Appendice sull'elaborazione dei dati nel cloud (clienti)

Il presente Addendum sull'elaborazione dei dati nel cloud, comprese le relative appendici (" *Addendum* "), è incorporato 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 â€œServiziâ €), al Cliente. Questo addendum era precedentemente noto come "Termini per l'elaborazione e la sicurezza dei dati" nell'ambito di un Accordo per Google Cloud Platform e "Emendamento sull'elaborazione dei dati" nell'ambito di un Accordo 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 definito di seguito).

2. Definizioni

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

- *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 altrimenti concordato dalle parti, il presente Addendum.
- *Controlli di sicurezza aggiuntivi* significa risorse di sicurezza, caratteristiche, funzionalità e/o controlli che il Cliente può utilizzare a propria discrezione e/o come stabilito, inclusi la Console di amministrazione, la crittografia, la registrazione e il monitoraggio, la gestione dell'identità e dell'accesso, la scansione della sicurezza e i firewall.
- *Paese adeguato* significa:

  (a) per i dati trattati soggetti al GDPR dell'UE: il SEE, o un paese o territorio riconosciuto 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 in grado di garantire 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 DFAE 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 l'informazione, oppure (ii) riconosciuto come un'adeguata protezione dal Consiglio Federale Svizzero nell'ambito dell'LPD;

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

- *Soluzione di trasferimento alternativa* indica una soluzione, diversa dalle SCC, che consente il trasferimento legittimo di dati personali a un paese terzo in conformità con la legge 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 verificati* indica i Servizi in quel momento indicati come rientranti nell'ambito della certificazione o del rapporto pertinente all'indirizzo https://cloud.google.com/security/compliance/services-in-scope . Google non può rimuovere un Servizio Cloud da questo URL a meno che il 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 nell'ambito di un Contratto autonomo.

- *I Dati del Cliente* hanno il significato indicato nell'Accordo applicabile o, in mancanza di tale significato, significano:

  (a) dati forniti da o per conto del Cliente o dei suoi Utenti finali tramite Google Cloud Platform nell'ambito dell'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, comprese eventuali categorie speciali di dati personali definite dalla legge europea sulla protezione dei dati.

- *Per SCC del cliente si* intendono le SCC (da titolare a responsabile del trattamento), le SCC (da responsabile a responsabile del trattamento) e/o le SCC (da responsabile a responsabile del trattamento), a seconda dei casi.

- *Per incidente di dati* si intende una violazione della sicurezza di Google che porta alla distruzione, alla perdita, all'alterazione, alla divulgazione non autorizzata o all'accesso accidentale o illegale ai Dati del cliente su sistemi gestiti o altrimenti controllati da Google.

- *SEE* significa Spazio economico europeo.

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

- *GDPR UE* significa 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 e alla libera circolazione di tali dati, e che abroga la Direttiva 95/ 46/CE.

- *Legge europea sulla protezione dei dati* significa, a seconda dei casi: (a) il GDPR; e/o (b) l'DFAE.

- *Per diritto europeo* si intende, a seconda dei casi: (a) il diritto dell'UE o degli Stati membri dell'UE (se il GDPR dell'UE si applica al trattamento dei Dati personali dei clienti); 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 dei clienti).

