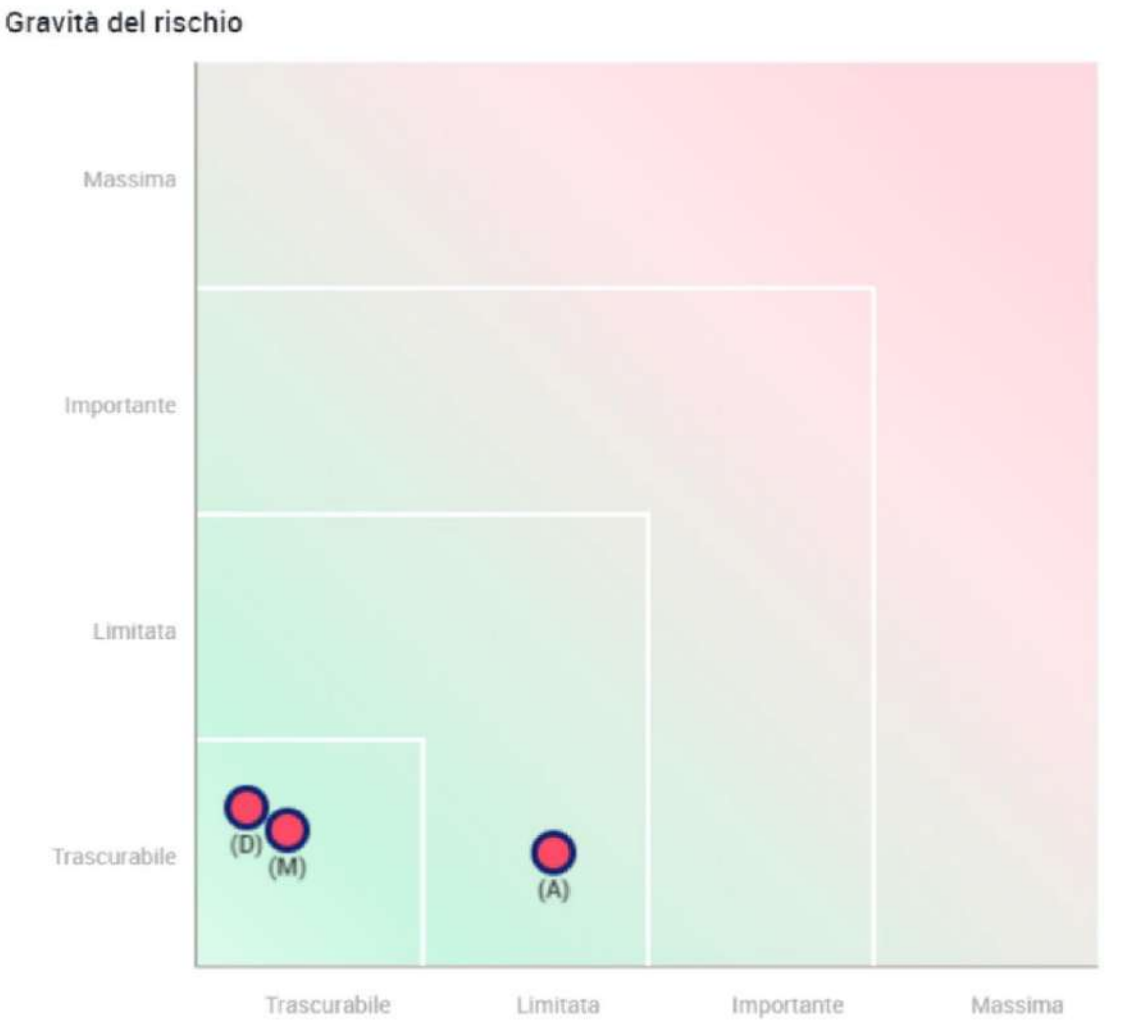
Trascurabile, Trascurabile per quanto riguarda il caricamento dei dati relativi alla didattica. Limitato per quanto concerne le prove valutative che comunque vengono scaricate ed archiviate su server locale.

Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

Trascurabile, Le misure messe in campo e l'utilizzo di un software cloud minimizzano il rischio di perdita di dati.

Rischi - Panoramica dei rischi





- Misure pianificate o esistenti
- Con le misure correttive implementate
- (A)ccesso illegittimo ai dati
- (M)odifiche indesiderate dei dati
- (P)erdita di dati

Elenco Allegati

- Allegato 1 – Contratto Google Workspace & Termini di servizio di Google Workspace
- Allegato 2 – Informativa Google Workspace
- Allegato 3 – Linee guida per la Didattica Digitale Integrata (DDI)
- Allegato 4 – Google Workspace for Education data protection implementation guide
- Allegato 5 – Garante Privacy: FAQ sulla sentenza Schrems II
- Allegato 6 – Provvedimento del 26 marzo 2020 - "Didattica a distanza: prime indicazioni" [9300784]
- Allegato 7 – DDI e tutela della privacy: indicazioni generali

https://workspace.google.it/intl/it/terms/2013/1/premier_terms.html

https://workspace.google.com/intl/en/terms/additional_services.html

https://workspace.google.com/terms/premier_terms.html

Contratto Google Workspace (Online)

Consultare i Termini aggiuntivi per i servizi disponibili con la nuova infrastruttura per gli account.

Il presente Contratto Google Workspace (online) (il "Contratto") viene stipulato tra Google e la persona giuridica che accetta i termini riportati nel presente documento (il "Cliente"). "Google" indica (i) Google Voice Canada Corporation, con sede all'indirizzo 44 Chipman Hill, Suite 1000, Saint John, New Brunswick E2L 2A9 Canada, limitatamente ai servizi di Google Voice per i quali l'indirizzo di fatturazione del Cliente è in Canada, e (ii) Google LLC, con sede all'indirizzo 1600 Amphitheatre Parkway, Mountain View, California 94043, USA, per tutti gli altri servizi Google Workspace. Il presente Contratto entrerà in vigore nella data in cui il Cliente farà clic sul pulsante "Accetto" visualizzato di seguito o, se applicabile, nella data in cui il Contratto verrà controfirmato ("Data di validità"). Se l'accettazione avviene per conto del proprio datore di lavoro o di un'altra persona giuridica, si dichiara e garantisce: (i) di avere la piena autorità legale di vincolare il proprio datore di lavoro o la persona giuridica applicabile ai presenti termini; (ii) di avere letto e compreso il presente Contratto e (iii) di accettare il presente Contratto per conto della parte rappresentata. Se non si dispone dell'autorità legale a vincolare il proprio datore di lavoro o l'entità applicabile, non fare clic sul pulsante "Accetto" riportato di seguito (o, secondo il caso, non firmare il presente Contratto). Il presente Contratto disciplina l'accesso ai Servizi, così come ordinati mediante l'apposito Modulo d'ordine, e l'utilizzo degli stessi da parte del Cliente.

- 1. **Servizi**. Google fornirà i Servizi ordinati nell'apposito Modulo d'ordine in conformità allo SLA (accordo sul livello del servizio) vigente. Il Cliente può utilizzare i Servizi ordinati nell'apposito Modulo d'ordine in conformità al presente Contratto
    - 1.1 **Risorse e trasferimento dei dati**. Tutte le strutture utilizzate per archiviare ed elaborare i Dati del cliente rispetteranno standard di sicurezza ragionevoli, non inferiori a quelli adottati nelle strutture in cui Google archivia ed elabora informazioni di tipo analogo di sua proprietà. Nell'ambito della fornitura dei Servizi, Google potrà trasferire, archiviare e trattare i Dati del Cliente negli Stati Uniti o in qualsiasi altro paese in cui operino Google o i suoi agenti. Mediante l'utilizzo dei Servizi, il Cliente acconsente al trasferimento, al trattamento e all'archiviazione dei propri dati.
    - 1.2 **Nessun annuncio**. In deroga a qualsiasi altro termine del presente Contratto, Google non tratterà i Dati del Cliente a scopi pubblicitari né pubblicherà Annunci pubblicitari nei Servizi.
    - 1.3 **Nuovi servizi o funzioni**. Di tanto in tanto Google potrà rendere disponibili per i Servizi nuove applicazioni, funzioni o funzionalità il cui utilizzo potrebbe dipendere dall'accettazione di termini aggiuntivi da parte del Cliente.

- 1.4 **Verifica preliminare all'uso dei Servizi**. Per poter utilizzare i Servizi, il Cliente deve verificare un Indirizzo email di dominio o un Nome di dominio. Se il Cliente non dispone di un'autorizzazione valida all'utilizzo dell'Indirizzo email di dominio o non possiede o non controlla il Nome di dominio, Google non sarà tenuta a fornire i Servizi al Cliente e potrà eliminare l'Account senza preavviso.
- 1.5 **Termini di servizio specifici**. I Termini di servizio specifici sono incorporati nel Contratto mediante questo riferimento.

- 2. **Modifiche**.
  - 2.1 **Modifiche ai Servizi**.
    - (a) **Norme sul ritiro**. Google notificherà il Cliente almeno 12 mesi prima di una Cessazione rilevante salvo qualora stabilisca ragionevolmente che: (a) non è autorizzata a farlo in base a disposizioni di legge o norme contrattuali (ivi incluso in caso di modifica a tali leggi o contratti vigenti) o (b) se continua a fornire il Servizio soggetto a Cessazione rilevante si potrebbe creare un (i) rischio per la sicurezza o (ii) un impegno economico o tecnico sostanziale.
    - (b) **(Altre modifiche)**. Fatto salvo quanto indicato nella Sezione 2.1(a) (Norme sul ritiro), Google potrà apportare ai Servizi modifiche che possono includere l'aggiunta, l'aggiornamento o l'interruzione di qualsiasi Servizio o porzione di una o più funzioni dei Servizi. Google invierà una notifica al Cliente in caso di qualsiasi modifica sostanziale ai Servizi principali.
  - 2.2 **Modifiche ai Termini URL.**
    - (a) **Cambiamenti nei Termini URL**. Google può modificare i Termini URL, fatto salvo quanto previsto nella Sezione 2.2(d) (Obiezioni alle modifiche).
    - (b) **Notifica di modifiche sostanziali**. Google invierà una notifica al Cliente in caso di qualsiasi modifica sostanziale ai Termini URL.
    - (c) **Quando diventano effettive le modifiche**. Le modifiche sostanziali ai Termini URL avranno decorrenza da 30 giorni dopo la notifica, con le seguenti eccezioni: (i) le modifiche negative sostanziali allo SLA entreranno in vigore 90 giorni dopo la notifica e (ii) le modifiche applicabili a nuovi Servizi o funzionalità avranno effetto immediato.
    - (d) **Obiezioni alle modifiche**. Salvo se la modifica apportata da Google ai Termini URL sia richiesta da un tribunale, da un ordine giudiziario o amministrativo emesso dall'autorità competente o dalla legge vigente o si applichi a nuovi Servizi o Funzionalità, si applica quanto segue:
      - (i) Se una modifica ai Termini URL ha un effetto negativo sostanziale sul Cliente, il Cliente potrà opporsi a tale modifica inviando una notifica a Google entro i 30 giorni successivi all'invio della notifica da parte di Google.
      - (ii) Se il Cliente invia una notifica a Google secondo le modalità previste, continuerà a essere soggetto ai Termini URL vigenti immediatamente prima della modifica fino all'evento che si verifica per primo tra: (A) fine del Periodo di validità dell'ordine al momento in vigore o (B) 12 mesi dopo la notifica.

- 3. **Obbligazioni del Cliente**.
    - 3.1 **Conformità**. Il Cliente è tenuto a (a) garantire che il proprio utilizzo dei Servizi (incluso l'utilizzo da parte dei propri Utenti finali) e ogni accesso ai Dati del Cliente da parte propria e dei propri Utenti finali, nonché l'utilizzo degli stessi, rispettino le disposizioni del presente Contratto e tutti i termini o le norme contrattuali vigenti, incluso qualsiasi contratto di lavoro o norme del datore di lavoro riguardanti l'utilizzo della tecnologia, la sicurezza o la riservatezza; (b) compiere ogni sforzo commercialmente ragionevole per evitare qualsiasi accesso o uso non autorizzato dei Servizi e (c) informare tempestivamente Google di qualsiasi utilizzo o accesso non autorizzato ai Servizi di cui il Cliente venga a conoscenza.
    - 3.2 **Prodotti aggiuntivi**. Google mette a disposizione del Cliente e dei suoi Utenti finali Prodotti aggiuntivi facoltativi. L'utilizzo dei Prodotti aggiuntivi è soggetto ai Termini per i Prodotti aggiuntivi.
    - 3.3 **Amministrazione dei Servizi**.
        - (a) **Console di amministrazione**. Google fornirà al Cliente l'accesso alla Console di amministrazione affinché l'Amministratore possa gestire il relativo utilizzo dei Servizi (nonché l'utilizzo dei Servizi da parte degli Utenti finali, secondo il caso). Il Cliente può utilizzare la Console di amministrazione per specificare uno o più Amministratori che avranno diritti di accesso agli Account amministrativi. È responsabilità del Cliente: (a) mantenere la riservatezza e la sicurezza degli Account utente finale e delle password associate e (b) qualsiasi utilizzo degli Account utente finale. Il Cliente concorda sul fatto che le responsabilità di Google non includono la gestione o l'amministrazione interna dei Servizi per il Cliente o per qualsiasi Utente finale.
        - (b) **Accesso come Amministratore agli Account utente finale**. L'Amministratore potrà accedere a, monitorare, utilizzare, modificare, trattenere o divulgare i Dati del Cliente associati a qualsiasi Account utente finale e controllare l'accesso dell'Utente finale ai Servizi. Un Amministratore potrebbe inoltre avere facoltà di: (i) controllare le impostazioni account degli Account utente finale (inclusa la modifica delle password degli Account utente finale) e (ii) rimuovere o disattivare qualsiasi Servizio o Prodotto aggiuntivo o altro servizio/prodotto attivato o installato utilizzando l'Account utente finale. L'utilizzo dei Prodotti aggiuntivi o di altri servizi/prodotti con gli Account utente finale è a rischio e pericolo del Cliente.
        - (c) **Rivenditore come Amministratore**. Se il Cliente ordina i Servizi tramite un Rivenditore, quest'ultimo potrà, a discrezione del Cliente, avere accesso all'Account del Cliente e agli Account utente finale del Cliente. Per quanto riguarda i rapporti tra Google e il Cliente, quest'ultimo è il solo e unico responsabile: (i) di qualsiasi accesso da parte del Rivenditore all'Account del Cliente o agli Account utente finale del Cliente e (ii) della definizione nel Contratto per i rivenditori di qualsiasi obbligo o diritto tra il Rivenditore e il Cliente in merito ai Servizi.
        - (d) **Consensi**. Il Cliente è tenuto a ottenere e mantenere tutti i consensi necessari che permettono: (i) l'utilizzo dei Servizi da parte del Cliente e, se applicabile, dei suoi Utenti finali e (ii) l'accesso, l'archiviazione e il trattamento dei Dati del Cliente ai sensi del presente Contratto.

- 3.4 **Restrizioni d'uso**. Il Cliente non metterà in atto e non consentirà a Utenti finali o terze parti soggetti al suo controllo di mettere in atto nulla di quanto segue: (a) copiare, modificare, creare opere derivate, decodificare, decompilare, tradurre, disassemblare o tentare in altro modo di estrarre qualunque parte del codice sorgente dei Servizi (tranne quando tale restrizione sia espressamente vietata dalle leggi vigenti); (b) concedere in licenza, trasferire o distribuire alcuno dei Servizi; (c) vendere, rivendere o rendere disponibili in altro modo i Servizi a una terza parte nell'ambito di un'offerta commerciale priva di un valore sostanziale indipendente dai Servizi o (d) accedere o utilizzare i Servizi: (i) per Attività ad alto rischio; (ii) in modo mirato a evitare di pagare le Tariffe dovute; (iii) per materiali o attività che sono soggetti alle normative sul traffico di armi a livello internazionale (ITAR, International Traffic in Arms Regulations) adottate dal Dipartimento di Stato degli Stati Uniti; (iv) in modo tale da violare o agevolare la violazione delle Leggi in materia di controllo delle esportazioni o (v) per trasmettere, archiviare o trattare dati sanitari soggetti alla normativa HIPAA degli Stati Uniti, salvo se consentito da un Contratto di società in affari (BAA) HIPAA. Salvo se diversamente consentito nei Termini di servizio specifici, il Cliente non utilizzerà, e non consentirà agli Utenti finali di utilizzare, i Servizi per effettuare chiamate ai servizi di emergenza o ricevere chiamate dagli stessi.
- 3.5 **Monitoraggio degli utilizzi illeciti**. Il Cliente è l'unico responsabile del monitoraggio, del trattamento e di eventuali risposte alle email inviate agli alias "abuse" o "postmaster" per qualsiasi Nome di dominio verificato per l'utilizzo con i Servizi. Google potrà monitorare le email inviate a tali alias per i Nomi di dominio, in modo da rilevare eventuali utilizzi illeciti dei Servizi.
- 3.6 **Richiesta di Account utente finale aggiuntivi durante il Periodo di validità dell'ordine**. Il Cliente può acquistare Account utente finale aggiuntivi durante un Periodo di validità dell'ordine: (a) mediante la presentazione di un Modulo d'ordine aggiuntivo a Google o al Rivenditore, secondo il caso, oppure (b) mediante la Console di amministrazione. Gli Account utente finale aggiunti avranno una durata proporzionale, che terminerà l'ultimo giorno del Periodo di validità dell'ordine.

- 4. **Pagamento.**
  - 4.1 **Ordini mediante il Rivenditore**. Se il Cliente ordina i Servizi presso il Rivenditore: (a) le tariffe relative ai Servizi verranno fissate tra il Cliente e il Rivenditore e i pagamenti saranno versati direttamente al Rivenditore ai sensi del Contratto per i rivenditori; (b) le restanti disposizioni della presente Sezione 4 (Pagamento) non si applicano ai Servizi; (c) il Cliente riceverà i Crediti per i Servizi (se esistenti) dal Rivenditore; (d) il Cliente può richiedere Account utente finale aggiuntivi durante il Periodo di validità dell'ordine contattando il Rivenditore ed (e) Google potrà divulgare Informazioni riservate del Cliente al Rivenditore in quanto Delegato soggetto alla Sezione 7.1 (Obbligazioni di riservatezza) del presente Contratto.
  - 4.2 **Utilizzo e fatturazione**. Il Cliente pagherà tutte le Tariffe dovute per i Servizi. Google fatturerà al Cliente l'importo corrispondente alle Tariffe per i Servizi. L'utilizzo dei Servizi da parte del Cliente sarà determinato mediante gli strumenti di misurazione di Google. Quando effettuerà l'ordine per i Servizi, il Cliente potrà scegliere una delle seguenti opzioni di fatturazione o una delle altre opzioni offerte da Google. Google può cambiare la propria offerta di opzioni di fatturazione, anche limitando o interrompendo l'offerta di qualsiasi opzione di fatturazione, previo invio al Cliente di un avviso scritto (anche via email) entro 30 giorni. Le opzioni di fatturazione potrebbero non essere disponibili per tutti i Clienti. Il Cliente può pagare l'importo dovuto per i Servizi utilizzando le opzioni di pagamento elencate nella Sezione 4.3 (Pagamento) più avanti.

- (a) **Piano mensile**. Qualora il Cliente scelga questa opzione, non si impegnerà ad acquistare i Servizi per una durata predefinita, ma potrà pagare i Servizi su base mensile. Google fatturerà al Cliente: (i) Tariffe in base al consumo giornaliero dei Servizi nel mese precedente; e (ii) posteriormente, a scadenza mensile in base all'uso dei Servizi. Google fornirà al Cliente la quota mensile per i Servizi quando verranno ordinati dal Cliente e la quota verrà utilizzata per calcolare le Tariffe, in proporzione all'uso giornaliero durante tale mese. L'utilizzo parziale dei Servizi in determinati giorni verrà arrotondato all'utilizzo per una giornata completa per facilitare il calcolo delle Tariffe.
- (b) **Piano annuale**. Qualora il Cliente scelga questa opzione, dovrà impegnarsi ad acquistare i Servizi da Google per un anno. Google addebiterà al Cliente i costi dovuti in base ai termini associati alle scelte effettuate dal Cliente nel Modulo d'ordine.

- 4.3 **Pagamento**. Tutti i pagamenti devono essere effettuati in dollari (USA) salvo se diversamente specificato sul Modulo d'ordine o sulla fattura.
  - (a) **Carta di credito o carta di debito**. Se il Cliente effettua il pagamento con carta di credito, carta di debito o altre modalità che non richiedono fatturazione, le Tariffe dovranno essere pagate alla fine del mese in cui il Cliente ha usufruito dei Servizi. Per le carte di credito o di debito, secondo il caso: (i) alla scadenza, Google addebiterà al Cliente tutte le Tariffe applicabili e (ii) il pagamento di tali Tariffe sarà considerato in ritardo 30 giorni dopo la fine del mese in cui il Cliente ha usufruito dei Servizi.
  - (b) **Fatture**. Salvo se diversamente specificato nel Modulo d'ordine, i pagamenti delle fatture scadono 30 giorni dopo la data della fattura; dopo tale data, sono considerati in ritardo.
  - (c) **Altre forme di pagamento**. Il Cliente può cambiare la modalità di pagamento scegliendo tra quelle disponibili nella Console di amministrazione. Google può abilitare altre modalità di pagamento rendendole disponibili nella Console di amministrazione. Tali altre forme di pagamento possono essere soggette a termini aggiuntivi che il Cliente dovrà accettare prima di poterle utilizzare.
- 4.4 **Pagamenti in ritardo**.
  - (a) Il pagamento delle Tariffe da parte del Cliente è in ritardo se non viene ricevuto da Google entro la data di scadenza del pagamento. In caso di ritardo del pagamento da parte del Cliente, Google può: (i) addebitare un interesse sull'importo in ritardo nella misura dell'1,5% al mese (o al massimo tasso consentito dalla legge, se inferiore) a partire dalla data di scadenza del pagamento fino al completo pagamento e (ii) Sospendere o cessare i Servizi.
  - (b) Il Cliente sarà tenuto a rimborsare a Google tutte le spese (incluse le spese legali) ragionevolmente sostenute da Google per la riscossione di importi relativi a pagamenti scaduti, tranne nei casi in cui tali pagamenti siano dovuti a imprecisioni nella fatturazione attribuibili a Google.
- 4.5 **Ordini di acquisto**. Se il Cliente richiede l'indicazione di un numero di ordine di acquisto nella fattura, dovrà fornire a Google tale numero nel Modulo d'ordine. Se il Cliente non fornisce un numero di ordine di acquisto, (a) Google emetterà per il Cliente una fattura senza un numero di ordine di acquisto e (b) il Cliente pagherà le fatture sprovviste di riferimenti al

numero di ordine di acquisto. Eventuali termini specificati nell'ordine di acquisto non sono validi.

- 4.6 **Tasse. Le Tariffe non includono le Tasse**. Il Cliente è tenuto a pagare le Tasse per i Servizi. Se la legge lo richiede, il Cliente tratterrà le Tasse dai pagamenti effettuati a favore di Google e fornirà un certificato di ritenuta fiscale. Il Cliente è tenuto a versare le Tasse incluse in fattura, fatti salvi i casi in cui possa esibire un certificato valido di esenzione. Senza alcuna limitazione all'obbligazione del Cliente a pagare le Tariffe, il Cliente tratterrà le Tasse se richiesto dalla legge.
- 4.7 **Revisioni dei Prezzi**. Google può modificare i Prezzi in qualsiasi momento salvo se diversamente concordato espressamente in un Addendum o nel Modulo d'ordine. Google invierà al Cliente una notifica almeno 30 giorni prima di qualsiasi aumento dei Prezzi.

- 5. **Servizi di assistenza tecnica**. Google fornirà Servizi di assistenza tecnica al Cliente nel corso del Periodo di validità dell'ordine, ai sensi delle Linee guida per i servizi di assistenza tecnica, dietro pagamento delle Tariffe per l'assistenza, se previste. Qualora ordini i Servizi presso il Rivenditore, il Cliente riconosce e accetta che il Rivenditore possa divulgare i Dati del Cliente a Google come ragionevolmente richiesto al fine di consentire al Rivenditore di gestire qualsiasi problema di assistenza che il Cliente inoltri al Rivenditore o tramite quest'ultimo.
- 6. **Sospensione**.
  - 6.1 **Limitazioni relative alla Sospensione dei Servizi**. Google può Sospendere i Servizi secondo quanto descritto nelle Sezioni 6.2 (Violazioni delle Norme di utilizzo accettabile) e 6.3 (Sospensione di emergenza). La portata e la durata di qualsiasi Sospensione ai sensi delle suddette Sezioni saranno quelle minime necessarie: (a) per prevenire o cessare l'utilizzo all'origine del problema, (b) per prevenire o risolvere il Problema di sicurezza di emergenza o (c) per l'osservanza delle normative vigenti.
  - 6.2 **Violazioni delle norme di utilizzo accettabile**. Se Google viene a conoscenza del fatto che l'utilizzo dei Servizi da parte del Cliente o di qualsiasi Utente finale viola le Norme di utilizzo accettabile, richiederà al Cliente di rettificare tale violazione. Se il Cliente non provvede a rettificare tale violazione entro 24 ore da suddetta richiesta o se Google è altrimenti tenuta per legge a intervenire, Google potrà Sospendere i Servizi.
  - 6.3 **Sospensione di emergenza**. Google può Sospendere immediatamente l'utilizzo dei Servizi da parte del Cliente o di qualsiasi Account utente finale se: (a) si verifica un Problema di sicurezza di emergenza o (b) Google è tenuta a Sospendere tale utilizzo per rispettare la legge vigente. Su richiesta del Cliente, salvo se vietato dalla legge, Google invierà al Cliente una notifica in merito ai presupposti della Sospensione non appena ciò sia ragionevolmente possibile. Relativamente alla Sospensione degli Account utente finale, Google fornirà all'Amministratore del Cliente la possibilità di ripristinare gli Account utente finale in determinate circostanze.
- 7. **Riservatezza**.
  - 7.1 **Obbligazioni**. In conformità a quanto disposto dalla Sezione 7.2 (Divulgazione di informazioni riservate), la parte ricevente utilizzerà le Informazioni riservate dell'altra parte al solo fine di esercitare i propri diritti e adempiere alle proprie obbligazioni ai sensi del presente Contratto. Il ricevente prenderà ogni ragionevole precauzione per impedire la divulgazione delle Informazioni riservate dell'altra parte a terzi che non siano dipendenti, agenti o consulenti professionali ("Delegati") del ricevente che debbano esserne a conoscenza e per le quali sussista l'obbligazione legale a mantenerne la riservatezza. Il destinatario si assicurerà che anche i suoi Delegati siano soggetti alle stesse obbligazioni di non divulgazione e di utilizzo.
  - 7.2 **Divulgazione di Informazioni riservate**.

- (a) **Disposizioni generali**. Indipendentemente da qualsiasi altra disposizione del Contratto, il ricevente o le sue Società consociate possono divulgare le Informazioni riservate dell'altra parte (i) in conformità a un Procedimento giudiziario, fatto salvo quanto indicato nella Sezione 7.2(b) (Notifica di Procedimento giudiziario), o (ii) previo consenso scritto dell'altra parte.
- (b) **Notifica di Procedimento giudiziario**. Il ricevente compirà ogni sforzo commercialmente ragionevole per inviare una notifica all'altra parte prima di divulgare le Informazioni riservate di tale parte in conformità al Procedimento giudiziario. La notifica non è richiesta prima della divulgazione se il ricevente è informato del fatto che (i) è legalmente vietato emettere tale notifica o (ii) il Procedimento giudiziario si riferisce a circostanze eccezionali che potrebbero causare la morte o un grave pregiudizio all'integrità fisica.
- (c) **Opposizione**. Il ricevente e le sue Società consociate sono tenuti a rispettare le richieste ragionevoli dell'altra parte qualora questa si opponga alla divulgazione delle proprie Informazioni riservate.

- 8. **Proprietà intellettuale**.
  - 8.1 **Diritti di proprietà intellettuale**. Ad eccezione di quanto espressamente indicato nel Contratto, il Contratto non concede ad alcuna parte alcun diritto, implicito o di altro tipo, relativo ai contenuti o alla Proprietà intellettuale dell'altra parte. Per ciò che concerne le parti, il Cliente conserva tutti i Diritti di proprietà intellettuale dei propri dati e Google conserva tutti i Diritti di proprietà intellettuale dei Servizi.
  - 8.2 **Elementi distintivi del brand**. Google mostrerà solo gli Elementi distintivi del brand che il Cliente l'autorizza a mostrare caricandoli nei Servizi. Google mostrerà tali Elementi distintivi del brand del Cliente all'interno delle aree designate delle pagine web che mostrano i Servizi al Cliente o ai suoi Utenti finali. Google potrà inoltre mostrare gli Elementi distintivi del brand Google nelle suddette pagine web per indicare che i Servizi sono forniti da Google.
  - 8.3 **Feedback**. Il Cliente può, a propria discrezione, fornire Feedback a Google in merito ai Servizi. Con la fornitura di Feedback, il Cliente assegna a Google tutti i diritti, i titoli e gli interessi relativi a tale Feedback.
- 9. **Marketing e Pubblicità**. Ciascuna parte può utilizzare gli Elementi distintivi del brand dell'altra parte in relazione al presente Contratto solo secondo quanto consentito dal Contratto stesso. Il Cliente può dichiarare pubblicamente di essere un cliente di Google e mostrare gli Elementi distintivi del brand di Google conformemente alle Linee guida del marchio. Google può (a) dichiarare oralmente che il Cliente è un cliente Google e (b) includere il nome o gli Elementi distintivi del brand del Cliente in un elenco di clienti Google nei propri materiali promozionali. L'eventuale utilizzo degli Elementi distintivi del brand di una parte andrà a vantaggio della parte che detiene i Diritti di proprietà intellettuale in relazione a tali Elementi distintivi del brand. Ciascuna parte potrà revocare all'altra parte il diritto di utilizzare gli Elementi distintivi del brand previa notifica scritta all'altra parte e concedendo un periodo ragionevole per interrompere l'utilizzo.
- 10. **Dichiarazioni, garanzie e disclaimer**.
  - 10.1 **Dichiarazioni e garanzie**. Ciascuna parte dichiara: (a) di disporre di pieni poteri e dell'autorità per stipulare il Contratto e (b) di rispettare tutte le leggi e i regolamenti vigenti per la fornitura o per l'utilizzo dei Servizi, secondo il caso.
  - 10.2 **Limitazioni di responsabilità**. **Salvo quanto espressamente specificato nel Contratto, nella misura massima consentita dalla legge vigente, Google (a) non offre altre garanzie di alcun tipo, siano**

esse espresse, implicite, statutarie o di altro genere, incluse garanzie di commerciabilità, di idoneità a uno scopo particolare, di non violazione o di utilizzo privo di errori e ininterrotto dei Servizi e (b) non risponde di contenuti o informazioni resi accessibili mediante i Servizi. Salvo se diversamente specificato nel Contratto, il Cliente riconosce che i Servizi non sono in grado di chiamare i servizi di emergenza o di ricevere chiamate dagli stessi.

- 11. **Durata e risoluzione**.
    - 11.1 **Periodo di validità del Contratto**. Il presente Contratto resterà in vigore per tutto il Periodo di validità previsto, salvo scadenza o recesso in conformità al Contratto.
    - 11.2 **Rinnovo**.
        - (a) **Con un Piano mensile**. Con il Piano mensile, il Cliente non si impegna ad acquistare i Servizi per un periodo di tempo predefinito. Di conseguenza, non è previsto alcun evento di rinnovo per il Piano mensile. Google continuerà invece a fatturare al Cliente le Tariffe come indicato nella precedente Sezione 4.1(a).
        - (b) **Con un Piano annuale**. Alla fine di ogni Periodo di validità dell'ordine, i Servizi verranno rinnovati secondo le scelte operate dal Cliente sul Modulo d'ordine o nella Console di amministrazione.
        - (c) **Informazioni generali**. Il Cliente può modificare il numero di Account utente finale da rinnovare dalla Console di amministrazione. Il Cliente continuerà a pagare a Google le Tariffe precedentemente stabilite per ogni Account utente finale rinnovato fino a quando il Cliente e Google non si accordino diversamente. Qualora una delle parti non intenda rinnovare i Servizi, dovrà notificarlo per iscritto all'altra parte almeno 15 giorni prima della fine del Periodo di validità dell'ordine al momento in vigore. La notifica del mancato rinnovo avrà effetto dopo la conclusione del Periodo di validità dell'ordine al momento in vigore.
    - 11.3 **Recesso per inadempienza**. Ciascuna parte può risolvere il Contratto se l'altra parte: (a) viola sostanzialmente il Contratto e non pone rimedio a tale violazione entro 30 giorni dalla ricezione della notifica scritta o (b) sospende la propria attività o diventa oggetto di procedure di insolvenza e le procedure non vengono respinte entro 90 giorni.
    - 11.4 **Recesso per inattività**. Google si riserva il diritto di risolvere il Contratto e interrompere la fornitura dei Servizi previa notifica di 30 giorni se, per un periodo di 60 giorni consecutivi, il Cliente, inclusi gli Utenti finali: (a) non ha eseguito l'accesso alla Console di amministrazione o (b) non ha utilizzato i Servizi.
    - 11.5 **Effetti del Recesso**. Se il Contratto viene risolto o scade, anche tutti i Moduli d'ordine sono risolti o scadono, secondo il caso. Se il Contratto viene risolto o scade: (a) tutti i diritti e l'accesso ai Servizi ai sensi del Contratto cessano (incluso l'accesso ai Dati del cliente) e (b) Google invia al Cliente una fattura finale.
    - 11.6 **Validità imperitura**. Le seguenti sezioni rimarranno in vigore anche dopo la scadenza o il recesso del presente Contratto: Sezione 4 (Pagamento), 7 (Riservatezza), 8 (Proprietà intellettuale), 10.2 (Limitazione di responsabilità), 11.5 (Effetti del Recesso), 12 (Indennizzo), 13 (Responsabilità), 14 (Disposizioni varie) e 15 (Definizioni).
- 12. **Indennizzo**.
    - 12.1 **Obbligazioni di indennizzo di Google**. Google si impegna a difendere il Cliente e le sue Società consociate partecipanti al Contratto

("Parti indennizzate del Cliente") e a tenerli indenni dalle Responsabilità indennizzate in qualsiasi Procedimento giudiziario iniziato da terze parti nella misura in cui questo derivi da accuse dichiaranti che l'utilizzo da parte delle Parti indennizzate del Cliente, in conformità con quanto disposto nel presente Contratto, di eventuali Materiali indennizzati di Google sia in violazione dei Diritti di proprietà intellettuale della terza parte.

- 12.2 **Obbligazioni di indennizzo del Cliente**. Salvo se vietato dalla legge vigente, il Cliente difenderà Google e le sue Società consociate e li terrà indenni dalle Responsabilità indennizzate in qualsiasi Procedimento giudiziario iniziato da terze parti nella misura in cui questo derivi da: (a) Materiali indennizzati del Cliente o (b) l'utilizzo dei Servizi da parte del Cliente o di un Utente finale in violazione delle Norme di utilizzo accettabile o delle Restrizioni d'uso.
- 12.3 **Esclusioni dall'indennizzo**. Le sezioni 12.1 (Obbligazioni di indennizzo di Google) e 12.2 (Obbligazioni di indennizzo del Cliente) non si applicano se la presunta accusa deriva da: (a) violazione del Contratto imputabile alla parte indennizzata o (b) una combinazione di Materiali indennizzati di Google o Materiali indennizzati del Cliente (secondo il caso) con materiali non forniti dalla parte indennizzante ai sensi del Contratto, salvo se la combinazione sia richiesta dal Contratto.
- 12.4 **Condizioni di indennizzo**. Le Sezioni 12.1 (Obbligazioni di indennizzo di Google) e 12.2 (Obbligazioni di indennizzo del Cliente) sono subordinate a quanto segue:
    - (a) La parte indennizzata deve tempestivamente notificare per iscritto alla parte indennizzante l'accusa o le accuse che hanno preceduto il Procedimento giudiziario iniziato da terze parti e collaborare in misura ragionevole con la parte indennizzante per risolvere l'accusa o le accuse e il Procedimento giudiziario iniziato da terze parti. Qualora una violazione della presente Sezione 12.4 (a) pregiudichi la difesa del Procedimento giudiziario iniziato da terze parti, le obbligazioni della parte indennizzante di cui alle Sezioni 12.1 (Obbligazioni di indennizzo di Google) o 12.2 (Obbligazioni di indennizzo del Cliente), secondo il caso, saranno ridotte proporzionalmente al pregiudizio.
    - (b) La parte indennizzata dovrà cedere il controllo esclusivo della porzione indennizzata del Procedimento giudiziario iniziato da terze parti alla parte indennizzante, in base a quanto segue: (i) la parte indennizzata può incaricare un proprio legale, senza facoltà di controllo, a proprie spese e (ii) qualsiasi soluzione che richieda alla parte indennizzata di ammettere responsabilità, pagare denaro o intraprendere (o astenersi dall'intraprendere) qualsiasi azione, richiederà il previo consenso scritto da parte della parte indennizzata, che non dovrà essere irragionevolmente trattenuto, condizionato o ritardato.
- 12.5 **Rimedi**.
    - (a) Se Google ritiene ragionevolmente che i Servizi violino i Diritti di proprietà intellettuale di una terza parte, può agire nel seguente modo a propria discrezione e a proprie spese: (i) ottenere il diritto per il Cliente di continuare a utilizzare i Servizi; (ii) modificare i Servizi in modo tale da ripristinarne la conformità senza ridurne sostanzialmente la funzionalità o (iii) sostituire i Servizi con un'alternativa conforme equivalente a livello funzionale.

