Ministero dell'Istruzione e del Merito
ISTITUTO COMPRENSIVO STATALE DI MOLTENO
Piazza don Biffi, 1 – 23847 Molteno (LC)
Tel. 031 850358 - C.F. 92058790137
e-mail uffici: lcic822006@istruzione.it – lcic822006@pec.istruzione.it
sito web: www.icsmolteno.edu.it

Addendum sull'elaborazione dei dati nel cloud (clienti)

Il presente Addendum sul trattamento dei dati nel cloud, inclusi i relativi allegati (" *Addendum* "), è parte integrante del/dei Contratto/i in base ai quali Google ha accettato di fornire al Cliente Google Cloud Platform, Google Workspace o Cloud Identity (ciascuno come definito di seguito), a seconda dei casi (i " *Servizi* "). Il presente Addendum era precedentemente noto come "Termini di trattamento e sicurezza dei dati" nell'ambito di un Contratto per Google Cloud Platform e come "Emendamento sul trattamento dei dati" nell'ambito di un Contratto per Google Workspace o Cloud Identity.

1. Inizio

Il presente Addendum entrerà in vigore e sostituirà qualsiasi termine precedentemente applicabile al trattamento dei Dati del Cliente, inclusi eventuali Termini di Trattamento e Sicurezza dei Dati o Modifiche al Trattamento dei Dati, a partire dalla Data di Entrata in Vigore dell'Addendum (come definita di seguito).

2. Definizioni

2.1 I termini in maiuscolo utilizzati ma non definiti nel presente Addendum hanno il significato loro attribuito nell'Accordo:

- *Per "Account"* si intende quanto specificato nel Contratto applicabile o, in mancanza di tale definizione, si intende l'account Google Cloud Platform, l'account Google Workspace o l'account Cloud Identity del Cliente, a seconda dei casi.

- *La Data di Entrata in Vigore dell'Addendum* indica la data in cui il Cliente ha accettato, o le parti hanno altrimenti concordato, il presente Addendum.

- *Per Controlli di sicurezza aggiuntivi* si intendono le risorse, le funzionalità e/o i controlli di sicurezza che il Cliente può utilizzare a sua discrezione e/o secondo le proprie esigenze, tra cui la Console di amministrazione, la crittografia, la registrazione e il monitoraggio, la gestione delle identità e degli accessi, la scansione di sicurezza e i firewall.

- *Per "Paese adeguato"* si intende:

(a) per i dati trattati in conformità al GDPR dell'UE: lo Spazio economico europeo (SEE) o un paese o territorio riconosciuto come in grado di garantire un'adeguata protezione ai sensi del GDPR dell'UE;

(b) per i dati trattati soggetti al GDPR del Regno Unito: il Regno Unito, o un paese o territorio riconosciuto come garante di un'adeguata protezione ai sensi del GDPR del Regno Unito e del Data Protection Act 2018; e/o

c) per i dati trattati soggetti alla FDPA svizzera: la Svizzera, o un paese o territorio che: i) è incluso nell'elenco degli stati la cui legislazione garantisce una protezione adeguata, pubblicato dal Commissario federale svizzero per la protezione dei dati e l'informazione, o ii) è riconosciuto dal Consiglio federale svizzero come in grado di garantire una protezione adeguata ai sensi della FDPA svizzera;

in ciascun caso, salvo sulla base di un quadro facoltativo di protezione dei dati.

- *Per Soluzione di Trasferimento Alternativa* si intende una soluzione, diversa dalle Clausole Contrattuali Standard (SCC), che consente il trasferimento lecito di dati personali verso un paese terzo in conformità con la normativa europea sulla protezione dei dati, ad esempio un quadro normativo sulla protezione dei dati riconosciuto come in grado di garantire che le entità partecipanti forniscano una protezione adeguata.

- *Per Servizi sottoposti ad audit* si intendono i Servizi attualmente in vigore indicati come rientranti nell'ambito della relativa certificazione o del relativo report, disponibili all'indirizzo https://cloud.google.com/security/compliance/services-in-scope . Google non può rimuovere alcun Servizio da questo URL a meno che tali Servizi non siano stati interrotti in conformità con l'Accordo applicabile.

- *Per Cloud Identity* si intendono i Servizi di identità cloud descritti all'indirizzo https://cloud.google.com/terms/identity/user-features , acquistati nell'ambito di un Contratto autonomo.

- *Per "Dati del Cliente"* si intende quanto stabilito nel Contratto applicabile o, in mancanza di tale definizione, si intende quanto segue:

(a) dati forniti dal Cliente o per conto del Cliente o dei suoi Utenti finali tramite Google Cloud Platform nell'ambito dell'Account; o

(b) dati inviati, archiviati, trasmessi o ricevuti dal Cliente o dai suoi Utenti finali o per conto di essi tramite Google Workspace o Cloud Identity nell'ambito dell'Account.

- *Per "Dati personali del cliente"* si intendono i dati personali contenuti nei Dati del cliente, comprese le categorie particolari di dati personali definite dalla normativa europea in materia di protezione dei dati.

- *Per "Clienti SCC del Cliente"* si intendono i Contratti SCC (Controller-to-Processor), i Contratti SCC (Processor-to-Processor) e/o i Contratti SCC (Processor-to-Controller), a seconda dei casi.

- *Per "Incidente dei dati "* si intende una violazione della sicurezza di Google che comporti la distruzione, la perdita, l'alterazione, la divulgazione non autorizzata o l'accesso non autorizzato ai Dati del Cliente su sistemi gestiti o comunque controllati da Google.

- *SEE* significa Spazio economico europeo.

- *EMEA* significa Europa, Medio Oriente e Africa.

- *Per GDPR UE* si intende 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.

- *Per "Legge europea sulla protezione dei dati"* si intende, a seconda dei casi: (a) il GDPR; e/o (b) la legge svizzera sulla protezione dei dati personali (FDPA).

- *Per "legge europea"* si intende, a seconda dei casi: (a) la legge dell'UE o dello Stato membro dell'UE (se il GDPR dell'UE si applica al trattamento dei dati personali del Cliente); e (b) la legge del Regno Unito o di una parte del Regno Unito (se il GDPR del Regno Unito si applica al trattamento dei dati personali del Cliente).

- *GDPR* significa, a seconda dei casi: (a) il GDPR dell'UE; e/o (b) il GDPR del Regno Unito.

- *Per Google Cloud Platform* si intendono i servizi di Google Cloud Platform descritti all'indirizzo https://cloud.google.com/terms/services , ad esclusione di eventuali offerte di terze parti.

- *Con Google Workspace* si intendono i servizi Google Workspace o Google Workspace for Education descritti all'indirizzo https://workspace.google.com/terms/user_features.html , a seconda dei casi.

- *Per "Revisore dei Conti di Google"* si intende un revisore dei conti terzo, qualificato e indipendente, nominato da Google, la cui identità, al momento della nomina, verrà comunicata al Cliente da Google.

- *Il termine "Istruzioni"* ha il significato indicato nella Sezione 5.2.1 (Conformità alle Istruzioni del Cliente).

- *Per "Legislazione extraeuropea sulla protezione dei dati"* si intendono le leggi sulla protezione dei dati o sulla privacy in vigore al di fuori dello Spazio economico europeo (SEE), del Regno Unito e della Svizzera.