- *GDPR* significa, 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 all'indirizzo https://cloud.google.com/terms/services , escluse eventuali 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 rivelerà al Cliente.
- *Istruzioni* ha il significato indicato nella Sezione 5.2.1 (Rispettamento delle Istruzioni del Cliente).
- *Legge non europea sulla protezione dei* dati indica le leggi sulla protezione dei dati o sulla privacy in vigore al di fuori del SEE, del Regno Unito e della Svizzera.
- *Indirizzo e-mail di notifica* indica 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 dell'utilizzo della Console di amministrazione per assicurarsi che il proprio indirizzo e-mail di notifica rimanga aggiornato e valido.
- *SCC* indica le SCC e/o le SCC del Cliente (da Processore a Responsabile, Esportatore Google), a seconda dei casi.
- *SCC (da controller a responsabile del trattamento)* indica i termini su: https://cloud.google.com/terms/sccs/eu-c2p
- *SCC (Processor-to-Controller)* indica i termini su: https://cloud.google.com/terms/sccs/eu-p2c
- *SCC (Processor-to-Processor)* indica i termini su: https://cloud.google.com/terms/sccs/eu-p2p
- *SCC (Processor-to-Processor, Google Exporter)* indica i termini su: https://cloud.google.com/terms/sccs/eu-p2p-google-exporter
- *Documentazione di sicurezza* indica tutti i documenti e le informazioni messi a disposizione da Google ai sensi della Sezione 7.5.1 (Revisioni della documentazione di sicurezza).
- *Misure di sicurezza* ha il significato indicato nella Sezione 7.1.1 (Misure di sicurezza di Google).
- *Subprocessore* indica una terza parte autorizzata come altro responsabile del trattamento 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 vigilanza* indica, a seconda dei casi: (a) un'"autorità di vigilanza" come definita nel GDPR dell'UE; e/o (b) il â€œCommissarioâ€ come definito nel GDPR del Regno Unito e/o nel FDPA svizzero.
- *Swiss DFAE* indica la legge federale sulla protezione dei dati del 19 giugno 1992 (Svizzera).
- *Durata* indica il periodo dalla Data di entrata in vigore dell'Addendum fino alla fine della fornitura dei Servizi da parte di Google, incluso, se applicabile, qualsiasi periodo durante il quale la fornitura dei Servizi potrebbe essere sospesa e qualsiasi periodo successivo alla risoluzione durante il quale Google potrebbe continuare a fornire i Servizi per finalità transitorie.
- *GDPR del Regno Unito* indica il GDPR dell'UE come modificato e incorporato nel diritto del Regno Unito ai sensi della legge sull'Unione europea (Recesso) del Regno Unito del 2018 e la legislazione secondaria applicabile resa ai sensi di tale legge.

2.2 I termini â€œdati personaliâ€ , â€œinteressatoâ€ , â€œtrattamentoâ€ , â€œtitolareâ€ e â€œresponsabile del trattamentoâ€ utilizzati nel presente Addendum hanno i significati attribuiti nel GDPR indipendentemente dal fatto che la Legge Europea 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 terminato o scaduto, il presente Addendum rimarrà in vigore e scadrà automaticamente quando Google eliminerà tutti i Dati del cliente come descritto

nel presente Addendum.

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 dei clienti se, ad esempio:

un. il trattamento è 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 agli interessati che si trovano nel SEE o nel Regno Unito e il trattamento si riferisce all'offerta loro di beni o servizi nel SEE o nel Regno Unito, o al monitoraggio del loro comportamento nel SEE o nel UK.

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

4.3 *Applicazione dell'Addendum* . Salvo ove diversamente indicato nel presente Addendum, il presente Addendum si applicherà indipendentemente dal fatto che al trattamento dei Dati personali dei clienti si applichino la Legge europea sulla protezione dei dati o la Legge non europea sulla protezione dei dati.

5. Trattamento dei dati

5.1 *Ruoli e conformità normativa; Autorizzazione* .

5.1.1 *Responsabilità del Responsabile e del Titolare* . Se la legge europea sulla protezione dei dati si applica al trattamento dei dati personali dei clienti:

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

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

c. Il Cliente è un titolare del trattamento o responsabile del trattamento, a seconda dei casi, dei 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 Processori* . 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 relativo titolare del trattamento ha autorizzato: (i) le Istruzioni, (ii) la nomina di Google da parte del Cliente come altro responsabile del trattamento e (iii) l'assunzione da parte di Google dei Subincaricati del trattamento come descritto nella Sezione 11 (Subincaricati);

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

c. Il cliente può:

io. richiedere l'accesso per il responsabile del trattamento pertinente ai Rapporti SOC in conformità con la Sezione 7.5.3(a); e

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

sui data center) e 11.2 (Informazioni sui sub-responsabili del trattamento).