        - (b) Se Google non ritiene che i rimedi riportati nella Sezione 12.5(a) siano commercialmente ragionevoli, potrà Sospendere o cessare i Servizi interessati.
    - 12.6 **Diritti e obbligazioni esclusivi**. Senza che ciò influisca sui diritti di recesso di ciascuna parte, la presente Sezione 12 (Indennizzo) determina il solo e unico rimedio delle parti, ai sensi del presente Contratto, in relazione alle accuse di presunte violazioni dei Diritti di proprietà intellettuale e ai Procedimenti giudiziari iniziati da terze parti descritti nella Sezione 12 (Indennizzo).
- 13. **Responsabilità**.
    - 13.1 **Responsabilità limitate**.
        - **(a) Nei limiti consentiti dalla legge vigente e secondo quanto stabilito nella Sezione 13.2 (Responsabilità illimitate), nessuna parte avrà Responsabilità derivanti da o in relazione al Contratto per: (i) perdita di fatturato, profitti, risparmi o reputazione o (ii) danni indiretti, speciali, incidentali, consequenziali o punitivi.**
        - **(b) La Responsabilità totale di ciascuna parte per i danni derivanti da o in relazione al Contratto è limitata alle Tariffe pagate dal Cliente ai sensi del Contratto durante i 12 mesi precedenti l'evento che ha dato origine alla responsabilità.**
    - 13.2 **Responsabilità illimitate**. **Nessuna parte del Contratto esclude o limita la Responsabilità di ciascuna parte in caso di: (a) morte, lesioni personali o danno tangibile alla proprietà, risultanti da negligenza di una delle parti o dei suoi dipendenti o agenti; (b) frode o dichiarazione fraudolenta; (c) obbligazioni ai sensi della Sezione 12 (Indennizzo); (d) violazione dei Diritti di proprietà intellettuale dell'altra parte; (e) obbligazioni di pagamento ai sensi del Contratto o (f) questioni per le quali la responsabilità non può essere esclusa o limitata ai sensi delle leggi vigenti.**
- 14. **Disposizioni varie**.
    - 14.1 **Notifiche**. Google può fornire qualsiasi notifica al Cliente: (a) inviando un'email all'Indirizzo email per le notifiche o (b) pubblicando una notifica nella Console di amministrazione. Il Cliente può fornire una notifica a Google inviando un'email all'indirizzo legal-notices@google.com. La notifica verrà considerata ricevuta quando (x) l'email viene inviata, indipendentemente dal fatto che l'altra parte la riceva o (y) la notifica viene pubblicata nella Console di amministrazione. È responsabilità del Cliente tenere aggiornato l'Indirizzo email per le notifiche per tutto il Periodo di validità.
    - 14.2 **Email**. Ai sensi del presente Contratto, le parti possono utilizzare le email per soddisfare i requisiti di approvazione e consenso scritti.
    - 14.3 **Trasferimento**. Nessuna delle parti può trasferire il Contratto senza il consenso scritto dell'altra parte, fatta eccezione per una Società consociata, laddove: (a) l'assegnatario abbia accettato per iscritto di essere vincolato dai termini del Contratto; (b) la parte cedente rimanga responsabile delle obbligazioni sostenute ai sensi del Contratto qualora l'assegnatario risulti inadempiente e (c) la parte cedente abbia notificato all'altra parte tale trasferimento. Qualsiasi altro tentativo di cessione sarà considerato nullo.
    - 14.4 **Passaggio di controllo**. Se una parte è oggetto di un passaggio di controllo che non sia una ristrutturazione o riorganizzazione interna: (a) tale parte invierà una notifica scritta all'altra parte entro 30 giorni dal passaggio del controllo e (b) l'altra parte potrà risolvere immediatamente il

Contratto in qualsiasi momento entro 30 giorni dalla ricezione della suddetta notifica scritta.

- 14.5 **Forza maggiore**. Nessuna delle parti sarà considerata responsabile in caso di inadempimento o adempimento tardivo delle proprie obbligazioni qualora ciò sia ascrivibile a circostanze che esulano dal controllo della parte inadempiente, inclusi eventi fortuiti, calamità naturali, terrorismo, rivolte o guerre.
- 14.6 **Cessione mediante subcontratto. Google può cedere mediante subcontratto le obbligazioni ai sensi del presente Contratto, ma rimane responsabile verso il Cliente di tutte le obbligazioni cedute mediante subcontratto.**
- 14.7 **Esclusione di rinuncia**. L'omissione o il ritardo nell'esercizio di un qualsiasi diritto previsto dal Contratto non costituirà una rinuncia ad alcun diritto da parte di nessuna delle parti.
- 14.8 **Clausola salvatoria**. Qualora qualsiasi Sezione del presente Contratto si rivelasse, in tutto o in parte, non valida, illegittima o inapplicabile, la parte restante del Contratto rimarrà in vigore a tutti gli effetti.
- 14.9**Mancata instaurazione di un rapporto di agenzia**. Il presente Contratto non dà luogo ad alcun mandato di agenzia, partnership o joint venture tra le parti.
- 14.10 **Efficacia nei confronti di terzi**. Il presente Contratto non conferisce benefici a favore di terze parti salvo quanto espressamente stabilito.
- 14.11 **Risarcimento in base all'equity relief**. Nulla nel presente Contratto limiterà la capacità delle parti di richiedere una compensazione a titolo equitativo.
- 14.12 **Legislazione vigente**. Tutte le rivendicazioni derivanti da o relative al presente Contratto o ai Servizi saranno disciplinate dalla legge della California, con l'esclusione delle norme di diritto internazionale privato della California, e saranno disputate esclusivamente nei tribunali federali o statali della contea di Santa Clara, California; le parti acconsentono alla giurisdizione personale in tali tribunali.
- 14.13 **Emendamenti**. Salvo diversa e specifica disposizione nel presente Contratto, qualsiasi modifica al Contratto deve espressamente indicare che rappresenta un emendamento del Contratto e deve essere formulata per iscritto e firmata da entrambe le parti.
- 14.14 **Sviluppo indipendente**. Nessuna disposizione del presente Contratto potrà essere interpretata come limitazione o restrizione di ciascuna parte relativamente allo sviluppo, alla fornitura o all'acquisizione indipendente di qualsiasi materiale, servizio, prodotto, programma o tecnologia che sia assimilabile all'oggetto del Contratto, a condizione che la parte non violi in tal modo le proprie obbligazioni ai sensi del Contratto.
- 14.15 **Indivisibilità del Contratto**. Il Contratto stabilisce tutti i termini concordati dalle parti e prevale su tutti i contratti precedenti o contemporanei tra le parti relativi allo stesso oggetto del presente Contratto. Al momento della stipula del presente Contratto, nessuna delle parti ha esercitato, né eserciterà, un diritto o un rimedio sulla base di qualsivoglia affermazione, dichiarazione o garanzia (fornita intenzionalmente o in buona fede), salvo quanto espressamente dichiarato nel presente Contratto. Il Contratto include link URL ad altri termini (inclusi i Termini URL) che sono incorporati nel Contratto mediante riferimento.
- 14.16 **Termini in conflitto**. Qualora si verifichi un conflitto tra i documenti che compongono il presente Contratto, l'ordine di precedenza dei documenti sarà il seguente: il Modulo d'ordine, il Contratto e i Termini URL.

- 14.17 **Documenti omologhi**. Le parti potranno stipulare il presente Contratto in più copie, ivi incluso via fax, in PDF o in altri formati elettronici, che nell'insieme costituiranno un unico documento.
- 14.18 **Firme elettroniche**. Le parti acconsentono all'utilizzo di firme elettroniche.
- 14.19 **Intestazioni**. Titoli e didascalie utilizzate nel Contratto hanno solo fini di riferimento e non avranno alcun effetto sull'interpretazione del Contratto.

- 15. **Definizioni**.
  - **"Norme di utilizzo accettabile"** o **"AUP"** (Acceptable Use Policy) indica le norme per l'utilizzo accettabile dei Servizi, disponibili all'indirizzo https://workspace.google.com/intl/it/terms/use_policy.html.
  - **"Account"** indica le credenziali dell'Account Google del Cliente e il relativo accesso ai Servizi ai sensi del presente Contratto.
  - **"Prodotti aggiuntivi"** indica i prodotti, i servizi e le applicazioni che non fanno parte dei Servizi, ma ai quali è possibile accedere per utilizzarli con i Servizi.
  - **"Termini per i Prodotti aggiuntivi"** indica i termini al momento in vigore disponibili all'indirizzo https://workspace.google.com/intl/it/terms/additional_services.html.
  - **"Account amministratore"** indica un tipo di Account utente finale che il Cliente (o il Rivenditore, secondo il caso) può utilizzare per amministrare i Servizi.
  - **"Console di amministrazione"** indica le console online e gli strumenti forniti da Google al Cliente per l'amministrazione dei Servizi.
  - **"Amministratori"** indica il personale tecnico designato dal Cliente, che amministra i Servizi per conto del Cliente e che può accedere ai Dati del Cliente e agli Account utente finale.
  - **"Annunci pubblicitari"** indica gli annunci online mostrati da Google agli Utenti finali, esclusi gli annunci che il Cliente sceglie esplicitamente di far mostrare da Google o dalle sue Società consociate in relazione ai Servizi sulla base di un accordo separato (ad esempio annunci di Google AdSense distribuiti dal Cliente in un sito web creato dal Cliente utilizzando la funzionalità "Google Sites" inclusa nei Servizi).
  - **"Società consociata"** indica qualsiasi entità che controlli una parte, ne sia controllata o sia sottoposta a comune controllo con tale parte, sia direttamente che indirettamente.
  - **"BAA"** o **"Contratto** di società in affari" è un addendum al presente Contratto che copre la gestione dei Dati sanitari protetti (così come definiti nell'HIPAA).
  - **"Elementi distintivi del brand"** indica i nomi commerciali, i marchi, i loghi, i nomi di dominio e altri elementi distintivi del brand di ciascuna parte.
  - **"Informazioni riservate"** indica le informazioni che una parte (o una società collegata) comunica all'altra parte ai sensi del presente Contratto e che sono contrassegnate come confidenziali o che normalmente sarebbero considerate informazioni confidenziali in tali circostanze. I Dati del Cliente sono Informazioni riservate. Le Informazioni riservate non includono informazioni sviluppate in modo indipendente dal ricevente, condivise con il ricevente da una terza parte senza obbligazioni di riservatezza o che diventino di dominio pubblico senza alcuna responsabilità del ricevente.
  - **"Controllo"** indica il controllo di oltre il 50% dei diritti di voto o di partecipazione al capitale di una parte.

- **"Servizi principali"** indica i Servizi principali di Google Workspace così come descritti nel Riepilogo dei servizi.
- **"Dati del Cliente"** indica i dati inviati, archiviati, spediti o ricevuti tramite i Servizi da parte del Cliente, le sue Società consociate o Utenti finali.
- **"Materiali indennizzati del Cliente"** indica i Dati del cliente e gli Elementi distintivi del brand del Cliente.
- **"Indirizzo email di dominio"** indica l'indirizzo email del Nome di dominio da utilizzare in relazione ai Servizi.
- **"Nome di dominio"** indica il nome di dominio specificato nel Modulo d'ordine, da utilizzare in relazione ai Servizi.
- **"Problema di sicurezza di emergenza"** può indicare: (a) l'utilizzo dei Servizi da parte del Cliente o dell'Utente finale in violazione delle Norme di utilizzo accettabile, in cui tale utilizzo può interrompere: (i) i Servizi, (ii) l'utilizzo dei Servizi da parte di altri clienti o (iii) la rete o i server di Google utilizzati per fornire i Servizi oppure (b) l'accesso non autorizzato di una terza parte ai Servizi.
- **"Utenti finali"** indica le persone a cui il Cliente consente di utilizzare i Servizi e che sono gestite dall'Amministratore.
- **"Account utente finale"** indica un account ospitato da Google creato dal Cliente tramite il proprio Amministratore per consentire a un Utente finale di utilizzare i Servizi.
- **"Leggi in materia di controllo delle esportazioni"** indica le leggi e normative vigenti relative al controllo delle esportazioni e delle riesportazioni, incluse (a) le disposizioni in materia di esportazioni previste dalle Export Administration Regulations ("EAR") del Dipartimento del Commercio degli Stati Uniti, (b) le sanzioni di carattere economico e commerciale adottate dall'Office of Foreign Assets Control del Dipartimento del Tesoro degli Stati Uniti e (c) le normative sul traffico di armi a livello internazionale ("ITAR", International Traffic in Arms Regulations) adottate dal Dipartimento di Stato degli Stati Uniti.
- **"Feedback"** indica il feedback o i suggerimenti che il Cliente fornisce a Google relativamente ai Servizi.
- **"Tariffe"** indica il prodotto dell'importo dei Servizi utilizzati o ordinati dal Cliente moltiplicato per i Prezzi e addizionato delle eventuali Tasse applicabili.
- **"Materiali indennizzati di Google"** indica la tecnologia di Google utilizzata per fornire i Servizi e gli Elementi distintivi del brand di Google.
- **"Attività ad alto rischio"** indica le attività, tra cui l'azionamento di impianti nucleari, il controllo del traffico aereo, i sistemi di supporto alla vita o le armi, nelle quali l'utilizzo o il mancato funzionamento dei Servizi può causare decesso, lesioni alla persona o danno ambientale.
- **"HIPAA"**: indica la legge statunitense Health Insurance Portability and Accountability Act del 1996, soggetta a possibili modifiche periodiche, nonché qualsiasi norma emessa in base a tale legge.
- **"incluso"** indica incluso a titolo esemplificativo.
- **"Responsabilità indennizzate"** indica (i) i costi di conciliazione approvati dalla parte indennizzante e (ii) i danni e i costi riconosciuti in via definitiva nei confronti della parte indennizzata e delle sue Società consociate da parte di un tribunale competente.
- **"Proprietà intellettuale" o "PI"** indica qualsiasi elemento tutelato da un diritto di proprietà intellettuale.
- **"Diritti di proprietà intellettuale"** indica tutti i diritti di brevetto, copyright, diritti di segreto commerciale (se presenti), diritti di marchio commerciale, diritti di progettazione, diritti di database, diritti di nome di dominio, diritti

morali e tutti gli altri diritti di proprietà intellettuale (registrati o non registrati) detenuti in tutto il mondo.

- **"Procedimento giudiziario"** indica una richiesta di divulgazione di informazioni presentata ai sensi di leggi, normative statali, ingiunzioni del tribunale, citazioni, mandati, su richiesta di un ente governativo o agenzia oppure altra valida autorità giuridica, atto giuridico o processo analogo.
- **"Responsabilità"** indica qualsiasi tipo di responsabilità, sia per inadempienza contrattuale, illecito civile (inclusa la negligenza) o altro, sia prevedibile che contemplato dalle parti.
- **"Indirizzo email di notifica"** indica gli indirizzi email specificati dal Cliente nella Console di amministrazione.
- **"Modulo d'ordine"** indica la pagina o le pagine dell'ordine online, o altro documento d'ordine accettabile per Google ai sensi del presente Contratto, emesso da Google e accettato da Google, che specifica i Servizi che Google fornirà al Cliente nell'ambito del presente Contratto.
- **"Periodo di validità dell'ordine"** indica il periodo di tempo che inizia dalla Data di inizio dei Servizi relativa ai Servizi e si protrae per il periodo indicato sul Modulo d'ordine, fatto salvo il recesso anticipato in conformità al presente Contratto.
- **"Altri Servizi"** indica gli "Altri Servizi per Google Workspace" così come descritti nel Riepilogo dei servizi.
- **"Prezzi"** indica i prezzi applicabili stabiliti all'indirizzo https://workspace.google.com/intl/it/pricing.html, salvo se diversamente concordato in un Modulo d'ordine o emendamento.
- **"Rivenditore"** indica, se applicabile, il rivenditore di terza parte, che non sia una Società consociata, che vende i Servizi al Cliente.
- **"Contratto per i rivenditori"** indica il contratto separato tra il Cliente e il Rivenditore riguardo ai Servizi. Il Contratto per i rivenditori è un contratto a sé ed esula dall'ambito del presente Contratto.
- **"Termini di servizio specifici"** indica i Termini applicabili specificamente a uno o più Servizi, consultabili all'indirizzo https://workspace.google.com/intl/it/terms/service-terms/.
- **"Servizi" indica i Servizi principali applicabili e gli Altri servizi ordinati nel Modulo d'ordine applicabile.**
- **"Data di inizio dei servizi"** indica la data indicata nel Modulo d'ordine o, se successiva, la data in cui Google rende disponibili i Servizi per il Cliente.
- **"Riepilogo dei servizi"** indica la descrizione al momento più aggiornata disponibile all'indirizzo https://workspace.google.com/intl/it/terms/user_features.html.
- **"Cessazione rilevante"** indica un'interruzione sostanziale o una modifica retroattiva incompatibile dei Servizi principali a causa delle quali il Cliente o gli Utenti finali non saranno più in grado di utilizzare i Servizi per: (1) inviare e ricevere messaggi email; (2) pianificare e gestire eventi; (3) creare, condividere, archiviare e sincronizzare file; (4) comunicare con altri Utenti finali in tempo reale o (5) eseguire ricerche nei messaggi email, archiviarli ed esportarli.
- **"SLA"** indica i termini al momento in vigore disponibili all'indirizzo https://workspace.google.com/intl/it/terms/sla.html.
- **"Sospendere"** o "Sospensione" indica la disattivazione dell'accesso ai Servizi, o ai relativi componenti, o dell'utilizzo degli stessi.
- **"Tasse"** indica tutte le tasse imposte dal governo, ad eccezione delle tasse basate sul reddito netto di Google o del Cliente, il patrimonio netto, il valore d'inventario, il valore proprietario o l'impiego.

- **"Periodo di validità"** indica il periodo che inizia con la Data di validità e rimane in vigore fintanto che è in essere un Modulo d'ordine attivo.
- **"Procedimento legale di terze parti"** indica ogni procedimento legale formale presentato da una parte terza non affiliata davanti a una corte o a un tribunale governativo (inclusi i procedimenti di ricorso).
- **"Linee guida del marchio"** indica i Termini e le condizioni del brand Google, disponibili all'indirizzo http://www.google.com/permissions/trademark/brand-terms.html.
- **"Servizi di assistenza tecnica"** indica i servizi di assistenza tecnica forniti da Google al Cliente ai sensi delle Linea guida per i servizi di assistenza tecnica.
- **"Linee guida per i servizi di assistenza tecnica"** indica le linee guida al momento più aggiornate per i servizi di assistenza tecnica, disponibili all'indirizzo: https://workspace.google.com/intl/it/terms/tssg.html.
- **"Termini URL"** indica le Norme di utilizzo accettabile, i Termini di servizio specifici, lo SLA (accordo sul livello del servizio) e le Linee guida per i servizi di assistenza tecnica.
- **"Restrizioni d'uso"** indica le restrizioni descritte nella Sezione 3.4 (Restrizioni d'uso) del Contratto ed eventuali altre restrizioni all'uso dei Servizi descritte nei Termini di servizio specifici.

Versione: 8 aprile 2020

Additional Product Terms

From time to time, Google may make available one or more Google product(s) and/or service(s) referred to as 'Additional Products' or 'Additional Services' in Customer's Google Workspace Agreement, Cloud Identity Agreement or Hire Agreement (as applicable, the "**Agreement**"). For the purposes of these Additional Product Terms, such product(s) and/or service(s) will be collectively referred to as "**Additional Products**".

If Customer or any End User uses any Additional Products, Customer agrees to these Additional Product Terms, which will be incorporated into the applicable Agreement. If Customer or any End User uses any such Additional Products, Customer also agrees that the separate terms of service applicable to such products will apply as described below. For clarity, such terms of service will each form a separate agreement and are not governed by, or incorporated into, the applicable Agreement.

If Customer does not wish to enable any Additional Products, or if you are acting on behalf of Customer but do not have the requisite authority to bind Customer to these Additional Product Terms, please disable such Additional Products via the functionality of the Services.

1. **Definitions**. All capitalized terms used in these Additional Product Terms have the meanings given to them in the applicable Agreement, unless otherwise defined or stated herein.
2. **Applicable Terms of Service**. The Additional Products will be governed by (a) these Additional Product Terms, and (b) the Google Terms of Service located at https://policies.google.com/terms or any other terms of service Google may make available (as applicable, the "**Terms of Service**"). Customer will be responsible under these Additional Product Terms for any failure by its End Users to comply with such Terms of Service. Further details of the Additional Products and Terms of Service are provided at http://www.google.com/support/a/bin/answer.py?hl=en&answer=181865 and/or will be otherwise made available by Google. The Additional Products and Terms of Service may be updated or modified by Google from time to time.

3. **Availability**. Additional Products may not be available in all countries.
4. **Technical Support**. Customer is responsible for responding to questions from End Users relating to Customer's or End Users' use of the Additional Products. Google only provides technical support services for the Additional Products to the extent described in the applicable Terms of Service, and will not provide other technical support for the Additional Products unless Google agrees otherwise in writing.
5. **Compliance with Laws**. Customer agrees that it will provide Additional Products to its End Users in compliance with all applicable laws and regulations, including privacy and data protection laws, the US Family Educational Rights and Privacy Act (FERPA) of 1974, the US Children's Internet Protection Act (CIPA), and the US Children's Online Privacy Protection Act (COPPA) of 1998.
6. **Customer Access to End User Data**. Customer may be able to access, monitor, delete, rectify, export, use or disclose data provided by and related to End Users in the context of Additional Products or to disable End User Accounts for Additional Products. To the extent Customer has any such abilities, Customer will provide End Users with relevant information and facilitate the exercise of any related rights of End Users under privacy or data protection laws. If Google receives any request from an End User pertaining to Customer's processing of his/her personal data in relation to any Additional Products, Google will advise the End User to submit his/her request to Customer, and Customer will be responsible for responding to the request.
7. **End User Consent**. Except in relation to End Users described in Section 8 (Parental Consent), Customer will, before it allows any End Users to access or use any Additional Products, obtain and maintain consents from those End Users to the collection and use of their personal information in connection with those Additional Products.
8. **Parental Consent**. Before Customer allows any End Users who are under the age of 16 (or such other minimum age as is specified in the relevant European Economic Area member state, the UK or Switzerland) and resident in the European Economic Area, the UK or Switzerland, or any other End Users under the age of 18, to access or use any Additional Products, Customer will obtain parental consent for the collection and use of personal data in connection with those Additional Products.
9. **Google Pay**. A Google Pay account opened by an End User is the End User's personal account and is subject to extensive regulatory requirements and prohibitions. While Customer may suspend an End User's access to his/her Google Pay account, Customer may not use an End User's Google Pay account or make any changes to the information in such Google Pay account. Customer may access information in an End User's Google Pay account only in accordance with Google Pay privacy policies and Customer's privacy policy.
10. **Refund for Paid Services**. If Customer disables an Additional Product for which Customer or an End User has provided payment, Google will not be obliged to refund any fees paid by Customer and/or the End User for unused paid services. Customer will indemnify Google from and against all liabilities, damages, losses, expenses and costs (including settlement costs and reasonable legal fees) arising out of End User claims concerning refunds for such paid services.
11. **Severability**. If any part of these Additional Product Terms is found to be unenforceable, the remainder of the Additional Product Terms will remain in full force and effect.
12. **Modifications**. Google may modify these Additional Product Terms from time to time.
13. **Interpretation of Conflicting Terms**. To the extent of any conflict or inconsistency between these Additional Product Terms and the remainder of the applicable Agreement, the remainder of the Agreement will prevail.

Termini di servizio di Google Workspace

Ultima modifica: 7 novembre 2022

Per le traduzioni in altre lingue del presente Contratto, fai clic qui.

Se hai sottoscritto una versione offline del presente Contratto per l'utilizzo dei Servizi Google Workspace con lo stesso account Google Workspace, i seguenti Termini non saranno a te applicabili e i termini offline disciplinano l'utilizzo dei Servizi Google Workspace da parte tua.

Se a sua conta para faturamento é no Brasil, por gentileza veja o Termos de Serviço (em português e em inglês), que seráo os Termos aplicáveis à sua utilização da Google Workspace.

I presenti Termini di servizio di Google Workspace (collettivamente, il "Contratto"), noti in precedenza come "Contratto Google Workspace (Online)" o "Contratto Google Workspace", vengono stipulati da Google e dalla persona giuridica o fisica che li sottoscrive ("Cliente") e disciplinano l'accesso e l'utilizzo dei Servizi da parte sua. "Google" ha il significato di cui all'indirizzo https://cloud.google.com/terms/google-entity.

Il presente Contratto entrerà in vigore nella data in cui il Cliente farà clic sul pulsante di accettazione (la "Data di validità"). Se l'accettazione avviene per conto del Cliente, si dichiara e garantisce: (i) di avere piena autorità legale per vincolare il Cliente al presente Contratto; (ii) di avere letto e compreso il presente Contratto e (iii) di accettare il presente Contratto per conto del Cliente.

- 1. **Fornitura dei Servizi**.
    - 1.1 **Utilizzo dei Servizi**. Durante il Periodo di validità, Google fornirà i Servizi in conformità al Contratto, incluso lo SLA (accordo sul livello del servizio). Il Cliente può utilizzare i Servizi ordinati nell'apposito Modulo d'ordine o Ordine rivenditore conformemente al presente Contratto.
    - 1.2 **Console di amministrazione**. Il Cliente avrà accesso alla Console di amministrazione, tramite la quale potrà gestire il proprio utilizzo dei Servizi.
    - 1.3 **Account; Verifica per l'utilizzo dei Servizi**.
        - (a) **Account**. Il Cliente deve avere un Account per utilizzare i Servizi ed è responsabile delle informazioni che fornisce per la creazione dell'Account, della sicurezza delle proprie password relative all'Account e di qualsiasi utilizzo del proprio Account. Google non ha alcun obbligo di fornire più di un account al Cliente.
        - (b) **Verifica per l'utilizzo dei Servizi**. Per poter utilizzare i Servizi, il Cliente deve verificare un Indirizzo email di dominio o un Nome di dominio. Se il Cliente non dispone di un'autorizzazione valida per l'utilizzo dell'Indirizzo email di dominio o non possiede né controlla il Nome di dominio, Google non avrà alcun obbligo di fornire i Servizi al Cliente e potrà eliminare l'Account senza preavviso.
    - 1.4 **Modifiche**.
        - (a) **Ai Servizi**. Google può apportare di tanto in tanto modifiche commercialmente ragionevoli ai Servizi. Google informerà il Cliente qualora venga apportata da Google una modifica sostanziale ai Servizi che abbia un impatto significativo sull'utilizzo degli stessi da parte del Cliente e se il Cliente ha accettato di essere informato da Google di tale variazione.

- (b) **Al Contratto**. Google può modificare di tanto in tanto i Termini del presente Contratto e pubblicherà tali eventuali modifiche all'indirizzo https://workspace.google.com/terms/premier_terms.html. Tali modifiche diventeranno effettive soltanto all'inizio del Periodo di validità del successivo ordine del Cliente, momento nel quale la prosecuzione dell'utilizzo dei servizi da parte del Cliente costituirà la sua accettazione delle modifiche. La presente Sezione 1.4(b) (Modifiche al Contratto) non si applica alle modifiche ai Termini URL.
- (c) **Ai Termini URL**. Google può modificare di tanto in tanto i Termini URL e informerà il Cliente in caso di modifiche sostanziali. Google può informare il Cliente in caso di modifiche sostanziali allo SLA (accordo sul livello del servizio) mediante la pagina web dello SLA pertinente. Le modifiche sostanziali ai Termini URL entreranno in vigore 30 giorni dopo che ne è stata data comunicazione, con le seguenti eccezioni: (i) le modifiche sostanziali allo SLA che comportano un'incidenza negativa entreranno in vigore 90 giorni dopo la relativa comunicazione e (ii) le modifiche applicabili a nuovi Servizi o funzionalità o all'Addendum per il trattamento dei dati Cloud, oppure richieste dalle leggi vigenti, entreranno in vigore immediatamente.
- (d) **All'Addendum per il trattamento dei dati Cloud**. Google può modificare l'Addendum per il trattamento dei dati Cloud soltanto se tale modifica è necessaria per ottemperare alle leggi vigenti, è espressamente consentita dall'Addendum per il trattamento dei dati Cloud oppure se la modifica:
    - (i) è commercialmente ragionevole;
    - (ii) non comporta un deterioramento sostanziale della sicurezza dei Servizi;
    - (iii) non estende l'ambito del trattamento dei "Dati personali del Cliente" da parte di Google né rimuove qualsiasi restrizione su tale trattamento, come descritto nella Sezione "Ambito del trattamento" dell'Addendum per il trattamento dei dati Cloud e
    - (iv) non ha altrimenti un'incidenza negativa sostanziale sui diritti del Cliente previsti dall'Addendum per il trattamento dei dati Cloud.
- Se Google apporta una modifica sostanziale all'Addendum per il trattamento dei dati Cloud ai sensi della presente Sezione 1.4(d) (Modifiche all'Addendum per il trattamento dei dati Cloud), tale modifica dovrà essere pubblicata da Google sulla pagina web contenente l'Addendum per il trattamento dei dati Cloud.
- (e) **Interruzione di Servizi principali**. Google informerà il Cliente almeno 12 mesi prima di interrompere qualsiasi Servizio principale (o funzionalità sostanziale associata) a meno che Google non sostituisca tale Servizio principale o funzionalità non più disponibili con una funzionalità o un Servizio sostanzialmente analoghi. Nessuna parte della presente Sezione 1.4(e) (Interruzione di Servizi principali) limita la facoltà di Google di apportare modifiche richieste per rispettare leggi vigenti, gestire un rischio sostanziale per

la sicurezza o evitare ingenti oneri di natura economica o tecnica. La presente Sezione 1.4(e) (Interruzione di Servizi principali) non si applica ad altri Servizi né a Servizi, offerte o funzionalità in disponibilità pre-generale.

- 2. **Termini di pagamento**.
    - 2.1 **Misurazione dell'utilizzo e opzioni di fatturazione**. Per determinare l'utilizzo dei Servizi da parte del Cliente verranno impiegati gli strumenti di misurazione di Google; qualsiasi misurazione di questo tipo effettuata da Google ai fini del calcolo delle Tariffe si intende definitiva. Il Cliente può selezionare una delle opzioni di fatturazione indicate di seguito o qualsiasi altra opzione resa disponibile da Google quando il Cliente effettua l'ordine per i Servizi.
        - (a) **Piano flessibile**. Scegliendo questa opzione, il Cliente non si impegna ad acquistare i Servizi per una durata predefinita, bensì pagherà le Tariffe in base ai giorni di utilizzo dei Servizi, con fatturazione mensile riferita al mese precedente. L'utilizzo dei Servizi per una sola porzione di giorno sarà arrotondato all'utilizzo per un giorno intero, per facilitare il calcolo delle Tariffe.
        - (b) **Piano annuale/con scadenza fissa**. Scegliendo questa opzione, il Cliente si impegna ad acquistare i Servizi per uno o più periodi della durata di un anno (in base alla selezione del Cliente). Google addebiterà al Cliente i costi dovuti in base ai termini associati alle scelte effettuate dal Cliente nel Modulo d'ordine.
    - Google può modificare la propria offerta di opzioni di fatturazione (anche limitando o interrompendo l'offerta di qualsiasi opzione) dando un preavviso di 30 giorni al Cliente; la modifica diventerà effettiva all'inizio del successivo Periodo di validità dell'ordine del Cliente. Le opzioni di fatturazione potrebbero non essere disponibili per tutti i clienti. Il Cliente può pagare l'importo dovuto per i Servizi utilizzando le opzioni di pagamento elencate nella Sezione 2.2 (Pagamento) di seguito.
    - 2.2 **Pagamento**. Tutti i pagamenti devono essere effettuati nella valuta indicata nel Modulo d'ordine o nella fattura.
        - (a) **Carta di credito o carta di debito**. Se il Cliente paga con carta di credito, carta di debito o altre forme di pagamento che non richiedono l'invio di una fattura, il pagamento dovrà essere effettuato alla fine del mese in cui il Cliente ha usufruito dei Servizi. Per le carte di credito o di debito, secondo il caso: (i) alla scadenza, Google emetterà una fattura elettronica per tutte le Tariffe applicabili e (ii) il pagamento di tali Tariffe sarà considerato in ritardo 30 giorni dopo la fine del mese in cui il Cliente ha usufruito dei Servizi.
        - (b) **Fatture**. Salvo se diversamente specificato nel Modulo d'ordine, i pagamenti delle fatture scadono 30 giorni dopo la data della fattura; dopo tale data, sono considerati in ritardo.
        - (c) **Altre forme di pagamento**. Il Cliente può cambiare il proprio metodo di pagamento selezionando qualsiasi altro metodo che Google abbia abilitato nella Console di amministrazione, sempre a condizione dell'accettazione da parte del Cliente di eventuali termini aggiuntivi applicabili a tale metodo di pagamento.
        - (d) **Dati di pagamento**. I pagamenti effettuati tramite bonifico bancario devono includere le informazioni bancarie fornite da Google.
    - 2.3 **Imposte**.

- (a) Il Cliente è responsabile del pagamento di eventuali Imposte e sarà tenuto a pagare a Google i costi dei Servizi senza dedurre gli importi delle Imposte. Qualora per Google sussista l'obbligo di riscuotere o pagare eventuali Imposte, il loro importo sarà fatturato al Cliente, che sarà responsabile del relativo pagamento a Google, a meno che il Cliente non fornisca prontamente a Google un certificato valido di esenzione fiscale in relazione a tali Imposte.
- (b) Il Cliente fornirà a Google tutte le informazioni applicabili ai fini dell'identificazione fiscale che Google può richiedere ai sensi delle leggi vigenti per accertarsi di ottemperare alle normative fiscali e alle disposizioni delle autorità fiscali in vigore nelle giurisdizioni applicabili. Il Cliente sarà responsabile del pagamento (o del rimborso a Google) di eventuali imposte, interessi, sanzioni o multe derivanti da qualsiasi dichiarazione erronea del Cliente.

- 2.4 **Controversie sui pagamenti**. Le eventuali contestazioni riguardanti i pagamenti devono essere presentate prima della relativa data di scadenza. Se le parti stabiliscono che determinate imprecisioni nella fatturazione sono attribuibili a Google, quest'ultima non emetterà una nuova fattura corretta, bensì una nota di credito in cui sarà specificato l'importo errato della fattura interessata. Se una fattura contestata non è ancora stata pagata, Google applicherà l'importo della nota di credito alla fattura contestata e il Cliente sarà responsabile del pagamento del saldo netto dovuto risultante della fattura. Nulla nel presente Contratto obbliga Google a estendere il credito ad alcun soggetto.
- 2.5 **Pagamenti insoluti; Sospensione**. I ritardi di pagamento possono produrre interessi al tasso dell'1,5% al mese (o al tasso massimo consentito dalla legge, se inferiore) a partire dalla data di scadenza del pagamento fino al suo saldo integrale. Il Cliente sarà responsabile di tutte le spese (comprese le parcelle degli avvocati) ragionevolmente sostenute da Google per la riscossione di tali importi insoluti. Google può altresì sospendere i Servizi in caso di ritardo del loro pagamento da parte del Cliente.
- 2.6 **Non obbligatorietà dell'indicazione del numero di ordine di acquisto**. Il Cliente è tenuto a pagare tutte le Tariffe applicabili senza alcun obbligo per Google di fornire un numero di ordine di acquisto sulla propria fattura (o in altro modo).
- 2.7 **Revisioni dei Prezzi**. Google può modificare i Prezzi in qualsiasi momento, salvo se diversamente concordato espressamente in un addendum o in un Modulo d'ordine. Google informerà il Cliente di qualsiasi modifica con almeno 30 giorni di preavviso. I Prezzi per il Cliente saranno modificati all'inizio del Periodo di validità dell'Ordine del Cliente successivo al periodo di 30 giorni.

- 3. **Obbligazioni del Cliente**.
  - 3.1 **Conformità**. Il Cliente (a) assicurerà che l'utilizzo dei Servizi da parte del Cliente e dei suoi Utenti finali avvenga in ottemperanza al Contratto; (b) compirà ogni sforzo commercialmente ragionevole per impedire e interrompere qualsiasi utilizzo o accesso non autorizzato ai Servizi e (c) informerà tempestivamente Google qualora venga a conoscenza di qualsivoglia utilizzo o accesso non autorizzato ai Servizi, all'Account o alla password del Cliente. Google si riserva il diritto di svolgere indagini su qualsiasi potenziale violazione delle AUP (Acceptable Use Policy, Norme di utilizzo accettabile) da parte del Cliente. Tali indagini possono includere la revisione dei Dati del cliente.
  - 3.2 **Privacy**. Il Cliente è responsabile dei consensi e delle comunicazioni richiesti per permettere (a) l'utilizzo e il ricevimento dei Servizi da parte del

Cliente e (b) l'accesso, l'archiviazione e il trattamento da parte di Google dei dati forniti dal Cliente (inclusi i Dati del cliente) ai sensi del Contratto.

- 3.3 **Limitazioni**. Il Cliente non potrà effettuare le seguenti operazioni, né consentire agli Utenti finali di effettuarle: (a) copiare, modificare i Servizi o crearne un'opera derivata; (b) eseguire processi di reverse engineering, decompilare, tradurre, disassemblare o tentare in altro modo di estrarre una parte o la totalità del codice sorgente dei Servizi (salvo nella misura in cui tale limitazione sia espressamente vietata dalla legge vigente); (c) vendere, rivendere, concedere in sublicenza, trasferire o distribuire una parte o la totalità dei Servizi oppure (d) accedere o utilizzare i Servizi (i) per Attività ad alto rischio; (ii) in violazione delle AUP (Acceptable Use Policy, Norme di utilizzo accettabile); (iii) in modo volto a evitare il pagamento delle Tariffe (inclusa la creazione di più Account Cliente che simuli o funga da singolo Account Cliente o al fine di aggirare quote o limiti di utilizzo specifici dei Servizi); (iv) per partecipare al mining di criptovaluta senza previa approvazione scritta di Google; (v) per effettuare o ricevere chiamate ai servizi di emergenza, salvo se diversamente indicato nei Termini specifici per i servizi; (vi) per materiali o attività soggetti alla normativa ITAR (International Traffic in Arms Regulations) emanata dal Dipartimento di Stato degli Stati Uniti; (vii) in modo tale da violare o causare la violazione di Leggi in materia di controllo delle esportazioni o (viii) per la trasmissione, l'archiviazione o il trattamento di informazioni sanitarie soggette alle normative HIPAA degli Stati Uniti, ad eccezione di quanto consentito da un BAA HIPAA sottoscritto.
- 3.4 **Prodotti aggiuntivi**. Google mette a disposizione del Cliente e dei suoi Utenti finali Prodotti aggiuntivi facoltativi. Il Cliente può attivare o disattivare i Prodotti aggiuntivi in qualsiasi momento tramite la Console di amministrazione. Qualsiasi utilizzo dei Prodotti aggiuntivi è soggetto ai Termini per i Prodotti aggiuntivi, che sono incorporati mediante riferimento nel presente Contratto e possono essere aggiornati da Google di volta in volta.
- 3.5 **Amministrazione dei Servizi**. Il Cliente può specificare tramite la Console di amministrazione uno o più Amministratori che avranno il diritto di accedere ad Account amministratore. È responsabilità del Cliente (a) mantenere la riservatezza e la sicurezza degli Account utente finale e delle password associate e (b) qualsiasi utilizzo degli Account utente finale. Il Cliente conviene che le responsabilità di Google non si estendono alla gestione o amministrazione interna dei Servizi per il Cliente o per qualsiasi Utente finale.
- 3.6 **Monitoraggio degli abusi**. Il Cliente è l'unico responsabile del monitoraggio e della risposta alle email inviate agli alias "abuse" e "postmaster", nonché di ogni altro loro trattamento, per i propri Nomi di dominio. Google potrà tuttavia monitorare le email inviate a tali alias al fine di identificare eventuali abusi riguardanti i Servizi.
- 3.7 **Richiesta di Account utente finale aggiuntivi durante il Periodo di validità degli ordini**. Il Cliente può acquistare Account utente finale aggiuntivi durante il Periodo di validità dell'ordine tramite un Modulo d'ordine o un Ordine rivenditore aggiuntivo oppure effettuando un ordine mediante la Console di amministrazione. Tali Account utente finale aggiuntivi avranno una durata proporzionale che terminerà l'ultimo giorno del Periodo di validità dell'ordine applicabile.
- 3.8 **Copyright**. Google risponde alle notifiche di presunta violazione del copyright e chiuderà gli Account dei trasgressori recidivi quando le circostanze lo richiedano per adeguarsi ai principi di approdo sicuro ("safe harbor") per i fornitori di servizi online ai sensi del Digital Millennium Copyright Act (Legge statunitense sul copyright).

