{% include '_facet/_init.html' con path='/terms/data-processing-addendum' %} {% include '_chat/_init.html' con bricks_path='/terms/data-processing-addendum' %} {% dynamic setvar bricks_experiment %}true{% dynamic endsetvar %}

- Torna alla directory dei termini di Google Cloud
- >
- Attuale

Appendice sull'elaborazione dei dati cloud (clienti)

La presente Appendice sul trattamento dei dati nella cloud, comprese le sue appendici (" *Appendice* "), è incorporata nei Contratti in base ai quali Google ha accettato di fornire Google Cloud Platform, Google Workspace o Cloud Identity (ciascuno come definito di seguito), a seconda dei casi (i " *Servizi* "), al Cliente. Questa Appendice era precedentemente nota come "Termini per l'elaborazione e la sicurezza dei dati" ai sensi di un Contratto per Google Cloud Platform e "Emendamento per l'elaborazione dei dati" ai sensi di un Contratto per Google Workspace o Cloud Identity.

1. Inizio

Il presente Addendum entrerà in vigore e sostituirà tutti i termini precedentemente applicabili al trattamento dei Dati del cliente, inclusi eventuali Termini per l'elaborazione e la sicurezza dei dati o l'Emendamento sull'elaborazione 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 nel Contratto:

- *Account* ha il significato indicato nel Contratto applicabile o, in mancanza di tale significato, indica l'account Google Cloud Platform, l'account Google Workspace o l'account Cloud Identity del Cliente, a seconda dei casi.
- *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.
- *Controlli di sicurezza aggiuntivi* indica le risorse, le caratteristiche, le funzionalità e/o i controlli di sicurezza che il Cliente può utilizzare a sua discrezione e/o come determina, tra cui Admin Console, crittografia, registrazione e monitoraggio, gestione di identità e accessi, scansione di sicurezza e firewall.
- *Paese adeguato* significa:

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

  (c) per i dati trattati soggetti al FDPA svizzero: la Svizzera, o un paese o territorio che è: (i) incluso nell'elenco degli Stati la cui legislazione garantisce una protezione adeguata, come pubblicato dal Commissario federale svizzero per la protezione dei dati e la protezione dei dati, o (ii) riconosciuta come garante di una protezione adeguata dal Consiglio federale svizzero ai sensi del FDPA svizzero;

in ogni caso, se non sulla base di un quadro facoltativo di protezione dei dati.

- *Soluzione di trasferimento alternativo* indica una soluzione, diversa dalle SCC, che consente il trasferimento legale di dati personali a un paese terzo in conformità con la normativa europea sulla protezione dei dati, ad esempio un quadro di protezione dei dati riconosciuto per garantire che le entità partecipanti forniscano una protezione adeguata.

- *Servizi controllati* indica i Servizi correnti indicati come rientranti nell'ambito della relativa certificazione o relazione all'indirizzo https://cloud.google.com/security/compliance/services-in-scope . Google non può rimuovere un Servizio Cloud da questo URL a meno che tale Servizio Cloud non sia stato interrotto in conformità con il Contratto applicabile.

- *Cloud Identity* indica i Servizi Cloud Identity descritti all'indirizzo https://cloud.google.com/terms/identity/user-features , se acquistati ai sensi di un Contratto autonomo.

- *Dati del cliente* ha il significato indicato nel Contratto applicabile o, in mancanza di tale significato, significa:

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

  (b) dati inviati, archiviati, inviati o ricevuti da o per conto del Cliente o dei suoi Utenti finali tramite Google Workspace o Cloud Identity nell'Account.

- *Dati personali del cliente* indica i dati personali contenuti nei Dati del cliente, incluse eventuali categorie speciali di dati personali definite dalla Legge europea sulla protezione dei dati.

- *SCC del cliente* indica le SCC (da titolare a responsabile), le SCC (da processore a responsabile) e/o le SCC (da processore a titolare), a seconda dei casi.

- *Incidente* con i dati indica una violazione della sicurezza di Google che comporta accidentalmente o illecitamente la distruzione, la perdita, l'alterazione, la divulgazione non autorizzata o l'accesso ai Dati del cliente su sistemi gestiti o altrimenti controllati da Google.

- *SEE* indica lo Spazio economico europeo.

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

- *GDPR UE* indica 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.

- *Legge europea sulla protezione dei dati* indica, a seconda dei casi: (a) il GDPR; e/o (b) il FDPA svizzero.

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

- *Google Cloud Platform* indica i servizi di Google Cloud Platform descritti su https://cloud.google.com/terms/services , escluse le Offerte di terze parti.

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

- *Revisore di terze parti* di Google indica un revisore di terze parti nominato da Google, qualificato e indipendente, la cui identità attuale Google comunicherà al Cliente.