- *Per "Indirizzo e-mail di notifica"* si intende l'indirizzo o gli indirizzi e-mail designati dal Cliente nella Console di amministrazione o nel Modulo d'ordine per ricevere determinate notifiche da Google. Il Cliente è responsabile di utilizzare la Console di amministrazione per assicurarsi che il proprio Indirizzo e-mail di notifica rimanga aggiornato e valido.

- *Per SCC* si intendono le Condizioni Generali di Contratto del Cliente e/o le Condizioni Generali di Contratto (da Processore a Processore, Google Exporter), a seconda dei casi.

- *Per SCC (Controller-to-Processor)* si intendono i termini riportati al seguente indirizzo: https://cloud.google.com/terms/sccs/eu-c2p

- *Per SCC (Processor-to-Controller)* si intendono i termini riportati al seguente indirizzo: https://cloud.google.com/terms/sccs/eu-p2c

- *Per SCC (Processor-to-Processor)* si intendono i termini e le condizioni riportati al seguente indirizzo: https://cloud.google.com/terms/sccs/eu-p2p

- *Per SCC (Processor-to-Processor, Google Exporter)* si intendono i termini e le condizioni riportati al seguente indirizzo: https://cloud.google.com/terms/sccs/eu-p2p-google-exporter

- *Per Documentazione di sicurezza* si intendono tutti i documenti e le informazioni resi disponibili da Google ai sensi della Sezione 7.5.1 (Revisione della documentazione di sicurezza).

- *Il termine "Misure di sicurezza"* ha il significato indicato nella Sezione 7.1.1 (Misure di sicurezza di Google).

- *Per "sub-responsabile del trattamento"* si intende una terza parte autorizzata, in qualità di ulteriore responsabile del trattamento ai sensi del presente Addendum, ad avere accesso logico ai Dati del Cliente e a elaborarli al fine di fornire parti dei Servizi e del TSS.

- *Per "Autorità di controllo"* si intende, a seconda dei casi: (a) un'"autorità di controllo" come definita nel GDPR dell'UE; e/o (b) il "Commissario" come definito nel GDPR del Regno Unito e/o nella FDPA svizzera.

- *Con FDPA svizzera* si intende la legge federale sulla protezione dei dati del 19 giugno 1992 (Svizzera).

- *Per "Termine"* si intende il periodo che intercorre tra la Data di entrata in vigore dell'Addendum e la fine della fornitura dei Servizi da parte di Google, inclusi, se del caso, eventuali periodi durante i quali la fornitura dei Servizi potrebbe essere sospesa e qualsiasi periodo successivo alla cessazione durante il quale Google potrebbe continuare a fornire i Servizi a fini transitori.

- *Per GDPR del Regno Unito* si intende il GDPR dell'UE, come modificato e incorporato nella legislazione del Regno Unito ai sensi dell'UK European Union (Withdrawal) Act 2018, e della relativa legislazione secondaria emanata in virtù di tale legge.

2.2 I termini "dati personali", "interessato", "trattamento", "titolare del trattamento" e "responsabile del trattamento", come utilizzati nel presente Addendum, hanno il significato loro attribuito dal GDPR, indipendentemente dal fatto che si applichi la normativa europea o extraeuropea in materia di protezione dei dati.

3. Durata

Indipendentemente dal fatto che l'Accordo applicabile sia stato risolto o sia scaduto, il presente Addendum rimarrà in vigore fino a quando Google non eliminerà tutti i Dati del Cliente come descritto nel presente Addendum e scadrà automaticamente quando ciò avverrà.

4. Ambito di applicazione della legge sulla protezione dei dati

4.1 *Applicazione del diritto europeo* . Le parti riconoscono che il diritto europeo in materia di protezione dei dati si applicherà al trattamento dei dati personali del Cliente se, ad esempio:

a. il trattamento viene effettuato nell'ambito delle attività di uno stabilimento del Cliente nel territorio dello Spazio economico europeo o del Regno Unito; e/o

b. I Dati Personali del Cliente sono dati personali relativi a soggetti interessati che si trovano nello Spazio Economico Europeo (SEE) o nel Regno Unito e il cui trattamento è correlato all'offerta di beni o servizi nello SEE o nel Regno Unito, oppure al monitoraggio del loro comportamento nello SEE o nel Regno Unito.

4.2 *Applicazione di leggi extraeuropee* . Le parti riconoscono che al trattamento dei Dati personali del Cliente possono applicarsi anche leggi extraeuropee in materia di protezione dei dati.

4.3 *Applicazione dell'Addendum* . Salvo quanto diversamente previsto nel presente Addendum, quest'ultimo si applicherà indipendentemente dal fatto che al trattamento dei Dati Personali del Cliente si applichi la normativa europea o extraeuropea in materia di protezione dei dati.

5. Elaborazione dei dati

5.1 *Ruoli e conformità normativa; Autorizzazione* .

5.1.1 *Responsabilità del Responsabile del trattamento e del Titolare del trattamento* . Qualora la normativa europea sulla protezione dei dati si applichi al trattamento dei Dati personali del Cliente:

a. L'oggetto e i dettagli del trattamento sono descritti nell'Appendice 1;

b. Google agisce in qualità di responsabile del trattamento dei dati personali del Cliente ai sensi della normativa europea sulla protezione dei dati;

c. Il Cliente è titolare o responsabile del trattamento, a seconda dei casi, dei Dati personali del Cliente ai sensi della normativa europea sulla protezione dei dati; e

d. ciascuna parte si impegna a rispettare gli obblighi ad essa applicabili ai sensi della normativa europea sulla protezione dei dati in relazione al trattamento dei dati personali del Cliente.

5.1.2 *Clienti responsabili del trattamento* . Qualora la normativa europea sulla protezione dei dati si applichi al trattamento dei dati personali del Cliente e quest'ultimo sia un responsabile del trattamento:

a. Il Cliente garantisce in modo continuativo che il titolare del trattamento competente ha autorizzato: (i) le Istruzioni, (ii) la nomina da parte del Cliente di Google quale ulteriore responsabile del trattamento e (iii) l'incarico da parte di Google di Subresponsabili del trattamento come descritto nella Sezione 11 (Subresponsabili del trattamento);

b. Il Cliente inoltrerà immediatamente al titolare del trattamento competente qualsiasi avviso fornito da Google ai sensi delle Sezioni 5.2.2 (Notifiche delle istruzioni), 7.2.1 (Notifica degli incidenti), 9.2.1 (Responsabilità per le richieste), 11.4 (Opportunità di opporsi alle modifiche del subappaltatore) o che faccia riferimento a qualsiasi SCC; e

c. Il cliente può:

i. richiedere l'accesso del responsabile competente ai report SOC in conformità alla Sezione 7.5.3(a); e

ii. mettere a disposizione del titolare del trattamento competente qualsiasi altra informazione resa disponibile da Google ai sensi delle Sezioni 10.4 (Misure e informazioni supplementari), 10.6 (Informazioni sul data center) e 11.2 (Informazioni sui subappaltatori).

5.1.3 *Responsabilità ai sensi del diritto extraeuropeo.* Qualora al trattamento dei Dati personali del Cliente da parte di una delle parti si applichi una normativa extraeuropea in materia di protezione dei dati, la parte interessata si conformerà a tutti gli obblighi ad essa applicabili ai sensi di tale normativa in relazione al trattamento di tali Dati personali del Cliente.

5.2 *Ambito del trattamento* .