- 4. **Sospensione**.

- 4.1 **Violazioni delle norme AUP (Acceptable Use Policy, norme di utilizzo accettabile)**. Se Google viene a conoscenza del fatto che l'utilizzo dei Servizi da parte del Cliente o di qualsiasi Utente finale viola le norme AUP, ne informerà il Cliente e richiederà al Cliente di porre rimedio alla violazione. Qualora il Cliente non riesca a porre rimedio alla violazione entro 24 ore da tale richiesta, Google potrà sospendere totalmente o parzialmente l'utilizzo dei Servizi da parte del Cliente finché la violazione non viene corretta. La Sospensione dei Servizi può includere la rimozione o l'annullamento della condivisione di contenuti che violano le norme AUP.
- 4.2 **Altre cause di Sospensione**. In deroga a quanto disposto dalla Sezione 4.1 (Violazioni delle norme AUP (Acceptable Use Policy, Norme di utilizzo accettabile)), Google può sospendere immediatamente, totalmente o in parte, l'utilizzo dei Servizi da parte del Cliente (incluso l'utilizzo dell'Account soggiacente) se (a) Google ritiene ragionevolmente che l'utilizzo dei Servizi da parte del Cliente o di qualsiasi Utente finale possa influire negativamente sui Servizi, sull'utilizzo dei Servizi da parte di altri Clienti o dei loro Utenti finali oppure sulla rete o i server Google utilizzati per fornire i Servizi; (b) esiste il sospetto che sia stato effettuato un accesso non autorizzato di terze parti ai Servizi; (c) Google ritiene ragionevolmente che sia necessaria la Sospensione immediata per ottemperare a qualsiasi legge vigente o (d) il Cliente viola le disposizioni di cui alla Sezione 3.3 (Limitazioni) o i Termini specifici per i Servizi. Google revocherà tale Sospensione quando le circostanze che hanno dato origine alla medesima siano risolte. Su richiesta del Cliente, salvo divieti previsti dalle leggi vigenti, Google comunicherà al Cliente il fondamento della Sospensione non appena ragionevolmente possibile.

- 5. **Diritti di proprietà intellettuale; Protezione dei Dati del Cliente; Feedback; Utilizzo degli Elementi distintivi del brand nell'ambito dei Servizi**.
  - 5.1 **Diritti di proprietà intellettuale**. Salvo quanto espressamente specificato nel presente Contratto, il Contratto non concede a nessuna delle due parti alcun diritto, implicito o di altro tipo, relativo ai contenuti o alla proprietà intellettuale dell'altra parte. Nei rapporti tra le parti, il Cliente possiede tutti i Diritti di proprietà intellettuale relativi ai propri Dati e Google possiede tutti i Diritti di proprietà intellettuale relativi ai Servizi.
  - 5.2 **Protezione dei Dati del Cliente**. Google accederà o utilizzerà i Dati del Cliente soltanto al fine di fornire i Servizi e i Servizi di assistenza tecnica (TSS) al Cliente o secondo quanto altrimenti indicato dal Cliente. Senza alcuna limitazione alla portata generale della frase precedente, Google non eseguirà alcun trattamento dei Dati del Cliente per scopi pubblicitari né pubblicherà Annunci pubblicitari nei Servizi. Google ha implementato e manterrà in vigore misure di salvaguardia amministrative, fisiche e tecniche per proteggere i Dati del Cliente, come illustrato in maggiore dettaglio nell'Addendum per il trattamento dei dati Cloud.
  - 5.3 **Feedback del Cliente**. Il Cliente può, a propria discrezione, fornire feedback o suggerimenti a Google in merito ai Servizi ("Feedback"). Se il Cliente fornisce il proprio Feedback, Google e le sue Società consociate possono utilizzare tale Feedback senza limitazioni e senza obblighi nei confronti del Cliente.
  - 5.4 **Utilizzo degli Elementi distintivi del brand nell'ambito dei Servizi**. Google mostrerà all'interno dei Servizi solo gli Elementi distintivi del brand del Cliente che il Cliente autorizza caricandoli nei Servizi. Google mostrerà tali Elementi distintivi del brand del Cliente all'interno delle aree designate delle pagine web che mostrano i Servizi al Cliente o ai suoi Utenti finali. Il Cliente può specificare i dettagli di tale utilizzo nella Console di amministrazione. Google può inoltre mostrare gli Elementi distintivi del brand Google nelle suddette pagine web per indicare che i Servizi sono forniti da Google.

- 6. **Servizi di assistenza tecnica**. Subordinatamente al pagamento delle Tariffe applicabili, Google fornirà Servizi di assistenza tecnica (TSS) al Cliente durante il Periodo di validità, in conformità con le Linee guida per i servizi di assistenza tecnica. Alcuni livelli dei TSS includono una Tariffa minima ricorrente, come descritto all'indirizzo https://workspace.google.com/terms/tssg.html. Se il Cliente esegue il downgrade del livello dei propri TSS durante un qualsiasi mese di calendario, Google può continuare a fornire i TSS allo stesso livello e con le stesse Tariffe TSS applicate prima del downgrade per il resto del mese.
- 7. **Informazioni riservate**.
    - 7.1 **Obbligazioni**. Il ricevente utilizzerà le Informazioni riservate della parte divulgante solo per esercitare i propri diritti e adempiere ai propri obblighi derivanti dal presente Contratto, adottando un livello di attenzione ragionevole per salvaguardare la riservatezza delle Informazioni riservate della parte divulgante. Il ricevente può divulgare le Informazioni riservate solo alle proprie Società consociate o ai propri dipendenti, agenti o consulenti professionali ("Delegati") che devono esserne a conoscenza e che abbiano accettato per iscritto di mantenerne la riservatezza (o, nel caso di consulenti professionali, che siano altrimenti vincolati a mantenerne la riservatezza). Il ricevente si assicurerà che anche i propri Delegati utilizzino le Informazioni riservate ricevute solo per esercitare i diritti e adempiere alle obbligazioni ai sensi del presente Contratto.
    - 7.2 **Obbligo di divulgazione**. In deroga a qualsiasi disposizione contraria riportata nel presente Contratto, il ricevente o la sua Società consociata possono anche divulgare Informazioni riservate nella misura richiesta da Procedimenti giudiziari applicabili, a condizione che il ricevente o la sua Società consociata compiano ogni sforzo commercialmente ragionevole per (a) informare tempestivamente l'altra parte prima di tale divulgazione delle sue Informazioni riservate e (b) soddisfare le ragionevoli richieste dell'altra parte riguardo ai suoi sforzi per opporsi alla divulgazione. In deroga a quanto sopra, le sottosezioni (a) e (b) di cui sopra non saranno applicabili se il ricevente stabilisce che il rispetto delle sottosezioni (a) e (b) potrebbe (i) comportare la violazione di un Procedimento giudiziario; (ii) ostacolare un'indagine governativa o (iii) causare morte o gravi lesioni fisiche a un privato.
- 8. **Periodo di validità e Risoluzione/recesso**.
    - 8.1 **Periodo di validità del Contratto**. Il Periodo di validità del presente Contratto ("Periodo di validità") decorrerà dalla Data di validità e si protrarrà fino alla risoluzione/recesso o mancato rinnovo del Contratto, come stabilito dalla presente Sezione 8 (Periodo di validità e Risoluzione/recesso).
    - 8.2 **Rinnovo**.
        - (a) **Con un piano flessibile**. I Periodi di validità degli ordini relativi al piano flessibile sono mensili. Alla fine di ogni mese, il Periodo di validità dell'ordine si rinnoverà automaticamente per un ulteriore mese, a meno che non venga annullato dal Cliente tramite la Console di amministrazione.
        - (b) **Con un piano annuale/con scadenza fissa**. Al termine del Periodo di validità di ciascun ordine relativo a un piano annuale/con scadenza fissa, i Servizi si rinnoveranno in linea con le scelte effettuate dal Cliente nel relativo Modulo d'ordine o nella Console di amministrazione.
        - (c) **Termini generali**. Il Cliente può utilizzare la Console di amministrazione per adeguare e modificare il numero di Account utente finale da rinnovare. Il Cliente continuerà a pagare a Google le Tariffe al momento in vigore per ogni Account utente finale rinnovato, salvo diversi accordi stipulati tra il Cliente e Google. Se una delle parti non intende

rinnovare i Servizi, deve notificare tale decisione all'altra parte almeno 15 giorni prima della fine del Periodo di validità dell'ordine al momento in vigore. Tale notifica avrà effetto dopo la conclusione del Periodo di validità dell'ordine al momento in vigore.

- 8.3 **Risoluzione per violazione**. Nella misura consentita dalla legge vigente, ciascuna delle parti può risolvere il presente Contratto con effetto immediato previa notifica scritta se l'altra parte (a) viola sostanzialmente il Contratto e non pone rimedio a tale violazione entro 30 giorni dalla ricezione della notifica scritta relativa alla violazione o (b) sospende la propria attività o diventa soggetta a procedure di insolvenza e tali procedure non vengono respinte entro 90 giorni.
- 8.4 **Recesso libero**. Il Cliente può interrompere l'utilizzo dei Servizi in qualsiasi momento. Subordinatamente all'adempimento di tutti gli impegni finanziari del Cliente previsti da un Modulo d'ordine o altrimenti dal presente Contratto (incluso il pagamento di tutte le Tariffe per il Periodo di validità dell'ordine), il Cliente può anche recedere dal presente Contratto per ragioni di convenienza in qualsiasi momento, previa notifica scritta.
- 8.5 **Risoluzione di diritto; Violazione di legge**. Google può risolvere il presente Contratto e/o qualsiasi Modulo d'ordine vigente con effetto immediato, previa notifica scritta, qualora ritenga ragionevolmente che (a) il proseguimento della fornitura di qualsiasi Servizio utilizzato dal Cliente violi la legge vigente o le leggi vigenti oppure che (b) il Cliente abbia violato o indotto Google a violare qualsiasi legge anticorruzione o legge in materia di controllo delle esportazioni.
- 8.6 **Effetti della risoluzione/del recesso o del mancato rinnovo**. Se il Contratto è oggetto di risoluzione o di recesso o non viene rinnovato, (a) ogni diritto e accesso ai Servizi cesserà (compreso l'accesso ai Dati del Cliente), salvo diversa indicazione nel presente Contratto, e (b) tutte le Tariffe dovute dal Cliente a Google diventeranno immediatamente esigibili non appena il Cliente riceverà la fattura elettronica finale o come indicato nella fattura finale.
- 8.7 **Esclusione di rimborso**. Salvo diversa disposizione esplicita del presente Contratto, la risoluzione/il recesso o il mancato rinnovo ai sensi di qualsiasi sezione del presente Contratto (incluso l'Addendum per il trattamento dei dati Cloud) non obbligherà Google a rimborsare alcuna Tariffa.

- 9. **Pubblicità**. Il Cliente può dichiarare pubblicamente di essere un cliente di Google e mostrare gli Elementi distintivi del brand di Google conformemente alle Linee guida del marchio. Google può utilizzare il nome e gli Elementi distintivi del brand del Cliente nei materiali promozionali online o offline dei Servizi. Ciascuna delle parti può utilizzare gli Elementi distintivi del brand dell'altra parte solo secondo quanto consentito dal Contratto stesso. L'eventuale utilizzo degli Elementi distintivi del brand di una parte andrà a vantaggio della parte che detiene i Diritti di proprietà intellettuale in relazione a tali Elementi distintivi del brand.
- 10. **Dichiarazioni e garanzie**. Ciascuna delle parti dichiara e garantisce (a) di avere pieno potere e autorità per stipulare il presente Contratto e (b) di impegnarsi a rispettare tutte le leggi vigenti applicabili alla fornitura, al ricevimento e all'utilizzo dei Servizi, a seconda dei casi.
- 11. **Disclaimer**. **Salvo quanto espressamente previsto dal Contratto, Google non fornisce, e limita espressamente nella misura massima consentita dalle leggi vigenti, (a) garanzie di qualsiasi tipo, esplicite, implicite, legali o di altro genere, incluse le garanzie di commerciabilità, idoneità a uno scopo particolare, titolo, non violazione di diritti di terzi o utilizzo privo di errori o ininterrotto dei Servizi e (b) dichiarazioni in merito ai contenuti o alle informazioni accessibili attraverso i Servizi.**
- 12. **Limitazione di responsabilità**.

- 12.1 **Limitazione della responsabilità indiretta. Nella misura consentita dalla legge vigente e fatta salva la Sezione 12.3 (Responsabilità illimitate), nessuna delle parti avrà Responsabilità derivanti da o relative al Contratto per eventuali (a) danni indiretti, consequenziali, speciali, incidentali o punitivi o (b) perdite di fatturato, profitti, risparmi o reputazione.**
- 12.2 **Limiti sull'importo di responsabilità. La Responsabilità complessiva totale in capo a ciascuna delle parti per i danni derivanti dal Contratto o a esso relativi è limitata all'importo delle Tariffe pagate dal Cliente nel corso dei 12 mesi precedenti l'evento che ha dato luogo alla Responsabilità.**
- 12.3 **Responsabilità illimitate. Nessuna disposizione nel presente Contratto esclude o limita la Responsabilità di ciascuna delle parti in caso di:**
  - **(a) frode o rappresentazione ingannevole fraudolenta;**
  - **(b) inadempienza ai propri obblighi ai sensi della Sezione 13 (Indennizzo);**
  - **(c) violazione dei Diritti di proprietà intellettuale dell'altra parte;**
  - **(d) inadempienza ai propri obblighi di pagamento previsti dal Contratto o**
  - **(e) questioni per cui non è possibile escludere o limitare la responsabilità ai sensi della legge vigente.**

- 13. **Indennizzo**.
  - 13.1 **Obblighi di indennizzo di Google**. Google difenderà il Cliente e le sue Società consociate che utilizzano i Servizi previsti per l'Account del Cliente e li terrà indenni dalle Responsabilità indennizzate in qualsiasi Procedimento legale di terze parti nella misura in cui questo derivi da un'accusa di presunta violazione dei Diritti di proprietà intellettuale di una terza parte da parte di qualsiasi Servizio o qualsiasi Elemento distintivo del brand di Google, in entrambi i casi utilizzati conformemente al Contratto.
  - 13.2 **Obblighi di indennizzo del Cliente**. Il Cliente difenderà Google e le sue Società consociate che forniscono i Servizi e le terrà indenni dalle Responsabilità indennizzate in qualsiasi Procedimento legale di terze parti nella misura in cui questo derivi (a) da Dati del Cliente o Elementi distintivi del brand del Cliente oppure (b) dall'utilizzo dei Servizi in violazione delle AUP o della Sezione 3.4 (Limitazioni) da parte del Cliente o di un Utente finale.
  - 13.3 **Esclusioni**. Le Sezioni 13.1 (Obblighi di indennizzo di Google) e 13.2 (Obblighi di indennizzo del Cliente) non si applicheranno nel caso in cui l'accusa soggiacente derivi da (a) una violazione del Contratto da parte della parte indennizzata o (b) una combinazione della tecnologia o degli Elementi distintivi del brand della parte indennizzante con materiali non forniti dalla parte indennizzante ai sensi del Contratto, a meno che la combinazione non sia richiesta dal Contratto stesso.
  - 13.4 **Condizioni**. Le sezioni 13.1 (Obblighi di indennizzo di Google) e 13.2 (Obblighi di indennizzo del Cliente) sono subordinate a quanto segue:
    - (a) Qualsiasi parte indennizzata deve tempestivamente notificare per iscritto alla parte indennizzante la pretesa o le pretese che hanno preceduto il Procedimento legale di terze parti e collaborare in misura ragionevole con la parte indennizzante per risolvere tali pretese e il Procedimento legale di terze parti. Qualora una violazione della presente Sezione 13.4(a) pregiudichi la difesa del Procedimento legale iniziato da terze parti, le obbligazioni della parte indennizzante di cui alla Sezione 13.1 (Obbligazioni di

indennizzo di Google) o 13.2 (Obbligazioni di indennizzo del Cliente), secondo il caso, saranno ridotte in misura proporzionale al pregiudizio.

- (b) Qualsiasi parte indennizzata deve cedere il controllo esclusivo della porzione indennizzata del Procedimento legale di terze parti alla parte indennizzante, in base a quanto segue: (i) la parte indennizzata può incaricare un proprio legale, senza facoltà di controllo, a proprie spese e (ii) qualsiasi soluzione che richieda alla parte indennizzata di ammettere responsabilità, pagare denaro o intraprendere (o astenersi dall'intraprendere) qualsiasi azione, richiederà il previo consenso scritto della parte indennizzata, che non dovrà essere irragionevolmente trattenuto, condizionato o ritardato.

- 13.5 **Rimedi**.
  - (a) Qualora Google ritenga ragionevolmente che i Servizi violino i Diritti di proprietà intellettuale di una terza parte, può a propria discrezione e a proprie spese (i) ottenere il diritto per il Cliente di continuare a utilizzare i Servizi; (ii) modificare i Servizi in modo tale da renderli conformi senza ridurne significativamente la funzionalità o (iii) sostituire i Servizi con un'alternativa conforme ed equivalente a livello funzionale.
  - (b) Se Google non ritiene che i rimedi di cui alla Sezione 13.5(a) siano commercialmente ragionevoli, potrà sospendere o interrompere l'utilizzo dei Servizi interessati da parte del Cliente. Nel caso in cui cessi l'erogazione dei Servizi interessati, Google rimborserà in forma proporzionale le Tariffe non dovute ed effettivamente pagate dal Cliente in relazione al periodo seguente la cessazione di tali Servizi.
- 13.6 **Diritti e obbligazioni esclusivi**. Senza pregiudicare qualsiasi altro diritto di risoluzione/recesso di ciascuna delle parti, la presente Sezione 13 (Indennizzo) determina il solo e unico rimedio a disposizione delle parti ai sensi del presente Contratto in relazione alle accuse di presunta violazione dei Diritti di proprietà intellettuale avanzate da terze parti e descritte nella presente Sezione 13 (Indennizzo).

- 14. **Clienti dei rivenditori**. La presente Sezione 14 (Clienti dei rivenditori) si applica solo se il Cliente ordina i Servizi presso un Rivenditore sulla base di un Contratto con il rivenditore (tali Servizi sono denominati "Servizi del rivenditore").
  - 14.1 **Termini applicabili**. Ai fini dei Servizi del rivenditore:
    - (a) non si applica la Sezione 2 (Termini di pagamento) del presente Contratto;
    - (b) si applicheranno, e saranno dovute direttamente al Rivenditore, le Tariffe di rivendita, e tutti i prezzi dei Servizi del rivenditore saranno determinati unicamente tra il Rivenditore e il Cliente;
    - (c) il Cliente riceverà dal Rivenditore gli eventuali crediti applicabili previsti dallo SLA (accordo sul livello del servizio);
    - (d) la Sezione 12.2 (Limiti sull'importo di responsabilità) è sostituita dalla seguente frase: "La Responsabilità complessiva totale in capo a ciascuna delle parti per i danni derivanti dal Contratto o a esso relativi è limitata alle Tariffe di rivendita pagate dal Cliente per i Servizi del rivenditore nel corso dei 12 mesi che precedono l'evento che ha dato luogo alla Responsabilità".

        - (e) l'eventuale rinnovo o gli eventuali rinnovi dei Servizi e/o gli eventuali Ordini rivenditore saranno concordati tra il Cliente e il Rivenditore.
        - (f) per "Periodo di validità dell'ordine", così come utilizzato nel Contratto, si intende il periodo di tempo che parte dalla Data di inizio dei Servizi o dalla Data di rinnovo (secondo i casi) per i Servizi del rivenditore e si protrae per il periodo specificato nell'Ordine rivenditore al momento in vigore, a meno che non venga cessato in conformità alle disposizioni del presente Contratto e
        - (g) per "Data di inizio dei servizi", così come utilizzata nel Contratto, si intende la data di inizio indicata nell'Ordine rivenditore o, se nessuna data è ivi specificata, la data in cui Google mette a disposizione del Cliente i Servizi del rivenditore.
    - 14.2 **Condivisione di informazioni riservate**. Google può condividere Informazioni riservate del Cliente con il Rivenditore in qualità di Delegato in conformità a quanto disposto dalla Sezione 7.1 (Obbligazioni).
    - 14.3 **Rivenditore come amministratore**. A discrezione del Cliente, il Rivenditore può accedere all'Account del Cliente o agli Account utente finale del Cliente. Nei rapporti tra Google e il Cliente, il Cliente è l'unico responsabile (a) di qualsiasi accesso da parte del Rivenditore all'Account del Cliente o agli Account utente finale del Cliente e (b) della definizione nel Contratto con il rivenditore di qualsiasi obbligazione o diritto tra il Rivenditore e il Cliente in merito ai Servizi del rivenditore.
    - 14.4 **Assistenza tecnica del Rivenditore**. Il Cliente riconosce e accetta che il Rivenditore può divulgare i Dati personali dell'Utente finale a Google come ragionevolmente richiesto al fine di consentire al Rivenditore di gestire qualsiasi problema di assistenza che il Cliente riassegni al Rivenditore o per suo tramite.
- 15. **Disposizioni varie**.
    - 15.1 **Comunicazioni**. Ai sensi del presente Contratto, le comunicazioni al Cliente devono essere inviate all'Indirizzo email di notifica e le comunicazioni a Google devono essere inviate a legal-notices@google.com. La comunicazione viene considerata ricevuta al momento dell'invio dell'email. È responsabilità del Cliente tenere aggiornato l'Indirizzo email di notifica per tutto il Periodo di validità.
    - 15.2 **Email**. Le parti possono utilizzare i messaggi email per soddisfare i requisiti di approvazione e consenso per iscritto previsti dal presente Contratto.
    - 15.3 **Trasferimento**. Nessuna delle parti può trasferire alcuna parte del presente Contratto senza il consenso scritto dell'altra parte, fatta eccezione per una Società consociata, laddove (a) l'assegnatario abbia accettato per iscritto di essere vincolato dai termini del presente Contratto e (b) la parte cedente abbia comunicato all'altra parte tale trasferimento. Qualsiasi altro tentativo di trasferimento sarà considerato nullo. Se il Cliente trasferisce il presente Contratto a una Società consociata in un'altra giurisdizione in modo da causare una modifica della persona giuridica Google contraente così come specificata all'indirizzo https://cloud.google.com/terms/google-entity: (i) il presente Contratto viene automaticamente trasferito alla nuova persona giuridica Google contraente e (ii) se l'account di fatturazione della Società consociata si trova in Brasile, a partire dal momento del trasferimento saranno applicati i Termini di servizio vigenti consultabili al link di cui sopra e non il presente Contratto.
    - 15.4 **Cambio di Controllo.**Se una parte è oggetto di un cambio di Controllo che non deriva da una ristrutturazione o una riorganizzazione interna (bensì, ad esempio, dall'acquisto o dalla vendita di azioni, da una

fusione o da un'altra forma di transazione aziendale), tale parte invierà una comunicazione scritta all'altra parte entro 30 giorni dal cambio di Controllo.

- 15.5 **Forza maggiore**. Nessuna parte sarà ritenuta responsabile in caso di mancato o ritardato adempimento causato da circostanze che esulano dal suo ragionevole controllo, inclusi eventi fortuiti, calamità naturali, terrorismo, rivolte o guerre.
- 15.6 **Subcontratto**. Google può stipulare un subcontratto riguardo alle obbligazioni previste dal presente Contratto, ma rimane responsabile verso il Cliente per qualsiasi obbligazione ceduta mediante subcontratto.
- 15.7 **Esclusione di rapporti di agenzia**. Il presente Contratto non determina la creazione di un rapporto di agenzia, partnership o joint venture tra le parti.
- 15.8 **Esclusione di rinuncia**. Il mancato o ritardato esercizio dei diritti spettanti alle parti ai sensi del presente Contratto non comporterà una rinuncia a tali diritti.
- 15.9 **Clausola salvatoria**. Se una qualsiasi parte del presente Contratto non è valida, è illegale o non azionabile, il resto del Contratto rimarrà in vigore.
- 15.10 **Esclusione di beneficiari terzi**. Il presente Contratto non conferisce alcun vantaggio a nessuna terza parte, salvo laddove espressamente dichiarato.
- 15.11 **Provvedimento equitativo**. Nulla nel presente Contratto limiterà la facoltà delle parti di richiedere un provvedimento equitativo.
- 15.12 **Legislazione vigente degli Stati Uniti**.
    - (a) **Enti governativi di città, contee e stati degli Stati Uniti d'America**. Se il Cliente è un ente governativo di una città, una contea o uno stato statunitensi, il Contratto non includerà disposizioni relative alla legislazione vigente e alla sede del processo.
    - (b) **Enti governativi federali degli Stati Uniti d'America**. Se il Cliente è un ente governativo federale statunitense, si applica quanto segue: TUTTE LE RIVENDICAZIONI RISULTANTI DAL PRESENTE CONTRATTO O DAI SERVIZI, O A QUESTI RELATIVE, SARANNO REGOLATE DALLE LEGGI DEGLI STATI UNITI D'AMERICA, A ESCLUSIONE DELLE NORME RELATIVE AL CONFLITTO DI LEGGI. ESCLUSIVAMENTE NELLA MISURA CONSENTITA DALLA LEGGE FEDERALE: (I) IN ASSENZA DI UNA LEGGE FEDERALE VIGENTE SI APPLICHERANNO LE LEGGI DELLO STATO DELLA CALIFORNIA, AD ESCLUSIONE DELLE NORME DI TALE STATO SUL CONFLITTO DI LEGGI, E (II) PER TUTTE LE RIVENDICAZIONI RISULTANTI DAL PRESENTE CONTRATTO O DAI SERVIZI, O A ESSI RELATIVE, LE PARTI CONCORDANO DI ACCETTARE COME GIURISDIZIONE PERSONALE E SEDE ESCLUSIVA DEL PROCESSO I TRIBUNALI DELLA CONTEA DI SANTA CLARA, CALIFORNIA (STATI UNITI).
    - (c) **Per tutte le altre persone giuridiche**. Se il Cliente è una persona giuridica non indicata nella Sezione 15.12 (a) (Legislazione vigente statunitense per gli Enti governativi di città, contee e stati degli Stati Uniti d'America) o (b) (Legislazione vigente statunitense per gli Enti governativi federali degli Stati Uniti d'America), si applicano le seguenti condizioni: TUTTE LE RIVENDICAZIONI RISULTANTI DAL PRESENTE CONTRATTO O DAI SERVIZI, O A ESSI

RELATIVE, SARANNO REGOLATE DALLE LEGGI DELLA CALIFORNIA, AD ESCLUSIONE DELLE NORME DI TALE STATO SUL CONFLITTO DI LEGGI E LE RELATIVE CONTROVERSIE SARANNO OGGETTO DI GIUDIZIO ESCLUSIVAMENTE PRESSO I TRIBUNALI FEDERALI O STATALI DELLA CONTEA DI SANTA CLARA, CALIFORNIA (STATI UNITI); LE PARTI ACCONSENTONO ALLA GIURISDIZIONE PERSONALE IN TALI TRIBUNALI.

- 15.13 **Emendamenti**. Fatto salvo quanto dichiarato nella Sezione 1.4 (b) (Modifiche: al Contratto), (c) (Modifiche: ai Termini URL) o (d) (Modifiche: all'Addendum per il trattamento dei dati Cloud), qualsiasi emendamento al presente Contratto dopo la Data di validità deve essere in forma scritta, firmato da entrambe le parti e con l'espressa indicazione che si tratta di un emendamento del presente Contratto. Per chiarezza, la fornitura da parte di Google di un URL aggiornato in sostituzione di qualsiasi URL indicato nel presente Contratto non costituisce un emendamento o una modifica dei termini del Contratto.
- 15.14 **Sopravvivenza**. Le seguenti Sezioni sopravviveranno alla scadenza o alla risoluzione del presente Contratto: Sezione 2 (Termini di pagamento), Sezione 5 (Diritti di proprietà intellettuale; Protezione dei Dati del cliente; Feedback; Utilizzo degli Elementi distintivi del brand nell'ambito dei Servizi), Sezione 7 (Informazioni riservate), Sezione 8.6 (Effetti della risoluzione o del mancato rinnovo), Sezione 11 (Disclaimer), Sezione 12 (Limitazione di responsabilità), Sezione 13 (Indennizzo), Sezione 14.1 (Termini applicabili), Sezione 14.2 (Condivisione di informazioni riservate) e Sezione 15 (Disposizioni varie).
- 15.15 **Intero contratto**. Il presente Contratto definisce tutti i termini concordati tra le parti e risolve e prevale su qualunque altro contratto stipulato tra le parti relativo allo stesso oggetto, incluse eventuali versioni precedenti del presente Contratto. Con la sottoscrizione del presente Contratto, nessuna delle parti ha fatto affidamento, né sarà titolare di alcun diritto o rimedio basati su affermazioni, dichiarazioni o garanzie (rese per negligenza o in buona fede), ad eccezione di quanto espressamente stabilito dal presente Contratto. I Termini URL sono incorporati nel Contratto mediante riferimento. Dopo la Data di validità, Google può fornire un URL aggiornato in sostituzione di qualsiasi URL nel presente Contratto.
- 15.16 **Termini in conflitto**. Qualora esista un conflitto tra i documenti che costituiscono il presente Contratto, i seguenti documenti prevarranno nel seguente ordine di priorità decrescente: il Modulo d'ordine, l'Addendum per il trattamento dei dati Cloud, il resto del Contratto (esclusi i Termini URL) e i Termini URL (diversi dall'Addendum per il trattamento dei dati Cloud).
- 15.17 **Intestazioni**. Le intestazioni e le didascalie utilizzati nel Contratto hanno solo fini di riferimento e non avranno alcun effetto sull'interpretazione del Contratto.
- 15.18 **Conflitto tra versioni in lingue diverse**. Se il presente Contratto viene tradotto in una lingua diversa dall'inglese ed esiste una discrepanza tra il testo in inglese e il testo tradotto, prevarrà il testo in inglese, salvo laddove espressamente specificato nella traduzione.
- 15.19 **Definizioni**.
    - Per "Account" si intendono le credenziali dell'Account Google del Cliente e il relativo accesso ai Servizi ai sensi del presente Contratto.
    - Per "Prodotti aggiuntivi" si intendono i prodotti, i servizi e le applicazioni che non fanno parte dei Servizi, ma che potrebbero essere accessibili per l'utilizzo insieme ai Servizi.
    - Per "Termini dei prodotti aggiuntivi" si intendono i termini al momento in vigore, definiti

all'indirizzo https://workspace.google.com/intl/it/terms/additional_services.html.

- Per "Account amministratore" si intende un tipo di Account utente finale che il Cliente (o il Rivenditore, a seconda dei casi) può utilizzare per amministrare i Servizi.
- Per "Console di amministrazione" si intendono la console, le console o la dashboard online fornite da Google al Cliente per amministrare i Servizi.
- Per "Amministratori" si intende il personale che amministra i Servizi per gli Utenti finali per conto del Cliente e da lui designato e che ha la possibilità di accedere ai Dati del cliente e agli Account utente finale. Tale accesso include la possibilità di accedere, monitorare, utilizzare, modificare, trattenere o divulgare qualsiasi dato disponibile agli Utenti finali associato ai loro Account utente finale.
- Per "Pubblicità" si intendono gli annunci online mostrati da Google agli Utenti finali, esclusi gli annunci che il Cliente sceglie esplicitamente di far mostrare da Google o dalle sue Società consociate in relazione ai Servizi sulla base di un contratto separato (ad esempio annunci di Google AdSense implementati dal Cliente su un sito web creato dal Cliente utilizzando qualsiasi funzionalità di "Google Sites" inclusa nei Servizi).
- Per "Società consociata" si intende qualsiasi persona giuridica che, direttamente o indirettamente, controlla, è controllata da o è soggetta a controllo comune con una delle parti.
- Per "Leggi anticorruzione" si intendono tutte le leggi anticorruzione commerciali e pubbliche vigenti, incluse la legge statunitense Foreign Corrupt Practices Act del 1977 e la legge britannica Bribery Act del 2010, che vietano l'offerta a fini di corruzione di qualsiasi bene di valore, sia direttamente sia indirettamente, a chiunque, inclusi funzionari governativi, ai fini di ottenere o mantenere opportunità commerciali o per assicurarsi qualsiasi altro vantaggio commerciale improprio. Sono considerati funzionari governativi tutti i dipendenti pubblici, i candidati a cariche pubbliche, i membri di famiglie reali nonché i dipendenti di società pubbliche o statali, organizzazioni internazionali pubbliche e partiti politici.
- Per "AUP (Acceptable Use Policy, norme di utilizzo accettabile)" si intendono le norme di utilizzo accettabile al momento in vigore, indicate all'indirizzo https://workspace.google.com/intl/it/terms/use_policy.html.
- Il "BAA" o "Contratto di società in affari" è un emendamento al presente Contratto che tratta la gestione dei dati sanitari protetti (così come definiti nell'HIPAA).
- Per "Elementi distintivi del brand" si intendono i nomi commerciali, i marchi, i marchi di servizio, i loghi, i nomi di dominio e altri elementi distintivi del brand di ciascuna delle parti, rispettivamente, come di volta in volta ottenuti da tale parte.
- Per "Addendum per il trattamento dei dati Cloud" si intendono i termini di volta in volta vigenti che descrivono le obbligazioni in materia di protezione e trattamento dei dati in relazione ai Dati del cliente, come descritto

all'indirizzo https://cloud.google.com/terms/data-processing-addendum.

- Per "Informazioni riservate" si intendono le informazioni che una delle parti (o una Società consociata) divulga all'altra parte ai sensi del presente Contratto e che sono contrassegnate come riservate o che normalmente, in base alle circostanze, sarebbero considerate informazioni riservate. Non includono le informazioni sviluppate in modo indipendente dal ricevente, divulgate legalmente al ricevente da una terza parte in assenza di obblighi di riservatezza o che diventino pubbliche senza alcuna colpa del ricevente. Ferme restando le disposizioni della frase precedente, i Dati del cliente sono considerati Informazioni riservate del Cliente.
- Per "Controllo" si intende il controllo di oltre il 50% dei diritti di voto o di partecipazioni al capitale di una delle parti.
- Per "Servizi principali" si intendono i "Servizi principali" al momento in vigore così come descritti nel Riepilogo dei servizi, ad esclusione di eventuali Offerte di terze parti.
- Per "Dati del cliente" si intendono i dati inoltrati, archiviati, inviati o ricevuti dal Cliente o dai suoi Utenti finali mediante i Servizi.
- Per "Indirizzo email di dominio" si intende l'indirizzo email del Nome di dominio da utilizzare in relazione ai Servizi.
- Per "Nome di dominio" si intende il nome di dominio specificato nel Modulo d'ordine o nell'Ordine rivenditore da utilizzare in relazione ai Servizi.
- Per "Utenti finali" si intendono i privati a cui il Cliente consente di utilizzare i Servizi e che sono gestiti da un Amministratore. Per chiarezza, tra gli Utenti finali possono essere compresi i dipendenti di Società consociate del Cliente e altre terze parti.
- Per "Account utente finale" si intende un account ospitato da Google e creato dal Cliente tramite i Servizi per consentire a un Utente finale di utilizzare i Servizi.
- Per "Leggi in materia di controllo delle esportazioni" si intendono tutte le leggi e le normative applicabili relative al controllo delle esportazioni e delle riesportazioni, comprese (a) le normative "EAR" (Export Administration Regulations) del Dipartimento del Commercio degli Stati Uniti, (b) le sanzioni di carattere commerciale ed economico previste dall'Ufficio di controllo dei beni stranieri del Dipartimento del Tesoro degli Stati Uniti e (c) le normative "ITAR" (International Traffic in Arms Regulations) del Dipartimento di Stato degli Stati Uniti.
- Per "Tariffe" si intendono (a) il prodotto della quantità dei Servizi utilizzati o ordinati dal Cliente moltiplicata per i Prezzi o (b) le tariffe applicabili per i TSS più eventuali Imposte applicabili.
- Per "Attività ad alto rischio" si intendono attività in cui l'utilizzo o il non funzionamento dei Servizi potrebbe ragionevolmente comportare morte, lesioni personali o danni all'ambiente o alle proprietà (come, ad esempio, la realizzazione o la gestione di impianti nucleari, il controllo del traffico aereo, i sistemi di supporto vitale o le armi).

- "HIPAA" indica l'Health Insurance Portability and Accountability Act del 1996, come di volta in volta modificato, e qualsiasi regolamento emanato in base allo stesso.
- Per "incluso" si intende incluso a titolo esemplificativo.
- Per "Responsabilità indennizzate" si intendono (i) i costi di conciliazione approvati dalla parte indennizzante e (ii) i danni e i costi riconosciuti in via definitiva nei confronti della parte indennizzata da un tribunale di giurisdizione competente.
- Per "Diritti di proprietà intellettuale" si intendono tutti i diritti di brevetto, copyright, diritti sui marchi, diritti sui segreti commerciali (se esistenti), diritti di progettazione, diritti sui database, diritti sui nomi di dominio, diritti morali e ogni altro diritto di proprietà intellettuale (registrato o non registrato) in tutto il mondo.
- Per "Procedimento giudiziario" si intende una richiesta di divulgazione di informazioni presentata ai sensi di legge, di regolamenti governativi, di ingiunzioni, citazioni o mandati di tribunali oppure di altra valida autorità giuridica, procedura legale o procedimento analogo.
- Per "Responsabilità" si intende qualsiasi tipo di responsabilità, sia contrattuale, sia per illecito civile (inclusa la negligenza) o altro, indipendentemente dal fatto che fosse prevedibile o contemplata dalle parti.
- Per "Indirizzo email di notifica" si intendono l'indirizzo o gli indirizzi email indicati dal Cliente nella Console di amministrazione.
- Per "Modulo d'ordine" si intende un modulo d'ordine eseguito dal Cliente o un ordine effettuato dal Cliente mediante un sito web di Google che specifichi, in ciascun caso, i Servizi che Google fornirà al Cliente ai sensi del Contratto.
- Per "Periodo di validità dell'ordine" si intende il periodo di tempo a partire dalla Data di inizio dei Servizi o dalla data di rinnovo (a seconda dei casi) e che si protrae per il periodo indicato sul Modulo d'ordine, a meno che non venga interrotto in conformità al presente Contratto.
- Per "Altri servizi" si intendono gli "Altri servizi" al momento in vigore descritti nel Riepilogo dei servizi, ad eccezione delle Offerte di terze parti.
- Per "Prezzi" si intendono i prezzi di volta in volta in vigore applicabili ai Servizi e descritti all'indirizzo https://workspace.google.com/intl/it/pricing.html (incorporati nel Contratto per mezzo di questo riferimento) salvo se diversamente concordato in un addendum o in un Modulo d'ordine. I Prezzi sono al netto delle Imposte.
- Per "Rivenditore" si intende, se applicabile, il rivenditore autorizzato di terza parte non affiliato, che vende i Servizi al Cliente.
- Per "Contratto con il rivenditore" si intende, se applicabile, il contratto separato tra il Cliente e il Rivenditore riguardo ai Servizi. Il Contratto con il rivenditore è un contratto a sé ed esula dall'ambito del presente Contratto.
- Per "Tariffe del rivenditore" si intendono le eventuali tariffe dei Servizi utilizzati o ordinati dal Cliente e concordate in un Contratto con il rivenditore, più eventuali Imposte applicabili.