5.1.3 *Responsabilità ai sensi del diritto non europeo.* Se la legge non europea sulla protezione dei dati si applica al trattamento dei Dati personali del cliente da parte di una delle parti, la parte interessata rispetterà tutti gli obblighi ad essa applicabili ai sensi di tale legge in relazione al trattamento dei Dati personali del cliente.

5.2 *Ambito del trattamento* .

5.2.1 *Rispetto delle Istruzioni del Cliente* . Il Cliente incarica Google di elaborare i Dati del Cliente in conformità con il Contratto applicabile (incluso il presente Addendum) e la legge applicabile esclusivamente: (a) per fornire, proteggere e monitorare i Servizi e 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 TSS, e (ii) qualsiasi altra istruzione scritta fornita dal Cliente e riconosciuta da Google come istruzione costitutiva nel presente Addendum (collettivamente, le " *Istruzioni*â€). Google rispetterà le Istruzioni a meno che non sia vietato dalla legge europea.

5.2.2 *Notifiche di 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) La legge europea vieta a Google di attenersi a un'Istruzione; (b) un'istruzione non è conforme alla legge europea sulla protezione dei dati; o (c) Google non è altrimenti in grado di rispettare un'Istruzione, in ogni caso a meno che tale avviso non sia vietato dalla legge europea.

5.3 *Prodotti aggiuntivi* . Se Google, a sua discrezione, mette a disposizione del Cliente Prodotti aggiuntivi per l'utilizzo con Google Workspace o Cloud Identity in conformità con i Termini per i prodotti aggiuntivi applicabili:

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

b. se il Cliente sceglie di installare qualsiasi Prodotto aggiuntivo o di utilizzarlo con Google Workspace o Cloud Identity, i Prodotti aggiuntivi possono accedere ai Dati del cliente come richiesto per interagire con Google Workspace o Cloud Identity (a seconda dei casi).

Per chiarezza, il presente Addendum non si applica al trattamento dei dati personali in connessione con la fornitura di Prodotti Aggiuntivi installati o utilizzati dal Cliente, compresi i dati personali trasmessi ao 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 la Durata in modo coerente con la funzionalità dei Servizi. Se il Cliente utilizza i Servizi per eliminare i Dati del cliente durante la Durata e tali Dati del cliente non possono essere recuperati dal Cliente, tale utilizzo costituirà un'istruzione per Google di 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 la conservazione.

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

6.3. *Istruzioni per la cancellazione differita* . Nella misura in cui i Dati del cliente coperti dall'istruzione di eliminazione descritta nella Sezione 6.2 (Restituzione o eliminazione alla scadenza del termine) vengono

elaborati, alla scadenza della Durata applicabile di cui alla Sezione 6.2, in relazione a un Accordo con una Durata continua, tale istruzione di eliminazione sarà entrano in vigore in relazione a tali Dati cliente solo alla scadenza del Periodo continuativo. Per chiarezza, il presente Addendum continuerà ad applicarsi a tali Dati del cliente fino alla sua 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 dei clienti; 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 la verifica periodica dell'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: (a) autorizzerà i suoi dipendenti, appaltatori e Sub-incaricati ad accedere ai Dati dei clienti solo se strettamente necessario per conformarsi alle Istruzioni; (b) adottare 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 al trattamento dei Dati del Cliente siano soggette all'obbligo di riservatezza.

7.1.3 *Ulteriori controlli di sicurezza* . 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 per la sicurezza di Google* . 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, del relativo titolare del trattamento) ai sensi degli Articoli 32 a 34 del GDPR, da:

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 sui dati);

d. fornire al Cliente la Documentazione di Sicurezza in conformità con la Sezione 7.5.1 (Revisioni della Documentazione di 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 relativo titolare del trattamento) di ottemperare a tali obblighi, su richiesta del Cliente, fornendo al Cliente ulteriore ragionevole cooperazione e assistenza.

7.2 *Incidenti sui dati* .

7.2.1 *Notifica di incidente* . Google avviserà il Cliente tempestivamente e senza indebito ritardo dopo essere venuto a conoscenza di un Incidente relativo ai dati e adotterà tempestivamente le misure ragionevoli per ridurre al minimo i danni e proteggere i Dati del cliente.