5.2.1 *Conformità alle istruzioni del Cliente* . Il Cliente incarica Google di elaborare i Dati del Cliente in conformità con l'Accordo applicabile (incluso il presente Addendum) e la legge applicabile esclusivamente: (a) per fornire, proteggere e monitorare i Servizi e il TSS; e (b) come ulteriormente specificato tramite (i) l'utilizzo da parte del Cliente dei Servizi (inclusa la Console di amministrazione e altre funzionalità dei Servizi) e del TSS, e (ii) qualsiasi altra istruzione scritta fornita dal Cliente e riconosciuta da Google come costituente istruzioni ai sensi del presente Addendum (collettivamente, le " *Istruzioni* "). Google si conformerà alle Istruzioni a meno che non sia vietato dalla legge europea.

5.2.2 *Notifiche relative alle istruzioni* . Fatto salvo quanto previsto dalla Sezione 5.2.1 (Conformità alle istruzioni del Cliente) o da qualsiasi altro diritto o obbligo di una delle parti ai sensi del Contratto applicabile, Google informerà immediatamente il Cliente qualora, a suo giudizio: (a) la legge europea impedisca a Google di conformarsi a un'Istruzione; (b) un'Istruzione non sia conforme alla legge europea sulla protezione dei dati; o (c) Google non sia altrimenti in grado di conformarsi a un'Istruzione, in ciascun caso a meno che tale notifica non sia vietata dalla legge europea.

5.3 *Prodotti aggiuntivi* . Qualora Google, a sua discrezione, renda disponibili al Cliente Prodotti aggiuntivi da utilizzare con Google Workspace o Cloud Identity in conformità con i Termini applicabili relativi ai Prodotti aggiuntivi:

a. Il cliente può abilitare o disabilitare i Prodotti aggiuntivi tramite la Console di amministrazione e non avrà bisogno di utilizzare Prodotti aggiuntivi per utilizzare Google Workspace o Cloud Identity; e

b. Se il Cliente sceglie di installare Prodotti Aggiuntivi o di utilizzarli con Google Workspace o Cloud Identity, i Prodotti Aggiuntivi potrebbero accedere ai Dati del Cliente nella misura necessaria all'interoperabilità con Google Workspace o Cloud Identity (a seconda dei casi).

A titolo di chiarimento, il presente Addendum non si applica al trattamento dei dati personali in relazione alla fornitura di eventuali Prodotti Aggiuntivi installati o utilizzati dal Cliente, inclusi i dati personali trasmessi da o verso tali Prodotti Aggiuntivi.

6. Eliminazione dei dati

6.1 *Cancellazione da parte del Cliente* . Google consentirà al Cliente di cancellare i Dati del Cliente durante il Periodo di validità del Contratto in modo coerente con le funzionalità dei Servizi. Qualora il Cliente utilizzi i Servizi per cancellare i Dati del Cliente durante il Periodo di validità del Contratto e tali Dati del Cliente non possano essere recuperati dal Cliente, tale utilizzo costituirà un'Istruzione a Google per la cancellazione dei relativi Dati del Cliente dai sistemi di Google in conformità con la legge applicabile. Google si conformerà a tale Istruzione non appena ragionevolmente possibile e comunque entro un periodo massimo di 180 giorni, a meno che la legge europea non ne richieda la conservazione.

6.2 *Restituzione o cancellazione al termine del Contratto* . Se il Cliente desidera conservare i Dati del Cliente dopo la scadenza del Contratto, può richiedere a Google, ai sensi della Sezione 9.1 (Accesso; Rettifica; Trattamento limitato; Portabilità), la restituzione di tali dati durante il Contratto. Fatto salvo quanto previsto dalla Sezione 6.3 (Istruzioni per la cancellazione differita), il Cliente richiede a Google di cancellare tutti i Dati del Cliente rimanenti (incluse le copie esistenti) dai sistemi di Google al termine del Contratto, in conformità con la legge applicabile. Dopo un periodo di recupero fino a 30 giorni da tale data, Google si conformerà a tale Istruzione non appena ragionevolmente possibile e comunque entro un periodo massimo di 180 giorni, salvo ove diversamente previsto dalla legge europea.

6.3. *Istruzioni di cancellazione differita* . Nella misura in cui i Dati del Cliente coperti dalle istruzioni di cancellazione descritte nella Sezione 6.2 (Restituzione o cancellazione alla scadenza del termine) vengano elaborati anche, alla scadenza del termine applicabile ai sensi della Sezione 6.2, in relazione a un Contratto con un termine continuativo, tali istruzioni di cancellazione avranno effetto rispetto a tali Dati del Cliente solo alla scadenza del termine continuativo. Per chiarezza, il presente Addendum continuerà ad applicarsi a tali Dati del Cliente fino alla loro cancellazione da parte di Google.

7. Sicurezza dei dati

7.1 *Misure di sicurezza, controlli e assistenza di Google* .

7.1.1 *Misure di sicurezza di Google* . Google implementerà e manterrà misure tecniche, organizzative e fisiche per proteggere i Dati del Cliente da distruzione, perdita, alterazione, divulgazione o accesso non autorizzati, accidentali o illeciti, come descritto nell'Appendice 2 (le " *Misure di sicurezza* "). Le Misure di sicurezza includono misure per crittografare i Dati del Cliente; per contribuire a garantire la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi di Google; per contribuire a ripristinare tempestivamente l'accesso ai Dati del Cliente a seguito di un incidente; e per testare regolarmente l'efficacia. Google può aggiornare le Misure di sicurezza di volta in volta, a condizione che tali aggiornamenti non comportino una riduzione sostanziale della sicurezza dei Servizi.

7.1.2 *Accesso e conformità* . Google si impegna a: (a) autorizzare i propri dipendenti, appaltatori e subappaltatori ad accedere ai Dati del Cliente solo nella misura strettamente necessaria per conformarsi alle Istruzioni; (b) adottare misure appropriate per garantire la conformità alle Misure di Sicurezza da parte dei propri dipendenti, appaltatori e subappaltatori

nella misura applicabile al loro ambito di attività; e (c) garantire che tutte le persone autorizzate a trattare i Dati del Cliente siano soggette a un obbligo di riservatezza.

7.1.3 *Controlli di sicurezza aggiuntivi* . Google renderà disponibili controlli di sicurezza aggiuntivi per: (a) consentire al Cliente di adottare misure per proteggere i Dati del Cliente; e (b) fornire al Cliente informazioni sulla protezione, l'accesso e l'utilizzo dei Dati del Cliente.

7.1.4 *Assistenza di Google in materia di sicurezza* . Google (tenendo conto della natura del trattamento dei Dati Personali del Cliente e delle informazioni a disposizione di Google) assisterà il Cliente nel garantire il rispetto dei propri obblighi (o, qualora il Cliente sia un responsabile del trattamento, degli obblighi del titolare del trattamento competente) ai sensi degli articoli da 32 a 34 del GDPR, mediante:

a. implementare e mantenere le Misure di Sicurezza in conformità con la Sezione 7.1.1 (Misure di Sicurezza di Google);

b. mettere a disposizione del Cliente Controlli di Sicurezza Aggiuntivi in conformità alla Sezione 7.1.3 (Controlli di Sicurezza Aggiuntivi);

c. rispettare le disposizioni della Sezione 7.2 (Incidenti relativi ai dati);

d. fornire al Cliente la Documentazione di Sicurezza in conformità alla Sezione 7.5.1 (Revisioni della Documentazione di Sicurezza) e alle informazioni contenute nell'Accordo applicabile (incluso il presente Addendum); e

e. se i paragrafi (a)-(d) di cui sopra non sono sufficienti affinché il Cliente (o il titolare del trattamento competente) possa adempiere a tali obblighi, su richiesta del Cliente, fornire al Cliente ulteriore ragionevole cooperazione e assistenza.