- *Istruzioni* ha il significato indicato nella Sezione 5.2.1 (Conformità alle istruzioni del cliente).
- *Legge sulla protezione dei dati non europea* indica le leggi sulla protezione dei dati o sulla privacy in vigore al di fuori del SEE, del Regno Unito e della Svizzera.
- *Indirizzo email di notifica* indica l'indirizzo o gli indirizzi email designati dal Cliente nella Console di amministrazione o nel Modulo d'ordine per ricevere determinate notifiche da Google. Il Cliente è responsabile dell'utilizzo della Console di amministrazione per garantire che il proprio indirizzo e-mail di notifica rimanga aggiornato e valido.
- *SCC* indica le SCC del cliente e/o le SCC (da responsabile a responsabile, esportatore di Google), a seconda dei casi.
- *SCC (Controller-to-Processor)* indica i termini all'indirizzo: https://cloud.google.com/terms/sccs/eu-c2p
- *SCC (Processor-to-Controller)* indica i termini all'indirizzo: https://cloud.google.com/terms/sccs/eu-p2c
- *SCC (Processor-to-Processor)* indica i termini disponibili all'indirizzo: https://cloud.google.com/terms/sccs/eu-p2p
- *SCC (Processor-to-Processor, Google Exporter)* indica i termini disponibili all'indirizzo: https://cloud.google.com/terms/sccs/eu-p2p-google-exporter
- *Documentazione sulla sicurezza* indica tutti i documenti e le informazioni resi disponibili da Google ai sensi della Sezione 7.5.1 (Revisioni della documentazione sulla sicurezza).
- *Misure di sicurezza* ha il significato indicato nella Sezione 7.1.1 (Misure di sicurezza di Google).
- *Sub* -responsabile indica una terza parte autorizzata come altro responsabile ai sensi del presente Addendum ad avere accesso logico ed elaborare i Dati del cliente al fine di fornire parti dei Servizi e TSS.
- *Autorità di controllo* indica, 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 nell'FDPA svizzero.
- *LFD svizzero* indica la legge federale sulla protezione dei dati del 19 giugno 1992 (Svizzera).
- *Durata* indica il periodo dalla Data di entrata in vigore dell'Appendice fino al termine della fornitura dei Servizi da parte di Google, incluso, se applicabile, qualsiasi periodo durante il quale la fornitura dei Servizi può essere sospesa e qualsiasi periodo successivo alla cessazione durante il quale Google può continuare a fornire i Servizi per finalità transitorie.
- *GDPR del Regno Unito* indica il GDPR dell'UE come modificato e incorporato nella legge del Regno Unito ai sensi dell'UK European Union (Withdrawal) Act 2018 e della legislazione secondaria applicabile adottata ai sensi di tale legge.

2.2 I termini "dati personali", "interessato", "trattamento", "titolare del trattamento" e "responsabile del trattamento" utilizzati nel presente Addendum hanno i significati indicati nel GDPR indipendentemente dal fatto che si tratti di diritto europeo sulla protezione dei dati o non -Si applica la legge europea sulla protezione dei dati.

3. Durata

Indipendentemente dal fatto che il Contratto applicabile sia stato risolto o scaduto, la presente Appendice rimarrà in vigore fino a quando, e scadrà automaticamente, quando Google eliminerà tutti i Dati del Cliente come descritto nella presente Appendice.

4. Ambito di applicazione della legge sulla protezione dei dati

4.1 *Applicazione del diritto europeo* . Le parti riconoscono che la legge europea sulla protezione dei dati si applicherà al trattamento dei dati personali del cliente se, ad esempio:

un. il trattamento viene effettuato nell'ambito delle attività di uno stabilimento del Cliente nel territorio del SEE o del Regno Unito; e/o

b. i Dati personali del cliente sono dati personali relativi a interessati che si trovano nel SEE o nel Regno Unito e il trattamento riguarda l'offerta loro di beni o servizi nel SEE o nel Regno Unito, o il monitoraggio del loro comportamento nel SEE o nel Regno Unito UK.

4.2 *Applicazione del diritto extraeuropeo* . Le parti riconoscono che al trattamento dei dati personali dei clienti può applicarsi anche la normativa sulla protezione dei dati non europea.

4.3 *Applicazione dell'Addendum* . Salvo nella misura in cui il presente Addendum stabilisca diversamente, il presente Addendum si applicherà indipendentemente dal fatto che al trattamento dei Dati personali del cliente si applichi la Legge europea sulla protezione dei dati o la Legge non europea sulla protezione dei dati.

5. Trattamento dei dati

5.1 *Ruoli e compliance normativa; Autorizzazione* .

5.1.1 *Responsabilità del responsabile e del controllore* . Se la legge europea sulla protezione dei dati si applica al trattamento dei dati personali del cliente:

un. l'oggetto e i dettagli del trattamento sono descritti nell'Appendice 1;

b. Google è un responsabile del trattamento dei Dati personali del Cliente ai sensi della Legge europea sulla protezione dei dati;

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

d. ciascuna parte rispetterà gli obblighi ad essa applicabili ai sensi della Legge europea sulla protezione dei dati in relazione al trattamento dei Dati personali del Cliente.

5.1.2 *Clienti responsabili del trattamento* . Se la legge europea sulla protezione dei dati si applica al trattamento dei dati personali del cliente e il cliente è un responsabile del trattamento:

un. Il Cliente garantisce su base continuativa che il titolare del trattamento pertinente ha autorizzato: (i) le Istruzioni, (ii) la nomina di Google da parte del Cliente come altro responsabile del trattamento e (iii) l'ingaggio di Sub-responsabili da parte di Google come descritto nella Sezione 11 (sub-responsabili);

b. Il Cliente inoltrerà immediatamente al titolare del trattamento pertinente qualsiasi avviso fornito da Google ai sensi delle Sezioni 5.2.2 (Notifiche di istruzione), 7.2.1 (Notifica di incidente), 9.2.1 (Responsabilità per le richieste), 11.4 (Opportunità di opporsi alle modifiche del Sub-responsabile) o che si riferisce a eventuali SCC; e

c. Il cliente può:

io. richiedere l'accesso del titolare del trattamento ai rapporti SOC in conformità alla sezione 7.5.3(a); e

ii. mettere a disposizione del titolare del trattamento pertinente 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 sub-responsabili).

5.1.3 *Responsabilità di diritto extra europeo.* Se al trattamento dei Dati personali del cliente da parte di una delle parti si applica una legge sulla protezione dei dati non europea, la parte interessata rispetterà tutti gli obblighi ad essa applicabili ai sensi di tale legge 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 ordina a Google di elaborare i Dati del cliente in conformità con il Contratto applicabile (incluso il presente Addendum) e solo con la legge applicabile: (a) per fornire, proteggere e monitorare i Servizi e il TSS; e (b) come ulteriormente specificato tramite (i) l'utilizzo dei Servizi da parte del Cliente (inclusa la Console di amministrazione e altre funzionalità dei Servizi) e TSS, e (ii) qualsiasi altra istruzione scritta fornita dal Cliente e riconosciuta da Google come istruzioni costitutive ai sensi del presente Addendum (collettivamente, le " *Istruzioni*â€). Google rispetterà le Istruzioni a meno che non sia proibito dalla legge europea.