- Per "Ordine del rivenditore" si intende, se applicabile, un modulo d'ordine (incluso un modulo d'ordine di rinnovo) emesso da un Rivenditore ed eseguito dal Cliente e dal Rivenditore, in cui sono specificati i Servizi che il Cliente ordina presso il Rivenditore.
- Per "Termini specifici dei servizi" si intendono i termini al momento in vigore e specifici di uno o più Servizi, indicati all'indirizzo https://workspace.google.com/intl/it/terms/service-terms/.
- Per "Servizi" si intendono i Servizi principali e gli Altri servizi al momento in vigore.
- Per "Data di inizio dei servizi" si intende la data di inizio indicata nel Modulo d'ordine o, se non è specificata nel Modulo d'ordine, la data in cui Google rende i Servizi disponibili per il Cliente.
- Per "Riepilogo dei servizi" si intende la descrizione al momento in vigore riportata all'indirizzo https://workspace.google.com/intl/it/terms/user_features.html.
- Per "SLA" (accordo sul livello del servizio) si intendono uno o più accordi sul livello del servizio al momento in vigore consultabili all'indirizzo https://workspace.google.com/intl/it/terms/sla.html.
- Per "Sospendere" o "Sospensione" si intende la disattivazione dell'accesso ai Servizi o ai relativi componenti o la disattivazione del loro utilizzo.
- Per "Imposte" si intendono tutte le tasse e imposte stabilite dallo Stato, ad eccezione delle imposte basate sull'utile netto, sul patrimonio netto, sul valore patrimoniale, sul valore degli immobili o sui dati occupazionali di Google.
- "Periodo di validità" avrà il significato di cui alla Sezione 8.1 (Periodo di validità del Contratto) del presente Contratto.
- Per "Procedimento legale di terze parti" si intende qualsiasi procedimento legale formale presentato da una parte terza non affiliata davanti a una corte o a un tribunale governativo (inclusi i procedimenti di ricorso).
- Per "Offerte di terze parti" si intendono i servizi, il software, i prodotti e altre offerte di terze parti che non sono integrati nei Servizi.
- Per "Linee guida sull'utilizzo del marchio" si intendono le linee guida al momento in vigore stabilite da Google relativamente all'utilizzo degli Elementi distintivi del brand Google da parte di Terze parti, consultabili all'indirizzo https://www.google.com/permissions/guidelines.html.
- Per "TSS" si intende il Servizio di assistenza tecnica di Google al momento in vigore.
- Per "Linee guida per i servizi di assistenza tecnica" si intendono le linee guida di Google al momento in vigore relative ai Servizi di assistenza tecnica, così come definite all'indirizzo https://workspace.google.com/intl/it/terms/tssg.html.
- Per "Termini URL" si intendono, collettivamente, le AUP (Acceptable Use Policy, Norme di utilizzo accettabile),

l'Addendum per il trattamento dei dati Cloud, i Termini specifici per i Servizi, lo SLA (accordo sul livello del servizio) e le Linee guida per i servizi di assistenza tecnica.

- 16. **Termini specifici per regione**. Se l'indirizzo di fatturazione del Cliente si trova in una regione applicabile sottoindicata, il Cliente accetta le modifiche al Contratto riportate di seguito:
    - **Asia-Pacifico - Tutte le regioni**
        - La Sezione 2.3 (Imposte) viene così sostituita:
        - 2.3 Imposte. Google riporterà nel dettaglio ogni Imposta fatturata. Se le Imposte devono essere trattenute da qualsiasi pagamento a Google, il Cliente aumenterà il pagamento a Google in modo che l'importo netto ricevuto da Google sia pari all'importo fatturato, senza riduzioni per le Imposte.
        - La definizione di "Imposte" della Sezione 15.19 (Definizioni) viene così sostituita:
        - 15.19 Definizioni.
        - Per "Imposte" si intendono tutte le imposte stabilite dallo Stato, conformemente alla legge vigente associata all'erogazione e all'esecuzione dei Servizi, inclusi, a titolo esemplificativo, eventuali dazi, dazi doganali e qualsiasi imposta diretta e indiretta e compresi eventuali interessi o sanzioni correlati, ad eccezione delle tasse e imposte basate sui profitti di Google.
    - **Asia-Pacifico (tutte le regioni ad eccezione di Australia, Giappone, India, Nuova Zelanda e Singapore) e America Latina (tutte le regioni ad eccezione del Brasile)**
        - La Sezione 15.12 (Legislazione vigente degli Stati Uniti) viene così sostituita:
        - 15.12 Legislazione vigente; Arbitrato.
        - (a) TUTTE LE RIVENDICAZIONI RISULTANTI DAL PRESENTE CONTRATTO O DAI PRODOTTI O SERVIZI GOOGLE O AI MEDESIMI CORRELATE (INCLUSE EVENTUALI CONTROVERSIE RELATIVE ALL'INTERPRETAZIONE O ALL'ADEMPIMENTO DEL CONTRATTO ("Controversia") SARANNO REGOLATE DALLE LEGGI DELLO STATO DELLA CALIFORNIA, STATI UNITI, AD ECCEZIONE DELLE RELATIVE NORME SUL CONFLITTO DI LEGGI.
        - (b) Le parti tenteranno in buona fede di risolvere qualsiasi Controversia entro 30 giorni dalla data in cui è sorta. Se la Controversia non viene risolta entro 30 giorni, dovrà essere risolta mediante arbitrato dall'International Centre for Dispute Resolution dell'American Arbitration Association, in conformità alle sue Expedited Commercial Rules in vigore alla data del presente Contratto ("Regole").
        - (c) Le parti selezioneranno di comune accordo un solo arbitro. L'arbitrato sarà condotto in inglese nella Contea di Santa Clara, California, USA.
        - (d) Ogni parte può richiedere a qualsiasi tribunale competente un provvedimento ingiuntivo necessario a tutelare i propri diritti in attesa della risoluzione dell'arbitrato. L'arbitro può disporre un provvedimento equitativo o un provvedimento ingiuntivo conforme ai rimedi e alle limitazioni del presente Contratto.

- (e) Fatti salvi i requisiti di riservatezza descritti nella Sottosezione (g), ciascuna delle parti potrà presentare a qualsiasi tribunale competente una richiesta di emissione di qualsiasi ingiunzione necessaria per proteggere i diritti o la proprietà di tale parte; la richiesta non sarà considerata una violazione o una rinuncia alla presente sezione relativa alla legislazione vigente e all'arbitrato e non pregiudicherà le competenze dell'arbitro, inclusa la sua facoltà di riesaminare una decisione giudiziaria. Le parti concordano che i tribunali della Contea di Santa Clara, California, USA, sono competenti ai fini dell'emissione di eventuali ingiunzioni in base alla presente Sottosezione 15.12 (e).
- (f) Il lodo arbitrale sarà definitivo e vincolante per le parti e la sua esecuzione potrà essere richiesta in qualsiasi tribunale competente, incluso qualsiasi tribunale che abbia giurisdizione su una delle parti o su qualsiasi bene di sua proprietà.
- (g) Qualsiasi procedura di arbitrato condotta in conformità alla presente Sezione 15.12 (Legislazione vigente; Arbitrato) sarà considerata Informazione riservata ai sensi della Sezione 7 (Informazioni riservate), inclusa: (i) l'esistenza di tali procedure di arbitrato, (ii) qualsiasi informazione divulgata durante tali procedure di arbitrato e (iii) qualsiasi comunicazione orale o documento relativi a tali procedure arbitrali. In aggiunta ai diritti di divulgazione ai sensi della Sezione 7 (Informazioni riservate), le parti possono divulgare le informazioni descritte nella presente Sottosezione 15.12 (g) a un tribunale competente nella misura necessaria ai fini della richiesta di eventuali ingiunzioni in base alla Sottosezione 15.12 (e) o dell'esecuzione di qualsiasi decisione arbitrale, ma dovranno richiedere che tali procedure giudiziarie siano condotte *a porte chiuse (in privato).*
- (h) Le parti saranno tenute a sostenere i costi per l'arbitro, le parcelle e le spese degli esperti nominati dall'arbitro, nonché le spese amministrative del centro arbitrale in conformità alle Regole. Nella sua decisione finale, l'arbitro stabilirà l'obbligazione della parte soccombente a rimborsare l'importo pagato in anticipo dalla parte prevalente a copertura di tali costi.
- (i) Ciascuna delle parti si farà carico delle parcelle e delle spese dei rispettivi avvocati ed esperti, a prescindere dalla decisione finale dell'arbitro in relazione alla Controversia.

- **Asia-Pacifico - India**
  - Google Asia Pacific Pte. Ltd. ("GAP") ha nominato Google India Private Limited rivenditore non esclusivo dei Servizi (come definito di seguito) in India. Per evitare ogni possibile dubbio, sebbene nel Contratto il termine "Google" faccia riferimento a entrambe le persone giuridiche, si precisa che, laddove le disposizioni facciano riferimento a Google per le vendite o per i relativi diritti e obbligazioni (inclusi eventuali termini inerenti alla fatturazione per la vendita di servizi, il massimale di credito, la risoluzione del presente Contratto e così via), "Google" starà a significare Google India Private Limited mentre, in tutti i casi in cui nel contratto le disposizioni facciano riferimento a "Google" in quanto fornitore dei Servizi o ai relativi diritti e obbligazioni, si intenderà "GAP".

- Google India Private Limited può eseguire il Modulo o i Moduli d'ordine facendo riferimento al Contratto, ma il Modulo d'ordine costituirà un contratto separato tra Google India e il Cliente e includerà tutti i termini del presente Contratto. In quanto rivenditore dei servizi, Google India Private Limited acquista i Servizi da GAP per rivenderli al Cliente, l'intera obbligazione di fornire tali servizi nel rispetto del Contratto sarà soddisfatta da GAP e, pertanto, Google India Private Limited non avrà alcuna obbligazione in merito alla prestazione dei Servizi.
- La Sezione 2 (Termini di pagamento) viene così sostituita:
- 2. Termini di pagamento.
- 2.1 Misurazione dell'utilizzo e opzioni di fatturazione. Per determinare l'utilizzo dei Servizi da parte del Cliente verranno impiegati gli strumenti di misurazione di Google; qualsiasi misurazione di questo tipo effettuata da Google ai fini del calcolo delle Tariffe si intende definitiva. Il Cliente può selezionare una delle opzioni di fatturazione indicate di seguito o qualsiasi altra opzione resa disponibile da Google quando il Cliente effettua l'ordine per i Servizi.
    - (a) Piano flessibile. Scegliendo questa opzione, il Cliente non si impegna ad acquistare i Servizi per una durata predefinita, bensì pagherà le Tariffe in base ai giorni di utilizzo dei Servizi, con fatturazione mensile riferita al mese precedente. L'utilizzo dei Servizi per una porzione di giornata sarà arrotondato all'utilizzo per un giorno intero, per facilitare il calcolo delle Tariffe.
    - (b) Piano annuale/con scadenza fissa. Scegliendo questa opzione, il Cliente si impegna ad acquistare i Servizi per uno o più periodi della durata di un anno (in base alla selezione del Cliente). Google addebiterà al Cliente i costi dovuti in base ai termini associati alle scelte effettuate dal Cliente nel Modulo d'ordine.
    - Google può modificare la propria offerta di opzioni di fatturazione (anche limitando o interrompendo l'offerta di qualsiasi opzione) dando un preavviso di 30 giorni al Cliente; la modifica diventerà effettiva all'inizio del successivo Periodo di validità dell'ordine del Cliente. Le opzioni di fatturazione potrebbero non essere disponibili per tutti i clienti. Il Cliente può pagare l'importo dovuto per i Servizi utilizzando le opzioni di pagamento elencate nella Sezione 2.2 (Pagamento) di seguito.
- 2.2 Pagamento. Tutti i pagamenti devono essere effettuati nella valuta indicata nel Modulo d'ordine o nella fattura.
    - (a) Carta di credito o carta di debito. Se il Cliente paga con carta di credito, carta di debito o altre forme di pagamento che non richiedono fatturazione, il pagamento dovrà essere effettuato alla fine del mese in cui il Cliente ha usufruito dei Servizi. Per le carte di

credito o di debito, secondo il caso: (i) alla scadenza, Google emetterà una fattura elettronica per tutte le Tariffe applicabili e (ii) il pagamento di tali Tariffe sarà considerato in ritardo 30 giorni dopo la fine del mese in cui il Cliente ha usufruito dei Servizi.

- (b) Fatture. Salvo se diversamente specificato nel Modulo d'ordine, i pagamenti delle fatture scadono 60 giorni dopo la data della fattura; dopo tale data, sono considerati in ritardo.
- (c) Altre forme di pagamento. Il Cliente può cambiare il proprio metodo di pagamento selezionando qualsiasi altro metodo che Google abbia abilitato nella Console di amministrazione, sempre a condizione dell'accettazione da parte del Cliente di eventuali termini aggiuntivi applicabili a tale metodo di pagamento.
- (d) Dati di pagamento. I pagamenti effettuati tramite bonifico bancario devono includere le informazioni bancarie fornite da Google.

- 2.3 Imposte.
  - (a) Come corrispettivo dei servizi, il Cliente accetta di corrispondere a Google le Tariffe secondo quando indicato sopra, più le Imposte applicabili. Qualora per Google sussista l'obbligo legale di versare o riscuotere tali Imposte, il relativo importo dovrà essere fatturato al Cliente, a meno che il Cliente non fornisca tempestivamente a Google un certificato valido di esenzione fiscale autorizzato dall'autorità fiscale competente.
  - (b) Se richiesto dalla legge vigente, il Cliente fornirà a Google i dati di identificazione fiscale applicabili, ovvero il codice "GSTIN" (Goods and Services Tax Identification Number, numero identificativo per l'imposta su beni e servizi), il luogo in cui il Cliente usufruirà dei Servizi, lo status fiscale e così via, che Google India potrà richiedere per assicurare la conformità alle leggi fiscali vigenti in India. Il Cliente conferma che tutti i dati forniti, quali ad esempio il codice GSTIN, il luogo in cui il Cliente usufruirà dei Servizi, lo status fiscale e così via, sono corretti. L'indirizzo e il codice GSTIN forniti corrispondono al luogo in cui il Cliente usufruirà dei Servizi. Il Cliente sarà responsabile del pagamento (o del rimborso a Google) di eventuali tasse, imposte, interessi, sanzioni o multe risultanti da qualsiasi dichiarazione erronea del Cliente.
  - (c) Qualora per il Cliente sussista l'obbligo di legge a trattenere eventuali importi per l'imposta sul reddito dai suoi pagamenti a Google, il Cliente dovrà fornire tempestivamente a Google una certificazione delle ritenute fiscali o altra documentazione

appropriata a supporto di tale ritenuta, conformemente alle leggi fiscali vigenti.

- 2.4 Controversie sui pagamenti. Le eventuali contestazioni riguardanti i pagamenti devono essere presentate prima della relativa data di scadenza. Se le parti stabiliscono che determinate imprecisioni nella fatturazione sono attribuibili a Google, quest'ultima non emetterà una nuova fattura corretta, bensì una nota di credito in cui sarà specificato l'importo errato della fattura interessata. Se una fattura contestata non è ancora stata pagata, Google India applicherà l'importo della nota di credito alla fattura contestata e il Cliente sarà responsabile del pagamento del saldo netto dovuto risultante nella fattura. Nulla nel presente Contratto obbliga Google India a estendere il credito ad alcun soggetto terzo.
- 2.5 Pagamenti insoluti; Sospensione. I ritardi di pagamento possono produrre interessi al tasso dell'1,5% al mese (o al tasso massimo consentito dalla legge, se inferiore) a partire dalla data di scadenza del pagamento fino al suo versamento integrale. Il Cliente sarà responsabile di tutte le spese (comprese le parcelle degli avvocati) ragionevolmente sostenute da Google India per la riscossione di tali importi insoluti. Inoltre, in caso di ritardo del pagamento dei Servizi da parte del Cliente, Google India potrà sospendere i Servizi tramite Google.
- 2.6 Non obbligatorietà dell'indicazione del numero di ordine di acquisto. Il Cliente è tenuto a pagare tutte le Tariffe applicabili senza alcun obbligo per Google India di fornire un numero di ordine di acquisto sulla fattura Google India (o in altro modo).
- 2.7 Revisioni dei Prezzi. Google India può modificare i Prezzi in qualsiasi momento, salvo se diversamente concordato espressamente in un Addendum o in un Modulo d'ordine. Google India informerà il Cliente di qualsiasi modifica con almeno 30 giorni di preavviso. I Prezzi per il Cliente saranno modificati all'inizio del Periodo di validità del successivo Ordine del Cliente dopo il periodo di 30 giorni.
- La Sezione 15.12 (Legislazione vigente degli Stati Uniti) viene così sostituita:
- 15.12 Legislazione vigente. Qualsiasi rivendicazione risultante dal presente Contratto o al medesimo correlata sarà regolata dalle leggi dell'India. In caso di controversie, avranno giurisdizione i tribunali di Nuova Delhi. Fatto salvo quanto sopra, il Cliente potrà e dovrà presentare a Google India Private Limited tutte le eventuali rivendicazioni riguardanti Google risultanti dal presente Contratto
- La definizione di "Imposte" della Sezione 15.19 (Definizioni) viene così sostituita:
- 15.19 Definizioni.
- Per "Imposte" si intendono tutte le imposte conformemente alla legge vigente, inclusi, a titolo esemplificativo, eventuali dazi o imposte (diverse dall'imposta sul reddito), comprese imposte dirette come l'imposta su beni e servizi ("GST") o imposte associate all'acquisto dei Servizi.

- **Asia-Pacifico - Indonesia**
  - Viene aggiunta la nuova Sezione 8.8:

- 8.8 Rinuncia in materia di risoluzione. Le parti convengono di rinunciare a qualsiasi disposizione ai sensi di qualsiasi legge vigente secondo la quale, per l'annullamento del presente Contratto, siano necessari una decisione o un'ingiunzione di un tribunale.
- La versione indonesiana del presente Contratto è consultabile qui; la Sezione 15.18 (Conflitto tra versioni in lingue diverse) viene sostituita come segue:
- 15.18 Conflitto tra versioni in lingue diverse. Il Contratto è redatto in indonesiano e in inglese. Entrambe le versioni sono ugualmente autentiche. In caso di incoerenza o diversa interpretazione tra la versione indonesiana e la versione inglese, le parti convengono di modificare la versione indonesiana per rendere la parte pertinente della versione indonesiana coerente con la parte pertinente della versione inglese.

- **Europa, Medio Oriente e Africa - Tutte le regioni**
  - La Sezione 2.2 (d) (Dati di pagamento) viene così sostituita:
  - 2.2 (d) Dati di pagamento. I pagamenti effettuati tramite bonifico bancario devono includere le informazioni bancarie fornite da Google. Se il Cliente ha stipulato il Contratto con Google Commerce Limited, Google può riscuotere i pagamenti tramite Google Payment Limited, una società costituita in Inghilterra e Galles con sede a Belgrave House, 76 Buckingham Palace Road, Londra, SW1W 9TQ, Regno Unito.
- **Europa, Medio Oriente e Africa - Spazio economico europeo, Regno Unito e Svizzera**
  - La Sezione 15.19 (Definizioni) viene rinominata Sezione 15.20 (Definizioni).
  - Viene aggiunta la nuova Sezione 15.19:
  - 15.19 Rinuncia all'EECC.
  - (a) Ai fini della presente Sezione 15.19 (Rinuncia all'EECC), i termini "microimpresa", "piccola impresa" e " organizzazione senza scopo di lucro" avranno i significati descritti nell'EECC. Per "EECC" si intende il Codice europeo delle comunicazioni elettroniche istituito dalla Direttiva (UE) 2018/1972 del Parlamento europeo e del Consiglio europeo dell'11 dicembre 2018.
  - (b) Le parti riconoscono che ai sensi dell'EECC: (i) determinati diritti si estendono alle microimprese, alle piccole imprese e alle organizzazioni senza scopo di lucro e (ii) i clienti che rientrano nelle categorie a cui si fa riferimento al punto (i) possono concordare in forma esplicita di rinunciare a determinati diritti.
  - (c) Se il Cliente è una microimpresa, una piccola impresa o un'organizzazione senza scopo di lucro, accetta di rinunciare a qualsiasi diritto di cui potrebbe essere titolare ai sensi di quanto segue:
    - (i) Articolo 102(1) dell'EECC, che permette al Cliente di ricevere determinate informazioni precontrattuali;
    - (ii) Articolo 102(3) dell'EECC, che permette al Cliente di ricevere una sintesi contrattuale concisa;

- (iii) Articolo 105(1) dell'EECC, che limita a 24 mesi la durata contrattuale massima per determinati servizi e
- (iv) Articolo 107(1) dell'EECC, che estende altri diritti contenuti nell'EECC (tra cui l'Articolo 102(3) e l'Articolo 105(1) sopra descritti) a tutti i servizi forniti nel quadro dello stesso contratto Google Workspace.

- **Europa, Medio Oriente, Africa - Algeria, Bahrein, Giordania, Kuwait, Libia, Mauritania, Marocco, Oman, Palestina, Qatar, Tunisia, Yemen, Egitto, Israele, Emirati Arabi Uniti e Libano**
  - Viene aggiunta la nuova Sezione 8.8, come segue:
  - 8.8 Non obbligatorietà dell'ingiunzione del tribunale. Le parti accettano e concordano che non sarà necessaria un'ingiunzione del tribunale per rendere effettivi qualsiasi risoluzione o emendamento del Contratto o per rendere effettiva qualsiasi altra sezione del Contratto.
  - La Sezione 15.12 (Legislazione vigente degli Stati Uniti) viene così sostituita:
  - 15.12 Legislazione vigente; Arbitrato.
    - (a) TUTTE LE RIVENDICAZIONI RISULTANTI DAL PRESENTE CONTRATTO O DAI PRODOTTI O SERVIZI GOOGLE O AI MEDESIMI CORRELATE (INCLUSE EVENTUALI CONTROVERSIE RELATIVE ALL'INTERPRETAZIONE O ALL'ADEMPIMENTO DEL CONTRATTO ("Controversia") SARANNO REGOLATE DALLE LEGGI DELLO STATO DELLA CALIFORNIA, STATI UNITI, AD ECCEZIONE DELLE RELATIVE NORME SUL CONFLITTO DI LEGGI.
    - (b) Le parti tenteranno in buona fede di risolvere qualsiasi Controversia entro 30 giorni dalla data in cui è sorta. Qualora non venga risolta entro 30 giorni, la Controversia dovrà essere risolta mediante arbitrato in conformità alle Arbitration Rules ("Regole") della London Court of International Arbitration (LCIA), che si intendono incorporate nella presente Sezione tramite riferimento.
    - (c) Le parti selezioneranno di comune accordo un solo arbitro. L'arbitrato sarà condotto in lingua inglese e il luogo e la sede legale per l'arbitrato sarà il Dubai International Financial Center, DIFC, Dubai, Emirati Arabi Uniti.
    - (d) Ogni parte può richiedere a qualsiasi tribunale competente un provvedimento ingiuntivo necessario a tutelare i propri diritti in attesa della risoluzione dell'arbitrato. L'arbitro può disporre un provvedimento equitativo o un provvedimento ingiuntivo conforme ai rimedi e alle limitazioni del presente Contratto.
    - (e) Il lodo arbitrale sarà definitivo e vincolante per le parti e la sua esecuzione potrà essere richiesta in qualsiasi tribunale competente,

incluso qualsiasi tribunale che abbia giurisdizione su una delle parti o su qualsiasi bene di sua proprietà.

- (f) Qualsiasi procedura di arbitrato condotta in conformità alla presente Sezione 15.12 (Legislazione vigente; Arbitrato) sarà considerata Informazione riservata ai sensi della Sezione 7 (Informazioni riservate), inclusi: (i) l'esistenza di tali procedure di arbitrato (ii) qualsiasi informazione divulgata durante tali procedure di arbitrato e (iii) qualsiasi comunicazione orale o documento relativi a tali procedure di arbitrato. In aggiunta ai diritti di divulgazione ai sensi della Sezione 7 (Informazioni riservate), le parti possono divulgare le informazioni specificate nella presente Sottosezione 15.12 (f) a un tribunale competente nella misura necessaria ai fini dell'esecuzione di qualsiasi decisione arbitrale, ma le parti dovranno richiedere che tali procedure giudiziarie siano condotte *a porte chiuse* (in privato).
- (g) Le parti saranno tenute a sostenere i costi per l'arbitro, le parcelle e le spese degli esperti nominati dall'arbitro e le spese amministrative del centro arbitrale in conformità alle Regole. Nella sua decisione finale, l'arbitro stabilirà l'obbligazione della parte soccombente a rimborsare l'importo pagato in anticipo dalla parte prevalente a copertura di tali costi.
- (h) Ciascuna parte pagherà le parcelle e le spese dei rispettivi avvocati ed esperti, a prescindere dalla decisione finale dell'arbitro in relazione alla Controversia.

- **Nord America - Stati Uniti**
  - La Sezione 15.19 (Definizioni) viene rinominata Sezione 15.20 (Definizioni).
  - Viene aggiunta la nuova Sezione 15.19:
  - 15.19 Utenti di agenzie federali degli Stati Uniti. I Servizi sono stati sviluppati esclusivamente a spese private e costituiscono software per computer commerciali e documentazione correlata ai sensi delle Federal Acquisition Regulations vigenti e dei relativi supplementi dell'agenzia.

Versioni precedenti

20 settembre 2022

20 settembre 2021

1° aprile 2021

21 dicembre 2020

India (21 dicembre 2020)

Americhe (6 ottobre 2020)

APAC (6 ottobre 2020)

EMEA - SEE (6 ottobre 2020)

Allegato 1

EMEA - Non SEE (6 ottobre 2020)

Allegato 1

INFORMATIVA PRIVACY ALLE FAMIGLIE – UTILIZZO PIATTAFORMA G-SUITE FOR EDUCATION

Redatta ai sensi degli Artt. da 13 a 15 del Regolamento U.E. 2016/679 (G.D.P.R.)

Per quale finalità saranno trattati i miei dati personali?	G Suite for Education consiste in una serie di strumenti per aumentare la produttività didattica forniti da Google, tra cui Gmail, Calendar, Documenti Google, Classroom, Google Drive e altri ancora, che sono utilizzati da decine di milioni di studenti in tutto il mondo. Nell'Istituto, gli studenti utilizzeranno i loro account G Suite per eseguire i compiti, comunicare con i loro insegnanti e apprendere le competenze di cittadinanza digitale del XXI secolo. Personale autorizzato dall'Istituto accederà ai dati inseriti in G-Suite**, per finalità formative, culturali e didattiche**.
Quali garanzie ho che i miei dati siano trattati nel rispetto dei miei diritti e delle mie libertà personali?	Google, titolare dei servizi G-Suite For Education, ha redatto delle informative dettagliate in ottemperanza a quanto previsto dal Regolamento Europeo 679/2016 GDPR. Le informative, i cui link sono riportati di seguito, rispondono alle domande più comuni su come Google può o non può utilizzare le informazioni personali di vostro figlio, tra cui: • Quali informazioni personali raccoglie Google? • In che modo Google utilizza queste informazioni? • Google divulga le informazioni personali di mio figlio? • Google utilizza le informazioni personali degli utenti delle scuole primarie e secondarie per mostrare pubblicità mirata? • Mio figlio può condividere informazioni con altre persone utilizzando l'account G Suite for Education? Vi invitiamo quindi a leggere con attenzione questi documenti: https://support.google.com/a/answer/60762?hl=it https://support.google.com/googlecloud/answer/6056694?hl=it https://safety.google/ https://www.google.com/edu/trust https://www.google.com/apps/intl/it/terms/education_terms.html
I miei dati entreranno nella disponibilità di altri soggetti?	I contenuti verranno divulgati all'interno del gruppo classe in modalità informatica (file in formato testo, immagine o video). Gli stessi non verranno trasferiti a destinatari residenti in paesi terzi rispetto all'Unione Europea né ad organizzazioni internazionali.
Per quanto tempo terrete i miei dati?	I dati saranno conservati presso la piattaforma G-Suite for Education ad accesso esclusivo da parte dell'Istituto per tutto il tempo in cui l'iscrizione sarà attiva ed in seguito, in caso di trasferimento ad altra Istituzione o cessazione del rapporto, verranno trattenuti esclusivamente i dati minimi necessari per permettere la continuità didattica all'interno del gruppo classe.
Quali sono i miei diritti?	L'interessato ha diritto di chiedere al Titolare del trattamento: - L'accesso ai propri dati, la loro rettifica o cancellazione; - La limitazione e di opporsi al trattamento dei dati personali che lo riguardano; - La portabilità dei dati; L'interessato ha inoltre diritto a proporre reclamo all'Autorità di controllo dello Stato di residenza, nonché a revocare il consenso al trattamento ai sensi dell'Art. 6 del G.D.P.R.
Cosa accade se non conferisco i miei dati?	In mancanza del vostro consenso, non verrà creato un account G Suite for Education per vostro figlio.
Chi è il Titolare del trattamento?	L'Istituto Scolastico nella persona del Dirigente Scolastico pro tempore
Responsabile della protezione dei dati (R.P.D. / D.P.O.)	Ferdinando Bassi c/o Easyteam.org SRL – via Walter Tobagi 2 – 20067 TRIBIANO (MI) e-mail: rpd@easyteam.org

RICHIESTE DI MANIFESTAZIONE DEL CONSENSO AI SENSI DELL'ART. 7 DEL REGOLAMENTO U.E.

RICHIESTA (APPORRE UNA **X** NELLE COLONNE A DESTRA IN CORRISPONDENZA DELLA SCELTA FATTA)	ACCONSENTO	NON ACCONSENTO
Creazione di un account G-Suite for Education per le finalità indicate nell'informativa allegata		
Gestione da parte di Google delle informazioni relative a mio figlio per gli scopi e nelle modalità descritte nelle Privacy Policies Google di cui all'informativa allegata.		
Utilizzo dei fogli di lavoro Google Drive e delle altre APP incluse in G-Suite for Education		

Luogo e data ……

COGNOME E NOME DELL'ALUNNO: _____

FIRME PER PRESA VISIONE

Cognome e nome 1° Genitore …… Firma …..... (*)

Cognome e nome 2° Genitore ……Firma …..

(*) Qualora l'informativa in oggetto venga firmata per presa visione da parte di un solo genitore, visti gli Artt. 316 comma 1 e 337 ter comma 3 del Codice Civile si presuppone la condivisione da parte di entrambi i genitori.

"firme assolte mediante pubblicazione sul sito web della scuola" ai sensi del D.P.C.M. del 08/03/2020".

Allegato A

Linee guida per la Didattica digitale integrata

Indice

IL QUADRO NORMATIVO DI RIFERIMENTO

L'emergenza sanitaria ha comportato l'adozione di provvedimenti normativi che hanno riconosciuto la possibilità di svolgere "a distanza" le attività didattiche delle scuole di ogni grado, su tutto il territorio nazionale (decreto-legge 25 marzo 2020, n. 19, articolo 1, comma 2, lettera *p)*).

La Nota dipartimentale 17 marzo 2020, n. 388, recante "Emergenza sanitaria da nuovo Coronavirus. Prime indicazioni operative per le attività didattiche a distanza" aveva già offerto alle istituzioni scolastiche il quadro di riferimento didattico operativo.

Il decreto-legge 8 aprile 2020, n. 22, convertito, con modificazioni, con Legge 6 giugno 2020, n. 41, all'articolo 2, comma 3, stabilisce che il personale docente assicura le prestazioni didattiche nelle modalità a distanza, utilizzando strumenti informatici o tecnologici a disposizione, ed integra pertanto l'obbligo, prima vigente solo per i dirigenti scolastici ai sensi del decreto del Presidente del Consiglio dei Ministri 4 marzo 2020, articolo 1, comma 1, lettera *g)*, di "attivare" la didattica a distanza, obbligo concernente, nel caso del dirigente, per lo più adempimenti relativi alla organizzazione dei tempi di erogazione, degli strumenti tecnologici, degli aiuti per sopperire alle difficoltà delle famiglie e dei docenti privi di sufficiente connettività. Con riferimento, nello specifico, alle modalità e ai criteri sulla base dei quali erogare le prestazioni lavorative e gli adempimenti da parte del personale docente, fino al perdurare dello stato di emergenza, si rimanda alle disposizioni del comma 3-ter del medesimo DL 22/2020.

Il decreto-legge 19 maggio 2020, n. 34 ha finanziato ulteriori interventi utili a potenziare la didattica, anche a distanza, e a dotare le scuole e gli studenti degli strumenti necessari per la fruizione di modalità didattiche compatibili con la situazione emergenziale, nonché a favorire l'inclusione scolastica e ad adottare misure che contrastino la dispersione.

Il decreto del Ministro dell'istruzione 26 giugno 2020, n. 39 ha fornito un quadro di riferimento entro cui progettare la ripresa delle attività scolastiche nel mese di settembre, con particolare riferimento, per la tematica in argomento, alla necessità per le scuole di dotarsi di un *Piano scolastico per la didattica digitale integrata*.

Le presenti Linee Guida forniscono indicazioni per la progettazione del *Piano scolastico per la didattica digitale integrata* (DDI) da adottare, nelle scuole secondarie di II grado, in modalità complementare alla didattica in presenza, nonché da parte di tutte le istituzioni scolastiche di qualsiasi grado, qualora emergessero necessità di contenimento del contagio, nonché qualora si rendesse necessario sospendere nuovamente le attività didattiche in presenza a causa delle condizioni epidemiologiche contingenti.

Su questa specifica ultima ed estrema eventualità, saranno gli Uffici scolastici regionali a intervenire a supporto delle istituzioni scolastiche, sulla base delle specifiche situazioni che avessero a manifestarsi, sulla scorta di quanto già previsto e sperimentato ai sensi dell'articolo 31, comma 3 dell'Ordinanza del Ministro dell'istruzione 16 maggio 2020, n. 10.

Nel richiamare integralmente, nel merito, quanto già espresso all'interno del Documento per la pianificazione di cui al DM39/2020, si evidenzia che tutte le scuole, a prescindere dal grado di istruzione, dovranno dotarsi del suddetto Piano.

L'elaborazione del Piano, allegato o integrato nel Piano Triennale dell'Offerta Formativa, riveste dunque carattere prioritario poiché esso individua i criteri e le modalità per riprogettare l'attività

didattica in DDI, a livello di istituzione scolastica, tenendo in considerazione le esigenze di tutti gli alunni e gli studenti, in particolar modo degli alunni più fragili.

COME ORGANIZZARE LA DIDATTICA DIGITALE INTEGRATA

Ogni istituzione scolastica del Sistema nazionale di istruzione e formazione definisce le modalità di realizzazione della didattica digitale integrata, in un equilibrato bilanciamento tra attività sincrone e asincrone.

La didattica digitale integrata, intesa come metodologia innovativa di insegnamento-apprendimento, è rivolta a tutti gli studenti della scuola secondaria di II grado, come modalità didattica complementare che integra la tradizionale esperienza di scuola in presenza, nonché, in caso di nuovo *lockdown*, agli alunni di tutti i gradi di scuola, secondo le indicazioni impartite nel presente documento.

La progettazione della didattica in modalità digitale deve tenere conto del contesto e assicurare la sostenibilità delle attività proposte e un generale livello di inclusività, evitando che i contenuti e le metodologie siano la mera trasposizione di quanto solitamente viene svolto in presenza.

L'ANALISI DEL FABBISOGNO

Le istituzioni scolastiche avviano una rilevazione di fabbisogno di strumentazione tecnologica e connettività, qualora il quadro rispetto ai mesi di sospensione delle attività didattiche sia mutato anche in considerazione dell'ingresso dei nuovi alunni nelle classi prime, al fine di prevedere la concessione in comodato d'uso gratuito degli strumenti per il collegamento, agli alunni che non abbiano l'opportunità di usufruire di *device* di proprietà.

La verifica del fabbisogno sarà necessaria per procedere, ove non già avvenuto, all'approvazione in Consiglio di Istituto dei criteri di concessione in comodato d'uso delle dotazioni strumentali dell'istituzione scolastica, avendo cura che essi contemplino una priorità nei confronti degli studenti meno abbienti, attraverso la definizione di criteri trasparenti di assegnazione nel rispetto della disciplina in materia di protezione dei dati personali, i cui aspetti saranno definiti in un apposito documento predisposto dal Ministero in collaborazione con l'Autorità garante per la protezione dei dati personali, al fine di fornire alle famiglie una specifica informativa.

La rilevazione potrà riguardare anche il personale docente a tempo determinato al quale, se non in possesso di propri mezzi, potrà essere assegnato un dispositivo in via residuale rispetto agli alunni e solo ove il fabbisogno da questi espresso sia completamente soddisfatto. Si ritiene che i docenti assunti a tempo indeterminato, in quanto da anni assegnatari delle somme della Carta del docente, siano nella possibilità di dotarsi di adeguati strumenti da utilizzare per la prestazione lavorativa, coerentemente con le politiche "BYOD" che ogni istituzione scolastica è chiamata ad adottare (Azione#6 del PNSD).

Per quanto attiene la garanzia di connettività, oltre alla prosecuzione degli accordi a livello nazionale con i principali gestori di telefonia mobile garantiti dall'AgID, le istituzioni scolastiche potranno riavviare o instaurare nuovi contratti per l'acquisto di *sim* dati, procedendo all'attivazione di procedure di acquisizione previste dalla normativa vigente, fermo restando che sono in corso contatti con gli operatori da parte dell'Amministrazione centrale.

GLI OBIETTIVI DA PERSEGUIRE

Il Collegio docenti è chiamato a fissare criteri e modalità per erogare didattica digitale integrata, adattando la progettazione dell'attività educativa e didattica in presenza alla modalità a distanza, anche in modalità complementare, affinché la proposta didattica del singolo docente si inserisca in una cornice pedagogica e metodologica condivisa, che garantisca omogeneità all'offerta formativa dell'istituzione scolastica. Al team dei docenti e ai consigli di classe è affidato il compito di rimodulare le progettazioni didattiche individuando i contenuti essenziali delle discipline, i nodi interdisciplinari, gli apporti dei contesti non formali e informali all'apprendimento, al fine di porre gli alunni, pur a distanza, al centro del processo di insegnamento-apprendimento per sviluppare quanto più possibile autonomia e responsabilità.