7.2 *Incidenti relativi ai dati* .

7.2.1 *Notifica degli incidenti* . Google informerà il Cliente tempestivamente e senza indebito ritardo dopo essere venuta a conoscenza di un incidente relativo ai dati e adotterà prontamente misure ragionevoli per ridurre al minimo i danni e proteggere i dati del Cliente.

7.2.2 *Dettagli dell'incidente relativo ai dati* . La notifica di Google relativa a un incidente relativo ai dati descriverà: la natura dell'incidente, comprese le risorse del Cliente interessate; le misure che Google ha adottato o prevede di adottare per affrontare l'incidente relativo ai dati e mitigarne il potenziale rischio; le misure, se del caso, che Google raccomanda al Cliente di adottare per affrontare l'incidente relativo ai dati; e i dettagli di un punto di contatto presso il quale è possibile ottenere ulteriori informazioni. Qualora non sia possibile fornire tutte queste informazioni contemporaneamente, la notifica iniziale di Google conterrà le informazioni disponibili al momento e ulteriori informazioni saranno fornite senza indebito ritardo non appena disponibili.

7.2.3 *Invio delle notifiche* . Le notifiche relative a eventuali incidenti di dati verranno inviate all'indirizzo e-mail di notifica.

7.2.4 *Nessuna valutazione dei dati del cliente da parte di Google* . Google non ha alcun obbligo di valutare i dati del cliente al fine di identificare informazioni soggette a specifici requisiti legali.

7.2.5 *Nessun riconoscimento di colpa da parte di Google* . La notifica o la risposta di Google a un Incidente relativo ai Dati ai sensi della presente Sezione 7.2 (Incidenti relativi ai Dati) non sarà interpretata come un riconoscimento da parte di Google di alcuna colpa o responsabilità in relazione all'Incidente relativo ai Dati.

7.3 *Responsabilità e valutazione della sicurezza del cliente* .

7.3.1 *Responsabilità del Cliente in materia di sicurezza* . Fermo restando quanto previsto dagli obblighi di Google ai sensi delle Sezioni 7.1 (Misure di sicurezza, controlli e assistenza di Google) e 7.2 (Incidenti relativi ai dati), e altrove nel Contratto applicabile, il Cliente è responsabile del proprio utilizzo dei Servizi e della conservazione di qualsiasi copia dei Dati del Cliente al di fuori dei sistemi di Google o dei Subappaltatori di Google, inclusi:

a. utilizzare i Servizi e i Controlli di Sicurezza Aggiuntivi per garantire un livello di sicurezza adeguato al rischio per i Dati del Cliente;

b. proteggere le credenziali di autenticazione dell'account, i sistemi e i dispositivi che il Cliente utilizza per accedere ai Servizi; e

c. eseguire il backup o conservare copie dei Dati del Cliente, a seconda dei casi.

7.3.2 *Valutazione della sicurezza del Cliente* . Il Cliente accetta che i Servizi, le Misure di sicurezza implementate e mantenute da Google, i Controlli di sicurezza aggiuntivi e gli impegni di Google ai sensi della presente Sezione 7 (Sicurezza dei dati) forniscano un livello di sicurezza adeguato al rischio per i Dati del Cliente (tenendo conto dello stato dell'arte, dei costi di implementazione e della natura, della portata, del contesto e delle finalità del trattamento dei Dati personali del Cliente, nonché dei rischi per le persone fisiche).

7.4 *Certificazioni di conformità e report SOC* . Google manterrà almeno quanto segue per i Servizi sottoposti ad audit al fine di valutare la continua efficacia delle Misure di sicurezza: (a) certificati ISO 27001, ISO 27017 e ISO 27018 e, per Google Cloud Platform, un'attestazione di conformità PCI DSS (le " *Certificazioni di conformità* "); e (b) report SOC 2 e SOC 3 prodotti dal revisore esterno di Google e aggiornati annualmente sulla base di un audit eseguito almeno una volta ogni 12 mesi (i " *Report SOC"*). Google può aggiungere standard in qualsiasi momento. Google può sostituire una Certificazione di conformità o un Report SOC con un'alternativa equivalente o migliorata.

7.5 *Revisioni e verifiche di conformità* .

7.5.1 *Revisione della documentazione di sicurezza* . Google renderà disponibili al Cliente le Certificazioni di conformità e i Report SOC per la revisione, al fine di dimostrare la conformità di Google ai propri obblighi ai sensi del presente Addendum.

7.5.2 *Diritti di verifica del cliente* .

a. Qualora la normativa europea sulla protezione dei dati sia applicabile al trattamento dei Dati personali del Cliente, Google consentirà al Cliente o a un revisore indipendente nominato dal Cliente di effettuare verifiche (incluse ispezioni) per accertare la conformità di Google ai propri obblighi ai sensi del presente Addendum, in conformità con la Sezione 7.5.3 (Termini commerciali aggiuntivi per revisioni e verifiche). Durante una verifica, Google renderà disponibili tutte le informazioni necessarie a dimostrare tale conformità e contribuirà alla

verifica come descritto nella Sezione 7.4 (Certificazioni di conformità e report SOC) e nella presente Sezione 7.5 (Revisioni e verifiche di conformità).

b. Qualora si applichino le Condizioni Generali di Contratto del Cliente come descritto nella Sezione 10.2 (Trasferimenti europei limitati), Google consentirà al Cliente (o a un revisore indipendente nominato dal Cliente) di condurre verifiche come descritto in tali Condizioni Generali di Contratto e, durante una verifica, di rendere disponibili tutte le informazioni richieste da tali Condizioni Generali di Contratto, in conformità con la Sezione 7.5.3 (Termini commerciali aggiuntivi per revisioni e verifiche).

c. Il Cliente può condurre un audit per verificare la conformità di Google ai propri obblighi ai sensi del presente Addendum esaminando la Documentazione sulla Sicurezza (che riflette l'esito degli audit condotti dal revisore esterno di Google).

7.5.3 *Termini commerciali aggiuntivi per revisioni e audit* .

a. Il cliente deve inviare qualsiasi richiesta di revisione del report SOC 2 ai sensi della Sezione 5.1.2(c)(i) o 7.5.1, o di audit ai sensi della Sezione 7.5.2(a) o 7.5.2(b), al team di protezione dei dati cloud di Google come descritto nella Sezione 12 (Team di protezione dei dati cloud; Registri di elaborazione).

b. A seguito della ricezione da parte di Google di una richiesta ai sensi della Sezione 7.5.3(a), Google e il Cliente discuteranno e concorderanno in anticipo su: (i) la/le data/e ragionevole/i e i controlli di sicurezza e riservatezza applicabili a qualsiasi revisione del report SOC 2 ai sensi della Sezione 5.1.2(c)(i) o 7.5.1; e (ii) la data di inizio ragionevole, l'ambito e la durata e i controlli di sicurezza e riservatezza applicabili a qualsiasi audit ai sensi della Sezione 7.5.2(a) o 7.5.2(b).

c. Google può addebitare un compenso (in base ai costi ragionevoli di Google) per qualsiasi verifica ai sensi della Sezione 7.5.2(a) o 7.5.2(b). Google fornirà al Cliente ulteriori dettagli su qualsiasi compenso applicabile e sulla base del suo calcolo, prima di qualsiasi verifica di questo tipo. Il Cliente sarà responsabile di tutti i compensi addebitati da qualsiasi revisore nominato dal Cliente per eseguire tale verifica.

d. Google può opporsi per iscritto alla nomina di un revisore contabile da parte del Cliente per condurre qualsiasi revisione ai sensi della Sezione 7.5.2(a) o 7.5.2(b) se, a ragionevole giudizio di Google, il revisore non possiede le qualifiche o l'indipendenza necessarie, è un concorrente di Google o è altrimenti manifestamente inadatto. Qualsiasi obiezione di questo tipo da parte di Google richiederà al Cliente di nominare un altro revisore o di condurre la revisione autonomamente.