7.2.2 *Dettagli dell'incidente con i dati*. La notifica di Google di 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 far fronte all'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 di dati verranno inviate 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 dei clienti al fine di identificare le 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 sui dati ai sensi della presente Sezione 7.2 (Incidenti sui dati) non sarà interpretata come un riconoscimento da parte di Google di qualsiasi colpa o responsabilità in relazione all'Incidente sui dati.

7.3 *Responsabilità e valutazione della sicurezza del cliente* .

7.3.1 *Responsabilità 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 (Incidenti relativi ai dati) e altrove nel Contratto applicabile, il Cliente è responsabile dell'utilizzo dei Servizi e dell'archiviazione dei qualsiasi copia dei Dati del cliente al di fuori dei sistemi di Google o dei suoi Subincaricati del trattamento, 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 utilizzati dal Cliente per accedere ai Servizi; e

c. eseguire il backup o la conservazione di copie dei propri Dati 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 di l'art, i costi di attuazione e la natura, la portata, il contesto e le finalità del trattamento dei Dati Personali del Cliente nonché i rischi per le persone).

7.4 *Certificazioni di conformità e rapporti SOC* . Google manterrà almeno quanto segue per i Servizi sottoposti a audit 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) i report SOC 2 e SOC 3 prodotti dal revisore dei conti di terze parti di Google e aggiornati annualmente sulla base di un audit eseguito almeno una volta ogni 12 mesi (i " *Report SOC*â€). Google può aggiungere standard in qualsiasi momento. Google può sostituire una certificazione di conformità o un rapporto SOC con un'alternativa equivalente o migliorata.

7.5 *Revisioni e verifiche di conformità* .

7.5.1 *Revisione della documentazione di sicurezza* . Google metterà a disposizione del Cliente le Certificazioni di conformità e i Rapporti SOC per dimostrare la conformità da parte di Google ai propri obblighi ai sensi del presente Addendum.

7.5.2 *Diritti di controllo del cliente* .

un. Se al trattamento dei Dati personali dei clienti si applica la legge europea sulla protezione dei dati, Google consentirà al Cliente o a un revisore indipendente nominato dal Cliente di condurre audit (comprese le ispezioni) per verificare il rispetto da parte di Google degli obblighi ai sensi del presente Addendum in conformità con la Sezione 7.5 .3 (Termini commerciali aggiuntivi per revisioni e audit). Durante un audit, Google metterà a disposizione tutte le informazioni necessarie per dimostrare tale conformità e contribuire all'audit 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 audit come descritto in tali SCC e, durante un audit, renderà disponibili tutte le informazioni richieste da tali SCC , entrambi in conformità con la Sezione 7.5.3 (Termini commerciali aggiuntivi per revisioni e audit).

c. Il Cliente può condurre un audit per verificare la conformità di Google agli obblighi previsti dal presente Addendum esaminando la Documentazione sulla sicurezza (che riflette l'esito degli audit condotti dal revisore di terze parti di Google).

7.5.3 *Termini commerciali aggiuntivi per revisioni e audit* .

un. Il Cliente deve inviare a Google qualsiasi richiesta di revisione del rapporto SOC 2 di cui alla Sezione 5.1.2(c)(i) o 7.5.1, o di audit di cui alla Sezione 7.5.2(a) o 7.5.2(b)' s Team per la protezione dei dati nel cloud come descritto nella Sezione 12 (Team per la protezione dei dati nel cloud; Registri di elaborazione).

b. Dopo la 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: (i) le date ragionevoli e i controlli di sicurezza e riservatezza applicabili a qualsiasi revisione del SOC 2 relazione 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 può addebitare una commissione (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 tariffa applicabile e sulla base del relativo 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 incaricato dal Cliente di condurre qualsiasi revisione ai sensi della Sezione 7.5.2(a) o 7.5.2(b) se il revisore è, secondo la ragionevole opinione di Google, non adeguatamente qualificato o indipendente, un concorrente di Google, o comunque manifestamente non idoneo. Qualsiasi obiezione di questo tipo da parte di Google richiederà al Cliente di nominare un altro revisore dei conti o di condurre l'audit stesso.