Va posta attenzione agli alunni più fragili. Nel caso in cui si propenda per attività di DDI come metodologia complementare alla didattica in presenza, si avrà cura di orientare la proposta verso gli studenti che presentino fragilità nelle condizioni di salute, opportunamente attestate e riconosciute, consentendo a questi per primi di poter fruire della proposta didattica dal proprio domicilio, in accordo con le famiglie, **anche attivando percorsi di istruzione domiciliare appositamente progettati e condivisi con le competenti strutture locali, ai fini dell'eventuale integrazione degli stessi con attività educativa domiciliare**. Nei casi in cui la fragilità investa condizioni emotive o socio culturali, ancor più nei casi di alunni con disabilità, **si suggerisce che sia privilegiata la frequenza scolastica in presenza, prevedendo l'inserimento in turnazioni che contemplino alternanza tra presenza e distanza solo d'intesa con le famiglie.**

I docenti per le attività di sostegno, **sempre in presenza a scuola assieme agli alunni,** curano l'interazione tra tutti i compagni in presenza e quelli eventualmente impegnati nella DDI, nonché con gli altri docenti curricolari, mettendo a punto materiale individualizzato o personalizzato da far fruire all'alunno medesimo in incontri quotidiani con il piccolo gruppo e concorrono, in stretta correlazione con i colleghi, allo sviluppo delle unità di apprendimento per la classe.

È necessario che la scuola fornisca alle famiglie una puntuale informazione sui contenuti del Piano scolastico per la didattica digitale integrata, sui criteri che saranno utilizzati dai docenti per operare la scelta degli studenti cui proporre la DDI, nel rispetto della disciplina in materia di protezione dei dati personali raccogliendo solo dati personali strettamente pertinenti e collegati alla finalità che si intenderà perseguire, assicurando la piena trasparenza dei criteri individuati, sulle caratteristiche che regoleranno tale metodologia e gli strumenti che potranno essere necessari.

Per le situazioni di fragilità, a qualsiasi tipologia esse siano riconducibili, è opportuno che le istituzioni scolastiche operino periodici monitoraggi al fine di poter attivare, in caso di necessità, tutte le azioni necessarie volte a garantire l'effettiva fruizione delle attività didattiche, in particolar modo per gli studenti con cittadinanza non italiana neo arrivati in Italia, anche con il supporto delle agenzie del territorio, per non trasformare le differenze linguistiche, socio-economico-culturali in elementi di aggravio del divario di opportunità tra studenti. L'individuazione degli alunni cui proporre percorsi alternativi in DDI dovrà avvenire adottando specifiche garanzie a tutela dei dati dei minori, considerata la delicatezza delle informazioni trattate.

GLI STRUMENTI DA UTILIZZARE

Ogni scuola assicura unitarietà all'azione didattica rispetto all'utilizzo di piattaforme, spazi di archiviazione, registri per la comunicazione e gestione delle lezioni e delle altre attività, al fine di

semplificare la fruizione delle lezioni medesime nonché il reperimento dei materiali, anche a vantaggio di quegli alunni che hanno maggiori difficoltà ad organizzare il proprio lavoro. A tale scopo, ciascuna istituzione scolastica individua **una piattaforma che risponda ai necessari requisiti di sicurezza** dei dati a garanzia della *privacy*[1], tenendo anche conto delle opportunità di gestione di tale forma di didattica che sono all'interno delle funzionalità del registro elettronico, assicuri un agevole svolgimento dell'attività sincrona anche, possibilmente, attraverso l'oscuramento dell'ambiente circostante e risulti fruibile, qualsiasi sia il tipo di *device* (*smartphone, tablet, PC*) o sistema operativo a disposizione.

Per il necessario adempimento amministrativo di rilevazione della presenza in servizio dei docenti e per registrare la presenza degli alunni a lezione, si utilizza il registro elettronico[2], così come per le comunicazioni scuola-famiglia e l'annotazione dei compiti giornalieri. La DDI, di fatto, rappresenta lo "spostamento" in modalità virtuale dell'ambiente di apprendimento e, per così dire, dell'ambiente giuridico in presenza.

L'Animatore e il Team digitale garantiscono il necessario supporto alla realizzazione delle attività digitali della scuola, attraverso collaborazione rivolta ai docenti meno esperti e, nel rispetto della normativa sulla protezione dei dati personali e adottando misure di sicurezza adeguate, la creazione e/o la guida all'uso di *repository*, in locale o *in cloud* rispetto ai quali va preventivamente valutata la modalità di gestione dei dati in esso contenuti come precisato più avanti, per la raccolta separata degli elaborati degli alunni e dei verbali delle riunioni degli organi collegiali, qualora svolte a distanza, in modo da garantire la corretta conservazione degli atti amministrativi e dei prodotti stessi della didattica.

La creazione di *repository* scolastiche, ove non già esistenti e disponibili sulle piattaforme multimediali in uso, che siano esplicitamente dedicate alla conservazione di attività o video-lezioni svolte e tenute dal docente, al di là dei prodotti a tal fine dedicati messi a disposizione dalle principali applicazioni di registro elettronico, potrà costituire strumento utile non solo per la conservazione, ma anche per ulteriore fruibilità nel tempo di quanto prodotto dai docenti stessi, anche in modalità asincrona, sempre nel rispetto della disciplina in materia di protezione dei dati personali con specifico riferimento alla necessaria regolazione dei rapporti con eventuali fornitori esterni, e della normativa di settore applicabile ai rapporti di lavoro, con particolare riguardo alla conservazione di immagini e/o audio.

Gli Uffici scolastici regionali, attraverso le reti di scopo per la formazione del personale e con l'ausilio dei referenti regionali per il PNSD, i *Future Labs*, le reti di scuole sulle metodologie innovative garantiscono il proprio supporto alle istituzioni scolastiche, sia in termini di formazione che di *know-how*, attivando se necessario forme di gemellaggio e monitoraggio che restituiscano i fabbisogni del territorio e consentano interventi immediati ed efficaci.

L'Amministrazione centrale proseguirà il suo impegno per garantire, attraverso appositi accordi con la RAI – Radiotelevisione italiana, l'erogazione di contenuti didattici sui canali tematici dell'emittente, secondo orari prestabiliti, organizzati per fasce d'età, dalla prima infanzia all'età adulta.

[1] Si rimanda al Provvedimento del 26 marzo 2020 - "Didattica a distanza: prime indicazioni" dell'Autorità garante per la protezione dei dati personali.
[2] Il Ministero dell'istruzione, in collaborazione con l'Autorità garante per la protezione dei dati personali, è in procinto di emanare indicazioni specifiche sulla protezione dei dati con riferimento al registro elettronico.

L'ORARIO DELLE LEZIONI

Nel corso della giornata scolastica dovrà essere offerta, agli alunni in DDI, una combinazione adeguata di attività in modalità sincrona e asincrona, per consentire di ottimizzare l'offerta didattica con i ritmi di apprendimento, avendo cura di prevedere sufficienti momenti di pausa.

Nel caso di attività digitale complementare a quella in presenza, il gruppo che segue l'attività a distanza rispetta per intero l'orario di lavoro della classe **salvo che la pianificazione di una diversa scansione temporale della didattica, tra alunni in presenza e a distanza, non trovi la propria ragion d'essere in motivazioni legate alla specificità della metodologia in uso.**

Nel caso in cui la DDI divenga strumento unico di espletamento del servizio scolastico, a seguito di eventuali nuove situazioni di *lockdown*, saranno da prevedersi quote orarie settimanali minime di lezione:

- **Scuola dell'infanzia**: l'aspetto più importante è mantenere il contatto con i bambini e con le famiglie. Le attività, oltre ad essere accuratamente progettate in relazione ai materiali, agli spazi domestici e al progetto pedagogico, saranno calendarizzate evitando improvvisazioni ed estemporaneità nelle proposte in modo da favorire il coinvolgimento attivo dei bambini. Diverse possono essere le modalità di contatto: dalla videochiamata, al messaggio per il tramite del rappresentante di sezione o anche la videoconferenza, per mantenere il rapporto con gli insegnanti e gli altri compagni. Tenuto conto dell'età degli alunni, è preferibile proporre piccole esperienze, brevi filmati o file audio.

È inoltre opportuno attivare una apposita sezione del sito della scuola dedicata ad attività ed esperienze per i bambini della scuola dell'infanzia. Si rimanda al documento di lavoro "Orientamenti pedagogici sui Legami educativi a Distanza. Un modo diverso per 'fare' nido e scuola dell'infanzia[3]".

- **Scuola del primo ciclo**: assicurare almeno quindici ore settimanali di didattica in modalità sincrona con l'intero gruppo classe (dieci ore per le classi prime della scuola primaria), organizzate anche in maniera flessibile, in cui costruire percorsi disciplinari e interdisciplinari, con possibilità di prevedere ulteriori attività in piccolo gruppo, nonché proposte in modalità asincrona secondo le metodologie ritenute più idonee.

- **Scuole secondarie di primo grado ad indirizzo musicale**: assicurare agli alunni, attraverso l'acquisto da parte della scuola di servizi web o applicazioni che permettano l'esecuzione in sincrono, sia le lezioni individuali di strumento che le ore di musica d'insieme.

- **Scuola secondaria di secondo grado**: assicurare almeno venti ore settimanali di didattica in modalità sincrona con l'intero gruppo classe, con possibilità di prevedere ulteriori attività in piccolo gruppo nonché proposte in modalità asincrona secondo le metodologie ritenute più idonee.

- **CPIA:** per i percorsi di primo livello, primo periodo didattico, assicurare almeno nove ore alla settimana di didattica in modalità sincrona con l'intero gruppo di apprendimento; per i percorsi di primo livello, secondo periodo didattico, assicurare almeno dodici ore alla settimana di didattica in modalità sincrona con l'intero gruppo di apprendimento; per i percorsi di alfabetizzazione e apprendimento della lingua italiana assicurare almeno otto ore alla settimana di didattica in

[3] https://www.miur.gov.it/web/guest/orientamenti-pedagogici-sui-legami-educativi-a-distanza-per-nido-e-infanzia-lead- Documento elaborato dalla Commissione nazionale per il sistema integrato zerosei (D.lgs. 65/2017) che raccoglie le buone pratiche realizzate per instaurare e mantenere relazioni educative a distanza con bambini e genitori.

modalità sincrona con ogni gruppo di apprendimento; per i percorsi di secondo livello assicurare almeno quattro ore al giorno di didattica in modalità sincrona con l'intero gruppo di apprendimento.

Fermo restando l'orario di servizio settimanale dei docenti stabilito dal CCNL, il Dirigente scolastico, sulla base dei criteri individuati dal Collegio docenti, predispone l'orario delle attività educative e didattiche con la quota oraria che ciascun docente dedica alla didattica digitale integrata, avendo cura di assicurare adeguato spazio settimanale a tutte le discipline sia che la DDI sia scelta come modalità complementare alla didattica in presenza, sia che essa costituisca lo strumento esclusivo derivante da nuove condizioni epidemiologiche rilevanti. Nella strutturazione dell'orario settimanale in DDI, è possibile fare ricorso alla riduzione dell'unità oraria di lezione, alla compattazione delle discipline, nonché adottare tutte le forme di flessibilità didattica e organizzativa previste dal Regolamento dell'Autonomia scolastica.

REGOLAMENTO PER LADIDATTICA DIGITALE INTEGRATA

Considerate le implicazioni etiche poste dall'uso delle nuove tecnologie e della rete, le istituzioni scolastiche integrano il Regolamento d'Istituto con specifiche disposizioni in merito alle norme di comportamento da tenere durante i collegamenti da parte di tutte le componenti della comunità scolastica relativamente al rispetto dell'altro, alla condivisione di documenti e alla tutela dei dati personali e alle particolari categorie di dati (ex. dati sensibili). In relazione a tale ultimo aspetto si sottolinea come qualsiasi forma di condivisione deve riguardare solo dati personali adeguati, pertinenti e limitati a quanto strettamente necessario rispetto alle finalità per le quali sono trattati secondo il principio di minimizzazione tenendo conto del ruolo e delle funzioni dei soggetti a cui tale condivisione è estesa. Inoltre, andranno disciplinate le modalità di svolgimento dei colloqui con i genitori, degli Organi Collegiali e delle assemblee studentesche e di ogni altra ulteriore riunione.

I docenti, ad esempio, nel predisporre le attività da proporre alla classe in modalità sincrona, hanno cura di predisporre un adeguato *setting* "d'aula" virtuale evitando interferenze tra la lezione ed eventuali distrattori. Ancor più in caso di DDI estesa a tutti i gradi scolastici per nuova emergenza epidemiologica, i docenti e tutto il personale della scuola, a vario titolo in contatto video con gli studenti e con le famiglie, rispettano le prescrizioni di cui agli artt. 3 e sgg. del decreto del Presidente della Repubblica 16 aprile 2013, n. 62.

Anche il Regolamento di disciplina degli studenti e delle studentesse della scuola secondaria sarà integrato con la previsione di infrazioni disciplinari legate a comportamenti scorretti assunti durante la didattica digitale integrata e con le relative sanzioni.

Le istituzioni scolastiche dovranno porre particolare attenzione alla formazione degli alunni sui rischi derivanti dall'utilizzo della rete e, in particolare, sul reato di cyberbullismo.

Le scuole inseriscono infine, nel Patto educativo di corresponsabilità, un'appendice specifica riferita ai reciproci impegni da assumere per l'espletamento della didattica digitale integrata.

METODOLOGIE E STRUMENTI PER LA VERIFICA

La lezione in videoconferenza agevola il ricorso a metodologie didattiche più centrate sul protagonismo degli alunni, consente la costruzione di percorsi interdisciplinari nonché di capovolgere la struttura della lezione, da momento di semplice trasmissione dei contenuti ad *agorà* di confronto, di rielaborazione condivisa e di costruzione collettiva della conoscenza. Alcune metodologie si adattano meglio di altre alla didattica digitale integrata: si fa riferimento, ad esempio, alla *didattica breve,* all'a*pprendimento cooperativo*, alla *flipped classroom,* al *debate* quali

metodologie fondate sulla costruzione attiva e partecipata del sapere da parte degli alunni che consentono di presentare proposte didattiche che puntano alla costruzione di competenze disciplinari e trasversali, oltre che all'acquisizione di abilità e conoscenze. Si raccomanda alle istituzioni scolastiche di procedere ad una formazione mirata che ponga i docenti nelle condizioni di affrontare in maniera competente queste metodologie, al fine di svilupparne tutte le potenzialità ed evitare che, in particolare alcune di esse, si sostanzino in un riduttivo studio a casa del materiale assegnato.

Ai consigli di classe e ai singoli docenti è demandato il compito di individuare gli strumenti per la verifica degli apprendimenti inerenti alle metodologie utilizzate. Si ritiene che qualsiasi modalità di verifica di una attività svolta in DDI non possa portare alla produzione di materiali cartacei, salvo particolari esigenze correlate a singole discipline o a particolari bisogni degli alunni. I docenti avranno cura di salvare gli elaborati degli alunni medesimi e di avviarli alla conservazione all'interno degli strumenti di *repository* a ciò dedicati dall'istituzione scolastica.

VALUTAZIONE

La normativa vigente attribuisce la funzione docimologica ai docenti, con riferimento ai criteri approvati dal Collegio dei docenti e inseriti nel Piano Triennale dell'Offerta formativa. Anche con riferimento alle attività in DDI, la valutazione deve essere costante, garantire trasparenza e tempestività e, ancor più laddove dovesse venir meno la possibilità del confronto in presenza, la necessità di assicurare *feedback* continui sulla base dei quali regolare il processo di insegnamento/apprendimento. La garanzia di questi principi cardine consentirà di rimodulare l'attività didattica in funzione del successo formativo di ciascuno studente, avendo cura di prendere ad oggetto della valutazione non solo il singolo prodotto, quanto l'intero processo. La valutazione formativa tiene conto della qualità dei processi attivati, della disponibilità ad apprendere, a lavorare in gruppo, dell'autonomia, della responsabilità personale e sociale e del processo di autovalutazione. In tal modo, la valutazione della dimensione oggettiva delle evidenze empiriche osservabili è integrata, anche attraverso l'uso di opportune rubriche e diari di bordo, da quella più propriamente formativa in grado di restituire una valutazione complessiva dello studente che apprende.

ALUNNI CON BISOGNI EDUCATIVI SPECIALI

Il Piano scuola 2020, allegato al citato DM 39/2020 prevede che l'Amministrazione centrale, le Regioni, gli Enti locali e le scuole, ciascuno secondo il proprio livello di competenza, operino per garantire la frequenza scolastica in presenza degli alunni con disabilità con il coinvolgimento delle figure di supporto (Operatori educativi per l'autonomia e la comunicazione e gli Assistenti alla comunicazione per gli alunni con disabilità sensoriale). Per tali alunni il punto di riferimento rimane il Piano Educativo Individualizzato, unitamente all'impegno dell'Amministrazione centrale e delle singole amministrazioni scolastiche di garantire la frequenza in presenza.

Particolare attenzione va dedicata alla presenza di alunni in possesso di diagnosi rilasciata ai sensi della Legge 170/2010 e di alunni non certificati, ma riconosciuti con Bisogni educativi speciali dal team docenti e dal consiglio di classe, per i quali si fa riferimento ai rispettivi Piani Didattici Personalizzati. Per questi alunni è quanto mai necessario che il team docenti o il consiglio di classe concordino il carico di lavoro giornaliero da assegnare e garantiscano la possibilità di registrare e riascoltare le lezioni, essendo note le difficoltà nella gestione dei materiali didattici ordinari nel rispetto della richiamata disciplina di settore e delle indicazioni fornite dal Garante (cfr. Vademecum scuola). L'eventuale coinvolgimento degli alunni in parola in attività di DDI complementare dovrà essere attentamente valutato, assieme alle famiglie, verificando che l'utilizzo

degli strumenti tecnologici costituisca per essi un reale e concreto beneficio in termini di efficacia della didattica. Le decisioni assunte dovranno essere riportate nel PDP.

Per gli alunni ricoverati presso le strutture ospedaliere o in cura presso la propria abitazione e frequentanti le scuole carcerarie l'attivazione della didattica digitale integrata, oltre a garantire il diritto all'istruzione, concorre a mitigare lo stato di isolamento sociale e diventa, pertanto, uno degli strumenti più efficaci per rinforzare la relazione. Il Dirigente scolastico attiva ogni necessaria interlocuzione con i diversi attori competenti per individuare gli interventi necessari ad attivare proficuamente la didattica digitale integrata.

PRIVACY

Sugli aspetti relativi al trattamento dei dati personali, il Ministero dell'istruzione, in collaborazione con l'Autorità garante per la protezione dei dati personali, predisporrà un apposito documento di dettaglio contenente indicazioni specifiche.

SICUREZZA

Il Dirigente scolastico, in qualità di datore di lavoro, ha il compito di tutelare la salute dei lavoratori attraverso attività di informazione mirata, anche se la prestazione avviene in ambienti di lavoro diversi dai locali scolastici. Pertanto è opportuno che il Dirigente trasmetta ai docenti a vario titolo impegnati nella didattica digitale integrata, nel caso in cui essa sia erogata dal loro domicilio, e al Responsabile dei Lavoratori per la Sicurezza una nota informativa, redatta in collaborazione con il Responsabile del Servizio di Prevenzione e Protezione, inerente i comportamenti di prevenzione da adottare per ridurre i rischi derivanti dall'esecuzione della prestazione lavorativa al di fuori dell'ambiente scolastico.

RAPPORTI SCUOLA-FAMIGLIA

Va favorito il necessario rapporto scuola-famiglia attraverso attività formali di informazione e condivisione della proposta progettuale della didattica digitale integrata. È opportuna, oltre alla menzionata tempestiva informazione alle famiglie sugli orari delle attività, per consentire loro la migliore organizzazione, la condivisione degli approcci educativi, finanche di materiali formativi, per supportare il percorso di apprendimento di quegli alunni con particolari fragilità che necessitino, in DDI, dell'affiancamento di un adulto per fruire delle attività proposte.

Anche in rinnovate condizioni di emergenza, le istituzioni scolastiche assicurano, comunque, tutte le attività di comunicazione, informazione e relazione con la famiglia previste all'interno del Contratto collettivo nazionale di Lavoro vigente e previsti dalle norme sulla valutazione, avendo cura di esplicitare i canali di comunicazione attraverso cui essi potranno avvenire.

FORMAZIONE DEI DOCENTI E DEL PERSONALE ASSISTENTE TECNICO

La formazione dei docenti rappresenta una leva fondamentale per il miglioramento e per l'innovazione del sistema educativo italiano. Il periodo di emergenza vissuto dalla scuola ha attivato processi di formazione dovuti all'impellente necessità di affrontare l'esperienza della didattica a distanza. È quanto mai opportuno che ciascuna scuola predisponga, all'interno del Piano della formazione del personale, attività che sappiano rispondere alle specifiche esigenze formative.

I percorsi formativi a livello di singola istituzione scolastica o di rete di ambito per la formazione potranno incentrarsi sulle seguenti priorità:

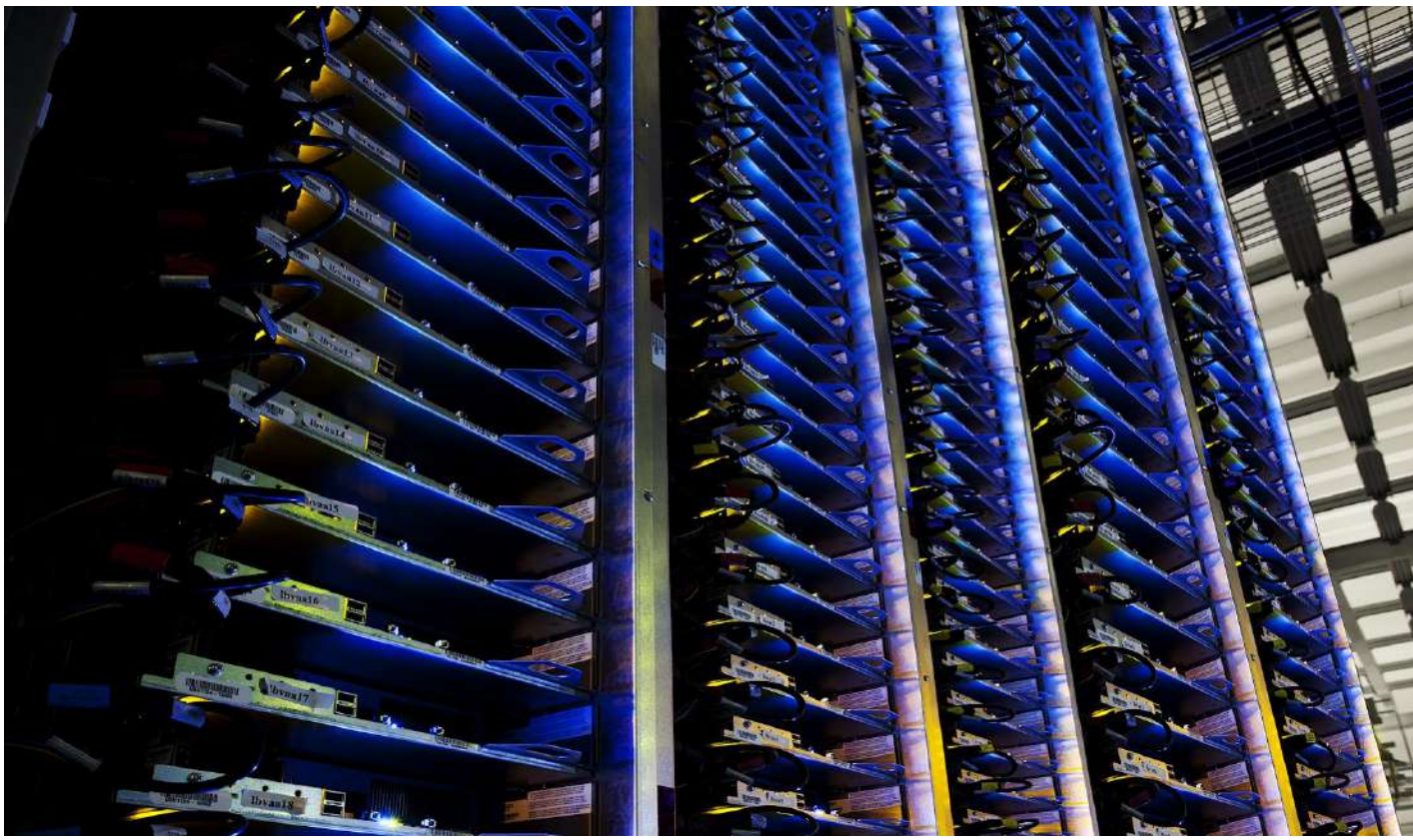
1. informatica (anche facendo riferimento al DigCompEdu[4]), con priorità alla formazione sulle piattaforme in uso da parte dell'istituzione scolastica;
2. con riferimento ai gradi di istruzione:
    a. metodologie innovative di insegnamento e ricadute sui processi di apprendimento (didattica breve, apprendimento cooperativo, *flipped classroom*, *debate*, *project based learning*);
    b. modelli inclusivi per la didattica digitale integrata e per la didattica interdisciplinare;
    c. gestione della classe e della dimensione emotiva degli alunni;
3. privacy, salute e sicurezza sul lavoro nella didattica digitale integrata;
4. formazione specifica sulle misure e sui comportamenti da assumere per la tutela della salute personale e della collettività in relazione all'emergenza sanitaria.

Per il personale Assistente tecnico impegnato nella predisposizione degli ambienti e delle strumentazioni tecnologiche per un funzionale utilizzo da parte degli alunni e dei docenti, si prevedranno specifiche attività formative, anche organizzate in rete con altre istituzioni scolastiche del territorio, al fine di ottimizzare l'acquisizione o il rafforzamento delle competenze necessarie allo scopo.

[4]Quadro europeo delle competenze digitali del personale scolastico.

Google Cloud Whitepaper
February 2023

Google Workspace for Education data protection implementation guide



Google Cloud

Table of contents

Disclaimer

This guide is intended for Google Workspace for Education administrators to help them better understand how to use and customize Google Workspace for Education services and settings to meet data protection compliance needs. 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.

The content in this guide is correct as of March 2021 and represents the status quo at the time it was written. Google's policies and systems may change going forward, as we continually improve protection for our customers.

Processing Customer Personal Data within our services

Understand your data protection requirements

Google is committed to helping our customers meet their data protection obligations globally—including the requirements set forth by the General Data Protection Regulation (GDPR)—by offering helpful products and tools, by building robust privacy and security protections into our services and contracts, and by providing certifications and audit reports.

Under the Google Workspace for Education Data Processing Amendment (DPA), Google acts as a processor of the Customer Personal Data that is submitted, stored, sent, or received by your organization via Google Workspace for Education services, and we process such data on your behalf and under your instructions. As a customer, you act as the controller of such Customer Personal Data[1], which means that you determine the purposes and means of processing.

We recommend that you conduct an assessment of your Google Workspace for Education Agreement, the Google Workspace for Education DPA, the Google Workspace for Education Privacy Notice, as well as the terms applicable to any other Google services that you choose to make available for your end users while signed in to their organization managed accounts (for example, the additional services you turned on for your domain).

[1] Customer Personal Data means the personal data contained within the Customer Data.

Our Privacy Commitments

Google makes these Cloud Enterprise Privacy Commitments for Google Workspace for Education products to describe our overarching responsibility to protect your business when you use our enterprise solutions. These commitments are backed by the strong contractual commitments we make available to you.

- **You control your data.** Customer Data[2] is your data, not Google's. We only process your data according to your agreement(s).
- **We never use your data for ads targeting.** We do not process your customer data or service data to create ads profiles or improve Google Ads products.
- **We are transparent about data collection and use.** We're committed to transparency, compliance with regulations like the GDPR, and privacy best practices.
- **We never sell customer data or service data.** We never sell customer data or service data[3] to third parties.
- **Security and privacy are primary design criteria for all of our products.** Prioritizing the privacy of our customers means protecting the data you trust us with. We build the strongest security technologies into our products.

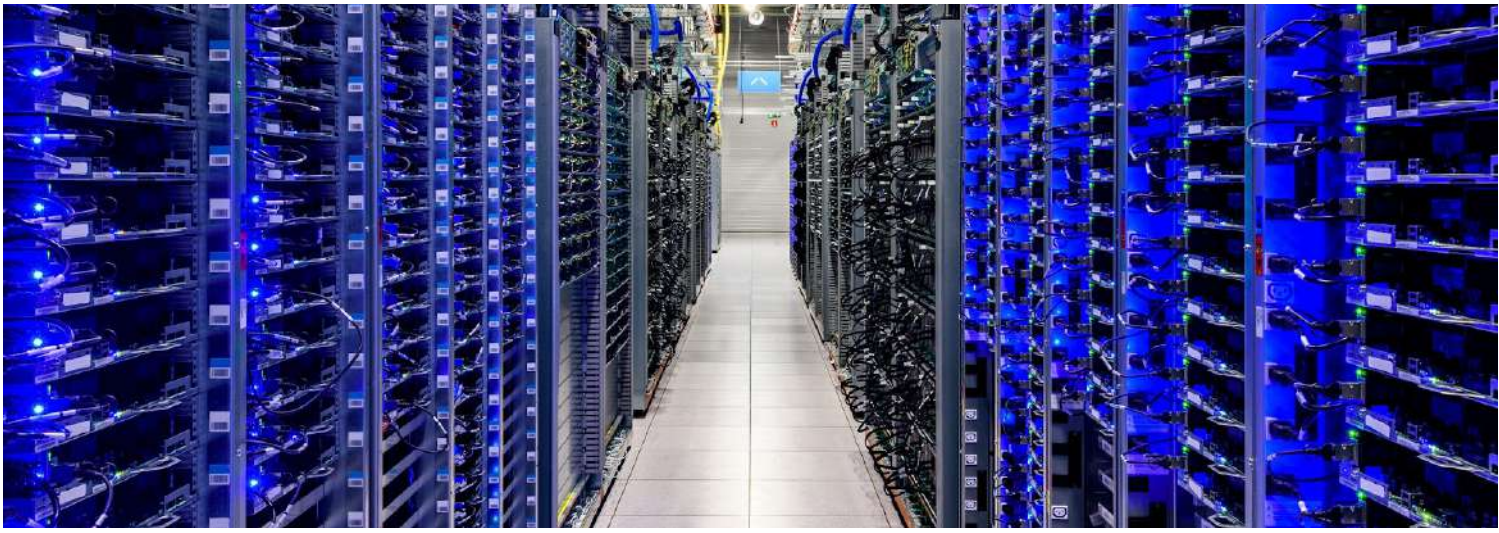
Google designed Google Workspace for Education to meet stringent privacy and security standards based on industry best practices.[4] In addition to strong contractual commitments regarding data ownership, data use, security, transparency, and accountability, we give you the tools you need to help meet your compliance and reporting requirements (see more information in Appendix 1). Additionally, our Privacy Commitments provide clarity about our privacy commitments and what you can expect when it comes to protecting and managing your data in the cloud.

Transparency is part of Google's DNA. At Google Cloud, we believe that trust is created through transparency, and we want to be transparent about our commitments and what you can expect when it comes to our shared responsibility for protecting and managing your data in the cloud. At Google Cloud, we strive to create a trusted ecosystem by focusing on three key areas: ensuring the privacy and security of our customers' data, the dependability of our services, and setting—as well as meeting—the highest industry standards around transparency and security.

---

[2] Customer data is the data you, including your organization and your users, provide to Google when you access Google Workspace for Education and the data you create using those services.
[3] Service data is the personal information Google collects or generates during the provision and administration of the Cloud Services, excluding any Customer Data and Partner Data. Service Data is subject to Google Cloud Privacy Notice.
[4] Please see our ISO/IEC certifications (ISO/IEC 27001, 27017, 27701, 27018) as well our SOC 3 Audit Report, available here. For our existing customers who want to learn more about Google's Security, we will be happy to facilitate a detailed SOC 2 report via the Compliance Reports Manager. You can see the full listing of all of our compliance offerings in our Compliance resource center.

Additionally, we also secure any service data. Service data is the information Google collects or generates while providing and administering Google Workspace for Education and is critical to help ensure the security and availability of our services. Service data does not include Customer Data. Service data includes information about security settings, operational details, and billing information. We process service data for various purposes that are detailed in our newly launched Google Cloud Privacy Notice, such as making recommendations to optimize your use of Google Workspace for Education, and improving performance and functionality.

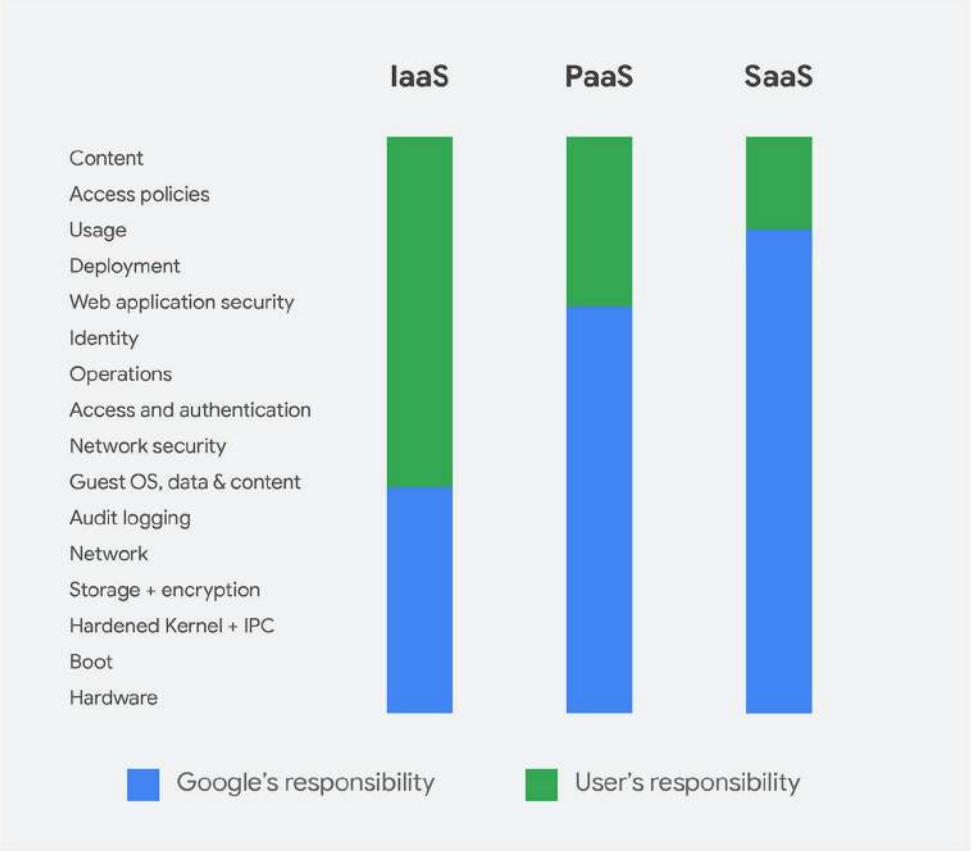


Google Shared Responsibility Model

Data protection is not only the responsibility of the business using Google Workspace for Education services; nor is it only that of Google in providing those services. Data protection in the cloud is instead a shared responsibility; a collaboration between the customer and the Cloud service provider (CSP).

The Google Shared Responsibility Model visually describes the various security responsibilities that our customer and Google are together responsible for Google Workspace for Education is software as a service (SaaS) where almost everything except the content and its access policy is the responsibility of the CSPs. In the SaaS model, CSPs manage all of the physical and virtual infrastructure and the platform layer while delivering cloud-based applications and services for customers to consume. Internet applications that run directly from a web browser or mobile applications are SaaS applications. With this model, customers don't have to worry about installing, updating, or supporting applications—they simply manage system and data access policies.

Important: As a Google Workspace for Education customer, you are responsible for the security of components that you provide or control, such as the content you put in Google Workspace for Education services, and establishing access control for your users.



Google Workspace *for Education (SaaS) responsibility diagram vs. other IaaS and PaaS services*

You can refer to the Shared Responsibility Model as a guide to secure your Customer Data on Google Workspace for Education. Under various data protection regulations, you are responsible for security controls protecting the Customer Personal Data in your possession, monitoring the processing of the Customer Personal Data, monitoring the access to the data, ensuring the accuracy of the data, and managing the lifecycle of the data.

Google protects the infrastructure underlying Google Workspace for Education throughout the information processing lifecycle. Security is provided at each layer through the hardware layer, inter-service communication, inter-service access management, data storage, Internet communication, and operational security. For more information on the topic, please read the Google Infrastructure Security Design Overview whitepaper.

Google services

In this section, we will provide you an overview of various services Google provided to you, including Google Workspace for Education Core Services, embedded features, Additional Services, organization managed Google Account, and technical support services.

- Google Workspace for Education **Core Services**: services listed and described in the services summary
- Google Workspace for Education **Core Services Embedded Features**: embedded in Google Workspace for Education Core Services and are available for all Google Workspace for Education users
- **Feedback**: suggested spelling & grammar corrections feedback and in-product feedback are subject to Google Privacy Policy
- **Additional Services**: not part of the Google Workspace for Education offering, and may be any Google service that can be used with an organization managed Google Account. A non-exhaustive list of Additional Google services is provided here
- **Organization managed Google Account**: an organization managed Google Account is needed for your use of Google Workspace for Education (separate from personal Google Account) and is managed by an administrator
- **Technical Support Services**: Google Workspace for Education admins can contact Google to get technical support services via phone, email, or chat

Google Workspace for Education Core Services

Google Workspace for Education Core Services are the services listed and described in the services summary of the Google Workspace for Education Terms of Service (for example, Classroom, Gmail, Docs, Sheets, and Slides). These are the services provided to Google Workspace for Education customers under your Google Workspace for Education agreement. Learn more about the Google Workspace for Education Core Services here.

The Google Workspace for Education Data Processing Amendment (DPA), as applicable[5], governs how Google processes Customer Data from the Core Services. Customer Data is the data that organizations and their users provide to Google for processing in Google Workspace for Education Core Services, including Customer Personal Data (as defined in the Data Processing Amendment). Customers can opt-in to the DPA in the Google Admin console if you are located outside of Europe and believe it meets your compliance needs.

[5] If the GDPR applies to Google's processing of your data—for example, if you are established in the European Union, or established outside the European Union but offer goods/services to data subjects who are in the European Union—it requires your contract with Google to contain certain data processing terms.