8. Valutazioni d'impatto e consultazioni

Google (tenendo conto della natura del trattamento e delle informazioni a disposizione di Google) assisterà il Cliente nel garantire il rispetto dei propri obblighi (o, qualora il Cliente sia un responsabile del trattamento, degli obblighi del titolare del trattamento competente) ai sensi degli articoli 35 e 36 del GDPR, mediante:

a. fornire Controlli di sicurezza aggiuntivi in conformità alla Sezione 7.1.3 (Controlli di sicurezza aggiuntivi) e la Documentazione di sicurezza in conformità alla Sezione 7.5.1 (Revisioni della Documentazione di sicurezza);

b. fornire le informazioni contenute nell'Accordo applicabile (incluso il presente Addendum); e

c. qualora i paragrafi (a) e (b) di cui sopra non siano sufficienti affinché il Cliente (o il titolare del trattamento competente) possa adempiere a tali obblighi, su richiesta del Cliente, fornire al Cliente ulteriore ragionevole cooperazione e assistenza.

9. Accesso ecc.; Diritti dell'interessato; Esportazione dei dati

9.1 *Accesso; Rettifica; Limitazione del trattamento; Portabilità* . Durante il Periodo di validità del Contratto, Google consentirà al Cliente, in modo coerente con le funzionalità dei Servizi, di accedere, rettificare e limitare il trattamento dei Dati del Cliente, anche tramite la funzionalità di cancellazione fornita da Google come descritto nella Sezione 6.1 (Cancellazione da parte del Cliente), e di esportare i Dati del Cliente. Qualora il Cliente venga a conoscenza del fatto che i Dati personali del Cliente siano inesatti o obsoleti, sarà sua responsabilità utilizzare tale funzionalità per rettificare o cancellare tali dati, se richiesto dalla normativa europea applicabile in materia di protezione dei dati.

9.2 *Richieste degli interessati* .

9.2.1 *Responsabilità per le richieste* . Durante il Periodo di validità, se il team di protezione dei dati di Google Cloud riceve una richiesta da un interessato relativa ai Dati personali del Cliente e che identifica il Cliente, Google: (a) consiglierà all'interessato di inoltrare la richiesta al Cliente; (b) informerà tempestivamente il Cliente; e (c) non risponderà in altro modo alla richiesta di tale interessato senza l'autorizzazione del Cliente. Il Cliente sarà responsabile di rispondere a qualsiasi richiesta di questo tipo, incluso, ove necessario, utilizzando le funzionalità dei Servizi.

9.2.2 *Assistenza di Google alle richieste degli interessati* . Google (tenendo conto della natura del trattamento dei Dati personali del Cliente) assisterà il Cliente nell'adempimento dei suoi obblighi (o, laddove il Cliente sia un responsabile del trattamento, degli obblighi del titolare del trattamento competente) ai sensi del Capitolo III del GDPR per rispondere alle richieste di esercizio dei diritti dell'interessato mediante:

a. fornire controlli di sicurezza aggiuntivi in conformità alla Sezione 7.1.3 (Controlli di sicurezza aggiuntivi);

b. conformarsi alle Sezioni 9.1 (Accesso; Rettifica; Trattamento limitato; Portabilità) e 9.2.1 (Responsabilità per le richieste); e

c. qualora i paragrafi (a) e (b) di cui sopra non siano sufficienti affinché il Cliente (o il titolare del trattamento competente) possa adempiere a tali obblighi, su richiesta del Cliente, fornire al Cliente ulteriore ragionevole cooperazione e assistenza.

10. Trasferimenti di dati

10.1 *Strutture di archiviazione ed elaborazione dei dati* . Fatti salvi gli impegni di Google in materia di localizzazione dei dati previsti dai Termini specifici del servizio e dalla restante parte della presente Sezione 10 (Trasferimenti di dati), i Dati del Cliente possono essere elaborati in qualsiasi paese in cui Google o i suoi subappaltatori dispongano di strutture.

10.2 *Trasferimenti europei limitati* . Le parti riconoscono che la normativa europea sulla protezione dei dati non richiede clausole contrattuali standard (SCC) o una soluzione di trasferimento alternativa affinché i dati personali del Cliente siano trattati o trasferiti in un Paese adeguato. Qualora i dati personali del Cliente vengano trasferiti in un altro Paese e la normativa europea sulla protezione dei dati si applichi ai trasferimenti (come certificato dal Cliente ai sensi della Sezione 10.3 (Certificazione da parte di clienti non EMEA) se il suo indirizzo di fatturazione è al di fuori dell'area EMEA) (" *Trasferimenti europei limitati* "), allora:

a. se Google ha adottato una Soluzione di Trasferimento Alternativa per eventuali Trasferimenti Europei Restritti, Google informerà il Cliente della soluzione pertinente e garantirà che tali Trasferimenti Europei Restritti siano effettuati in conformità con essa; e/o

b. se Google non ha adottato, o informa il Cliente che Google non sta più adottando, una Soluzione di Trasferimento Alternativa per eventuali Trasferimenti Europei Restritti, allora:

i. se l'indirizzo di Google si trova in un Paese adeguato:

A. le SCC (da processore a processore, Google Exporter) si applicheranno a tali trasferimenti europei limitati da Google ai subappaltatori; e

B. Inoltre, se l'indirizzo di fatturazione del Cliente non si trova in un Paese adeguato, si applicheranno le Condizioni Generali di Contratto (dal Responsabile del trattamento al Titolare del trattamento) (indipendentemente dal fatto che il Cliente sia un titolare del trattamento e/o un responsabile del trattamento) in relazione a tali Trasferimenti Europei Restritti tra Google e il Cliente; oppure

ii. Se l'indirizzo di Google non si trova in un Paese adeguato, si applicheranno le Clausole Contrattuali Standard (dal Titolare al Responsabile) e/o le Clausole Contrattuali Standard (dal Responsabile al Responsabile) (a seconda che il Cliente sia titolare e/o responsabile) in relazione a tali Trasferimenti Europei Restritti tra Google e il Cliente.

10.3 *Certificazione da parte di clienti extra-EMEA* . Se l'indirizzo di fatturazione del Cliente si trova al di fuori dell'area EMEA e il trattamento dei Dati Personali del Cliente è soggetto alla normativa europea sulla protezione dei dati, il Cliente dovrà certificarlo e identificare la propria Autorità di controllo competente tramite la Console di amministrazione di Google Cloud Platform o Google Workspace e Cloud Identity, a seconda dei casi.

10.4 *Misure supplementari e informazioni* . Google fornirà al Cliente informazioni pertinenti ai trasferimenti europei limitati, comprese informazioni sui controlli di sicurezza aggiuntivi e altre misure supplementari per proteggere i dati personali del Cliente:

a. come descritto nella Sezione 7.5.1 (Revisione della documentazione di sicurezza);

b. nella documentazione relativa ai Servizi, disponibile all'indirizzo https://cloud.google.com/docs ; e

c. nel sito web Google Cloud Trust and Security, disponibile all'indirizzo https://cloud.google.com/security .