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, del relativo titolare) 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 di sicurezza in conformità con la Sezione 7.5.1 (Revisioni della documentazione di 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 relativo titolare del trattamento) di ottemperare 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 la Durata, 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), ed esportare i dati del cliente. Se il Cliente viene a conoscenza 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 dell'Interessato* .

9.2.1 *Responsabilità delle Richieste* . Durante il Periodo, se il team di protezione dei dati cloud di Google riceve una richiesta da un interessato che si riferisce ai Dati personali del cliente e identifica il Cliente, Google: (a) consiglierà all'interessato di presentare la richiesta al Cliente; (b) avvisare tempestivamente il Cliente; e (c) non rispondere in altro modo alla richiesta dell'interessato senza l'autorizzazione del Cliente. Il Cliente sarà responsabile di rispondere a tale richiesta incluso, ove necessario, utilizzando la funzionalità dei Servizi.

9.2.2 *L'interessato di Google richiede assistenza* . Google (tenendo conto della natura del trattamento dei Dati Personali del Cliente) assisterà il Cliente nell'adempimento dei propri obblighi (o, qualora il Cliente sia 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:

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

b. nel rispetto delle Sezioni 9.1 (Accesso; Rettifica; Trattamento limitato; Portabilità) e 9.2.1 (Responsabilità delle Richieste); e

c. se le sottosezioni (a) e (b) di cui sopra non sono sufficienti per consentire al Cliente (o al relativo titolare del trattamento) di ottemperare 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 di Google relativi all'ubicazione dei dati ai sensi dei Termini specifici del servizio e del resto della presente Sezione 10 (Trasferimenti di dati), i Dati dei clienti possono essere elaborati in qualsiasi Paese in cui Google o i suoi Sub-responsabili del trattamento 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 dei clienti possano essere 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'EMEA) (â€œ *Trasferimenti europei limitati* â€), quindi:

un. se Google ha adottato una Soluzione di trasferimento alternativa per eventuali Trasferimenti europei limitati, 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 qualsiasi Trasferimento Europeo Limitato, allora:

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

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

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

ii. se l'indirizzo di Google non è in un Paese adeguato, si applicheranno le SCC (da titolare a responsabile del trattamento) e/o le SCC (da responsabile a responsabile del trattamento) (a seconda che il Cliente sia un titolare del trattamento e/o responsabile del trattamento) per quanto riguarda 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'EMEA e il trattamento dei Dati personali del Cliente è soggetto alla legge europea sulla protezione dei dati, il Cliente certificherà come tale e identificherà la propria 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 europei soggetti a restrizioni, comprese 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 di sicurezza);

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

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

10.5 *Cessazione* . 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 garanzie adeguate per i Dati personali del Cliente, il Cliente può risolvere immediatamente il Contratto applicabile per comodità notificandolo Google.

10.6 *Informazioni sul centro dati* . Le posizioni dei data center di Google sono descritte all'indirizzo:

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 del Subincaricato* . Il Cliente autorizza specificamente l'assunzione in qualità di Sub-responsabili del trattamento di quei soggetti indicati nella Sezione 11.2 (Informazioni sui Sub-responsabili del trattamento) a partire dalla Data di entrata in vigore dell'Addendum. Inoltre, senza pregiudizio della Sezione 11.4 (Opportunità di opporsi alle modifiche del Subresponsabile), il Cliente autorizza generalmente l'assunzione di altre terze parti come Subresponsabili (â€œ *Nuovi Subincaricatiâ* €).

11.2 *Informazioni sui sub-responsabili del trattamento* . Nomi, sedi e attività dei Subincaricati 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 Subincaricato* . Quando si impegna qualsiasi Sub-responsabile del trattamento, Google:

un. assicurare tramite contratto scritto che:

io. il Subincaricato accede e utilizza i Dati del Cliente solo nella misura necessaria per adempiere agli obblighi ad esso 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, paragrafo 3, del GDPR, se applicabile), sono imposti al Sub-responsabile del trattamento; e

b. rimangono pienamente responsabili per tutti gli obblighi subappaltati e per tutti gli atti e le omissioni del Sub-responsabile del trattamento.