5.2.2 *Notifiche istruzioni* . Fatti salvi gli obblighi di Google ai sensi della Sezione 5.2.1 (Conformità alle istruzioni del Cliente) o qualsiasi altro diritto o obbligo di una delle parti ai sensi del Contratto applicabile, Google informerà immediatamente il Cliente se, secondo Google: (a) il diritto europeo vieta a Google di rispettare un'istruzione; (b) un'istruzione non è conforme alla normativa europea sulla protezione dei dati; o (c) Google non sia in altro modo in grado di rispettare un'Istruzione, in ogni caso a meno che tale avviso non sia proibito dalla Legge europea.

5.3 *Prodotti aggiuntivi* . Se Google, a sua discrezione, mette a disposizione del Cliente Prodotti aggiuntivi da utilizzare con Google Workspace o Cloud Identity in conformità con i Termini dei prodotti aggiuntivi applicabili:

un. Il Cliente può abilitare o disabilitare Prodotti aggiuntivi tramite la Console di amministrazione e non sarà necessario utilizzare Prodotti aggiuntivi per utilizzare Google Workspace o Cloud Identity; e

b. se il Cliente sceglie di installare eventuali Prodotti aggiuntivi o di utilizzarli con Google Workspace o Cloud Identity, i Prodotti aggiuntivi possono accedere ai Dati del cliente come richiesto per l'interoperabilità con Google Workspace o Cloud Identity (se applicabile).

Per chiarezza, 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 a o da tali Prodotti aggiuntivi.

6. Cancellazione dei dati

6.1 *Cancellazione da parte del Cliente* . Google consentirà al Cliente di eliminare i Dati del cliente durante il Periodo di validità in modo coerente con la funzionalità dei Servizi. Se il Cliente utilizza i Servizi per eliminare i Dati del cliente durante il Periodo di validità e tali Dati del cliente non possono essere recuperati dal Cliente, tale utilizzo costituirà un'istruzione a Google per eliminare i Dati del cliente pertinenti dai sistemi di Google in conformità con la legge applicabile. Google rispetterà queste istruzioni non appena ragionevolmente possibile ed entro un periodo massimo di 180 giorni, a meno che la legge europea non richieda l'archiviazione.

6.2 *Restituzione o cancellazione al termine del periodo*. Se il Cliente desidera conservare i Dati del cliente dopo la scadenza del Periodo di validità, può richiedere a Google in conformità con la Sezione 9.1 (Accesso; Rettifica; Trattamento limitato; Portabilità) di restituire tali dati durante il Periodo di validità. Ai sensi della Sezione 6.3 (Istruzioni per l'eliminazione differita), il Cliente richiede a Google di eliminare tutti i restanti Dati del cliente (comprese le copie esistenti) dai sistemi di Google alla fine del Periodo di validità in conformità con la legge applicabile. Dopo un periodo di recupero fino a 30 giorni da tale data,

6.3. *Istruzione di cancellazione differita* . Nella misura in cui vengono elaborati anche i Dati del cliente coperti dalle istruzioni di cancellazione descritte nella Sezione 6.2 (Restituzione o cancellazione al termine del periodo), quando scade il Periodo applicabile ai sensi della Sezione 6.2, in relazione a un Contratto con un Periodo continuativo, tale istruzione di cancellazione sarà entrano in vigore in relazione a tali Dati del

Cliente solo alla scadenza del Periodo di validità. Per chiarezza, la presente Appendice continuerà ad applicarsi a tali Dati del cliente fino alla loro eliminazione 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 o accidentali, come descritto nell'Appendice 2 (le " *Misure di sicurezza*â€). Le misure di sicurezza includono misure per crittografare i dati del cliente; contribuire a garantire la riservatezza, l'integrità, la disponibilità e la resilienza costanti dei sistemi e dei servizi di Google; per aiutare a ripristinare l'accesso tempestivo ai dati del cliente a seguito di un incidente; e per test regolari di efficacia. Google può aggiornare periodicamente le Misure di sicurezza, a condizione che tali aggiornamenti non comportino una riduzione sostanziale della sicurezza dei Servizi.

7.1.2 *Accesso e conformità* . Google: (a) autorizzerà i propri dipendenti, appaltatori e Sub-responsabili ad accedere ai Dati del Cliente solo nella misura strettamente necessaria per rispettare le Istruzioni; (b) adottare le misure appropriate per garantire il rispetto delle Misure di sicurezza da parte dei propri dipendenti, appaltatori e Subincaricati nella misura applicabile al loro ambito di prestazione; 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 metterà a disposizione 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 per la sicurezza di Google* . Google assisterà il Cliente (tenendo conto della natura del trattamento dei Dati personali del Cliente e delle informazioni a sua disposizione) (tenendo conto della natura del trattamento dei Dati personali del cliente) nell'assicurare il rispetto dei propri obblighi (o, se il Cliente è un responsabile del trattamento, del relativo titolare del trattamento) ai sensi degli Articoli da 32 a 34 del GDPR, tramite:

un. 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 con la Sezione 7.1.3 (Controlli di sicurezza aggiuntivi);

c. rispettare i termini della Sezione 7.2 (Incidenti relativi ai dati);

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

e. se le sottosezioni (a)-(d) di cui sopra non sono sufficienti per consentire al Cliente (o al responsabile del trattamento) di adempiere a tali obblighi, su richiesta del Cliente, fornendo al Cliente ulteriore ragionevole cooperazione e assistenza.

7.2 *Incidenti relativi ai dati* .

