# **Addendum per il trattamento dei dati Cloud** (ATDC) e dei **Termini di servizio specifici per Google Workspace**

La presente Appendice sull'elaborazione dei dati cloud (comprese le sue appendici, l'" *Appendice* ") è incorporata nei Contratti (come definiti di seguito) tra Google e il Cliente. La presente Appendice era precedentemente nota come "Termini per l'elaborazione e la sicurezza dei dati" ai sensi di un contratto per Google Cloud Platform, Looker (originale) o i servizi Google SecOps o "Emendamento sull'elaborazione dei dati" ai sensi di un contratto per Google Workspace o Cloud Identity.

Sommario:

Termini generali

1. Panoramica

Il presente Addendum descrive gli obblighi delle parti, anche ai sensi delle leggi applicabili sulla privacy, sulla sicurezza dei dati e sulla protezione dei dati, in relazione al trattamento e alla sicurezza dei dati del cliente (come definiti di seguito). Il presente Addendum entrerà in vigore alla Data di entrata in vigore dell'Addendum (come definita di seguito) e sostituirà tutti i termini precedentemente applicabili al trattamento e alla sicurezza dei Dati del Cliente. I termini in maiuscolo utilizzati ma non definiti nel presente Addendum hanno il significato loro attribuito nel Contratto.

2. Definizioni

2.1 Nel presente Addendum:

- Per " *Data di entrata in vigore dell'Addendum* " si intende la data in cui il Cliente ha accettato, o le parti hanno altrimenti concordato, il presente Addendum.
- Per " *Controlli di sicurezza aggiuntivi* " si intendono le risorse, le caratteristiche, le funzionalità e i controlli di sicurezza che il Cliente può utilizzare a sua discrezione e come determina, tra cui la Console di amministrazione, la crittografia, la registrazione e il monitoraggio, la gestione dell'identità e degli accessi, la scansione di sicurezza e i firewall.
- Per " *Contratto* " si intende il contratto in base al quale Google ha accettato di fornire i Servizi applicabili al Cliente.
- Per " *Legge sulla privacy applicabile* " si intende, se applicabile al trattamento dei dati personali del cliente, qualsiasi legge o regolamento nazionale, federale, dell'Unione Europea, statale, provinciale o altra legge o regolamento sulla privacy, sulla sicurezza dei dati o sulla protezione dei dati.
- Per " *Servizi controllati* " si intendono i Servizi allora correnti indicati come rientranti nell'ambito della relativa certificazione o rapporto all'indirizzo https://cloud.google.com/security/compliance/services-in-scope . Google non può rimuovere alcun Servizio da questo URL a meno che non sia stato interrotto in conformità al Contratto applicabile.
- " *Certificazioni di conformità* " ha il significato indicato nella Sezione 7.4 (Certificazioni di conformità e rapporti SOC).
- " *Dati del Cliente* ", se non definito nel Contratto, ha il significato indicato nell'Appendice 4 (Prodotti specifici).
- Per " *Dati personali del cliente* " si intendono i dati personali contenuti nei Dati del cliente, comprese eventuali categorie speciali di dati personali o dati sensibili definiti dalla legge sulla privacy applicabile.
- Per " *Incidente relativo ai dati* " si intende una violazione della sicurezza di Google che comporta la distruzione, la perdita, l'alterazione, la divulgazione non autorizzata o l'accesso accidentale o illegale ai Dati del cliente su sistemi gestiti o altrimenti controllati da Google.
- " *EMEA* " significa Europa, Medio Oriente e Africa.
- Per " *GDPR UE* " si intende il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio, del 27 aprile 2016, sulla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché sulla libera circolazione di tali dati, e che abroga la Direttiva 95/46/CE.
- Per " *Legge europea sulla protezione dei dati* " si intende, a seconda dei casi: (a) il GDPR; oppure b) la LPD svizzera.
- 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 del cliente); (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); o (c) la legge svizzera (se la LPD svizzera si applica al trattamento dei dati personali del cliente).
- Per " *GDPR* " si intende, a seconda dei casi: (a) il GDPR dell'UE; o (b) il GDPR del Regno Unito.