11.4 *Opportunità di opporsi alle modifiche del subprocessore* .

un. Quando un nuovo Subresponsabile viene assunto durante la Durata, Google, almeno 30 giorni prima che il Nuovo Subresponsabile inizi a elaborare i Dati del cliente, notificherà al Cliente l'impegno (inclusi il nome, l'ubicazione e le attività del Nuovo Subresponsabile).

b. Il Cliente può, entro 90 giorni dalla notifica dell'assunzione di un Nuovo Sub-responsabile del trattamento, opporsi risolvendo immediatamente il Contratto applicabile per comodità notificandolo 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 team di protezione dei dati cloud di Google fornirà assistenza tempestiva e ragionevole per qualsiasi domanda del cliente relativa all'elaborazione 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 dell'Accordo applicabile.

12.2 *Registri di elaborazione di Google* . Google conserverà un'adeguata documentazione delle proprie attività di trattamento 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 Vigilanza se richiesto dal GDPR.

12.3 *Richieste del Titolare* . Durante il Periodo, se il Team di protezione dei dati cloud 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. presente 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 dell'Accordo (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 ciascuno degli Accordi separatamente.

13.2 *SCC del Regno Unito legacy* . I termini supplementari per i trasferimenti del GDPR nel 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 *Nessuna modifica delle SCC* . Nulla nell'accordo (incluso il presente Addendum) è inteso a modificare o contraddire eventuali 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

Fornitura da parte di Google dei Servizi e del 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 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 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 comprendono le persone per le quali i 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'Addendum, 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 geograficamente distribuiti. 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 doppi, 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 apparecchiature e le strutture ambientali hanno procedure di manutenzione preventiva documentate che descrivono in dettaglio il processo e la frequenza delle prestazioni in conformità con le specifiche interne o del produttore.

Potenza. 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 critici dell'infrastruttura nel data center. L'alimentazione di backup è fornita da vari meccanismi come le batterie dei gruppi di continuità (UPS), che forniscono una protezione dell'alimentazione costantemente affidabile durante le interruzioni di alimentazione, i blackout, le condizioni di sovratensione, sottotensione e 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 prendono il sopravvento. 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 i prodotti di sicurezza negli ambienti di produzione.

Continuità aziendale . Google ha progettato, pianificato e testato regolarmente i suoi 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 o il trasporto elettronico o durante la registrazione su supporti di memorizzazione dei dati. Google trasferisce i dati tramite i protocolli standard di Internet.

Superficie di attacco esterna . Google utilizza più livelli di dispositivi di rete e rilevamento delle intrusioni per proteggere la sua superficie di attacco esterna. Google considera potenziali vettori di attacco e incorpora appropriate tecnologie appositamente progettate nei sistemi di rivestimento esterno.

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

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

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

3. utilizzando tecnologie che risolvono automaticamente determinate situazioni pericolose.

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

Tecnologie di crittografia . Google rende disponibile la crittografia HTTPS (denominata anche connessione SSL o TLS). I server di Google supportano lo scambio di chiavi crittografiche Diffie-Hellman a curva ellittica effimera firmato con RSA ed ECDSA. Questi metodi di 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. Controlli di accesso 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 dei data center fisici 24 ore al giorno, 7 giorni alla settimana. Il personale operativo di sicurezza in loco monitora le telecamere della TV a circuito chiuso (CCTV) e tutti i sistemi di allarme. Il personale addetto alle 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 all'operazione di sicurezza in loco. Tutti i partecipanti al data center devono identificarsi e mostrare una prova di 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 tessera

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 dai gestori 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 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 dai gestori 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 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 dai gestori 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 preventivamente l'approvazione dai gestori dei 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 preventivamente l'approvazione dai gestori dei 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.