10.5 *Risoluzione* . Se il Cliente giunge alla conclusione, in base all'utilizzo attuale o previsto dei Servizi, che la Soluzione di Trasferimento Alternativa e/o le Condizioni Generali di

Contratto, a seconda dei casi, non offrono garanzie adeguate per i Dati Personali del Cliente, il Cliente può risolvere immediatamente il Contratto applicabile per convenienza dandone comunicazione a Google.

10.6 *Informazioni sui data center* . Le posizioni dei data center di Google sono descritte ai seguenti indirizzi:

a. https://cloud.google.com/about/locations/ per Google Cloud Platform; e

b. Consultare il sito https://www.google.com/about/datacenters/locations/ per informazioni su Google Workspace e Cloud Identity.

11. Sottoprocessori

11.1 *Consenso all'incarico di sub-responsabili del trattamento* . Il Cliente autorizza espressamente l'incarico di sub-responsabili del trattamento delle entità indicate nella Sezione 11.2 (Informazioni sui sub-responsabili del trattamento) a partire dalla Data di entrata in vigore dell'Addendum. Inoltre, fatto salvo quanto previsto dalla Sezione 11.4 (Possibilità di opporsi alle modifiche dei sub-responsabili del trattamento), il Cliente autorizza in generale l'incarico di altre terze parti in qualità di sub-responsabili del trattamento (" *Nuovi sub-responsabili del trattamento* ").

11.2 *Informazioni sui subappaltatori* . I nomi, le sedi e le attività dei subappaltatori sono descritti ai seguenti indirizzi:

a. https://cloud.google.com/terms/subprocessors per Google Cloud Platform; e

b. Consultare https://workspace.google.com/intl/en/terms/subprocessors.html per Google Workspace e Cloud Identity.

11.3 *Requisiti per l'ingaggio di un sub-responsabile del trattamento* . Quando si incarica un sub-responsabile del trattamento, Google dovrà:

a. garantire tramite un contratto scritto che:

i. il Sub-responsabile del trattamento accede e utilizza i Dati del Cliente solo nella misura necessaria per adempiere agli obblighi subappaltati e lo fa in conformità con l'Accordo applicabile (incluso il presente Addendum); e

ii. se il trattamento dei Dati personali del Cliente è soggetto alla normativa europea sulla protezione dei dati, gli obblighi in materia di protezione dei dati descritti nel presente Addendum (come indicato nell'articolo 28(3) del GDPR, se applicabile), sono imposti al Sub-responsabile del trattamento; e

b. rimanere pienamente responsabile per tutti gli obblighi subappaltati al Subappaltatore e per tutti gli atti e le omissioni del Subappaltatore.

11.4 *Possibilità di opporsi alle modifiche apportate dal subprocessore* .

a. Qualora venga incaricato un Nuovo Sub-responsabile del trattamento durante il Periodo di validità del Contratto, Google, almeno 30 giorni prima che il Nuovo Sub-responsabile del

trattamento inizi a elaborare i Dati del Cliente, informerà il Cliente dell'incarico (indicando nome, sede e attività del Nuovo Sub-responsabile del trattamento).

b. Il Cliente può, entro 90 giorni dalla notifica dell'incarico di un Nuovo Sub-responsabile del trattamento, opporsi risolvendo immediatamente il Contratto applicabile per convenienza, dandone comunicazione a Google.

12. Team per la protezione dei dati nel cloud; Elaborazione dei record

12.1 *Team di protezione dei dati nel cloud* . Il team di protezione dei dati nel cloud di Google fornirà assistenza tempestiva e ragionevole per qualsiasi domanda del Cliente relativa al trattamento dei Dati del Cliente ai sensi del Contratto applicabile e può essere contattato:

a. all'indirizzo https://support.google.com/cloud/contact/dpo per Google Cloud Platform;

b. su https://support.google.com/a/contact/googlecloud_dpr per Google Workspace e Cloud Identity (mentre gli amministratori hanno effettuato l'accesso al proprio account amministratore); oppure

c. come descritto nella sezione Avvisi del Contratto applicabile.

12.2 *Registri di trattamento di Google* . Google manterrà la documentazione appropriata delle proprie attività di trattamento come richiesto dal GDPR. Nella misura in cui il GDPR richieda a Google di raccogliere e conservare registri di determinate informazioni relative al Cliente, quest'ultimo utilizzerà la Console di amministrazione per fornire tali informazioni e mantenerle accurate e aggiornate. Google potrà rendere disponibili tali informazioni alle Autorità di controllo qualora richiesto dal GDPR.

12.3 *Richieste del Titolare del trattamento* . Durante il Periodo di validità, se il team di protezione dei dati di Google Cloud riceve una richiesta o un'istruzione da una terza parte che si dichiara titolare del trattamento dei Dati personali del Cliente, Google consiglierà a tale terza parte di contattare il Cliente.

13. Interpretazione

13.1 *Precedenza* .

a. Nella misura di qualsiasi conflitto o incoerenza tra:

i. il presente Addendum e il resto dell'Accordo, il presente Addendum prevarrà; e

ii. in caso di applicazione delle Condizioni Generali di Contratto del Cliente (che sono incorporate per riferimento nel presente Addendum) e del resto dell'Accordo (incluso il presente Addendum), prevarranno le Condizioni Generali di Contratto del Cliente.

b. Per maggiore chiarezza, qualora il Cliente abbia stipulato più di un Contratto, il presente Addendum modificherà ciascuno dei Contratti separatamente.

13.2 *Clausole contrattuali standard (SCC) precedenti del Regno Unito* . A partire dal 21 settembre 2022, le clausole supplementari relative ai trasferimenti ai sensi del GDPR del Regno Unito o del Data Protection Act 2018, sostituiranno e risolveranno qualsiasi clausola

contrattuale standard approvata ai sensi del GDPR del Regno Unito o del Data Protection Act 2018 e precedentemente stipulata tra il Cliente e Google.

13.3 *Nessuna modifica delle Clausole Contrattuali Standard* . Nulla nel presente Contratto (incluso il presente Addendum) è inteso a modificare o contraddire le Clausole Contrattuali Standard o a pregiudicare i diritti o le libertà fondamentali degli interessati ai sensi della normativa europea sulla protezione dei dati.

Appendice 1: Oggetto e dettagli del trattamento dei dati

Argomento

Fornitura da parte di Google dei Servizi e del TSS al Cliente.

Durata dell'elaborazione

Il Periodo di validità più il periodo che intercorre dalla fine del Periodo di validità fino alla cancellazione di tutti i Dati del Cliente da parte di Google in conformità con il presente Addendum.

Natura e finalità del trattamento

Google tratterà i Dati personali del Cliente allo scopo di fornire i Servizi e il TSS al Cliente in conformità con il presente Addendum.

Categorie di dati

Dati relativi a persone fisiche forniti a Google tramite i Servizi, dal Cliente (o su sua indicazione) o dai suoi Utenti finali.

Interessati ai dati

Per interessati si intendono le persone fisiche i cui dati vengono forniti a Google tramite i Servizi dal Cliente o dai suoi Utenti finali (o su sua indicazione).