7.2.1 *Notifica di incidente* . Google informerà il Cliente tempestivamente e senza indebito ritardo dopo essere venuta a conoscenza di un Incidente con i dati e adotterà tempestivamente 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 con i dati descriverà: la natura dell'incidente con i dati, comprese le risorse del cliente interessate; le misure che Google ha adottato, o prevede di adottare, per affrontare l'Incidente con i dati e mitigarne il potenziale rischio; le eventuali misure che Google consiglia al Cliente di adottare per affrontare l'Incidente con i dati; e i dettagli di

un punto di contatto dove è possibile ottenere maggiori informazioni. Se non è possibile fornire tutte queste informazioni contemporaneamente,

7.2.3 *Consegna della notifica* . Le notifiche di qualsiasi incidente relativo ai dati verranno consegnate all'indirizzo e-mail di notifica.

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

7.2.5 Mancato *riconoscimento della colpa da parte di Google* . La notifica o la risposta di Google a un incidente con i dati ai sensi della presente Sezione 7.2 (incidenti con i dati) non sarà interpretata come un riconoscimento da parte di Google di eventuali colpe o responsabilità in relazione all'incidente con i dati.

7.3 *Responsabilità e valutazione della sicurezza del cliente* .

7.3.1 *Responsabilità in materia di sicurezza del Cliente* . Fatti salvi gli obblighi di Google ai sensi delle Sezioni 7.1 (Misure di sicurezza, controlli e assistenza di Google) e 7.2 (Interventi relativi ai dati) e altrove nel Contratto applicabile, il Cliente è responsabile dell'utilizzo dei Servizi e dell'archiviazione di eventuali copie dei Dati del cliente al di fuori dei sistemi di Google o dei Sub-responsabili di Google, tra cui:

un. 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 propri 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 gestite 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 di l'arte, i costi di attuazione e la natura, l'ambito, il contesto e le finalità del trattamento dei dati personali del cliente, nonché i rischi per le persone).

7.4 *Certificazioni di conformità e report SOC* . Google manterrà almeno quanto segue per i Servizi controllati al fine di valutare la continua efficacia delle Misure di sicurezza: (a) certificati per ISO 27001, ISO 27017 e ISO 27018 e, per Google Cloud Platform, un attestato di conformità PCI DSS (le " *Certificazioni di Conformità* "); e (b) rapporti SOC 2 e SOC 3 prodotti dal revisore di terze parti di Google e aggiornati annualmente sulla base di un controllo eseguito almeno una volta ogni 12 mesi (i " *Rapporti SOC*â€). 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 audit di conformità* .

7.5.1 *Revisioni della documentazione sulla sicurezza* . Google metterà a disposizione del Cliente le Certificazioni di conformità e i Rapporti SOC affinché possano essere esaminati dal Cliente per dimostrare la conformità di Google ai propri obblighi ai sensi della presente Appendice.

7.5.2 *Diritti di verifica del cliente* .

un. Se al trattamento dei Dati personali del Cliente si applica la Legge europea sulla protezione dei dati, Google consentirà al Cliente o a un revisore indipendente nominato dal Cliente di condurre controlli (comprese ispezioni) per verificare il rispetto da parte di Google dei suoi obblighi ai sensi della presente Appendice in conformità con la Sezione 7.5 .3 (Condizioni commerciali aggiuntive per revisioni e controlli). Durante un controllo, Google metterà a disposizione tutte le informazioni necessarie per dimostrare tale conformità e contribuirà al controllo come descritto nella Sezione 7.4 (Certificazioni di conformità e rapporti SOC) e nella presente Sezione 7.

b. Se si applicano le SCC 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 controlli come descritto in tali SCC e, durante un controllo, renderà disponibili tutte le informazioni richieste da tali SCC , entrambi in conformità con la Sezione 7.5.3 (Termini commerciali aggiuntivi per revisioni e controlli).

c. Il Cliente può condurre un controllo per verificare la conformità di Google ai propri obblighi ai sensi del presente Addendum esaminando la Documentazione sulla sicurezza (che riflette l'esito dei controlli condotti dal revisore di terze parti di Google).

7.5.3 *Condizioni commerciali aggiuntive per revisioni e audit* .

un. 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 audit ai sensi della Sezione 7.5.2(a) o 7.5.2(b), a Google s Cloud Data Protection Team come descritto nella Sezione 12 (Cloud Data Protection Team; Processing Records).

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 SOC 2 rapporto ai sensi della Sezione 5.1.2(c)(i) o 7.5.1; e (ii) la ragionevole data di inizio, l'ambito e la durata dei controlli di sicurezza e riservatezza applicabili a qualsiasi audit ai sensi della Sezione 7.5.2(a) o 7.5.2(b).

c. Google potrebbe addebitare una tariffa (basata sui 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 commissione applicabile e la base del suo calcolo prima di tale verifica. Il Cliente sarà responsabile di eventuali commissioni addebitate da qualsiasi revisore nominato dal Cliente per eseguire tale verifica.

d. Google può opporsi per iscritto a un revisore nominato dal Cliente per condurre qualsiasi controllo ai sensi della Sezione 7.5.2(a) o 7.5.2(b) se il revisore è, secondo ragionevole parere di Google, non adeguatamente qualificato o indipendente, un concorrente di Google, o comunque manifestamente inidoneo. Qualsiasi obiezione di questo tipo da parte di Google richiederà al Cliente di nominare un altro revisore o di condurre il controllo stesso.