Dispositivi di sicurezza del data center in loco. I data center di Google utilizzano un sistema di controllo dell'accesso a doppia autenticazione collegato a un allarme di sistema. Il sistema di controllo accessi monitora e registra la chiave elettronica di ogni individuo e quando accedono alle porte perimetrali, alla spedizione e alla ricezione e ad altre aree critiche. Le attività non autorizzate ei tentativi di accesso non riusciti vengono registrati dal sistema di controllo dell'accesso e analizzati, a seconda dei casi. L'accesso autorizzato in tutte le operazioni aziendali e nei 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 le altre, il perimetro, le porte dell'edificio del data center e la spedizione/ricezione. Il personale addetto alle operazioni di sicurezza in loco gestisce le apparecchiature di monitoraggio, registrazione e controllo CCTV. Cavi sicuri in tutti i data center collegano le apparecchiature TVCC. Le telecamere registrano in loco tramite videoregistratori digitali 24 ore su 24, 7 giorni su 7. I record 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 suo personale e richiede una formazione sulla sicurezza come parte del pacchetto di formazione per il suo 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 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 accesso unico per poter utilizzare i Servizi.

Processi e politiche interne di accesso ai dati - Politica di accesso. Le procedure e le politiche interne di Google per l'accesso ai dati sono progettate per impedire a persone e/o sistemi non autorizzati di accedere ai sistemi utilizzati per elaborare i Dati dei clienti. Google progetta i suoi sistemi per (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, alterati o rimossi senza autorizzazione durante l'elaborazione, l'uso e dopo la registrazione. I sistemi sono progettati per rilevare qualsiasi accesso inappropriato. 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 agli host del sito, ai registri, ai dati e alle 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 di 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 conservano i record di controllo di tutte le modifiche. L'accesso ai sistemi viene registrato per creare una pista di controllo per la responsabilità. Laddove le password vengono utilizzate per l'autenticazione (ad es. accesso alle workstation), vengono implementate politiche di password che seguono almeno le pratiche standard del settore. Questi standard includono restrizioni sul riutilizzo delle password e una sicurezza sufficiente della password. Per l'accesso a informazioni estremamente sensibili (es. dati di 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. Fatte salve eventuali Istruzioni contrarie (ad es. sotto forma di selezione della posizione dei dati), Google replica i Dati del cliente tra più data center geograficamente dislocati. Google isola inoltre logicamente i Dati dei clienti 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 verranno mostrati a un altro Utente finale (a meno che l'ex 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 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 mette a disposizione tramite i Servizi.

(b) *Dischi dismessi e politica di cancellazione del disco*. I dischi contenenti dati potrebbero presentare problemi di prestazioni, errori o guasti hardware che ne determinano la disattivazione ("Disco rimosso"). Ogni disco disattivato è soggetto a una serie di processi di distruzione dei dati (le "Norme sulla cancellazione del disco") prima di lasciare la sede di Google per il riutilizzo o la distruzione. I dischi dismessi vengono cancellati in un processo a più fasi e verificati come completi da almeno due validatori indipendenti. I risultati della cancellazione vengono registrati dal numero di serie del disco dismesso per il monitoraggio. Infine, il disco 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, utilizzo appropriato e standard professionali. Google conduce controlli in background ragionevolmente appropriati nella misura consentita dalla legge e in conformità con il diritto del lavoro e le normative locali applicabili.

Il personale è tenuto a sottoscrivere un accordo di riservatezza e deve accusare ricevuta e conformità alle norme sulla riservatezza e sulla privacy di Google. Il personale riceve una formazione sulla sicurezza. Il personale che tratta i Dati dei Clienti è tenuto a completare requisiti aggiuntivi adeguati al proprio ruolo (es. certificazioni). Il personale di Google non tratterà i Dati dei clienti senza autorizzazione.

5. Sicurezza del subincaricato

Prima di inserire i Sub-responsabili del trattamento, Google conduce un controllo delle pratiche di sicurezza e privacy dei Sub-responsabili del trattamento 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 Subresponsabile del trattamento, fatti salvi i requisiti descritti nella Sezione 11.3 (Requisiti per il coinvolgimento del Subprocessore) del presente Addendum, il Subprocessore è tenuto a stipulare condizioni contrattuali di sicurezza, riservatezza e privacy appropriate.

Versioni precedenti dei Termini di trattamento e sicurezza dei dati:

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