Appendice 2: Misure di sicurezza

A partire dalla data di entrata in vigore dell'Addendum, Google implementerà e manterrà le misure di sicurezza descritte nella presente Appendice 2.

1. Sicurezza del data center e della rete

(a) Centri dati.

Infrastruttura . Google gestisce data center distribuiti geograficamente. Google archivia tutti i dati di produzione in data center fisicamente sicuri.

Ridondanza . I sistemi infrastrutturali sono stati progettati per eliminare i singoli punti di guasto e ridurre al minimo l'impatto dei rischi ambientali previsti. Circuiti, switch, reti o altri dispositivi necessari doppi contribuiscono a fornire questa ridondanza. I Servizi sono progettati per consentire a Google di eseguire determinati tipi di manutenzione preventiva e correttiva senza interruzioni. Tutte le apparecchiature e le strutture ambientali dispongono di

procedure di manutenzione preventiva documentate che descrivono in dettaglio il processo e la frequenza di esecuzione in conformità con le specifiche del produttore o interne. La manutenzione preventiva e correttiva delle apparecchiature del data center è programmata tramite un processo di cambio standard secondo procedure documentate.

Alimentazione . I sistemi di alimentazione elettrica dei data center sono progettati per essere ridondanti e manutenibili senza interruzioni operative, 24 ore su 24, 7 giorni su 7. Nella maggior parte dei casi, per i componenti critici dell'infrastruttura del data center sono previste sia una fonte di alimentazione primaria che una alternativa, entrambe con pari capacità. L'alimentazione di backup è fornita da diversi meccanismi, come le batterie degli UPS (gruppi di continuità), che garantiscono una protezione affidabile durante cali di tensione, blackout, sovratensioni, sottotensioni e condizioni di frequenza fuori tolleranza. In caso di interruzione dell'alimentazione di rete, l'alimentazione di backup è progettata per fornire energia transitoria al data center, a piena capacità, per un massimo di 10 minuti, fino all'attivazione dei generatori di backup. Questi ultimi sono in grado di avviarsi automaticamente in pochi secondi per fornire energia elettrica di emergenza sufficiente a far funzionare il data center a piena capacità, in genere per diversi giorni.

Sistemi operativi server . I server di Google utilizzano un'implementazione basata su Linux, personalizzata per l'ambiente applicativo. I dati vengono archiviati utilizzando algoritmi proprietari per rafforzare la sicurezza e la ridondanza dei dati. Google adotta un processo di revisione del codice per aumentare la sicurezza del codice utilizzato per fornire i Servizi e migliorare i prodotti di sicurezza negli ambienti di produzione.

Continuità aziendale . Google ha progettato e pianifica e testa regolarmente i propri programmi di continuità aziendale/recupero in caso di disastro.

(*b) Reti e trasmissione.*

Trasmissione dei dati . I data center sono in genere collegati tramite collegamenti privati ad alta velocità per garantire un trasferimento dati sicuro e rapido tra di essi. Questo sistema è progettato per impedire che i dati vengano letti, copiati, modificati o rimossi senza autorizzazione durante il trasferimento o il trasporto elettronico o durante la registrazione su supporti di memorizzazione. Google trasferisce i dati tramite protocolli standard di Internet.

Superficie di attacco esterna . Google utilizza più livelli di dispositivi di rete e sistemi di rilevamento delle intrusioni per proteggere la propria superficie di attacco esterna. Google valuta i potenziali vettori di attacco e integra tecnologie specifiche e appropriate nei sistemi rivolti verso l'esterno.

Rilevamento delle intrusioni . Il rilevamento delle intrusioni ha lo scopo di fornire informazioni sulle attività di attacco in corso e di fornire dati adeguati per rispondere agli incidenti. Il sistema di rilevamento delle intrusioni di Google comprende:

1. Controllare rigorosamente le dimensioni e la composizione della superficie di attacco di Google attraverso misure preventive;

2. impiegando controlli di rilevamento intelligenti nei punti di immissione dei dati; e

3. impiegando tecnologie che risolvono automaticamente determinate situazioni pericolose.

Risposta agli incidenti . Google monitora diversi canali di comunicazione per individuare eventuali incidenti di sicurezza e il personale addetto alla sicurezza di Google interviene tempestivamente in caso di incidenti noti.

Tecnologie di crittografia . Google mette a disposizione la crittografia HTTPS (nota anche come connessione SSL o TLS). I server di Google supportano lo scambio di chiavi crittografiche Diffie-Hellman a curva ellittica effimera, firmate con RSA ed ECDSA. Questi metodi di Perfect Forward Secrecy (PFS) contribuiscono a proteggere il traffico e a minimizzare l'impatto di una chiave compromessa o di una violazione crittografica.

2. Controllo degli accessi e del sito

(a) Controlli del sito.

Servizio di sicurezza in loco per i data center . I data center di Google dispongono di un servizio di sicurezza in loco responsabile di tutte le funzioni di sicurezza fisica del data center, 24 ore su 24, 7 giorni su 7. Il personale addetto alla sicurezza in loco monitora le telecamere a circuito chiuso (CCTV) e tutti i sistemi di allarme. Il personale addetto alla sicurezza in loco effettua regolarmente pattugliamenti interni ed esterni del data center.

Procedure di accesso ai data center . Google adotta procedure di accesso formali per consentire l'accesso fisico ai data center. I data center sono ospitati in strutture che richiedono l'accesso tramite badge elettronico, con allarmi collegati al sistema di sicurezza in loco. Tutti coloro che accedono al data center sono tenuti a identificarsi e a mostrare un documento d'identità al personale di sicurezza in loco. Solo i dipendenti, i collaboratori e i visitatori autorizzati possono accedere ai data center. Solo i dipendenti e i collaboratori autorizzati possono richiedere l'accesso tramite badge elettronico a queste strutture. Le richieste di accesso tramite badge elettronico ai data center devono essere inviate via e-mail e richiedono l'approvazione del responsabile del richiedente e del direttore del data center. Tutti gli altri utenti che necessitano di un accesso temporaneo al data center devono: (i) ottenere l'approvazione preventiva dai responsabili del data center per il data center specifico e le aree interne che desiderano visitare; (ii) registrarsi presso il personale di sicurezza in loco; e (iii) fare riferimento a un registro di accesso al data center approvato che identifichi l'individuo come autorizzato.

Dispositivi di sicurezza in loco per i data center . I data center di Google utilizzano un sistema di controllo accessi a doppia autenticazione collegato a un sistema di allarme. Il sistema di controllo accessi monitora e registra la chiave elettronica di ciascun individuo e i suoi accessi alle porte perimetrali, alle aree di carico e scarico merci e ad altre aree critiche. Le attività non autorizzate e i tentativi di accesso non riusciti vengono registrati dal sistema di controllo accessi e, se necessario, oggetto di indagine. L'accesso autorizzato alle attività aziendali e ai data center è limitato in base alle zone e alle mansioni individuali. Le porte tagliafuoco dei data center sono dotate di allarme. Telecamere a circuito chiuso (CCTV) sono operative sia all'interno che all'esterno dei data center. Il posizionamento delle telecamere è stato progettato per coprire aree strategiche, tra cui, a titolo esemplificativo, il perimetro, le porte dell'edificio del data center e le aree di carico e scarico merci. Il personale addetto alla sicurezza in loco gestisce le apparecchiature di monitoraggio, registrazione e controllo CCTV. Cavi sicuri in tutto il data center collegano le apparecchiature CCTV. Le telecamere registrano in loco tramite videoregistratori digitali 24 ore su 24, 7 giorni su 7. Le registrazioni di sorveglianza vengono conservate per un massimo di 30 giorni, a seconda dell'attività.