8. Valutazioni d'impatto e consultazioni

Google (tenendo conto della natura del trattamento e delle informazioni a sua disposizione) assisterà il Cliente nell'assicurare il rispetto dei propri obblighi (o, se il Cliente è un responsabile del trattamento, del relativo titolare del trattamento) ai sensi degli articoli 35 e 36 del GDPR , di:

un. fornire controlli di sicurezza aggiuntivi in conformità con la Sezione 7.1.3 (Controlli di sicurezza aggiuntivi) e la Documentazione sulla sicurezza in conformità con la Sezione 7.5.1 (Revisioni della Documentazione sulla sicurezza);

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

c. se le sottosezioni (a) e (b) di cui sopra non sono sufficienti per consentire al Cliente (o al responsabile del trattamento) di adempiere a tali obblighi, su richiesta del Cliente, fornendo al Cliente ulteriore ragionevole cooperazione e assistenza.

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

9.1 *Accesso; Rettifica; Trattamento limitato; Portabilità*. Durante il Periodo di validità, Google consentirà al Cliente, in modo coerente con la funzionalità dei Servizi, di accedere, rettificare e limitare l'elaborazione dei Dati del cliente, anche tramite la funzionalità di eliminazione fornita da Google come descritto nella Sezione 6.1 (Eliminazione da parte del Cliente), e per esportare i dati del cliente. Se il Cliente viene a conoscenza del fatto che i Dati personali del Cliente sono imprecisi o obsoleti, il Cliente sarà responsabile dell'utilizzo di tale funzionalità per rettificare o eliminare tali dati, se richiesto dalla Legge europea sulla protezione dei dati applicabile.

9.2 *Richieste degli interessati* .

9.2.1 *Responsabilità per le Richieste* . Durante il Periodo di validità, se il Cloud Data Protection Team di Google riceve una richiesta da un interessato relativa ai Dati personali del Cliente e identifica il Cliente, Google: (a) consiglierà all'interessato di inviare la propria richiesta al Cliente; (b) avvisare tempestivamente il Cliente; e (c) non rispondere altrimenti alla richiesta dell'interessato senza l'autorizzazione del Cliente. Il Cliente sarà responsabile di rispondere a qualsiasi richiesta di questo tipo, incluso, ove necessario, utilizzando la funzionalità dei Servizi.

9.2.2 *Richiesta di assistenza da parte dell'interessato da parte di Google* . Google (tenendo conto della natura del trattamento dei Dati personali del cliente) assisterà il Cliente nell'adempimento dei propri obblighi (o, se il Cliente è un responsabile del trattamento, del relativo titolare del trattamento) ai sensi del Capo III del GDPR per rispondere alle richieste di esercizio i diritti dell'interessato da parte di:

un. fornire controlli di sicurezza aggiuntivi in conformità con la Sezione 7.1.3 (Controlli di sicurezza aggiuntivi);

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

c. se le sottosezioni (a) e (b) di cui sopra non sono sufficienti per consentire al Cliente (o al responsabile del trattamento) di adempiere a tali obblighi, su richiesta del Cliente, fornendo al Cliente ulteriore ragionevole cooperazione e assistenza.

10. Trasferimenti di dati

10.1 *Strutture per l'archiviazione e l'elaborazione dei dati* . Fatti salvi gli impegni sulla posizione dei dati di Google ai sensi dei Termini specifici del servizio e del resto della presente Sezione 10 (Trasferimenti di dati), i Dati del cliente possono essere elaborati in qualsiasi Paese in cui Google o i suoi Sub-responsabili hanno strutture.

10.2 *Trasferimenti europei limitati* . Le parti riconoscono che la Legge europea sulla protezione dei dati non richiede SCC o una soluzione di trasferimento alternativa affinché i Dati personali del cliente vengano elaborati o trasferiti in un Paese adeguato. Se i Dati personali del cliente vengono trasferiti in qualsiasi altro paese e ai trasferimenti si applica la Legge europea sulla protezione dei dati (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* "), quindi:

un. se Google ha adottato una Soluzione di trasferimento alternativa per qualsiasi Trasferimento europeo limitato, Google informerà il Cliente della soluzione pertinente e si assicurerà che tali Trasferimenti europei limitati 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 Limitati, allora:

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

A. le SCC (da responsabile a responsabile, esportatore di Google) si applicheranno in relazione a tali trasferimenti europei limitati da Google ai sub-responsabili; e

B. inoltre, se l'indirizzo di fatturazione del Cliente non si trova in un Paese adeguato, si applicheranno le SCC (da Responsabile a Titolare) (indipendentemente dal fatto che il Cliente sia un titolare e/o responsabile del trattamento) in relazione a tali Trasferimenti europei limitati tra Google e Cliente; o

ii. se l'indirizzo di Google non si trova in un Paese adeguato, si applicheranno le SCC (da titolare a responsabile) e/o le SCC (da responsabile a responsabile) (a seconda che il Cliente sia un titolare e/o responsabile del trattamento) in relazione a tali Trasferimenti europei limitati tra Google e il Cliente.

10.3 *Certificazione da parte di clienti non EMEA* . Se l'indirizzo di fatturazione del Cliente è al di fuori dell'area EMEA e il trattamento dei Dati personali del Cliente è soggetto alla Legge europea sulla protezione dei dati, il Cliente certificherà in quanto tale e identificherà l'autorità di vigilanza competente tramite la Console di amministrazione per Google Cloud Platform o Google Workspace e Cloud Identity, a seconda dei casi.

10.4 *Misure e informazioni supplementari* . Google fornirà al Cliente le informazioni relative ai Trasferimenti limitati in Europa, incluse le informazioni sui Controlli di sicurezza aggiuntivi e altre misure supplementari per proteggere i Dati personali del Cliente:

un. come descritto nella Sezione 7.5.1 (Revisioni della Documentazione sulla Sicurezza);

b. nella documentazione dei Servizi, disponibile su 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 conclude, in base all'uso attuale o previsto dei Servizi, che la Soluzione di trasferimento alternativa e/o le SCC, a seconda dei casi, non forniscono tutele adeguate per i Dati personali del Cliente, il Cliente può risolvere immediatamente l'Accordo applicabile per comodità notificandolo Google.