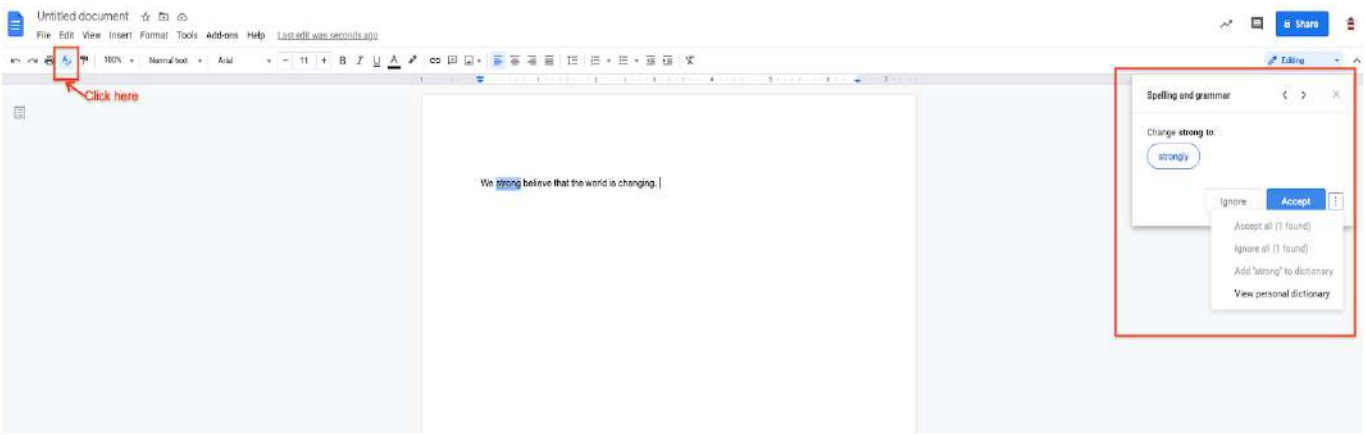
Google Workspace for Education Core Service Embedded Features

The Core Services include a number of features such as spelling & grammar, Explore, Calendar geo-location integration and Translate. These features are embedded in Google Workspace for Education Core Services and are available for all Google Workspace for Education users. Google is a **data processor** of Customer Personal Data processed through the embedded features in Google Workspace for Education Core Services. Features are governed by the Google Workspace for Education DPA when used in conjunction with the Google Workspace for Education Core Services.

Users can choose to turn off some embedded features (for example, turn off autocorrect and suggestions in spelling & grammar in Google Docs and Gmail) or elect not to use the embedded features (for example, "Translate document" and Explore). Please note that if you use Explore to navigate to a third party site, use of the third party site is **not** subject to the protections of the Google Workspace for Education DPA.

Spelling & Grammar

Spelling & grammar is an embedded feature in Google Docs and Gmail. It is important to highlight that your Customer Data is not used to improve spelling & grammar services for other customers' accounts. As highlighted above, Google is a **data processor** in relation to Spelling & grammar where the user accepts or rejects suggested changes. However, if the user takes proactive steps to provide feedback to the suggested spelling and grammar, Google is the **controller** of that feedback data. See below "Feedback" section for more information.

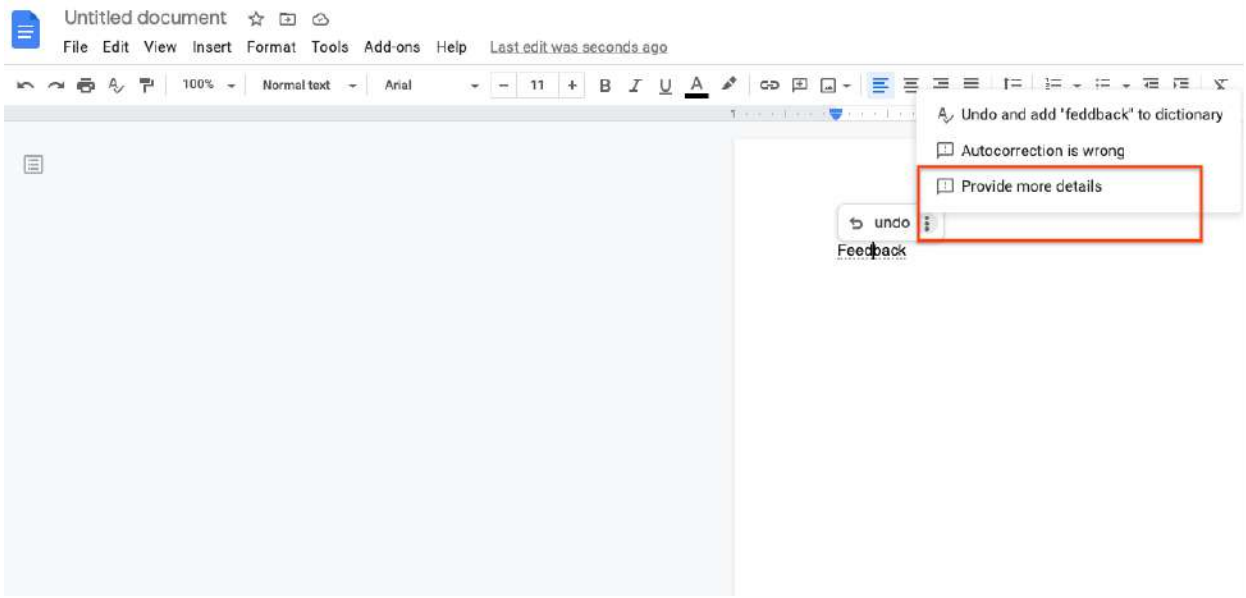


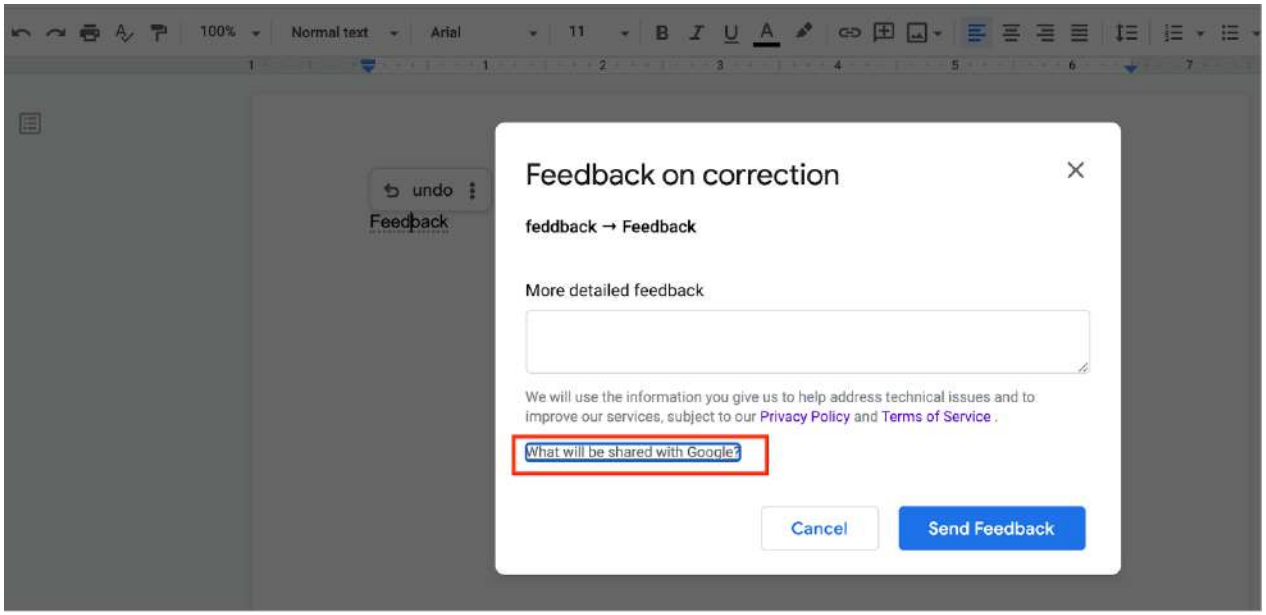
Please note that in addition to the spelling & grammar embedded feature, there are also spell checkers available in Chrome (which is **not** a Google Workspace Core Service). For further information on the basic spell check in Chrome and the enhanced spell check in Chrome, please see "enhanced spell check" section for more information.

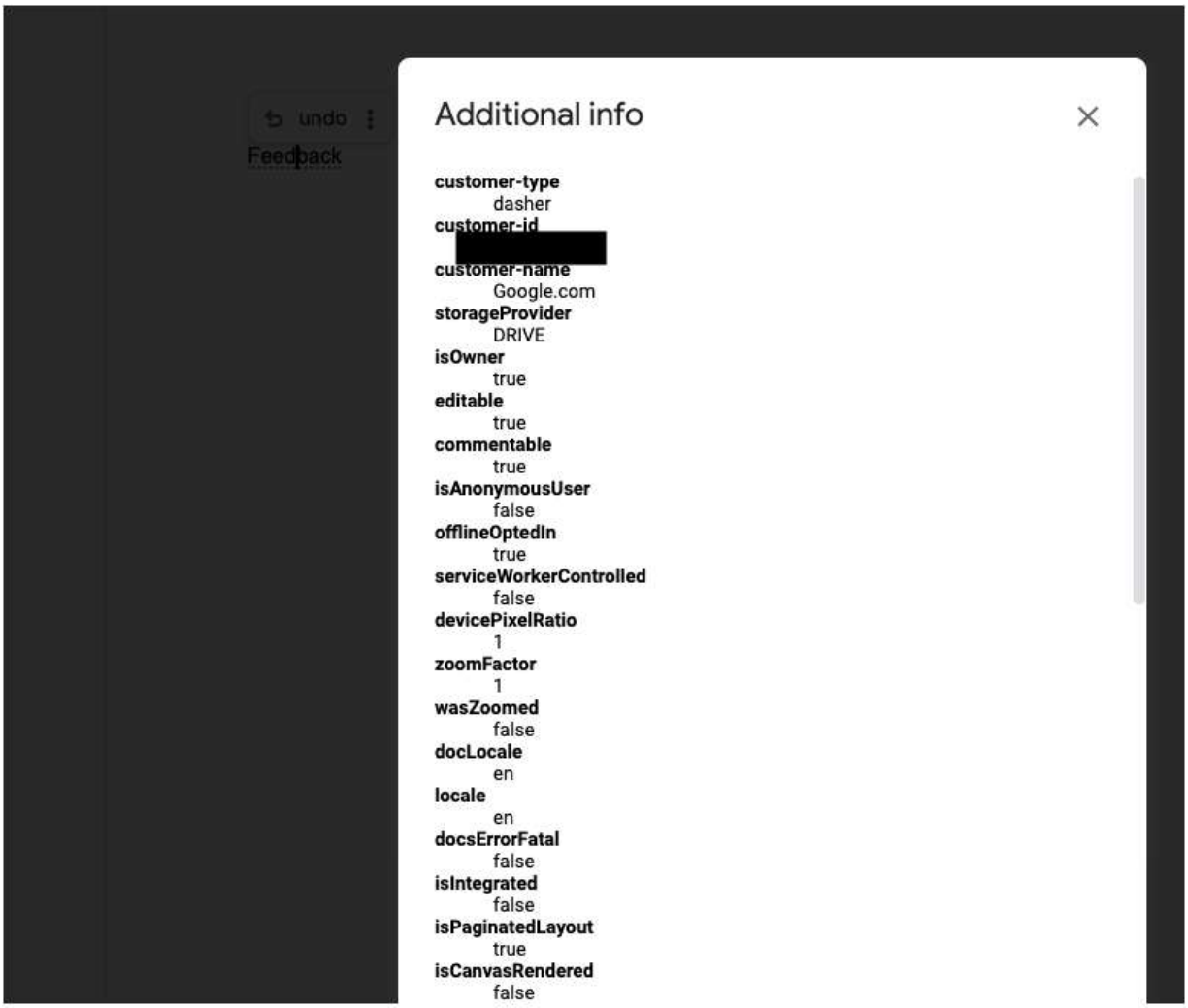
Feedback

Please note that any feedback voluntarily provided through our feedback tools will be processed according to the Google Privacy Policy, and we provide users with notice of these terms at all feedback ingress points. Google acts as **controller** for the feedback we collected through feedback. Please remove any personal information and sensitive information before providing feedback to Google.

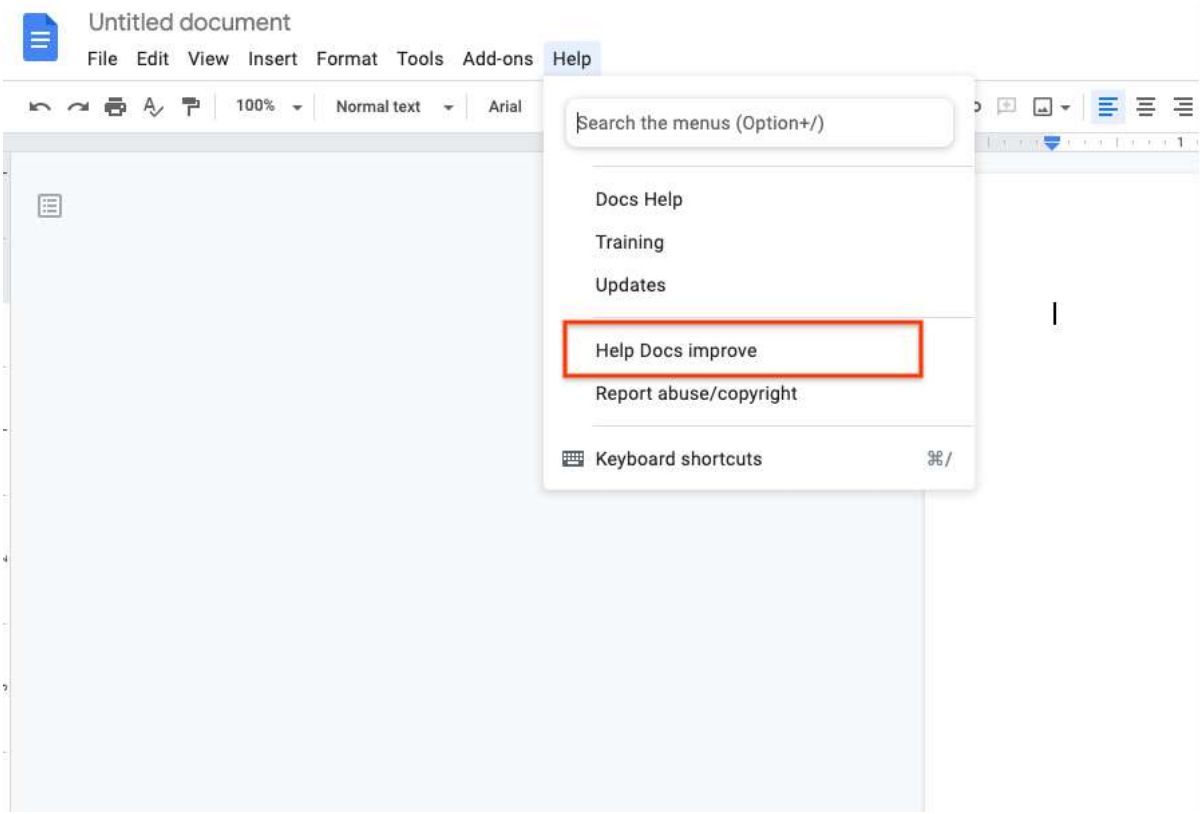
Users can provide feedback for suggested spelling & grammar corrections (see example below).

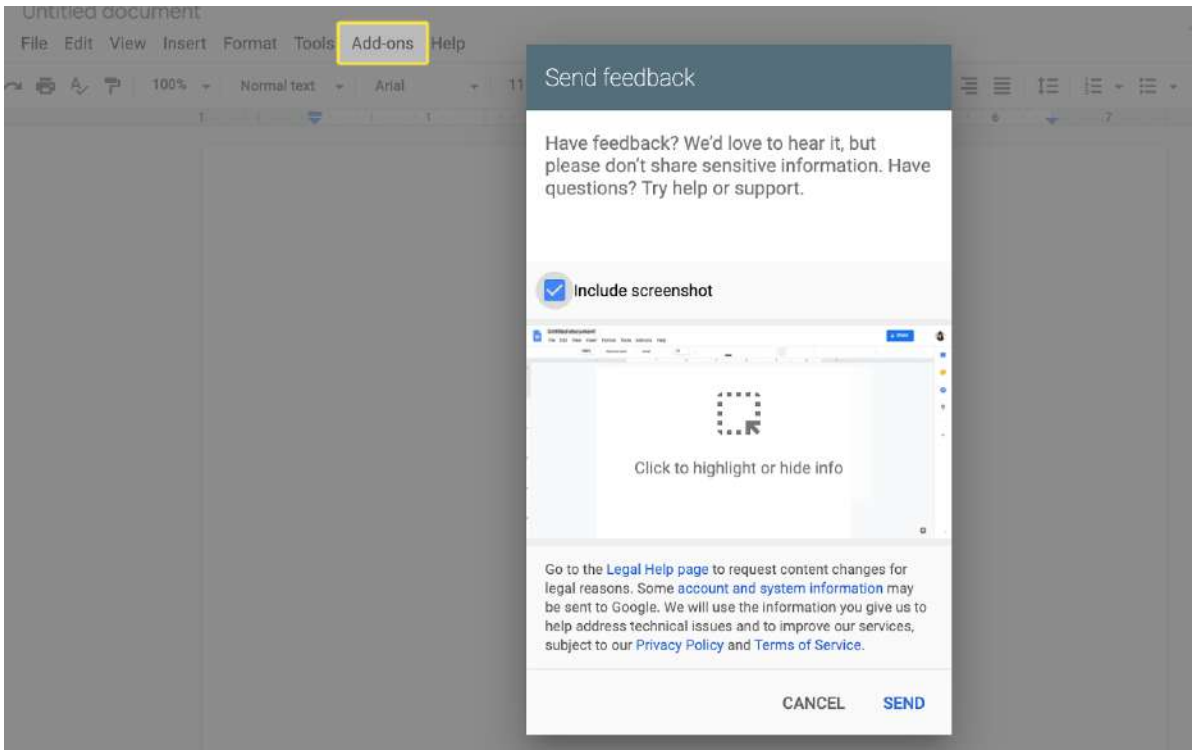






We also provide users with an option to provide in-product feedback (for example, in Google Doc). Users may choose to provide screenshots of an issue that they are encountering, and we provide a tool to hide sensitive information.


Untitled document
File Edit View Insert Format Tools Add-ons Help
100% Normal text Arial
Search the menus (Option+/)
Docs Help
Training
Updates
Help Docs improve
Report abuse/copyright
Keyboard shortcuts ⌘/


File Edit View Insert Format Tools Add-ons Help
Send feedback
Have feedback? We'd love to hear it, but please don't share sensitive information. Have questions? Try help or support.
Include screenshot
Click to highlight or hide info
Go to the Legal Help page to request content changes for legal reasons. Some account and system information may be sent to Google. We will use the information you give us to help address technical issues and to improve our services, subject to our Privacy Policy and Terms of Service.
CANCEL
SEND

Additional Services

Additional Services are not automatically provisioned as part of the Google Workspace for Education offering, and may be any Google service that can be used with an organization managed Google Account. A non-exhaustive list of Additional Google services is provided here. **Because these services and products are not part of the Google Workspace for Education offering, they are not governed by the Google Workspace for Education DPA and Google Workspace for Education Agreement**.

To offer a smooth experience to Google Workspace for Education customers, Google Additional Services are accessible to users via their organization managed Google Accounts. As detailed on the Additional Services page, most Additional Services are governed by the Google Terms of Service and Privacy Policy, and some Additional Services also have service-specific terms. To review these terms, see Additional Google services and go to the section titled, *Services with an individual On or Off control*. To learn more about Additional Services as it relates to Google Workspace for Education, see here.

Important: Google Workspace for Education administrators might need to turn Additional Services off for users while signed in to their organization managed Google Account for compliance reasons.

Administrators (also called *admins*) can turn each Additional Service *on* or *off* for users in the Google Admin console. These settings can be configured before the admin provisions any user accounts. For instructions, see Additional Google services and go to the section titled, *Turn services on or off for users*. In addition to Google Workspace for Education and other Google services that admins can manage individually with an *on* or *off* control in the Admin console, the admins can manage access to unlisted Google services that don't have an individual control (such as Chromecast, and Google Surveys). For details on how to turn these services On or Off, see manage services that aren't controlled individually.

Note: Even if a Google Workspace for Education admin has turned an Additional Service “Off”, users may still access and use some Additional Services in an unauthenticated state or retain some limited functionality, for example, for purposes of accessing purchased content. For example, if the admin has disabled YouTube in the Admin console for the organization, a user can still visit YouTube and use the service in a logged out state, but login using their organization managed Google Account will fail. In this case, Google will not process data that can be linked to the user’s organization managed Google Account.

We recommend that your organization’s Legal Counsel, Data Protection Officer (DPO), or equivalent, when applicable, should conduct an impact assessment of the processing of Customer Personal Data with these products to determine whether, and how, your organization can fulfill its obligations as a data controller or a data processor, as applicable, for each of these products.

Organization managed Google Account

For users in your organization to use your Google Workspace for Education services, you must give each user an account. An organization managed Google Account gives each user a name and password for signing in to Google services and a profile. Users can provide information directly, when providing a name and profile picture, or indirectly, when Google collects information about when and for what purposes and in what context (app/web, platform and device) a user signs in. When a user signs in to their new organization managed Google Account you created, they receive a notice explaining how their data is collected and accessed by their admin, and how their use of Google Workspace for Education Core Services is governed by your organization's Google Workspace for Education terms. The notice also explains that use of Additional Services when used with the organization managed Google Account are governed by Google Privacy Policy and Google Terms of Service, and applicable service-specific terms. For more information about organization managed Google Account creation, see Options for adding users.

For help setting up your account, creating users, and enabling services, see the Google Workspace for Education Quickstart IT Setup Guide.

Technical Support Services

Online, phone, and chat support is available to Google Workspace for Education admins. Data collected and processed as part of providing technical support services for your use of Google Workspace for Education Core Services are governed by the Google Workspace Technical Support Services Guidelines (TSSG) and Google Cloud Privacy Notice. Google collects and processes data for the purpose of providing the support services described in the TSSG and maintaining those Services. Google has no obligation under the Google Workspace for Education Agreement (or the TSSG) to provide support for any of the Additional Services.

Privacy best practices

In this section, we provide some best practices you can apply for customizing Google Workspace for Education services to meet your organization's data protection compliance needs. Please note this is not a comprehensive and exhaustive list of all potential practices and that tools referenced within this Guide may vary by edition. We recommend that you consult with a legal expert or your organization's data protection officer to obtain guidance on the specific requirements applicable to your organization, as this guide does not constitute legal advice.

Account setup and settings

Upon account creation, Customers are contractually required to obtain all required consents from end users and, where applicable, parents or guardians, to allow Google's provision of services. For more information about communicating with parents or guardians, see here.

For Google Workspace for Education primary and secondary education (K-12) accounts in particular, the following are recommended account settings:

- Control which third-party & internal apps access Google Workspace data and restrict access to Google Workspace services.
- In Drive, under "Sharing options," turn off external file sharing for students (or restrict external sharing to allow listed domains only) and set "Access checker" to "Recipients only"
- Turn off chat in Docs editors
- In Google Meet, only allow faculty and staff to create meetings. Users who can't create meetings can still join Meet video meetings created by others.
- For all K-12 and higher education accounts, it is recommended to avoid using students' names for email addresses and usernames.

Additional recommendations can be found in the following documents:

- Quickstart IT Setup Guide
- Domain Best Practices
- Deployment Guide

Control access to Google services by age

To make it easier to tailor experiences for your users, you can set access to some Google services based on age. The default age-based access setting depends on your institution type:

- **Higher education institutions –** All users are designated as 18 and over by default and have no additional restrictions for Google services. However, administrators in those organizations are required to identify any users under the age of 18. All users designated as under the age of 18 will have an age-restricted experience for some Google services.
- **Primary and secondary education institutions –** All users are designated as under the age of 18 by default, and have an age-restricted experience for some Google services.

You can use organizational units or access groups and apply age-based settings to certain subsets of users.

- Change the setting of any staff, teacher, and faculty organizational unit or configuration group to be 18 or older. Be sure that all users in the organizational unit and any sub-organizational unit or the configuration group are 18 or older.
- Move any users under 18 in your staff, teacher, or faculty organizational units or access groups to another organizational unit or group and apply the appropriate age-level setting.

Additional recommendations and restrictions to Google Services can be found in the following documents:

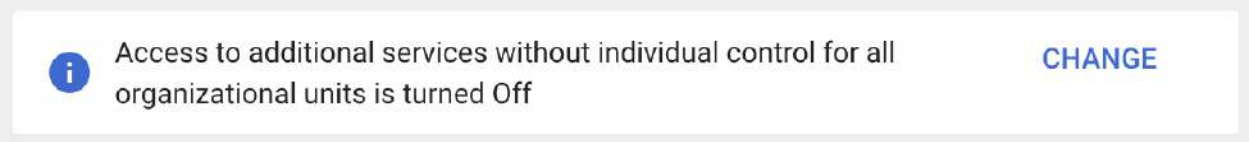
- Control Access to Google Services by Age

Choose which Additional Services to enable for your users

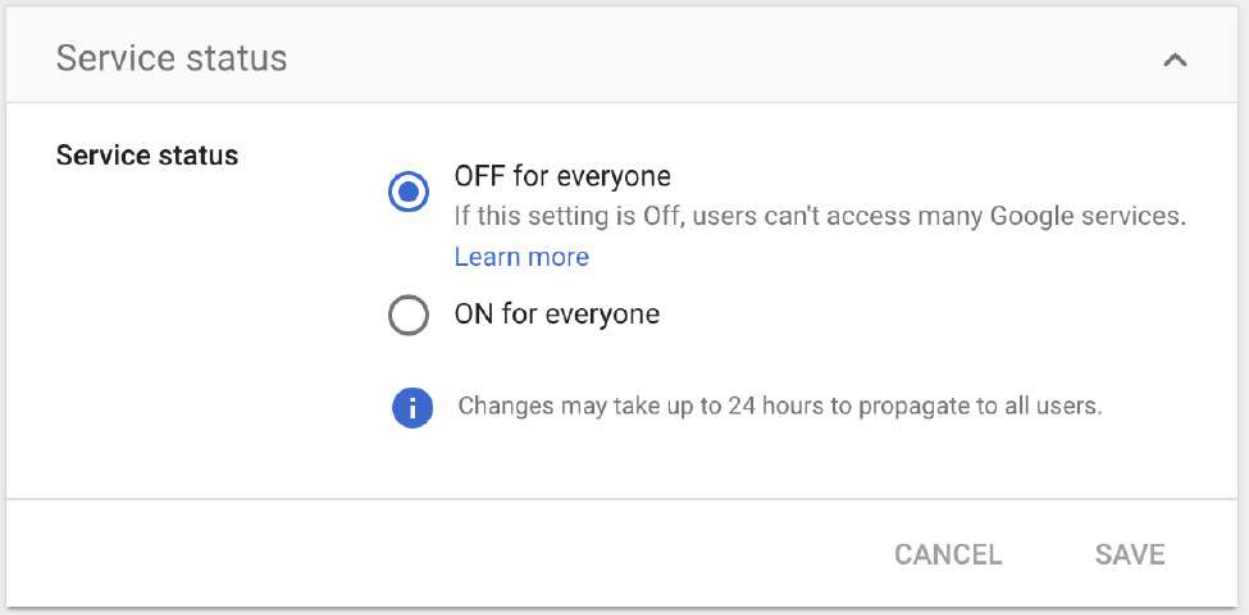
Additional Services are not part of the Google Workspace for Education offering and are not covered by the Google Workspace for Education DPA and Google Workspace for Education Agreement. Customers are contractually required to obtain all required consents from end users and, where applicable, parents or guardians, to allow Google's provision of Additional Services.

As an admin, we recommend that you carefully choose which Additional Services (for example, YouTube, Maps, and Blogger) to turn on/off for your users, especially for customers with age restrictions or who handle highly regulated or sensitive data (for example, financial data, health data, and government data). Please check the Additional Services section within this Guide for more information.

Admins can also limit access to additional services without an individual on/off control within the Admin Console. By clicking on Additional Google services from the home dashboard, admins can toggle whether access is turned on or off for a certain organizational unit on the left column or leave it at the top level OU which will cover the entire organization.



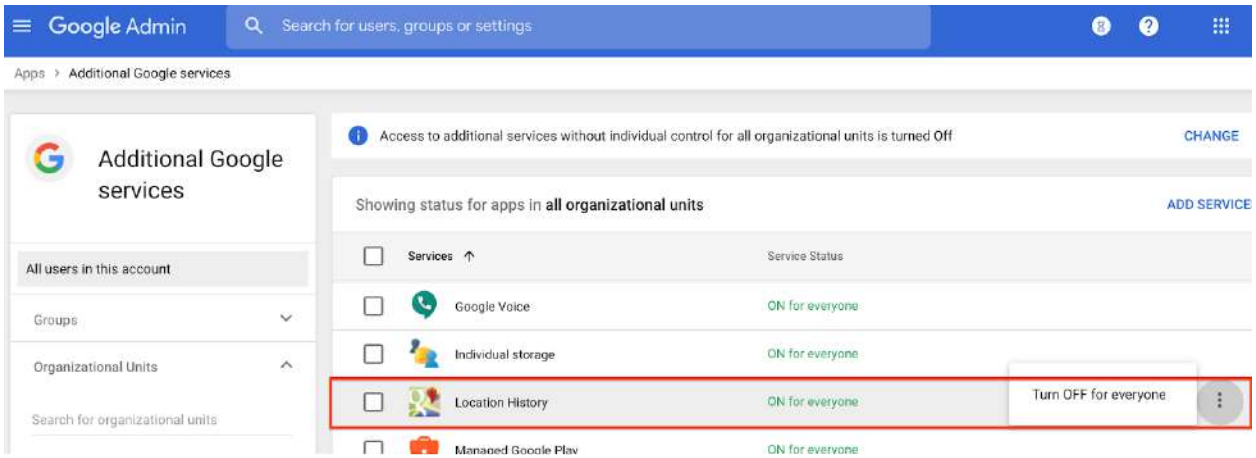
Clicking the **OFF** toggle will restrict services for that organizational unit. Clicking the **ON** toggle will not restrict services.



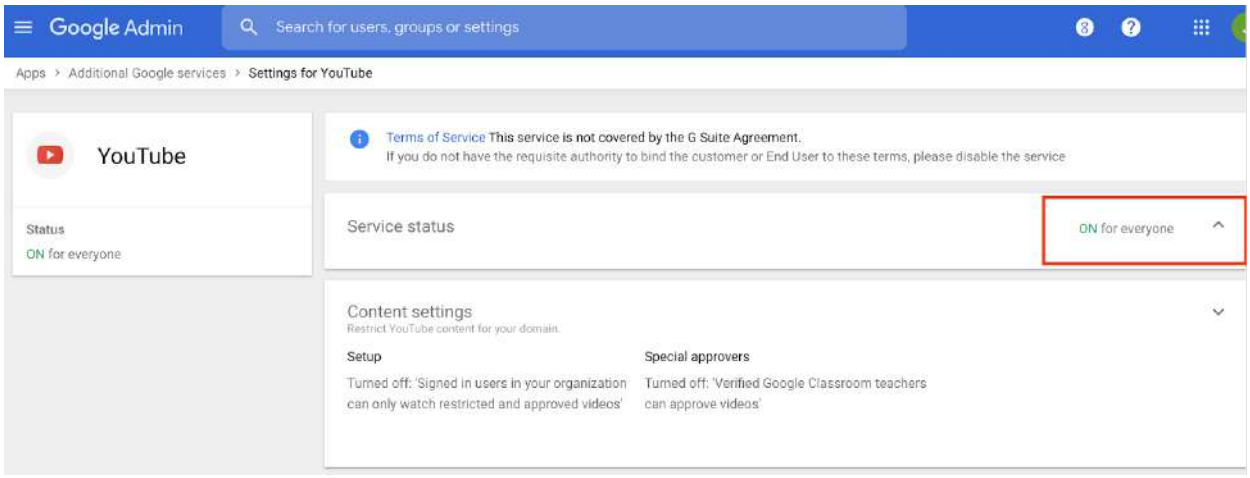
Help your users with their privacy activity controls

Advise your users to opt in to the appropriate activity controls that comply with your school's privacy policies and that meet your users' personal needs. If your users don't wish Google to store their activity history and provide a personalized user experience for their organization managed Google Account, instruct them to turn off certain settings from the Activity controls page. For more details, see the instructions and guidelines below.

- **Location History**—Consider whether you should turn on/off Location History for your users' organization managed Google Accounts. By default, Location History is turned **off** for your users. Location History can only be turned on if you have enabled it in the Google Admin console (after obtaining parental consent where required) **and** if your users have also enabled it. From the Admin console, go to *Apps > Additional Google services > Location History*. Instruct your users to turn Location History on or off by going to the Activity controls page for their organization managed Google Account. For user instructions, see Manage your Location History.



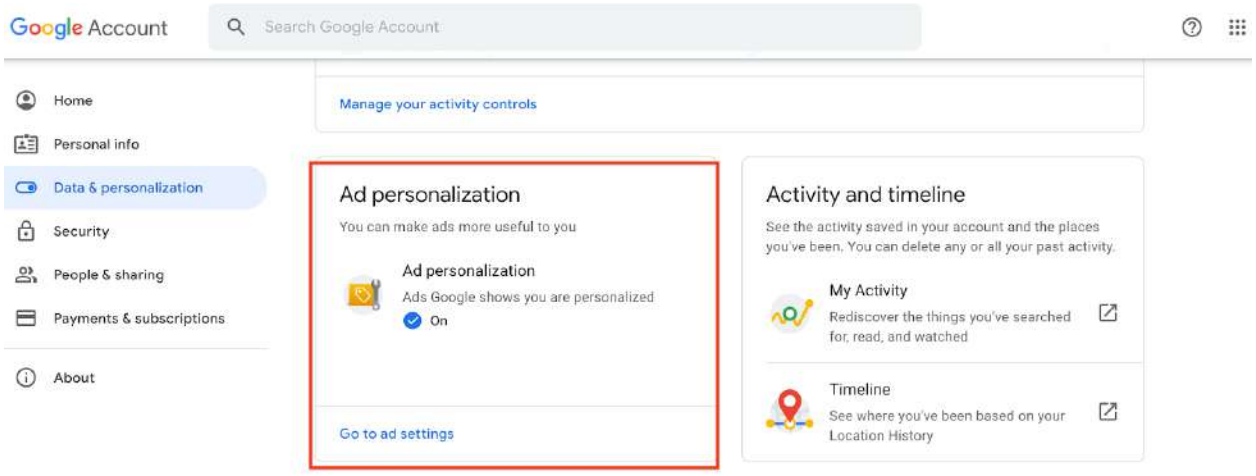
- **YouTube History**—Consider whether you should turn on/off YouTube for your users. For K-12 users, search history is off by default. From the Admin console, go to *Apps > Additional Google services > YouTube*. For Higher Education domains, once you turn on YouTube in the Admin console, your users have options to turn **YouTube History** on or off individually in the Activity controls page. Any videos they watch while history is off won't show in their history. The history also won't be used to improve their recommendations. For user instructions, see View, clear, or pause watch history.



- **Ads -** There are no ads in Google Workspace for Education Core Services and we do not collect or use student data for advertising purposes or create advertising profiles. K-12 Google Workspace for Education users also don't see ads when they use Google Search while signed in to their Google Workspace for Education accounts. Some of Google's additional services such as Blogger and YouTube do show ads to students, however, these ads are not personalized and we give Administrators the ability to restrict access to these services.

- **Ad personalization**—Ads are based on personal information that a user has added to their organization managed Google Account, data from advertisers that partner with Google, and Google's estimation of a user's interests. For K-12 users, ads personalization is off by default. When Ad personalization is turned on for Higher Education domains, it enables a personalized ad experience for individual users. However, your users have the option to turn on/off this setting from the Activity controls page. When ads personalization is turned off, Google will no longer use their information to personalize their ads. Please consider instructing your users to go to the Activity controls page to turn on/off Ad personalization.

  Note: Google Workspace for Education does not use Customer Data for advertising purposes. Ad personalization is only applicable to Google services offered outside of Google Workspace for Education.

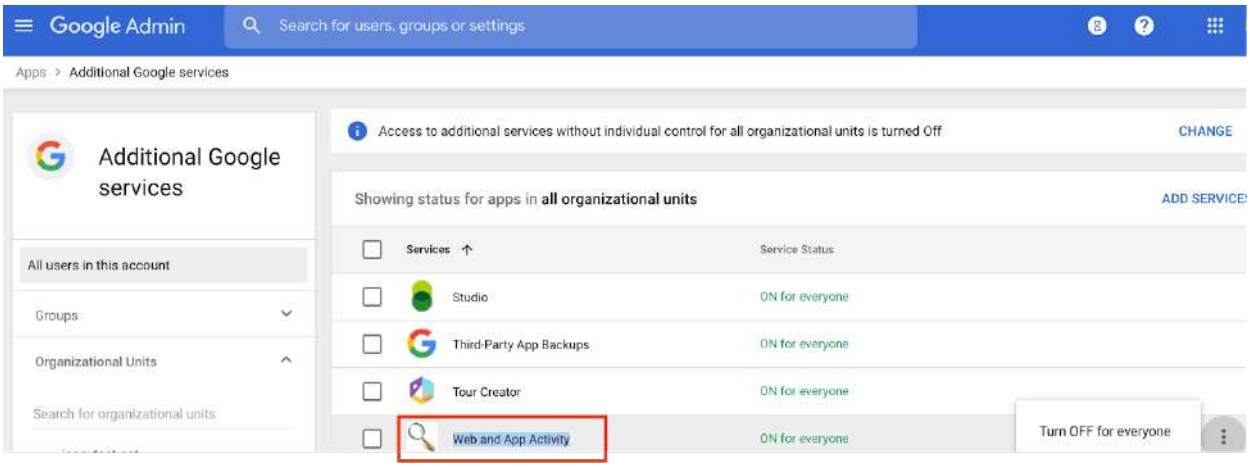


- **Web & App Activity**—Consider whether you should turn on/off Web & App Activity (WAA) for your users. From the Admin console, go to *Apps > Additional Google services > Web and App Activity*. By default, for K-12 accounts, the admin WAA control is off by default and the WAA personalization setting for your end users is turned off. When the WAA service is turned **on** for the organization, the end users have the option to turn it on/off at their preference. If the admin turns the admin WAA control **off** for their organization in the Admin console, end users won't be able to turn it on individually.

  If users choose to turn on the WAA individually, their searches and activity from other Google services are saved in their organization managed Google Accounts, which provides them with a

more personalized experience. Users can see and delete their Web & App Activity from the Activity controls page. For user instructions, go to See & control your Web & App Activity.

Note: As a reminder, there are no ads in Google Workspace for Education core services and we do not use core service student data for advertising purposes or create advertising profiles.