(b) Controllo degli accessi.

Personale addetto alla sicurezza dell'infrastruttura . Google adotta e mantiene una politica di sicurezza per il proprio personale e richiede una formazione in materia di sicurezza come parte integrante del pacchetto formativo. Il personale addetto alla sicurezza dell'infrastruttura di Google è responsabile del monitoraggio continuo dell'infrastruttura di sicurezza di Google, della revisione dei Servizi e della gestione degli incidenti di sicurezza.

Controllo degli accessi e gestione dei privilegi . Gli amministratori del cliente e gli utenti finali devono autenticarsi tramite un sistema di autenticazione centralizzato o tramite un sistema di single sign-on per poter utilizzare i Servizi.

Processi e politiche interne di accesso ai dati – Politica di accesso . I processi e le politiche interne di accesso ai dati di Google sono progettati per impedire a persone e/o sistemi non autorizzati di accedere ai sistemi utilizzati per elaborare i Dati del Cliente. Google progetta i suoi sistemi in modo da (i) consentire solo alle persone autorizzate di accedere ai dati a cui sono autorizzate ad accedere; e (ii) garantire che i Dati del Cliente non possano essere letti, copiati, modificati o rimossi senza autorizzazione durante l'elaborazione, l'utilizzo e dopo la registrazione. I sistemi sono progettati per rilevare qualsiasi accesso improprio. Google utilizza un sistema centralizzato di gestione degli accessi per controllare l'accesso del personale ai server di produzione e fornisce l'accesso solo a un numero limitato di personale autorizzato. I sistemi di autenticazione e autorizzazione di Google utilizzano certificati SSH e chiavi di sicurezza e sono progettati per fornire a Google meccanismi di accesso sicuri e flessibili. Questi meccanismi sono progettati per concedere solo diritti di accesso approvati a host del sito, log, dati e informazioni di configurazione. Google richiede l'uso di ID utente univoci, password complesse, autenticazione a due fattori ed elenchi di accesso attentamente monitorati per ridurre al minimo il potenziale utilizzo non autorizzato dell'account. La concessione o la modifica dei diritti di accesso si basa su: l'autorizzazione Le responsabilità lavorative del personale; i requisiti delle mansioni necessarie per svolgere i compiti autorizzati; e il principio della necessità di conoscere. La concessione o la modifica dei diritti di accesso deve inoltre essere conforme alle politiche interne di Google in materia di accesso ai dati e alla relativa formazione. Le approvazioni sono gestite da strumenti di workflow che mantengono registri di controllo di tutte le modifiche. L'accesso ai sistemi viene registrato per creare una traccia di controllo a fini di responsabilità. Laddove vengano utilizzate password per l'autenticazione (ad esempio, l'accesso alle workstation), vengono implementate politiche relative alle password che seguono almeno gli standard di settore. Questi standard includono restrizioni sul riutilizzo delle password e requisiti di robustezza sufficienti. Per l'accesso a informazioni estremamente sensibili (ad esempio, i dati delle carte di credito), Google utilizza token hardware.

3. Dati

(a) *Archiviazione, isolamento e registrazione dei dati* . Google archivia i dati in un ambiente multi-tenant su server di proprietà di Google. Salvo diversa indicazione (ad esempio, tramite la selezione della posizione dei dati), Google replica i Dati del Cliente tra più data center geograficamente distribuiti. Google isola inoltre logicamente i Dati del Cliente e, per Google Workspace e Cloud Identity: (i) Google separa logicamente i dati di ciascun Utente finale dai dati degli altri Utenti finali; e (ii) i dati di un Utente finale autenticato non saranno visualizzati da un altro Utente finale (a meno che il precedente Utente finale o un Amministratore non consenta la condivisione dei dati). Il Cliente avrà il controllo su specifiche politiche di condivisione dei dati. Tali politiche, in conformità con le funzionalità dei Servizi, consentiranno al Cliente di determinare le impostazioni di condivisione del prodotto applicabili ai propri Utenti finali per scopi specifici. Il Cliente può scegliere di utilizzare le funzionalità di registrazione che Google mette a disposizione tramite i Servizi.

(b) *Dischi dismessi e politica di cancellazione dei dischi* . I dischi contenenti dati possono presentare problemi di prestazioni, errori o guasti hardware che ne comportano la dismissione ("Disco dismesso"). Ogni Disco dismesso è soggetto a una serie di processi di distruzione dei dati (la "Politica di cancellazione dei dischi") prima di lasciare i locali di Google per il riutilizzo o la distruzione. I Dischi dismessi vengono cancellati con un processo in più fasi e la loro completa esecuzione viene verificata da almeno due validatori indipendenti. I risultati della cancellazione vengono registrati tramite il numero di serie del Disco dismesso per consentirne il tracciamento. Infine, il Disco dismesso cancellato viene inserito nell'inventario per il riutilizzo e la ridistribuzione. Se, a causa di un guasto hardware, il Disco dismesso non può essere cancellato, viene conservato in modo sicuro fino a quando non può essere distrutto. Ogni struttura viene sottoposta a verifiche periodiche per monitorare la conformità con la Politica di cancellazione dei dischi.

4. Sicurezza del personale

Il personale di Google è tenuto a comportarsi in modo coerente con le linee guida aziendali in materia di riservatezza, etica aziendale, uso appropriato e standard professionali. Google effettua controlli sui precedenti, nei limiti consentiti dalla legge e in conformità con le leggi sul lavoro e i regolamenti locali applicabili.

Il personale è tenuto a sottoscrivere un accordo di riservatezza e a confermare di aver ricevuto e di rispettare le norme di Google in materia di riservatezza e privacy. Il personale riceve una formazione sulla sicurezza. Il personale che gestisce i Dati dei Clienti è tenuto a soddisfare ulteriori requisiti appropriati al proprio ruolo (ad esempio, certificazioni). Il personale di Google non tratterà i Dati dei Clienti senza autorizzazione.

5. Sicurezza del sottoprocessore

Prima di integrare i subappaltatori, Google effettua un audit delle loro pratiche di sicurezza e privacy per garantire che forniscano un livello di sicurezza e privacy adeguato al loro accesso ai dati e alla portata dei servizi che sono incaricati di fornire. Una volta valutati i rischi presentati dal subappaltatore, nel rispetto dei requisiti descritti nella Sezione 11.3 (Requisiti per l'ingaggio dei subappaltatori) del presente Addendum, il subappaltatore è tenuto a stipulare contratti con termini appropriati in materia di sicurezza, riservatezza e privacy.

Versioni precedenti dei Termini relativi al trattamento e alla sicurezza dei dati:

30 giugno 2022 24 settembre 2021 19 agosto 2020 10 agosto 2020 17 luglio 2020 11 ottobre 2019 1 ottobre 2019 25 maggio 2018 13 marzo 2018 9 novembre 2017 11 ottobre 2017 7 febbraio 2017 6 ottobre 2016

Versioni precedenti della modifica relativa al trattamento dei dati:

7 luglio 2022 24 settembre 2021 27 maggio 2021 29 ottobre 2019 25 maggio 2018 25 aprile 2018 11 luglio 2017 28 novembre 2016 7 gennaio 2016 24 aprile 2015 1 aprile 2014 14 novembre 2012

(Ultimo aggiornamento: 20 settembre 2022)