10.6 *Informazioni sul centro dati* . Le ubicazioni dei data center di Google sono descritte in:

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

b. https://www.google.com/about/datacenters/locations/ per Google Workspace e Cloud Identity.

11. Subincaricati

11.1 *Consenso all'incarico di sub-responsabile* . Il Cliente autorizza specificamente l'incarico come Sub-responsabili di quelle entità divulgate nella Sezione 11.2 (Informazioni sui Sub-responsabili) a partire dalla Data di entrata in vigore dell'Addendum. Inoltre, fatta salva la Sezione 11.4 (Opportunità di opporsi alle modifiche del Sub-responsabile), il Cliente generalmente autorizza l'assunzione di altre terze parti come Sub-responsabili (" *Nuovi Sub-responsabili* ").

11.2 *Informazioni sui sub-responsabili* . I nomi, le sedi e le attività dei sub-responsabili sono descritti all'indirizzo:

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

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

11.3 *Requisiti per l'incarico del subresponsabile* . Nel coinvolgere qualsiasi Sub-responsabile, Google:

un. garantire tramite contratto scritto che:

io. il Sub-responsabile accede e utilizza i Dati del cliente solo nella misura necessaria per adempiere agli obblighi a lui 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 Legge Europea sulla Protezione dei Dati, gli obblighi di protezione dei dati descritti nel presente Addendum (di cui all'Articolo 28(3) del GDPR, se applicabile), sono imposti al Subincaricato; e

b. rimangono pienamente responsabili per tutti gli obblighi subappaltati e per tutti gli atti e le omissioni del Subincaricato.

11.4 *Opportunità di opporsi alle modifiche del subresponsabile* .

un. Quando un Nuovo Sub-responsabile viene assunto durante il Periodo di validità, Google, almeno 30 giorni prima che il Nuovo Sub-responsabile inizi a elaborare i Dati del cliente, informerà il Cliente dell'incarico (inclusi il nome, l'ubicazione e le attività del Nuovo Sub-responsabile).

b. Il Cliente può, entro 90 giorni dalla notifica dell'ingaggio di un Nuovo Sub-responsabile, opporsi risolvendo immediatamente il Contratto applicabile per comodità mediante notifica a Google.

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

12.1 *Team per la protezione dei dati nel cloud* . Il Cloud Data Protection Team 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:

un. su https://support.google.com/cloud/contact/dpo per Google Cloud Platform;

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

c. come descritto nella sezione Avvisi del Contratto applicabile.

12.2 *Record di elaborazione di Google* . Google conserverà la documentazione appropriata delle sue attività di elaborazione come richiesto dal GDPR. Nella misura in cui il GDPR richiede a Google di raccogliere e conservare registrazioni di determinate informazioni relative al Cliente, il Cliente utilizzerà la Console di amministrazione per fornire tali informazioni e mantenerle accurate e aggiornate. Google può mettere tali informazioni a disposizione delle Autorità di controllo se richiesto dal GDPR.

12.3 *Richieste del controllore* . Durante il Periodo di validità, se il Cloud Data Protection Team di Google riceve una richiesta o un'istruzione da una terza parte che si dichiara titolare del trattamento dei Dati personali del Cliente, Google consiglierà alla terza parte di contattare il Cliente.

13. Interpretazione

13.1 *Precedenza* .

un. Nella misura di qualsiasi conflitto o incoerenza tra:

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

ii. eventuali SCC del Cliente (che sono incorporate per riferimento nel presente Addendum) e il resto del Contratto (incluso il presente Addendum), prevarranno le SCC del Cliente.

b. Per chiarezza, se il Cliente ha stipulato più di un Contratto, il presente Addendum modificherà separatamente ciascuno dei Contratti.

13.2 *SCC precedenti nel Regno Unito* . I termini supplementari per i trasferimenti del GDPR del Regno Unito nelle SCC, a partire dal 21 settembre 2022, sostituiranno e risolveranno qualsiasi clausola contrattuale standard approvata ai sensi del GDPR del Regno Unito o del Data Protection Act 2018 e precedentemente stipulata dal Cliente e da Google.

13.3 *Divieto di modifica delle SCC* . Nulla nell'Accordo (incluso il presente Addendum) è inteso a modificare o contraddire qualsiasi SCC o pregiudicare i diritti o le libertà fondamentali degli interessati ai sensi della Legge europea sulla protezione dei dati.

Appendice 1: Oggetto e dettagli del trattamento dei dati

Argomento

La fornitura da parte di Google dei Servizi e dei TSS al Cliente.

Durata del Trattamento

La Durata più il periodo dalla fine della Durata fino all'eliminazione di tutti i Dati del cliente da parte di Google in conformità con la presente Appendice.

Natura e finalità del trattamento

Google elaborerà i Dati personali del Cliente allo scopo di fornire i Servizi e i TSS al Cliente in conformità con la presente Appendice.

Categorie di dati

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

Interessati

Gli interessati includono le persone i cui dati vengono forniti a Google tramite i Servizi dal (o su indicazione del) Cliente o dai suoi Utenti finali.

Appendice 2: Misure di sicurezza

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

1. Data Center e sicurezza della rete

(a) Data Center.

Infrastrutture . Google gestisce data center distribuiti geograficamente. Google memorizza tutti i dati di produzione in data center fisicamente sicuri.

Ridondanza. I sistemi infrastrutturali sono stati progettati per eliminare i singoli punti di errore e ridurre al minimo l'impatto dei rischi ambientali previsti. Doppi circuiti, interruttori, reti o altri dispositivi necessari aiutano 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 attrezzature e le strutture ambientali hanno procedure di manutenzione preventiva documentate che dettagliano il processo e la frequenza delle prestazioni in conformità con le specifiche interne o del produttore.