Control which users can use Chrome sync and advice on other Chrome settings

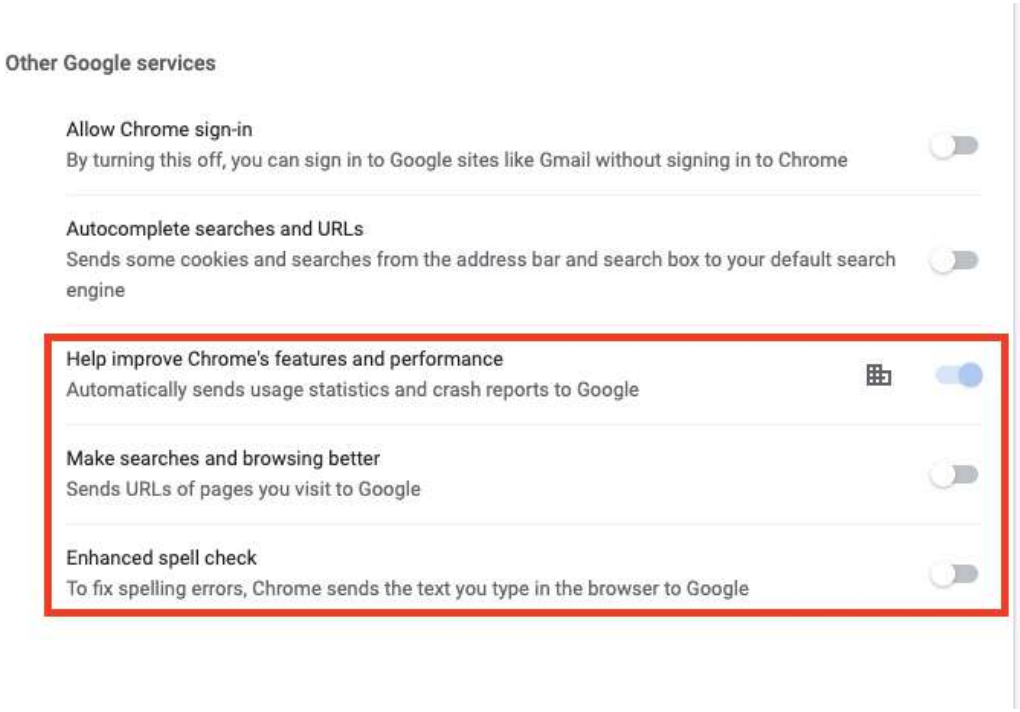
Chrome sync saves your users' bookmarks, history, passwords, and other settings securely to their organization managed Google Accounts and enables your users to access these settings from Chrome on any device. For Google Workspace for EDU domains, Chrome sync is a Core Service. As an admin, you can control who uses Chrome sync from their organization managed account by turning it on/off or let users decide if they want to use sync. When Chrome sync is turned on, users can see and update synced info on any device, like bookmarks, history, passwords, and other settings.

Additionally, admins can also set other features in Chrome to on/off, or let users decide:

- **Help improve Chrome's features and performance**—The transmission of crash reports and usage statistics to Google is enabled by default. Administrators can turn this feature on or off for both ChromeOS or Chrome.[6] Usage statistics contain information such as preferences, button clicks, performance statistics, and memory usage. In general, Chrome usage statistics do not include web page URLs or personal data. However, if the user has turned on "*Make searches and browsing better*" in the Chrome settings, then Chrome usage statistics will include information about the web pages visited by a user, and the user's usage of those pages. If Chrome sync is enabled, Chrome may also combine any declared age and gender information from the user's organization managed Google account with our statistics to help us build better products for all demographics. This information does not personally identify the user and is used only in

[6] On desktop Chrome, the administrator can enable, disable this setting, or give users the choice. On Chrome OS, the administrator must make a decision and can't leave it to the user.

aggregate form. Crash reports contain system information gathered at the time of the crash, and may contain web page URLs or personal data depending on what was happening at the time the crash report was triggered.



- **Enhanced spell check**—The basic spell check uses a local dictionary, while the enhanced spell check is cloud-based and sends the text that your users type to Google. By default, basic spell check is turned on for your users. If your users want to enable enhanced spell check, they can do so from the Chrome menu by clicking *Preferences > Advanced > Languages*. If the enhanced spell check is enabled, Chrome sends the entire contents of text fields as you type in them to Google, along with the browser's default language. Please note the enhanced spell check is not part of the Google Workspace for Education Core Services, and therefore it's not governed by Google Workspace for Education Agreements and DPA. The data sent back to Google by enhanced spell check is processed in accordance with the Google Privacy Policy, and Chrome and Chrome OS Additional Terms of Service.

If you've opted into "Make Searches and Browsing Better (sends URLs of the pages you visit to Google)", Chrome sends a request to Safe Browsing each time you visit a page that isn't in Chrome's local list of safe sites in order to gather the latest reputation of that website ("real-time checks"). If you sync your browsing history without a sync passphrase, this request also contains a temporary authentication token tied to your Google account to provide better protections to some users whose account may be under attack. If the website is deemed unsafe by Safe Browsing, you may be shown a warning. This mechanism is designed to catch unsafe sites that switch domains very quickly or hide from Google's crawlers.

Finally, when ChromeOS or desktop users grant websites access to their location, that location is also shared with Google Location Services (GLS). Admins can disable this by disabling Geolocation via Devices > Chrome > Settings > User & Browser Settings > Security > Geolocation.

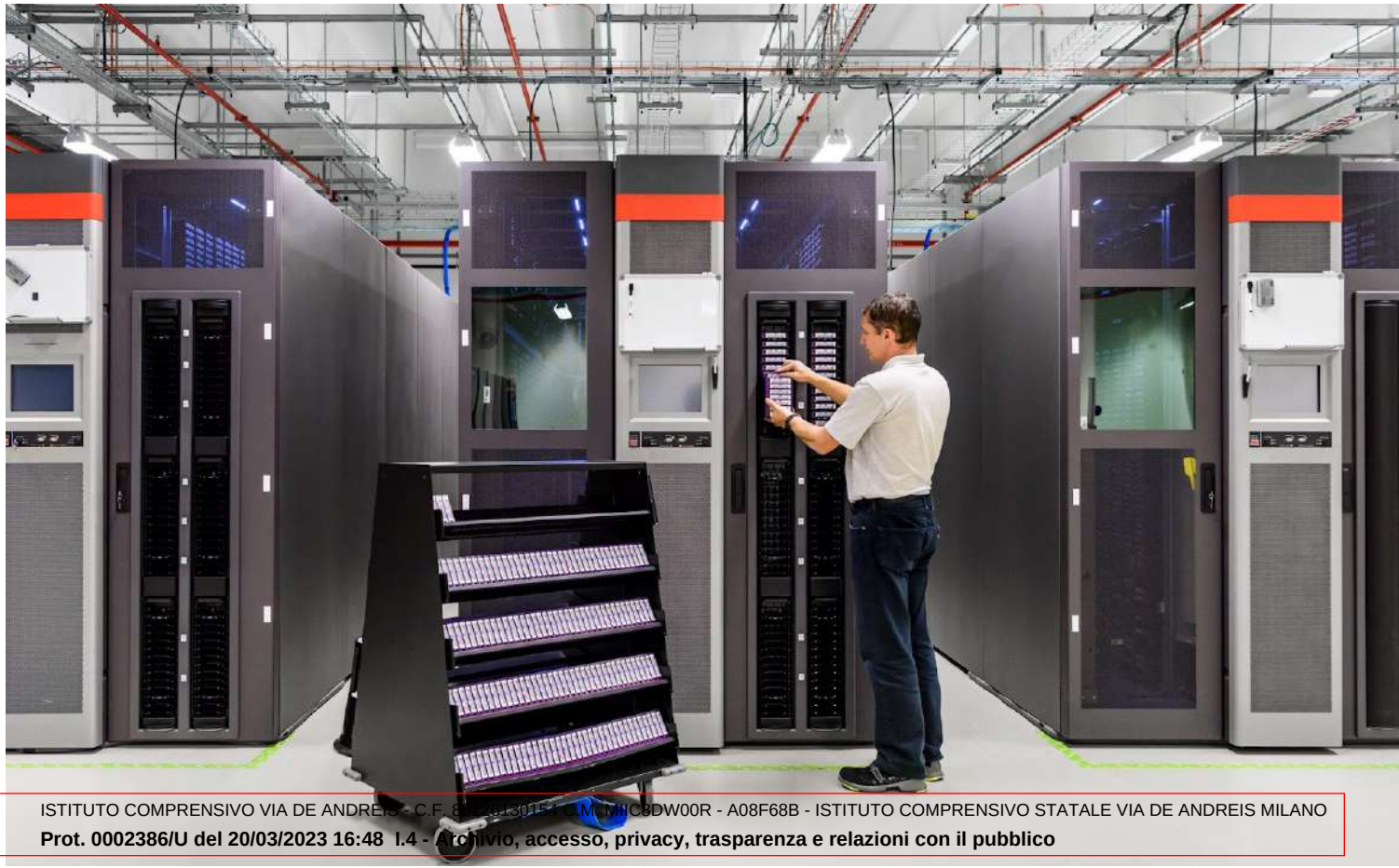
If your organization needs stricter admin control over Chrome settings and needs to control what data is being shared with Google and third parties through Chrome, please consider using our Chrome Education Upgrade offering. Chrome Education Upgrade gives admins options to set various policies for their organization. For example, admins can set up the Metrics Reporting policy to disable crash-related data being sent to Google for all users in their organization and anonymous reporting of usage.

For more information on Chrome privacy settings, see our Google Chrome Privacy Whitepaper.

Separate user access within the domain

As an admin, you can manage user access to different sets of Google Workspace for Education Services and Additional Products by creating organizational units. By doing this, you can separate into different groups the users who manage personal/sensitive data and the users who don't. Once these organizational units are set up, you can turn on or off specific services/products for groups of users.

For example, the Human Resources (HR) department may manage personal/sensitive data, but only a subset of HR users may actually need access to this data. In this case, you can configure an HR organizational unit for users using Google Workspace for Education Core Services with personal/sensitive data, with certain services disabled and settings configured appropriately.



Advise users to keep organization managed Google Accounts and personal accounts separate

We recommend that users keep the access to their organization managed Google Account and personal Google Account separate from each other. As an admin, we recommend that you advise users not to sign in to multiple Google Accounts simultaneously in the same Chrome browser. Users can also sign into their Google Workspace for Education account as a secondary account. This mitigates the risk of human error that leads to the accidental storage of Customer Data in a user's personal account or the application of privacy settings from a personal Google Account to an organization managed Google Account.

If your organization needs stricter control, you can prevent users from signing in to Google services using any accounts other than those you provide them with. For example, you might not want users to use their personal Gmail account or an organization managed Google Account from another domain. For instructions, see Block access to consumer personal accounts.[7]

Additionally, as an admin you can securely manage school apps and data on Android devices and leave personal apps and data under the user's control. A work profile[8] can be set up on an Android device to separate work apps and data from personal apps and data. Learn more about how to set up the work profile and allowlist preferred work apps for Android devices.

Review security health recommendations

To increase the safety and security of your organization's data, consider reviewing the recommendations provided by the security health page in the Admin console. You can also check the security checklist for medium and large businesses in the Admin Help Center.

Admins also have many powerful security tools at their disposal and are empowered to customize their individual security settings to meet their business needs. For example, the Alert Center for Google Workspace for Education provides alerts and actionable security insights about activity in your domain to help protect your organization from the latest security threats, like phishing and suspicious device activity. The security investigation tool allows you to identify, triage, and take action on security and privacy issues in your domain. Admins can also automate actions in the investigation tool by creating activity rules to detect and remediate such issues more quickly and efficiently. In addition, Google Vault allows you to retain, hold, search, and export data in support of your organization's retention and eDiscovery needs. These and many more security tools are available and detailed within the Google Workspace Security page.

[7] You need to sign up the Chrome Browser Cloud Management to set group policies for enrolled browsers.
[8] Setting up a work profile requires advanced mobile management. Learn more about how to set up advanced mobile management.

Review your organization's use of third-party applications

Some Google Workspace for Education services may make it possible for a user to share Customer Personal Data with a third party (or a third-party application) based on your settings for the domain. As such, customers are responsible for ensuring that appropriate, compliant measures are in place with any third party (or third-party application) before sharing or transmitting Customer Personal Data. Your organization is responsible for determining whether any other data-protection terms need to be in place before sharing personal/sensitive data with the third party using Google Workspace for Education services, or applications that integrate with them.

As an admin, you have three choices in managing the Google Workspace Marketplace. You can prohibit the installation of all apps, allow only the installation of allowlisted apps, or allow the installation of any app. Admins can also choose to install apps, and grant consent for these apps, on behalf of Google Workspace for Education users. By default, Google Workspace for Education primary/secondary (K-12) users are prevented from installing all apps. We recommend that you review the school policy and allowlist only selective third-party applications that can access API scopes across Google Workspace for Education services.

Using app access control, you can further control which third-party and domain-owned apps can access sensitive Google Workspace for Education data. Use app access control to:

- Restrict access to most Google Workspace for Education services, or leave them unrestricted.
- Trust specific apps so they can access restricted Google Workspace for Education services.
- Trust all domain-owned apps.

We recommend that you review the school's policy and change the setting to restricted or limited access to your Google Workspace for Education Customer Data if needed.

Monitor account activity

Admin console reports and audit logs make it easy to examine potential security risks, measure user collaboration, track who signs in and when, analyze admin activity, and much more. To monitor logs, admins can configure notifications to send them alerts when Google detects certain activities—including suspicious login attempts, users suspended by an admin, new users who are added, suspended users who are made active, users who are deleted, password changes by an admin, users who are granted an admin privilege, and users who have their admin privilege revoked. The admin can also review reports and audit logs on a regular basis to examine potential security risks. In particular, the key trends in the highlights section, overall exposure to data breaches in security, files created in apps usage activity, account activity, and audits provide helpful security risk insights.

While admin audit logs provide information about actions taken by members within your own organization, Access Transparency[9] provides logs of the actions taken by Google personnel. The access transparency logs include information about the accessed resource and action, the time of the action, and the reason for the action (for example, the case number associated with a customer support request).

Establish privacy policies for file names and path names

As an additional security precaution, to restrict sharing of Customer Personal Data, we recommend that you establish policies to prevent users from including sensitive information when naming and organizing files in Google Workspace for Education Core Services (for example, Docs, Sheets, Slides, Forms, Drive, Gmail), or naming the Google Chat room or Meet invite with sensitive personal information. Examples of sensitive Customer Personal Data includes an individual's full name, email address, mailing address, telephone number, or any unique account identifiers (for example, customer ID, project ID, and screen name).

Additionally, you can take advantage of data loss prevention (DLP) capabilities in Google Workspace for Education to inspect, classify, and de-identify sensitive data to help restrict exposure. See Prevent data loss using DLP for Drive and Scan your email traffic using DLP rules. We provide a library of predefined content detectors to make setup easy. Once the DLP policy is in place, for example, Gmail can automatically check all outgoing email for sensitive information and automatically take action to prevent data leakage: either quarantine the email for review, tell users to modify the information, or block the email from being sent and notify the sender. With easy-to-configure rules and optical character recognition (OCR) of content stored in images, DLP for Drive makes it easy for administrators to audit files containing sensitive content and configure rules that warn and prevent users from sharing confidential information externally. Learn more in our DLP whitepaper.

[9] This feature is only available with Google Workspace for Education Standard and Plus.

COPPA

The Children's Online Privacy Protection Act of 1998 (COPPA) is a U.S. regulation applicable to the collection of personal information from children under the age of 13. COPPA imposes certain requirements on operators of websites or online services directed to children under 13 years of age, and on operators of other websites or online services that have actual knowledge that they are collecting personal information online from a child under 13 years of age.

Google Workspace for Education Core Services can be used in compliance with COPPA. Google contractually requires that schools using Google Workspace for Education and any Additional Services, if applicable, obtain parental consent required under COPPA.

FERPA

Student educational records are protected under FERPA (The Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g; 34 CFR Part 99). This federal law applies to any school with certain programs funded by the U.S. Department of Education.

Google Workspace for Education can be used in compliance with FERPA, our commitment to which is included in our agreements.

Online safety

It's important that children know about online safety and how to safeguard their valuable information, recognise scams and phishing attempts, and keep private information private. Our Be Internet Awesome Family Guide gives families tools and resources to learn about online safety and citizenship at home. Our Digital Wellbeing Family Guide helps you start a conversation about tough tech questions and navigate the digital world as a family. Parents and guardians may also find the Parent and Guardian Security Resource helpful.

Additional resources

To help our customers with compliance and reporting, we share privacy-related instructions and best practices, and provide easy access to documentation. Our products regularly undergo independent verification of security, privacy, and compliance controls, achieving certifications against global standards to earn your trust. For a list of Google Workspace for Education standards, regulations, and certifications, see our Compliance resource center.

For easy, on-demand access to these critical compliance resources, at no additional cost, see our Compliance Reports Manager. Key resources include our latest ISO/IEC certificates, SOC reports, and self assessments. Select resources may require sign-in with your Google Cloud Platform or Google Workspace for Education account.

For more information on how Google Workspace for Education services are designed with privacy, confidentiality, integrity, and availability of data in mind, see the following:

- **Google Cloud Privacy** - Includes the list of Enterprise Privacy Principles for Google Cloud
- **Google Workspace Security page** - Homepage for Google Cloud security, with links to security white papers and other resources related to privacy, transparency, infrastructure, and security products
- **Google Workspace Admin Help Center** - Homepage that links to instructions and technical documentation for Google Workspace products and security features
- **GDPR Resource Center** - Includes regulatory, compliance, and product information to help you with GDPR compliance
- **Security resource center** - Includes whitepapers, videos, articles, blog posts, and documentation on privacy and security
- **Google for Education Privacy & Security Center** - Resource for Google Workspace for Education customers.
- **Google for Education Guardian's Guides to Google Tools** - Digital resources to help parents support their child's learning from home

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.

[Traduzione a cura dell'Ufficio del Garante]

COMITATO EUROPEO PER LA PROTEZIONE DEI DATI - EDPB

Domande frequenti sulla sentenza della Corte di giustizia dell'Unione europea nella causa C-311/18 — *Data Protection Commissioner/Facebook Ireland Ltd e Maximillian Schrems*

Adottate il 23 luglio 2020

Il presente documento mira a fornire risposte ad alcune domande frequenti ricevute dalle autorità di controllo e sarà sviluppato e integrato con ulteriori analisi man mano che il comitato europeo per la protezione dei dati prosegue nell'esame e nella valutazione della sentenza della Corte di giustizia dell'Unione europea ("la Corte").
La sentenza C-311/18 è disponibile qui e il comunicato stampa della Corte è disponibile qui.

1) Che cosa ha stabilito la Corte nella sua sentenza?

- → Nella sua sentenza, la Corte ha esaminato la validità della decisione n. 2010/87/CE della Commissione europea sulle clausole contrattuali tipo ("SCC") e ne ha ritenuto la validità. Infatti, la validità di tale decisione non è in dubbio per il semplice motivo che le clausole tipo di protezione dei dati di cui alla suddetta decisione non sono vincolanti per le autorità del paese terzo verso il quale i dati possono essere trasferiti, avendo esse natura contrattuale.

Tuttavia, tale validità, ha aggiunto la Corte, dipende dall'esistenza all'interno della decisione 2010/87/CE di meccanismi efficaci che consentano, in pratica, di garantire il rispetto di un livello di protezione sostanzialmente equivalente a quello garantito dal RGPD all'interno dell'Unione europea, e che prevedano la sospensione o il divieto dei trasferimenti di dati personali ai sensi di tali clausole in caso di violazione delle clausole stesse o in caso risulti impossibile garantirne l'osservanza.

A tale riguardo, la Corte rileva, in particolare, che la decisione 2010/87/CE impone all'esportatore di dati e al destinatario dei dati ("l'importatore dei dati") l'obbligo di verificare, prima di qualsiasi trasferimento, alla luce delle circostanze del trasferimento stesso, se tale livello di protezione sia rispettato nel paese terzo in questione. Inoltre, la Corte rileva che la decisione 2010/87/CE impone all'importatore di informare l'esportatore di qualsiasi impossibilità di rispettare le clausole tipo di protezione dei dati nonché, ove necessario, eventuali misure supplementari a quelle offerte da tali clausole, nel qual caso l'esportatore di dati è tenuto a sospendere, a sua volta, il trasferimento dei dati e/o a risolvere il contratto con l'importatore.

- ➔ La Corte ha inoltre esaminato la validità della decisione relativa allo scudo per la privacy (*Privacy Shield*) (Decisione 2016/1250 sull'adeguatezza della protezione offerta dallo scudo UE-USA per la privacy), poiché i trasferimenti in esame nell'ambito della controversia nazionale che ha portato alla domanda di pronuncia pregiudiziale si sono svolti tra l'UE e gli Stati Uniti ("USA").

La Corte ha ritenuto che i requisiti del diritto interno degli Stati Uniti, e in particolare determinati programmi che consentono alle autorità pubbliche degli Stati Uniti di accedere ai dati personali trasferiti dall'UE agli Stati Uniti ai fini della sicurezza nazionale, comportino limitazioni alla protezione dei dati personali che non sono configurate in modo da soddisfare requisiti sostanzialmente equivalenti a quelli previsti dal diritto dell'UE[1] e che tale legislazione non accordi ai soggetti interessati diritti azionabili in sede giudiziaria nei confronti delle autorità statunitensi.

Alla luce di tale grado di ingerenza nei diritti fondamentali delle persone i cui dati sono trasferiti verso il suddetto paese terzo, la Corte ha dichiarato invalida la decisione sull'adeguatezza dello scudo per la privacy (Privacy Shield).

2) La sentenza della Corte ha implicazioni sugli strumenti di trasferimento diversi dallo scudo per la privacy?

→ In generale, per i paesi terzi, la soglia fissata dalla Corte si applica anche a tutte le garanzie adeguate ai sensi dell'articolo 46 del RGPD delle quali ci si avvalga per trasferire dati dal SEE a qualsiasi paese terzo. La normativa statunitense cui fa riferimento la Corte (vale a dire l'articolo 702 della FISA e l'Executive Order (EO) 12333) si applica a qualsiasi trasferimento verso gli Stati Uniti per via elettronica che rientra nell'ambito di applicazione della suddetta normativa, indipendentemente dallo strumento utilizzato per il trasferimento[2].

3) È previsto un periodo di grazia durante il quale continuare a trasferire i dati verso gli USA senza valutare la base giuridica per il trasferimento?

→ No, la Corte ha annullato la decisione relativa allo scudo per la privacy senza preservarne gli effetti, in quanto la normativa americana che è oggetto di valutazione da parte della Corte non fornisce un livello di protezione sostanzialmente equivalente a quello dell'UE. Tale valutazione deve essere tenuta presente con riguardo a ogni trasferimento verso gli Stati Uniti.

4) Trasferisco dati a un importatore di dati statunitense aderente allo scudo per la privacy, cosa devo fare adesso?

→ I trasferimenti sulla base di tale quadro giuridico sono illegali. Qualora desideri continuare a trasferire i dati verso gli Stati Uniti, occorre verificare se ciò sia possibile alle condizioni di seguito indicate.

5) Mi avvalgo di SCC con un importatore di dati negli Stati Uniti, cosa devo fare?

[1] La Corte sottolinea che taluni programmi di sorveglianza che consentono alle autorità pubbliche statunitensi di accedere ai dati personali trasferiti dall'UE agli Stati Uniti per motivi di sicurezza nazionale non prevedono limitazioni al potere conferito alle autorità statunitensi né garanzie per soggetti non statunitensi potenzialmente sottoposti a tale sorveglianza.

[2] L'articolo 702 della FISA si applica a ogni "fornitore di servizi di comunicazione elettronica" (cfr. la definizione di cui all'articolo 1881 dell'USC 50, lettera b) (4)), mentre l'Executive Order 12 333 disciplina la sorveglianza elettronica, definita come "acquisizione di una comunicazione non pubblica con mezzi elettronici senza il consenso di una persona che è parte di una comunicazione elettronica o, in caso di comunicazione non elettronica, senza il consenso di una persona visibilmente presente nel luogo della comunicazione, con l'esclusione dell'impiego di dispositivi radio di direzionamento al solo scopo di stabilire la posizione di un apparato trasmittente" (3.4;b)).

→ La Corte ha rilevato che la normativa degli Stati Uniti (Art. 702 della FISA ed EO 12333) non garantisce un livello di protezione sostanzialmente equivalente.

La possibilità o meno di trasferire dati personali sulla base di SCC dipende dall'esito della valutazione che dovrà compiere, tenuto conto delle circostanze del trasferimento e delle misure supplementari eventualmente messe in atto. Le misure supplementari unitamente alle SCC, alla luce di un'analisi caso per caso delle circostanze del trasferimento, dovrebbero garantire che la normativa statunitense non interferisca con l'adeguato livello di protezione garantito dalle SCC e dalle misure supplementari stesse.

Se si è giunti alla conclusione che, tenuto conto delle circostanze del trasferimento e delle eventuali misure supplementari, non vi sarebbero adeguate garanzie, occorre sospendere o porre fine al trasferimento di dati personali. Tuttavia, se si intende continuare ciononostante a trasferire i dati, occorre informarne la SA competente[3].

6) Utilizzo le norme vincolanti d'impresa ("BCR") con un soggetto stabilito negli Stati Uniti, cosa devo fare?

→ Tenuto conto della sentenza della Corte, che ha annullato lo scudo per la privacy a causa del grado di interferenza creato dalla normativa degli Stati Uniti con i diritti fondamentali delle persone i cui dati sono trasferiti verso tale paese terzo, e alla luce della circostanza per cui lo scudo per la privacy era stato concepito anche al fine di apportare garanzie ai dati trasferiti utilizzando altri strumenti, come le norme vincolanti d'impresa, la valutazione della Corte si applica anche con riguardo alle norme vincolanti d'impresa, in quanto la normativa statunitense prevarrà anche sull'applicazione di quest'ultimo strumento.

La possibilità di trasferire o meno dati personali sulla base delle BCR dipenderà dall'esito della valutazione, tenuto conto delle circostanze del trasferimento e delle misure supplementari eventualmente messe in atto. Le misure supplementari unitamente alle BCR, alla luce di un'analisi caso per caso delle circostanze del trasferimento, dovrebbero garantire che la normativa statunitense non interferisca con l'adeguato livello di protezione garantito dalle BCR e dalle misure supplementari stesse.

Se si è giunti alla conclusione che, tenuto conto delle circostanze del trasferimento e delle eventuali misure supplementari, non vi sarebbero adeguate garanzie, occorre sospendere o porre fine al trasferimento di dati personali. Tuttavia, se si intende continuare ciononostante a trasferire i dati, occorre informarne la SA competente[4].

[3] V., in particolare, il punto 145 della sentenza della Corte e la clausola 4, lettera g), della decisione n. 2010/87/UE della Commissione, nonché la clausola 5 (a) della decisione n. 2001/497/CE della Commissione e l'allegato II (c) della decisione n. 2004/915/CE della Commissione.

[4] V., in particolare, il punto 145 della sentenza della Corte e la clausola 4, lettera g), della decisione n. 2010/87/UE della Commissione. Cfr. anche sezione 6.3 WP256 rev.01 (Gruppo di lavoro articolo 29, documento di lavoro che stabilisce una tabella con gli elementi e i principi contenuti nelle BCR per titolari del trattamento, approvato dal comitato europeo per la protezione dei dati, http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614109), e sezione 6.3 WP257 rev.01 (Gruppo di lavoro articolo 29, documento di lavoro che stabilisce una tabella con gli elementi e i principi contenuti nelle BCR per responsabili del trattamento, approvato dal comitato europeo per la protezione dei dati, http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614110).

7) E che succede rispetto agli altri strumenti di trasferimento previsti dall'articolo 46 del RGPD?

→ Il Comitato europeo per la protezione dei dati valuterà le conseguenze della sentenza sugli strumenti di trasferimento diversi dalle SCC e dalle BCR. La sentenza chiarisce che il parametro per l'adeguatezza delle garanzie di cui all'Art. 46 RGPD è costituito dalla "equivalenza sostanziale".

Come sottolineato dalla Corte, occorre rilevare che l'articolo 46 figura nel capo V del RGPD e, di conseguenza, deve essere letto alla luce dell'articolo 44 del regolamento stesso, in base al quale *"tutte le disposizioni di detto capo devono essere applicate al fine di garantire che non sia compromesso il livello di protezione delle persone fisiche garantito da tale regolamento*".

8) Posso utilizzare una delle deroghe di cui all'articolo 49 del regolamento generale sulla protezione dei dati al fine di trasferire i dati negli Stati Uniti?

→ È ancora possibile trasferire dati dal SEE agli Stati Uniti sulla base delle deroghe previste dall'articolo 49 del regolamento generale sulla protezione dei dati, purché siano soddisfatte le condizioni di cui a tale articolo. Il Comitato europeo per la protezione dei dati rinvia alle proprie linee-guida in merito[5].

In particolare, è opportuno ricordare che, quando i trasferimenti sono basati sul consenso dell'interessato, esso dovrebbe essere:

- esplicito,
- specifico con riguardo al particolare trasferimento o insieme di trasferimenti (il che significa che l'esportatore deve assicurarsi di ottenere un consenso specifico prima che il trasferimento sia messo in atto anche se ciò avviene dopo la raccolta dei dati), e
- informato, in particolare sui possibili rischi del trasferimento (il che significa che l'interessato dovrebbe essere informato anche dei rischi specifici derivanti dal trasferimento dei dati verso un paese che non fornisce una protezione adeguata, e dell'assenza di misure di salvaguardia adeguate volte a proteggere i dati).

Per quanto riguarda i trasferimenti necessari all'esecuzione di un contratto tra l'interessato e il titolare del trattamento, occorre tenere presente che i dati personali possono essere trasferiti solo su base occasionale. Dovrebbe essere stabilito caso per caso se i trasferimenti di dati in questione abbiano natura "occasionale" ovvero "non occasionale". In ogni caso, tale deroga può essere invocata solo quando il trasferimento è oggettivamente necessario all'esecuzione del contratto.

In relazione ai trasferimenti necessari per importanti motivi di interesse pubblico (che devono essere riconosciuti nella legislazione dell'UE o degli Stati membri[6]), il Comitato europeo per la protezione dei dati ricorda che il requisito essenziale per l'applicabilità di tale deroga è la constatazione della sussistenza di importanti motivi di interesse pubblico, e non già la natura del soggetto coinvolto nel trasferimento, e che, sebbene tale deroga non sia limitata ai trasferimenti di

[5] Cfr. le linee-guida del comitato europeo per la protezione dei dati 2/2018 sulle deroghe di cui all'articolo 49 del regolamento (CE) n. 2016/679, adottate il 25 maggio 2018, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_it.pdf, pag. 3.

[6] I riferimenti agli "Stati membri" vanno intesi come riferimenti agli "Stati membri del SEE".

dati aventi natura "occasionale", ciò non significa che i trasferimenti di dati sulla base della deroga relativa alla sussistenza di importanti motivi di interesse pubblico possano configurarsi su larga scala e in modo sistematico. Occorre semmai rispettare il principio generale per cui le deroghe previste all'articolo 49 del regolamento generale sulla protezione dei dati non dovrebbero trasformarsi di fatto in una regola, essendo necessario limitarne l'applicazione a situazioni specifiche e purché ogni esportatore di dati garantisca che il trasferimento soddisfa un rigoroso test di necessità.

9) Posso continuare a utilizzare le SCC o le BCR per il trasferimento dei dati verso un paese terzo diverso dagli Stati Uniti?

→ La Corte ha indicato che è ancora possibile utilizzare le SCC per trasferire dati in un paese terzo; tuttavia, la soglia fissata dalla Corte per i trasferimenti verso gli Stati Uniti si applica a qualsiasi paese terzo. Lo stesso vale per le norme vincolanti d'impresa (BCR).

La Corte ha sottolineato che spetta all'esportatore e all'importatore di dati valutare se il livello di protezione richiesto dal diritto dell'UE sia rispettato nel paese terzo in questione al fine di determinare se le garanzie fornite dalle SCC o dalle BCR possano essere rispettate nella pratica. In caso contrario, occorre valutare se sia possibile prevedere misure supplementari per garantire un livello di protezione sostanzialmente equivalente a quello previsto nel SEE, e se la legislazione del paese terzo non consenta ingerenze nei riguardi delle suddette misure supplementari tali da comprometterne di fatto l'efficacia.

È possibile rivolgersi all'importatore di dati per verificare la legislazione del rispettivo paese ed effettuarne una valutazione congiunta. Qualora l'esportatore o l'importatore dei dati nel paese terzo constati che i dati trasferiti ai sensi delle SCC o delle BCR non godono di un livello di protezione sostanzialmente equivalente a quello garantito all'interno del SEE, occorre sospendere immediatamente i trasferimenti. In caso contrario, occorre informarne la competente SA[7].

- ➔ Sebbene, come sottolineato dalla Corte, spetti in via primaria agli esportatori e agli importatori di dati valutare direttamente che la legislazione del paese terzo di destinazione consente all'importatore di dati di rispettare le clausole tipo di protezione dei dati o le BCR, prima di trasferire i dati personali a tale paese terzo, anche le autorità di controllo avranno un ruolo fondamentale da svolgere in sede di applicazione del regolamento generale sulla protezione dei dati e al momento di adottare ulteriori decisioni in materia di trasferimenti verso paesi terzi.

Come sollecitato dalla Corte, al fine di evitare decisioni divergenti, le autorità di controllo proseguiranno i lavori in seno al comitato europeo al fine di garantire approcci coerenti, in particolare qualora debbano essere vietati determinati trasferimenti verso paesi terzi.

[7] V., in particolare, il punto 145 della sentenza della Corte. In relazione alle SCC, cfr. la clausola 4, lettera g), della decisione n. 2010/87/UE della Commissione, nonché la clausola 5 (a) della decisione n. 2001/497/CE della Commissione e l'allegato II (c) della decisione n. 2004/915/CE della Commissione. Per le norme vincolanti d'impresa, cfr. sezione 6.3 WP256 rev.01 (approvato dal comitato europeo per la protezione dei dati), e sezione 6.3 WP257 rev.01 (approvato dal comitato europeo per la protezione dei dati).

10) Quali misure supplementari posso introdurre in caso di utilizzo di SCC o BCR per il trasferimento dei dati verso paesi terzi?

→ Le misure supplementari eventualmente da introdurre, ove necessario, dovrebbero essere stabilite caso per caso, tenendo conto di tutte le circostanze del trasferimento e a seguito della valutazione della legislazione del paese terzo, al fine di verificare se essa garantisca un livello di protezione adeguato.

La Corte ha sottolineato che spetta in primo luogo all'esportatore e all'importatore di dati effettuare tale valutazione e fornire le necessarie misure supplementari.

Al momento il Comitato europeo per la protezione dei dati sta analizzando la sentenza della Corte per stabilire quali misure supplementari potrebbero essere fornite in aggiunta alle SCC o alle BCR, siano esse misure giuridiche, tecniche o organizzative, per trasferire dati verso paesi terzi in cui le SCC o le BCR non potranno assicurare isolatamente un livello sufficiente di garanzie.

→ Il Comitato europeo per la protezione dei dati intende approfondire l'analisi relativa alla tipologia delle misure supplementari e fornire ulteriori orientamenti in merito.

11) Mi avvalgo di un responsabile del trattamento che tratta dati per mio conto, essendo io il titolare del trattamento. Come posso sapere se il mio responsabile del trattamento trasferisce i dati verso gli Stati Uniti o un altro paese terzo?

→ Il contratto stipulato con il responsabile in conformità dell'articolo 28, paragrafo 3, del RGPD deve stabilire se i trasferimenti siano o meno autorizzati (occorre tenere presente che costituisce un trasferimento anche l'accesso ai dati effettuato a partire da un paese terzo, ad esempio a fini amministrativi).

→Occorre un'autorizzazione anche per consentire a un responsabile di affidare a sub-responsabili del trattamento il trasferimento di dati verso paesi terzi. È necessaria particolare attenzione perché numerose soluzioni informatiche possono comportare il trasferimento di dati personali verso un paese terzo (ad esempio, a fini di conservazione o manutenzione).

12) Che cosa posso fare per continuare a utilizzare i servizi del mio responsabile del trattamento se il contratto firmato a norma dell'articolo 28, paragrafo 3, RGPD indica che i dati possono essere trasferiti verso gli USA o verso un altro paese terzo?

→ Se è previsto che i dati siano trasferiti verso gli Stati Uniti e non possono essere introdotte misure supplementari per garantire che la normativa statunitense non incida sul livello di protezione sostanzialmente equivalente a quello offerto nel SEE assicurato dagli strumenti di trasferimento, né si applicano le deroghe di cui all'articolo 49 del RGPD, l'unica soluzione è negoziare un emendamento o una clausola aggiuntiva al contratto per vietare il trasferimento di dati verso gli USA. Non solo la conservazione, ma anche la gestione dei dati dovrebbero quindi avvenire in paesi diversi dagli USA.

- → Se è previsto che i dati siano trasferiti verso un altro paese terzo, occorre analizzare anche la legislazione di tale paese terzo per verificarne la conformità ai requisiti della Corte e al livello di protezione dei dati personali atteso. Se non è possibile individuare un'idonea base

giuridica per il trasferimento verso un paese terzo, non dovrebbe aver luogo alcun trasferimento di dati personali al di fuori del SEE e tutte le attività di trattamento dovrebbero aver luogo all'interno del SEE.