Energia. I sistemi di alimentazione elettrica del data center sono progettati per essere ridondanti e manutenibili senza impatto sulle operazioni continue, 24 ore al giorno, 7 giorni alla settimana. Nella maggior parte dei casi, viene fornita una fonte di alimentazione primaria e alternativa, ciascuna con la stessa capacità, per i componenti dell'infrastruttura critica nel data center. L'alimentazione di backup è fornita da vari meccanismi come le batterie UPS (Uninterruptible Power Supply), che forniscono una protezione dell'alimentazione costantemente affidabile durante interruzioni di servizio, blackout, sovratensione, sottotensione e condizioni di frequenza fuori tolleranza. Se l'alimentazione di rete viene interrotta, l'alimentazione di backup è progettata per fornire alimentazione transitoria al data center, a piena capacità, per un massimo di 10 minuti fino a quando i sistemi del generatore di backup non subentrano. I generatori di backup sono in grado di avviarsi automaticamente in pochi secondi per fornire energia elettrica di emergenza sufficiente per far funzionare il data center a piena capacità, in genere per un periodo di giorni.

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

Continuità delle imprese . Google ha progettato e pianifica e testa regolarmente i propri programmi di pianificazione della continuità aziendale/ripristino di emergenza.

(*b) Reti e trasmissione.*

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

Superficie di attacco esterno . Google utilizza più livelli di dispositivi di rete e rilevamento delle intrusioni per proteggere la sua superficie di attacco esterna. Google prende in considerazione i potenziali vettori di attacco e incorpora tecnologie appositamente progettate nei sistemi rivolti all'esterno.

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

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

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

3. impiegando tecnologie che risolvono automaticamente determinate situazioni di pericolo.

Risposta agli incidenti . Google monitora una varietà di canali di comunicazione per gli incidenti di sicurezza e il personale addetto alla sicurezza di Google reagirà prontamente agli incidenti noti.

Tecnologie di crittografia . Google rende disponibile la crittografia HTTPS (nota anche come connessione SSL o TLS). I server di Google supportano lo scambio di chiavi crittografiche Diffie-Hellman con curva ellittica temporanea firmato con RSA ed ECDSA. Questi metodi Perfect Forward Secrecy (PFS) aiutano a proteggere il traffico e a ridurre al minimo l'impatto di una chiave compromessa o di una svolta crittografica.

2. Controllo degli accessi e del sito

(a) Controlli del sito.

Operazione di sicurezza del data center in loco . I data center di Google mantengono un'operazione di sicurezza in loco responsabile di tutte le funzioni di sicurezza del data center fisico 24 ore al giorno, 7 giorni alla settimana. Il personale delle operazioni di sicurezza in loco monitora le telecamere a circuito chiuso (CCTV) e tutti i sistemi di allarme. Il personale delle operazioni di sicurezza in loco esegue regolarmente pattugliamenti interni ed esterni del data center.

Procedure di accesso al data center. Google mantiene procedure di accesso formali per consentire l'accesso fisico ai data center. I data center sono ospitati in strutture che richiedono l'accesso con chiave elettronica, con allarmi collegati alle operazioni di sicurezza in loco. Tutti i partecipanti al data center sono tenuti a identificarsi e a mostrare un documento d'identità alle operazioni di sicurezza in loco. Solo i dipendenti, gli appaltatori e i visitatori autorizzati possono accedere ai data center. Solo i dipendenti e gli appaltatori autorizzati possono richiedere l'accesso con chiave elettronica a queste strutture. Le richieste di accesso alla chiave della scheda elettronica del data center devono essere effettuate tramite e-mail e richiedono l'approvazione del responsabile del richiedente e del direttore del data center. Tutti gli altri partecipanti che richiedono l'accesso temporaneo al data center devono: (i) ottenere preventivamente l'approvazione da parte dei responsabili del data center per il data center specifico e le aree interne che desiderano visitare; (ii) accedere alle operazioni di sicurezza in loco; e (iii) fare riferimento a un record di accesso al data center approvato che identifichi l'individuo come approvato. e richiedere l'approvazione del responsabile del richiedente e del direttore del data center. Tutti gli altri partecipanti che richiedono l'accesso temporaneo al data center devono: (i) ottenere preventivamente l'approvazione da parte dei responsabili del data center per il data center specifico e le aree interne che desiderano visitare; (ii) accedere alle operazioni di sicurezza in

loco; e (iii) fare riferimento a un record di accesso al data center approvato che identifichi l'individuo come approvato. e richiedere l'approvazione del responsabile del richiedente e del direttore del data center. Tutti gli altri partecipanti che richiedono l'accesso temporaneo al data center devono: (i) ottenere preventivamente l'approvazione da parte dei responsabili del data center per il data center specifico e le aree interne che desiderano visitare; (ii) accedere alle operazioni di sicurezza in loco; e (iii) fare riferimento a un record di accesso al data center approvato che identifichi l'individuo come approvato. (i) ottenere l'approvazione preventiva dai responsabili del data center per lo specifico data center e le aree interne che intendono visitare; (ii) accedere alle operazioni di sicurezza in loco; e (iii) fare riferimento a un record di accesso al data center approvato che identifichi l'individuo come approvato. (i) ottenere l'approvazione preventiva dai responsabili del data center per lo specifico data center e le aree interne che intendono visitare; (ii) accedere alle operazioni di sicurezza in loco; e (iii) fare riferimento a un record di accesso al data center approvato che identifichi l'individuo come approvato.