Per il comitato europeo per la protezione dei dati

La presidente
Andrea Jelinek

Provvedimento del 26 marzo 2020 - "Didattica a distanza: prime indicazioni" [9300784]

VEDI ANCHE:

- Comunicato del 30 marzo 2020

- Nota istituzionale del Presidente del Garante, Antonello Soro, alla Signora Ministro dell'Istruzione, al Signor Ministro dell'Università e della ricerca e alla Signora Ministro per le pari opportunità e la famiglia in tema di didattica a distanza

[doc. web n. 9300784]

Provvedimento del 26 marzo 2020 - "Didattica a distanza: prime indicazioni"

Registro dei provvedimenti
n. 64 del 26 marzo 2020

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del dott. Antonello Soro, presidente, della dott.ssa Augusta Iannini, vicepresidente, della dott.ssa Giovanna Bianchi Clerici e della prof.ssa Licia Califano, componenti, e del dott. Giuseppe Busia, segretario generale;

Visto il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati), di seguito Regolamento;

Visto il decreto legislativo 30 giugno 2003, n. 196, recante il Codice in materia di protezione dei dati personali, così come modificato dal decreto legislativo 10 agosto 2018, n. 101, di seguito Codice;

CONSIDERATA la necessità di assicurare con urgenza, in ragione dell'improvvisa sospensione dell'attività didattica in presenza, con rilevanti sforzi per superare le notevoli difficoltà derivanti dall'assenza di adeguati mezzi e risorse, il diritto fondamentale all'istruzione, attraverso modalità di apprendimento a distanza;

VISTO il decreto legge 23 febbraio 2020, n. 6, recante misure urgenti in materia di contenimento e gestione dell'emergenza epidemiologica da COVID-19;

VISTI i decreti del Presidente del Consiglio dei Ministri adottati in attuazione del decreto legge n. 6 del 2020 e, in particolare, il decreto dell'8 marzo 2020 che, nel disporre la sospensione dei servizi educativi per l'infanzia e delle attività didattiche nelle scuole di ogni ordine e grado, nonché la frequenza delle attività scolastiche e di formazione superiore, comprese le Università e le Istituzioni di Alta formazione artistica musicale e coreutica, di corsi professionali (art. 1, comma 1, lett. h)), prevede che siano attivate, per tutta la durata della sospensione, modalità di didattica a distanza (art. 2, comma 1, lett. m) e n));

VISTI altresì gli articoli 101, 120 e 121 del decreto legge del 17 marzo 2020 n. 18 "Misure di potenziamento del Servizio sanitario nazionale e di sostegno economico per famiglie, lavoratori e imprese connesse all'emergenza epidemiologica da COVID-19" che contengono misure urgenti per garantire la continuità formativa e la didattica;

VISTA le note del Ministero dell'Istruzione del 6 marzo 2020, prot. n. 278, e dell'8 marzo 2020, prot. n. 279, con le quali sono state

fornite istruzioni operative alle istituzioni scolastiche sull'attivazione e sul potenziamento di modalità di apprendimento a distanza, ottimizzando le risorse didattiche del registro elettronico e utilizzando classi virtuali, ovvero altri strumenti e canali digitali, per favorire la produzione e la condivisione di contenuti;

VISTA, inoltre, al riguardo, la nota del Ministero dell'Istruzione del 17 marzo 2020, prot. n. 388, nella quale sono state fornite, tra l'altro, alcune indicazioni sulla protezione dei dati personali trattati nell'ambito della didattica a distanza;

VISTA la Dichiarazione sul trattamento dei dati personali nel contesto dell'epidemia di COVID-19, adottata dal Comitato europeo per la protezione dei dati (EDPB) in data 19 marzo 2020 (doc. web n. 9295504, pubblicato in https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9295504);

VISTE le segnalazioni e i quesiti pervenuti al Garante da parte di responsabili della protezione dei dati di istituti scolastici, associazioni, docenti e famiglie in ordine alle modalità di trattamento dei dati personali effettuato nel predetto contesto emergenziale e agli adempimenti necessari a rispettare il Regolamento e il Codice;

RITENUTA l'opportunità di fornire, nell'attuale contesto emergenziale, al sistema scolastico, alle università, alle istituzioni di alta formazione artistica musicale e coreutica, ai docenti, alle famiglie e agli studenti, talune prime utili indicazioni, ai sensi dell'art. 57, par. 1, lett. b) e d), del Regolamento (v. anche cons. nn. 122 e 132), che attribuisce al Garante il compito di promuovere la consapevolezza e di favorire la comprensione del pubblico riguardo ai rischi, alle norme, alle garanzie e ai diritti in relazione ai trattamenti, con particolare attenzione alle attività destinate specificamente ai minori, nonché agli obblighi imposti ai titolari e i responsabili del trattamento;

RITENUTO che, alla luce delle predette indicazioni, superata la prima fase emergenziale in cui sono state avviate d'urgenza iniziative di didattica a distanza, le scuole e le università potranno gradualmente valutare di adottare ulteriori misure per rafforzare la piena conformità al Regolamento e al Codice;

CONSIDERATO che l'Autorità valuterà, in ogni caso, l'opportunità di avviare verifiche sui fornitori delle principali piattaforme per la didattica a distanza per assicurare il rispetto del Regolamento e del Codice in relazione ai trattamenti effettuati per conto delle scuole e delle università;

RITENUTO di adottare il documento denominato "Didattica a distanza: prime indicazioni" (all. n. 1), che forma parte integrante del presente provvedimento, recante talune prime indicazioni al fine di promuovere la consapevolezza delle scelte da effettuare e favorire la più ampia comprensione riguardo alle norme, alle garanzie e ai diritti che, anche nel contesto dell'emergenza, devono essere rispettati in relazione al trattamento dei dati personali degli interessati;

VISTA la documentazione in atti;

VISTE le osservazioni formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

RELATORE il dott. Antonello Soro;

TUTTO CIÒ PREMESSO IL GARANTE

adotta, ai sensi dell'art. 57, par. 1, lett. b) e d), del Regolamento, il documento denominato "Didattica a distanza: prime indicazioni" (all. n. 1), che forma parte integrante del presente provvedimento, recante talune prime indicazioni al fine di promuovere la consapevolezza delle scelte da effettuare e favorire la più ampia comprensione riguardo alle norme, alle garanzie e ai diritti che, anche nel contesto dell'emergenza, devono essere rispettati in relazione al trattamento dei dati personali degli interessati.

Roma, 26 marzo 2020

IL PRESIDENTE
Soro

IL RELATORE

Soro

IL SEGRETARIO GENERALE
Busia

_____

All: n. 1

Didattica a distanza: prime indicazioni

1. Base giuridica del trattamento dei dati personali

Le scuole e le università sono autorizzate a trattare i dati, anche relativi a categorie particolari, di insegnanti, alunni (anche minorenni), genitori e studenti, funzionali all'attività didattica e formativa in ambito scolastico, professionale, superiore o universitario (art. 6, parr. 1, lett. e), 3, lett. b) e 9, par. 2, lett. g) del Regolamento e artt. 2-ter e 2-sexies del Codice).

In tal senso dispone la normativa di settore, comprensiva anche delle disposizioni contenute nei decreti, emanati ai sensi dell'art. 3 del d.l. 23 febbraio 2020, n. 6, che hanno previsto- per tutta la durata della sospensione delle attività didattiche "in presenza" nelle scuole, nelle università e nelle istituzioni di alta formazione- l'attivazione di modalità di didattica a distanza, avuto anche riguardo alle specifiche esigenze degli studenti con disabilità (cfr. spec. art. 2, lett. m) e n), del d.P.C.M. dell'8 marzo 2020).

Non deve pertanto essere richiesto agli interessati (docenti, alunni, studenti, genitori) uno specifico consenso al trattamento dei propri dati personali funzionali allo svolgimento dell'attività didattica a distanza, in quanto riconducibile – nonostante tali modalità innovative – alle funzioni istituzionalmente assegnate a scuole ed atenei.

2. Privacy by design e by default: scelta e configurazione degli strumenti da utilizzare

Spetta in primo luogo alle scuole e alle università- quali titolari del trattamento - la scelta e la regolamentazione, anche sulle base delle indicazioni fornite dalle autorità competenti, degli strumenti più utili per la realizzazione della didattica a distanza (cfr. anche, ove applicabile, art. 39 del Regolamento (UE) 2016/679, infra: "Regolamento").

Tali scelte dovranno conformarsi ai principi di privacy by design e by default, tenendo conto, in particolare, del contesto e delle finalità del trattamento, nonché dei rischi per i diritti e le libertà degli interessati (artt. 24 e 25 del Regolamento).

Varie piattaforme o servizi on line permettono di effettuare attività di didattica a distanza, consentendo la configurazione di "classi virtuali", la pubblicazione di materiali didattici, la trasmissione e lo svolgimento on line di video-lezioni, l'assegnazione di compiti, la valutazione dell'apprendimento e il dialogo in modo "social" tra docenti, studenti e famiglie. Alcune piattaforme offrono anche molteplici ulteriori servizi, non sempre specificamente rivolti alla didattica.

Tra i criteri che devono orientare la scelta degli strumenti da utilizzare è, dunque, opportuno includere, oltre all'adeguatezza rispetto alle competenze e capacità cognitive di alunni e studenti, anche le garanzie offerte sul piano della protezione dei dati personali (artt. 5 e ss. del Regolamento).

La valutazione di impatto, che l'art. 35 del Regolamento richiede per i casi di rischi elevati, non è necessaria se il trattamento effettuato dalle istituzioni scolastiche e universitarie, ancorché relativo a soggetti in condizioni peculiari quali minorenni e lavoratori, non presenta ulteriori caratteristiche suscettibili di aggravarne i rischi per i diritti e le libertà degli interessati. Ad esempio, non è richiesta la valutazione di impatto per il trattamento effettuato da una singola scuola (non, quindi, su larga scala) nell'ambito dell'utilizzo di un servizio on line di videoconferenza o di una piattaforma che non consente il monitoraggio sistematico degli utenti o comunque non ricorre a nuove soluzioni tecnologiche particolarmente invasive (quali, tra le altre, quelle che comportano nuove forme di utilizzo dei dati di geolocalizzazione o biometrici).

3. Il ruolo dei fornitori dei servizi on line e delle piattaforme

Qualora la piattaforma prescelta comporti il trattamento di dati personali di studenti, alunni o dei rispettivi genitori per conto della

scuola o dell'università, il rapporto con il fornitore (quale responsabile del trattamento) dovrà essere regolato con contratto o altro atto giuridico (art. 28 del Regolamento). E' il caso, ad esempio, del registro elettronico, il cui fornitore tratta i dati per conto della scuola e, pertanto, assume il ruolo di responsabile del trattamento. Le eventuali, ulteriori attività di didattica a distanza, talora fornite da alcuni registri elettronici, possono essere in alcuni casi già disciplinate nello stesso contratto di fornitura stipulato.

Diversamente, qualora il registro elettronico non consentisse videolezioni o altre forme di interazione tra i docenti e gli studenti, potrebbe essere sufficiente – per non dover designare ulteriori responsabili del trattamento- utilizzare servizi on line accessibili al pubblico e forniti direttamente agli utenti, con funzionalità di videoconferenza ad accesso riservato. Alcuni di questi servizi sono, peraltro, facilmente utilizzabili anche senza la necessaria creazione di un account da parte degli utenti.

Laddove, invece, si ritenga necessario ricorrere a piattaforme più complesse e "generaliste", che non eroghino servizi rivolti esclusivamente alla didattica, si dovranno attivare, di default, i soli servizi strettamente necessari alla formazione, configurandoli in modo da minimizzare i dati personali da trattare, sia in fase di attivazione dei servizi, sia durante l'utilizzo degli stessi da parte di docenti e studenti (evitando, ad esempio, il ricorso a dati sulla geolocalizzazione, ovvero a sistemi di social login che, coinvolgendo soggetti terzi, comportano maggiori rischi e responsabilità).

Le istituzioni scolastiche e universitarie dovranno assicurarsi (anche in base a specifiche previsioni del contratto stipulato con il fornitore dei servizi designato responsabile del trattamento), che i dati trattati per loro conto siano utilizzati solo per la didattica a distanza. Saranno, in tal senso, utili specifiche istruzioni, tra l'altro, sulla conservazione dei dati, sulla cancellazione - al temine del progetto didattico - di quelli non più necessari, nonché sulle procedure di gestione di eventuali violazioni di dati personali.

L'Autorità vigilerà sull'operato dei fornitori delle principali piattaforme per la didattica a distanza, per assicurare che i dati di docenti, studenti e loro familiari siano trattati nel pieno rispetto della disciplina di protezione dati e delle indicazioni fornite dalle istituzioni scolastiche e universitarie.

Al fine di garantire la massima consapevolezza nell'utilizzo di strumenti tecnologici - delle cui implicazioni non tutti gli studenti (soprattutto se minorenni) hanno piena cognizione- sarebbero auspicabili, in ogni caso, iniziative di sensibilizzazione in tal senso, rivolte a famiglie e ragazzi.

4. Limitazione delle finalità del trattamento

Ancora, con riferimento al trattamento dei dati degli studenti svolti dalle piattaforme quali responsabili del trattamento stesso, si ricorda che esso deve limitarsi a quanto strettamente necessario per la fornitura dei servizi richiesti ai fini della didattica on line, senza l'effettuazione di operazioni ulteriori, preordinate al perseguimento di finalità proprie del fornitore. L'ammissibilità di tali operazioni dovrà, infatti, essere valutata di volta in volta, rispetto ai requisiti richiesti dal Regolamento quali, in particolare, i presupposti di liceità e i principi applicabili al trattamento dei dati personali (artt. 5 e ss.). Il trattamento ulteriore dei dati degli utenti, da parte dei gestori delle piattaforme, nella diversa veste di titolari del trattamento, dovrà naturalmente osservare, tra gli altri, gli obblighi di informazione e trasparenza secondo quanto previsto dall'art. 13 del Regolamento.

E' peraltro inammissibile il condizionamento, da parte dei gestori delle piattaforme, della fruizione dei servizi di didattica a distanza alla sottoscrizione di un contratto o alla prestazione– da parte dello studente o dei genitori – del consenso al trattamento dei dati connesso alla fornitura di ulteriori servizi on line, non necessari all'attività didattica. Il consenso non sarebbe, infatti, validamente prestato perché, appunto, indebitamente condizionato al perseguimento di finalità ultronee rispetto a quelle proprie della didattica a distanza (art. 7; cons. 43 del Regolamento).

I dati personali dei minori, del resto, "meritano una specifica protezione relativamente ai loro dati personali, in quanto possono essere meno consapevoli dei rischi, delle conseguenze e delle misure di salvaguardia interessate nonché dei loro diritti in relazione al trattamento dei dati personali" (cons. 38 del Regolamento). Tale specifica protezione dovrebbe, in particolare, riguardare l'utilizzo di tali dati a fini di marketing o di profilazione e, in senso lato, la relativa raccolta nell'ambito della fornitura di servizi ai minori stessi (cons. 38 cit.).

5. Liceità, correttezza e trasparenza del trattamento

Al fine di garantire la trasparenza e la correttezza del trattamento, le istituzioni scolastiche e universitarie devono assicurare la trasparenza del trattamento informando gli interessati (alunni, studenti, genitori e docenti), con un linguaggio comprensibile anche

ai minori, in ordine, in particolare, alle caratteristiche essenziali del trattamento, che deve peraltro limitarsi all'esecuzione dell'attività didattica a distanza, nel rispetto della riservatezza e della dignità degli interessati (d.P.R. 24 giugno 1998, n. 249, spec. art. 1; art. 13 del Regolamento).

Nel trattare i dati personali dei docenti funzionali allo svolgimento della didattica a distanza, le scuole e le università dovranno rispettare presupposti e condizioni per il legittimo impiego di strumenti tecnologici nel contesto lavorativo (artt. 5 e 88, par. 2, del Regolamento, art. 114 del Codice in materia di protezione dei dati personali e art. 4 della legge 20 maggio 1970, n. 300) limitandosi a utilizzare quelli strettamente necessari, comunque senza effettuare indagini sulla sfera privata (art. 113 del citato Codice) o interferire con la libertà di insegnamento.

Ministero dell'Istruzione

Didattica Digitale Integrata e tutela della privacy: indicazioni generali

I principali aspetti della disciplina in materia di protezione dei dati personali nella Didattica Digitale Integrata

Premessa

Tenuto conto del carattere fortemente innovativo che caratterizza la didattica digitale integrata (DDI) e della necessità di guidare le scuole nell'implementazione di questo nuovo strumento, il Ministero dell'istruzione ritiene di accompagnare le Linee guida sulla DDI, adottate con D.M. n. 89 del 7 agosto 2020, con specifiche indicazioni, di carattere generale, sui profili di sicurezza e protezione dei dati personali sulla base di quanto previsto dal Regolamento (UE) 2016/679 (Regolamento).
A tale scopo, è stato predisposto il presente documento da parte del Gruppo di lavoro congiunto Ministero dell'istruzione-Ufficio del Garante per la protezione dei dati personali, di cui al Decreto del Capo di Gabinetto prot. n. 1885 del 5 giugno 2020, con il fine di fornire alle istituzioni scolastiche linee di indirizzo comuni e principi generali per l'implementazione della DDI con particolare riguardo agli aspetti inerenti alla sicurezza in rete e alla tutela dei dati personali.

Si premette che spetta alla singola istituzione scolastica, in qualità di titolare del trattamento, la scelta e la regolamentazione degli strumenti più adeguati al trattamento dei dati personali di personale scolastico, studenti e loro familiari per la realizzazione della DDI. Tale scelta è effettuata del Dirigente scolastico, con il supporto del Responsabile della protezione dei dati personali (RPD), sentito il Collegio dei Docenti.

I criteri che orientano l'individuazione degli strumenti da utilizzare tengono conto sia dell'adeguatezza rispetto a competenze e capacità cognitive degli studenti sia delle garanzie offerte sul piano della protezione dei dati personali. In generale, nella scelta degli strumenti tecnologici e dei relativi servizi è necessario tenere conto delle specifiche caratteristiche, anche tecniche, degli stessi, prediligendo quelli che, sia nella fase di progettazione che di sviluppo successivo, abbiano proprietà tali da consentire ai titolari e ai responsabili del trattamento di adempiere agli obblighi di protezione dei dati fin dalla progettazione e di protezione per impostazione predefinita (*privacy by design e by default*, cfr. "Considerando" (78) e art. 25 del Regolamento). Tale scelta, in merito alle tecnologie più appropriate per la DDI, va effettuata anche sulla base delle indicazioni fornite dal RPD, il quale dovrà essere tempestivamente coinvolto affinché fornisca il necessario supporto tecnico-giuridico.

Per questo motivo il Dirigente scolastico incaricherà il RPD, ai sensi di quanto previsto dall'art. 39, par. 1, lett. *a*) del Regolamento, di fornire consulenza rispetto alle principali decisioni da assumere, ad esempio, in merito alla definizione del rapporto con il fornitore della piattaforma prescelta e alle istruzioni da impartire allo stesso, all'adeguatezza delle misure di sicurezza rispetto ai rischi connessi a tale tipologia di trattamenti e alle misure necessarie affinché i dati siano utilizzati solo in relazione alla finalità della DDI e alle modalità per assicurare la trasparenza del trattamento mediante l'informativa a tutte le categorie di interessati. Ciò, in particolare, suggerendo il ricorso a piattaforme che eroghino servizi rivolti esclusivamente alla didattica, ovvero, nei casi in cui siano preferite quelle più complesse e generaliste, raccomandando di attivare i soli servizi strettamente necessari alla DDI, verificando che dati di personale scolastico, studenti e loro familiari non vengano trattati per finalità diverse e ulteriori che siano riconducibili al fornitore.

Risulta fondamentale che l'istituzione scolastica, coinvolga nell'attività di verifica sul monitoraggio del corretto trattamento dei dati personali nella DDI tutti gli attori (personale scolastico, famiglie, studenti) di questo processo, anche attraverso specifiche iniziative di sensibilizzazione atte a garantire la massima consapevolezza nell'utilizzo di strumenti tecnologici e nella tutela dei dati personali al fine di evitare l'utilizzo improprio e la diffusione illecita dei dati personali trattati per

mezzo delle piattaforme e il verificarsi di accessi non autorizzati e di azioni di disturbo durante lo svolgimento della didattica.

In ogni caso l'istituzione scolastica dovrà fornire al personale autorizzato al trattamento dei dati attraverso la piattaforma (personale docente e non docente) adeguate istruzioni (art. 4, par. 10, 29, 32, par. 4 del Regolamento; art. 2 *quaterdecies* del Decreto legislativo 30giugno 2003, n.196, recante il "Codice in materia di protezione dei dati personali", in seguito Codice).

Figure previste dal Regolamento e principali attori coinvolti nella DDI

- Il Titolare del Trattamento è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali (art. 4. par. 1, n. 7 del Regolamento). Nell'ambito dell'istituzione scolastica questa figura è identificata nella persona del Dirigente scolastico.
- Il Responsabile della Protezione dei Dati personali (RPD), figura prevista dall'art.37 del Regolamento, assicura l'applicazione della normativa in materia di protezione dei dati personali in relazione ai trattamenti svolti dal titolare del trattamento. Nell'ambito dell'istituzione scolastica il RPD, individuato internamente o all'esterno sulla base di un contratto, è appositamente designato dal Dirigente scolastico. Nello specifico tale figura, per l'implementazione della DDI, collabora con il Dirigente scolastico nelle seguenti attività, assicurando:
  - ✓ consulenza in ordine alla necessità di eseguire la valutazione di impatto;
  - ✓ supporto nella scelta delle tecnologie più appropriate per la DDI;
  - ✓ consulenza nell'adozione delle misure di sicurezza più adeguate;
  - ✓ supporto nella predisposizione del contratto o altro atto giuridico con il fornitore dei servizi per la DDI;
  - ✓ supporto nella designazione del personale autorizzato al trattamento dei dati personali;
  - ✓ supporto nelle campagne di sensibilizzazione rivolte al personale autorizzato e agli interessati sugli aspetti inerenti alla tutela dei dati personali e sull'uso consapevole delle tecnologie utilizzate per la DDI.
- Le persone autorizzate al trattamento (art. 4, n. 10, del Regolamento) effettuano operazioni sui dati personali sotto l'autorità del titolare del trattamento e sulla base di istruzioni fornite dallo stesso. Nell'ambito dell'istituzione scolastica questa figura è rappresentata dal personale scolastico in relazione al quale le istruzioni dovranno essere integrate, ove già non previsto, con indicazioni relative all'utilizzo delle piattaforme di erogazione della DDI.
- Il Responsabile del trattamento è la persona fisica, giuridica, pubblica amministrazione o ente che tratta i dati personali per conto del titolare del trattamento(art. 4, par. 1, n. 8 del Regolamento). Pertanto, il responsabile del trattamento è un soggetto terzo che tratta dati personali per conto del titolare, mettendo in atto misure di sicurezza adeguate di tipo tecnico ed organizzativo. Nell'ambito dell'istituzione scolastica questa figura è identificata nei fornitori delle piattaforme o dei servizi per la DDI.

Base giuridica del trattamento

Come chiarito dal Garante nel Provvedimento del 26 marzo 2020, n. 64 (doc web n. 9300784 "Didattica a distanza: prime indicazioni"), in relazione alla attività di DDI, il trattamento dei dati personali da parte delle istituzioni scolastiche è necessario in quanto collegato all'esecuzione di un compito di interesse pubblico di cui è investita la scuola attraverso una modalità operativa prevista

dalla normativa, con particolare riguardo anche alla gestione attuale della fase di emergenza epidemiologica.

Il consenso dei genitori, che non costituisce una base giuridica idonea per il trattamento dei dati in ambito pubblico e nel contesto del rapporto di lavoro, non è richiesto perché l'attività svolta, sia pure in ambiente virtuale, rientra tra le attività istituzionalmente assegnate all'istituzione scolastica, ovvero di didattica nell'ambito degli ordinamenti scolastici vigenti. Pertanto, le istituzioni scolastiche sono legittimate a trattare tutti i dati personali necessari al perseguimento delle finalità collegate allo svolgimento della DDI nel rispetto dei principi previsti dalla normativa di settore.

Principio di trasparenza e correttezza nei confronti degli interessati

In base alle disposizioni contenute negli artt. 13 e 14 del Regolamento UE 2016/679, le Istituzioni scolastiche devono informare gli interessati in merito ai trattamenti dei dati personali effettuati nell'ambito dell'erogazione dell'offerta formativa. Poiché attraverso l'utilizzo della piattaforma per l'erogazione della DDI sono trattati sia dati degli studenti che dei docenti e, in taluni casi, anche dei genitori, è opportuno che le scuole forniscano a tutte queste categorie di interessati, di regola all'inizio dell'anno scolastico, anche nell'ambito di una specifica sezione dell'informativa generale o in un documento autonomo, tutte le informazioni relative a tali trattamenti.

Tale informativa dovrà essere redatta in forma sintetica e con un linguaggio facilmente comprensibile anche dai minori e dovrà specificare, in particolare, i tipi di dati e le modalità di trattamento degli stessi, i tempi di conservazione e le altre operazioni di trattamento, specificando che i dati raccolti saranno trattati esclusivamente per l'erogazione di tale modalità di didattica, sulla base dei medesimi presupposti e con garanzie analoghe a quelli della didattica tradizionale.

In tale sezione devono essere puntualmente indicati i soggetti dai quali saranno trattati i dati nell'ambito della DDI, specificando le diverse modalità di fruizione (App, Piattaforma web, ...), informando sull'eventuale utilizzo di tecnologie in *cloud* e precisando se queste comportano un trasferimento di dati al di fuori dell'Unione Europea.

Inoltre, le istituzioni scolastiche che facciano ricorso a nuove piattaforme per l'erogazione della DDI, laddove non abbiano già provveduto, dovranno provvedere ad aggiornare l'informativa rilasciata agli interessati al momento dell'iscrizione o, nel caso del personale scolastico, al momento della stipula del contratto di lavoro, indicando gli eventuali nuovi fornitori del servizio che, in qualità di responsabili del trattamento, trattano i dati per conto dell'istituzione stessa.

Principio di limitazione della conservazione dei dati

In relazione alla conservazione dei dati personali, prevista dall'art.5, lettera *e*) del regolamento, il titolare del trattamento è chiamato ad assicurare che i dati non siano conservati più a lungo del necessario, ad esempio, disponendo che i dati siano cancellati al termine del progetto didattico. Pertanto, il Dirigente scolastico, coadiuvato dal RPD, dovrà assicurarsi che il sistema scelto per l'erogazione della DDI preveda il rispetto del termine per la conservazione e la successiva cancellazione dei dati, tenendo altresì conto, nella definizione del limite temporale della conservazione dei dati nell'ambito della DDI, della molteplicità e della quantità di soggetti coinvolti e del numero delle attività di trattamento connesse.

Ruolo dei fornitori

In qualità di titolare del trattamento dei dati personali, l'istituzione scolastica, che riterrà opportuno ricorrere a un soggetto esterno per la gestione dei servizi per la DDI che comportino il trattamento di dati di personale scolastico, studenti e/o dei loro familiari per conto della scuola stessa, è tenuta a nominare tale soggetto come responsabile del trattamento con contratto o altro atto giuridico (art. 28 del Regolamento), indicando conseguentemente tale circostanza nel registro dei trattamenti (art. 30 del Regolamento).

Attraverso tale atto, l'istituzione scolastica circoscriverà l'ambito, la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento, ricorrendo a fornitori che presentino garanzie sufficienti a mettere in atto misure tecniche e organizzative adeguate agli specifici trattamenti posti in essere per conto dell'istituzione stessa. In particolare, le istituzioni scolastiche dovranno assicurarsi che i dati trattati per loro conto siano utilizzati solo per la DDI, senza l'introduzione di ulteriori finalità estranee all'attività scolastica. Sarà, pertanto, necessario prevedere, nell'atto che disciplina il rapporto con il responsabile del trattamento, specifiche istruzioni sulla conservazione dei dati, sulla cancellazione o sulla restituzione dei dati al temine dell'accordo tra scuola e fornitore, nonché sulle procedure di gestione di eventuali violazioni di dati personali, secondo quanto disposto dal Regolamento.

Qualora le istituzioni scolastiche dovessero avvalersi di piattaforme o strumenti per la DDI offerti da operatori che già forniscono alla scuola altri servizi (es. registro elettronico, altri applicativi di gestione, ecc.), le stesse possono procedere - a seconda dei casi - disciplinando le ulteriori attività di DDI con una integrazione del contratto di fornitura già esistente.

Anche nel caso di utilizzo per la DDI di una piattaforma disponibile a titolo gratuito dovrà essere disciplinato in ogni caso il rapporto con il fornitore con riguardo al trattamento di dati personali attraverso un contratto o altro atto giuridico ai sensi dell'art. 28 del Regolamento.

Diversamente, nei casi in cui le istituzioni scolastiche facciano ricorso a strumenti e piattaforme per la DDI gestite in via autonoma, senza il ricorso a soggetti esterni, non è richiesto alcun atto di nomina a responsabile del trattamento.

Laddove l'istituzione scolastica ritenga opportuno ricorrere a piattaforme più complesse che includono una più vasta gamma di servizi, anche non rivolti esclusivamente alla didattica, sarà necessario verificare, con il supporto del RPD, come già evidenziato, che siano attivati solo i servizi strettamente correlati con la DDI configurando i servizi in modo da minimizzare i dati personali da trattare sia in fase di attivazione dei servizi sia durante l'utilizzo degli stessi da parte di docenti e studenti (evitando, ad esempio, il ricorso a dati sulla geolocalizzazione, ovvero a sistemi di *social login* che, coinvolgendo soggetti terzi, comportano maggiori rischi e responsabilità).

Si fa presente che il tipo di misure e condizioni va calibrato sulle categorie di dati trattati e sulle modalità di trattamento da parte del responsabile del trattamento.

In particolare, nel suddetto atto dovrà essere specificato che, nel caso in cui il fornitore dei servizi per la DDI si avvalga di altro fornitore per il trattamento dei dati, dovrà essere esplicitamente autorizzato per iscritto dall'istituzione scolastica a designarlo sub-responsabile, in maniera specifica o generale, rendendo disponibile al titolare del trattamento l'elenco di tali soggetti (art. 28, par. 2 del Regolamento). Il sub-responsabile dovrà attenersi agli stessi obblighi in materia di protezione dei dati contenuti nel contratto o in altro atto giuridico tra l'istituzione scolastica e il primo

responsabile. Il fornitore che si avvalga di sub-responsabili risponde direttamente nei confronti dell'istituzione scolastica in relazione ad eventuali inadempimenti o violazioni della propria catena di subfornitura.

Misure tecniche e organizzative legate alla sicurezza

L'istituzione scolastica, sulla base di quanto previsto dal Regolamento, anche avvalendosi della consulenza offerta dal proprio RPD, deve adottare, anche per mezzo dei fornitori designati responsabili del trattamento, misure tecniche e organizzative adeguate sulla base del rischio. Pertanto, il Dirigente scolastico dovrà assicurarsi che i dati vengano protetti da trattamenti non autorizzati o illeciti, dalla perdita, dalla distruzione o da danni accidentali.

A tal fine si esemplificano alcune misure:

- adozione di adeguate procedure di identificazione e di autenticazione informatica degli utenti;
- utilizzo di robusti processi di assegnazione agli utenti di credenziali o dispositivi di autenticazione;
- definizione di differenti profili di autorizzazione da attribuire ai soggetti autorizzati in modo da garantire un accesso selettivo ai dati;
- definizione di password policy adeguate (es. regole di composizione, scadenza periodica, ecc.);
- conservazione delle password degli utenti, mediante l'utilizzo di funzioni di *hashing* allo stato dell'arte (es. PBKDF2, bcrypt, ecc.) e di *salt* di lunghezza adeguata;
- utilizzo di canali di trasmissione sicuri tenendo conto dello stato dell'arte;
- adozione di misure atte a garantire la disponibilità dei dati (es. *backup* e *disaster recovery*);
- utilizzo di sistemi di protezione perimetrale, adeguatamente configurati in funzione del contesto operativo;
- utilizzo di sistemi antivirus e anti *malware* costantemente aggiornati;
- aggiornamento periodico dei software di base al fine di prevenirne la vulnerabilità;
- registrazione degli accessi e delle operazioni compiute in appositi file di log, ai fini della verifica della correttezza e legittimità del trattamento dei dati;
- definizione di istruzioni da fornire ai soggetti autorizzati al trattamento;
- formazione e sensibilizzazione degli utenti.

In caso di utilizzo di tecnologie *in cloud* risulta necessaria la verifica del rispetto della normativa in materia di protezione dati personali da parte del fornitore del servizio designato come responsabile del trattamento. Inoltre, nel caso sia previsto che le informazioni vengono trasferite fuori dall'Unione Europea (UE), occorre verificare che sussistano tutti i presupposti giuridici richiesti dalla disciplina per assicurare un adeguato livello di protezione.

Infine, particolare attenzione va rivolta alla configurazione dei siti e delle App messe a disposizione dell'istituzione scolastica per la fruizione dei materiali e per l'erogazione delle attività didattiche a distanza, nel rispetto del principio di *privacy by design e by default* previsto dal Regolamento. In particolare, nell'uso di tali strumenti, è necessario evitare l'inserimento di *tracker* e *analytics*,

notifiche *push* (per le App), *font* resi disponibili da terze parti, *advertising* o *in-appurchasing*, o altri elementi che possono peraltro comportare il trasferimento di dati fuori dall'Unione Europea e/o il monitoraggio delle attività degli utenti.

Con riferimento a questi aspetti il Dirigente scolastico, sentito il RPD, dovrà richiedere al fornitore dei servizi per DDI che vengano assicurate, inserendo specifici obblighi anche nel contratto o altro atto giuridico di cui all'art. 28 del Regolamento, le necessarie garanzie legate all'utilizzo di tecnologie *in cloud*, alla progettazione e alla configurazione dei siti, delle App e delle piattaforme utilizzate per la didattica.

Per quanto riguarda le misure organizzative interne alla scuola, occorrerà verificare che il sistema utilizzato per la DDI preveda che i diversi utenti autorizzati (personale docente e non docente), possano accedere solo alle informazioni e funzioni di competenza per tipologia di utenza sulla base delle specifiche mansioni assegnate (art. 4, par. 10, 29, 32, par. 4 del Regolamento; art. 2 *quaterdecies* del Codice). I soggetti autorizzati al trattamento dei dati personali sono tenuti a conformare i trattamenti a loro assegnati alla normativa in materia di protezione dei dati personali e alle istruzioni ricevute. Le istruzioni operative impartite a tali soggetti da parte delle istituzioni scolastiche dovranno riguardare principalmente l'utilizzo e la custodia delle credenziali di accesso, il divieto di condivisione delle stesse, il divieto di far accedere alla piattaforma persone non autorizzate, la protezione da *malware* e attacchi informatici, nonché i comportamenti da adottare durante la DDI e le conseguenze in caso di violazione di tali istruzioni.

Occorre inoltre sensibilizzare, più in generale, anche gli altri soggetti intestatari di utenze, come gli studenti e i genitori, sul corretto utilizzo del proprio *account*, fornendo specifiche istruzioni da declinare con un linguaggio chiaro e comprensibile in ragione delle fasce di età degli utenti.

L'utilizzo degli strumenti e la tutela dei dati

Le istituzioni scolastiche, con il supporto del RPD, dovranno verificare che, in applicazione dei principi generali del trattamento dei dati e nel rispetto delle disposizioni nazionali che trovano applicazione ai rapporti di lavoro (art. 5 e 88 del Regolamento), le piattaforme e gli strumenti tecnologici per l'erogazione della DDI consentano il trattamento dei soli dati personali necessari alla finalità didattica, configurando i sistemi in modo da prevenire che informazioni relative alla vita privata vengano, anche accidentalmente, raccolte e da rispettare la libertà di insegnamento dei docenti.

In ragione del fatto che le piattaforme e gli strumenti tecnologici impiegati per la didattica possono comportare il trattamento di informazioni associate in via diretta o indiretta ai dipendenti, con possibilità di controllarne a distanza l'attività, dovrà essere verificata, sempre con il supporto del RPD, la sussistenza dei presupposti di liceità stabiliti dell'art. 4 della l. 20 maggio 1970, n. 300 cui fa rinvio l'art.114 del Codice, valutando, in via preliminare, se, tenuto conto delle concrete caratteristiche del trattamento, trovi applicazione il comma 1 o il comma 2 dello stesso articolo. Nel rispetto del principio di responsabilizzazione, l'istituzione scolastica dovrà adottare le misure tecniche e organizzative affinché il trattamento sia conforme alla richiamata normativa di settore, fornendo a tal fine le necessarie indicazioni al fornitore del servizio (cfr. artt. 24 e 25 del Regolamento).

A riguardo il Garante, nel Provvedimento del 26 marzo u.s. - "Didattica a distanza: prime indicazioni", - ha, infatti, precisato che *"nel trattare i dati personali dei docenti funzionali allo*

svolgimento della didattica a distanza, le scuole e le università dovranno rispettare presupposti e condizioni per il legittimo impiego di strumenti tecnologici nel contesto lavorativo (artt. 5 e 88, par. 2, del Regolamento, art. 114 del Codice in materia di protezione dei dati personali e art. 4 della legge 20 maggio 1970, n. 300) limitandosi a utilizzare quelli strettamente necessari, comunque senza effettuare indagini sulla sfera privata (art. 113 del citato Codice) o interferire con la libertà di insegnamento."

Atteso che lo svolgimento delle videolezioni in modalità telematica rientra nell'ambito dell'attività di DDI ed è, pertanto, riconducibile alle funzioni di formazione istituzionalmente svolte dagli istituti scolastici, occorre precisare che l'utilizzo della *webcam* deve in ogni caso avvenire nel rispetto dei diritti delle persone coinvolte e della tutela dei dati personali.

Nel contesto della didattica digitale, l'utilizzo della *webcam* durante le sessioni educative costituisce la modalità più immediata attraverso la quale il docente può verificare se l'alunno segue la lezione, ma spetta in ogni caso alle istituzioni scolastiche stabilire le modalità di trattamento dei dati personali e in che modo regolamentare l'utilizzo della *webcam* da parte degli studenti che dovrà avvenire esclusivamente, come sopra precisato, nel rispetto dei diritti delle persone coinvolte.

A tal fine è opportuno ricordare a tutti i partecipanti, attraverso uno specifico *"disclaimer*", i rischi che la diffusione delle immagini e, più in generale, delle lezioni può comportare, nonché le responsabilità di natura civile e penale. In generale, anche attraverso specifiche campagne di sensibilizzazione rivolte ai docenti, studenti e famiglie, va evidenziato che il materiale caricato o condiviso sulla piattaforma utilizzata per la DDI o in *repository*, in locale o *in cloud*, sia esclusivamente inerente all'attività didattica e che venga rispettata la tutela della protezione dei dati personali e i diritti delle persone con particolare riguardo alla presenza di particolari categorie di dati.

La valutazione di impatto (DPIA)

La valutazione di impatto deve essere effettuata solo se e quando ricorrono i presupposti dell'articolo 35 del Regolamento. Occorre precisare innanzitutto che, poiché l'istituzione scolastica, in genere, non effettua trattamenti di dati personali su larga scala, non è richiesta la valutazione di impatto per il trattamento effettuato da una singola scuola nell'ambito dell'utilizzo di un servizio *on line* di videoconferenza o di una piattaforma che non consente il monitoraggio sistematico degli utenti o comunque non ricorre a nuove soluzioni tecnologiche particolarmente invasive (quali, tra le altre, quelle che comportano nuove forme di utilizzo dei dati di geolocalizzazione o biometrici).
La valutazione di impatto va effettuata, infatti, nel caso di ricorso a piattaforme di gestione della didattica che offrono funzioni più avanzate e complesse che la scuola decida di utilizzare e che comportano un rischio elevato per i diritti e le libertà delle persone fisiche. In particolare, l'istituzione scolastica per individuare i trattamenti da sottoporre a valutazione di impatto dovrà verificare se il trattamento in questione:

1. rientra nei casi previsti dall'art.35, par. 3 del Regolamento (trattamento automatizzato, profilazione, trattamento su larga scala di categorie particolari di dati personali, ecc.),tenendo conto sempre del contesto in cui il trattamento stesso si colloca;
2. comporta la compresenza di almeno di due criteri individuati come indici sintomatici del "rischio elevato" dal Gruppo di lavoro ex articolo 29 delle Linee guida in materia di valutazione d'impatto sulla protezione dei dati (trattamenti valutativi o di *scoring*), compresa la profilazione, processo decisionale automatizzato, monitoraggio sistematico, dati sensibili o dati aventi carattere altamente personale, trattamento di dati su larga scala espressi in percentuale della popolazione di riferimento, creazione di corrispondenze o combinazione di insiemi di dati, dati relativi a interessati vulnerabili, uso innovativo o applicazione di nuove

soluzioni tecnologiche od organizzative, trattamento che in sé "impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto".

Indipendentemente dalle scelte effettuate nel contesto dell'emergenza nel corso del precedente anno scolastico, a seconda delle caratteristiche delle piattaforme utilizzate, è opportuno che, se sussistono i requisiti sopra indicati, la scuola verifichi nuovamente, con l'assistenza del RPD, che è tenuto a fornire il proprio parere al riguardo, l'esigenza dell'effettuazione di una valutazione di impatto.
In questa attività il fornitore del servizio, in qualità del responsabile del trattamento, è tenuto ad assistere l'istituzione scolastica e a fornire ogni elemento utile nello svolgimento della valutazione d'impatto e delle analisi relative alla valutazione del rischio in riferimento alla protezione dei dati.

Per ulteriori informazioni sulla valutazione di impatto è possibile accedere all'infografica messa a disposizione sul sito del Garante Privacy.