Dispositivi di sicurezza del data center in loco. I data center di Google utilizzano un sistema di controllo degli accessi a doppia autenticazione collegato a un sistema di allarme. Il sistema di controllo degli accessi monitora e registra la chiave della scheda elettronica di ogni individuo e quando accede alle porte perimetrali, alla spedizione e alla ricezione e ad altre aree critiche. Le attività non autorizzate e i tentativi di accesso non riusciti vengono registrati dal sistema di controllo degli accessi e investigati, a seconda dei casi. L'accesso autorizzato a tutte le operazioni aziendali e ai data center è limitato in base alle zone e alle responsabilità lavorative dell'individuo. Le porte tagliafuoco dei data center sono allarmate. Le telecamere a circuito chiuso sono in funzione sia all'interno che all'esterno dei data center. Il posizionamento delle telecamere è stato progettato per coprire aree strategiche tra cui, tra l'altro, il perimetro, le porte dell'edificio del data center e la spedizione/ricezione. Il personale delle operazioni di sicurezza in loco gestisce le apparecchiature di monitoraggio, registrazione e controllo TVCC. Cavi sicuri in tutti i data center collegano le apparecchiature TVCC. Le telecamere registrano in loco tramite videoregistratori digitali 24 ore al giorno, 7 giorni alla settimana. I registri di sorveglianza vengono conservati per un massimo di 30 giorni in base all'attività.

(b) Controllo degli accessi.

Personale addetto alla sicurezza delle infrastrutture . Google ha e mantiene una politica di sicurezza per il proprio personale e richiede una formazione sulla sicurezza come parte del pacchetto di formazione per il proprio personale. 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 risposta agli incidenti di sicurezza.

Controllo degli accessi e gestione dei privilegi . Gli Amministratori e gli Utenti finali del Cliente devono autenticarsi tramite un sistema di autenticazione centrale o tramite un sistema di single sign on per poter utilizzare i Servizi.

Processi e politiche di accesso ai dati interni - Politica di accesso. I processi e le norme di accesso ai dati interni di Google sono concepiti per impedire a persone e/o sistemi non autorizzati di accedere ai sistemi utilizzati per elaborare i Dati del cliente. Google progetta i propri 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 inappropriato. Google utilizza un sistema di gestione degli accessi centralizzato 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, registri, 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: le responsabilità lavorative del personale autorizzato; requisiti di mansione lavorativa necessari per svolgere compiti autorizzati; e la necessità di conoscere le basi. La concessione o la modifica dei diritti di accesso deve inoltre essere conforme alle norme e alla formazione interne di Google sull'accesso ai dati. Le approvazioni sono gestite da strumenti del flusso di lavoro che mantengono i record di controllo di tutte le modifiche. L'accesso ai sistemi viene registrato per

creare un audit trail per la responsabilità. Laddove le password vengono utilizzate per l'autenticazione (ad es. accesso alle postazioni di lavoro), vengono implementate politiche di password che seguono almeno le pratiche standard del settore. Questi standard includono restrizioni sul riutilizzo della password e una sicurezza sufficiente della password. Per l'accesso a informazioni estremamente sensibili (ad es. i dati della carta 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. Fatte salve istruzioni contrarie (ad es. sotto forma di selezione della posizione dei dati), Google replica i Dati del cliente tra più data center dislocati geograficamente. Google inoltre isola logicamente i Dati del cliente e, per Google Workspace e Cloud Identity: (i) Google separa logicamente i dati di ciascun Utente finale dai dati di altri Utenti finali; e (ii) i dati di un Utente finale autenticato non verranno visualizzati da un altro Utente finale (a meno che l'Utente finale precedente 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 la 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 la funzionalità di registrazione che Google rende disponibile tramite i Servizi.

(b) *Dischi disattivati e politica di cancellazione del disco*. I dischi contenenti dati possono presentare problemi di prestazioni, errori o guasti hardware che li portano a essere disattivati ("Disco disattivato"). Ogni disco disattivato è soggetto a una serie di processi di distruzione dei dati (la "Norma di cancellazione del disco") prima di lasciare la sede di Google per il riutilizzo o la distruzione. I dischi disattivati vengono cancellati in un processo in più passaggi e verificati completi da almeno due validatori indipendenti. I risultati della cancellazione vengono registrati dal numero di serie del disco disattivato per il monitoraggio. Infine, il disco disattivato cancellato viene rilasciato nell'inventario per il riutilizzo e la ridistribuzione. Se, a causa di un guasto hardware, il disco disattivato non può essere cancellato, viene archiviato in modo sicuro fino a quando non può essere distrutto. Ogni struttura viene controllata regolarmente per monitorare la conformità con la politica di cancellazione del disco.

4. Sicurezza del personale

Il personale di Google è tenuto a comportarsi in modo coerente con le linee guida dell'azienda in materia di riservatezza, etica aziendale, uso appropriato e standard professionali. Google conduce controlli dei precedenti ragionevolmente appropriati nella misura consentita dalla legge e in conformità con le leggi sul lavoro locali applicabili e le normative statutarie.

Il personale è tenuto a sottoscrivere un accordo di riservatezza e deve confermare la ricezione e il rispetto delle norme sulla riservatezza e sulla privacy di Google. Il personale riceve formazione sulla sicurezza. Il personale che gestisce i Dati del Cliente è tenuto a completare requisiti aggiuntivi adeguati al proprio ruolo (ad es. certificazioni). Il personale di Google non elaborerà i dati dei clienti senza autorizzazione.

5. Sicurezza del sub-responsabile

Prima dell'onboarding dei Sub-responsabili, Google conduce un controllo delle pratiche di sicurezza e privacy dei Sub-responsabili per garantire che i Sub-responsabili forniscano un livello di sicurezza e privacy adeguato al loro accesso ai dati e all'ambito dei servizi che sono impegnati a fornire. Una volta che Google ha valutato i rischi presentati dal Sub-responsabile, in base ai requisiti descritti nella Sezione 11.3 (Requisiti per l'incarico del Sub-responsabile) del presente Addendum, il Sub-responsabile è tenuto a stipulare termini contrattuali di sicurezza, riservatezza e privacy appropriati.

Versioni precedenti dei Termini per il trattamento e la sicurezza dei dati:

30 giugno 2022 *24 settembre 2021* *19 agosto 2020*