- Per " *Revisore dei conti di terze parti di Google* " si intende un revisore dei conti di terze parti, qualificato e indipendente nominato da Google, la cui identità attuale verrà rivelata da Google al Cliente.
- " *Istruzioni* " ha il significato indicato nella Sezione 5.2 (Conformità alle Istruzioni del Cliente).
- " *Indirizzo email di notifica* " indica gli indirizzi email indicati dal Cliente nella Console di amministrazione o nel Modulo d'ordine per ricevere determinate notifiche da Google.
- Per " *Documentazione di Sicurezza* " si intendono le Certificazioni di Conformità e i Rapporti SOC.
- " *Misure di sicurezza* " ha il significato indicato nella Sezione 7.1.1 (Misure di sicurezza di Google).
- Per " *Servizi* " si intendono i servizi applicabili descritti nell'Appendice 4 (Prodotti specifici).
- " *Rapporti SOC* " ha il significato indicato nella Sezione 7.4 (Certificazioni di conformità e Rapporti SOC).
- Per " *Sub-responsabile* " si intende una terza parte autorizzata come altro responsabile del trattamento ai sensi del presente Addendum a trattare i Dati del Cliente al fine di fornire parti dei Servizi e di TSS.
- Per " *Autorità di controllo* " si intende, a seconda dei casi: (a) una "autorità di controllo" come definita nel GDPR dell'UE; o (b) il "Commissario" come definito nel GDPR del Regno Unito o nella FADP svizzera.
- Per " *LPD svizzero* " si intende, a seconda dei casi, la legge federale sulla protezione dei dati del 19 giugno 1992 (Svizzera) (con l'ordinanza sulla legge federale sulla protezione dei dati del 14 giugno 1993) o la revisione della legge federale sulla protezione dei dati del 25 settembre 2020. (Svizzera) (con l'ordinanza sulla legge federale del 31 agosto 2022 sulla protezione dei dati).
- Per " *Durata* " si intende il periodo compreso tra la Data di entrata in vigore dell'Addendum e la 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 può continuare a fornire i Servizi Servizi per scopi transitori.
- Per " *GDPR del Regno Unito* " si intende il GDPR dell'UE come modificato e incorporato nella legge del Regno Unito ai sensi della legge britannica sull'Unione europea (di ritiro) del 2018 e la legislazione secondaria applicabile adottata ai sensi di tale legge.

2.2 I termini "dati personali", "interessato", "trattamento", "responsabile del trattamento" e "responsabile del trattamento" utilizzati nel presente Addendum hanno il significato attribuito dalla legge sulla privacy applicabile o, in assenza di tale significato o legge, dall'UE GDPR.

2.3 I termini "interessato", "responsabile del trattamento" e "responsabile del trattamento" includono rispettivamente "consumatore", "azienda" e "fornitore di servizi", come richiesto dalla normativa sulla privacy applicabile.

3. Durata

Indipendentemente dal fatto che il Contratto applicabile sia terminato 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. Ruoli; Conformità legale

4.1 *Ruoli delle parti.* Google è un responsabile del trattamento e il Cliente è un titolare del trattamento o responsabile del trattamento, a seconda dei casi, dei Dati personali del Cliente.

4.2 *Riepilogo del trattamento.* L'oggetto e i dettagli del trattamento dei dati personali del cliente sono descritti nell'Appendice 1 (Oggetto e dettagli del trattamento).

4.3 *Conformità alla legge.* Ciascuna parte rispetterà i propri obblighi relativi al trattamento dei dati personali del cliente ai sensi della legge sulla privacy applicabile.

4.4 *Termini legali aggiuntivi* . Nella misura in cui il trattamento dei dati personali del cliente è soggetto a una legge sulla privacy applicabile descritta nell'Appendice 3 (Leggi sulla privacy specifiche), i termini

corrispondenti nell'Appendice 3 si applicheranno in aggiunta alle presenti Condizioni generali e prevarranno come descritto nella Sezione 14.1 (Precedenza) .

## 5. Trattamento dei dati

5.1 *Clienti Processori* . Se il Cliente è un responsabile del trattamento:

UN. Il Cliente garantisce su base continuativa che il titolare del trattamento in questione ha autorizzato:

io. le istruzioni;

ii. assunzione da parte del cliente di Google come altro responsabile del trattamento; E.

iii. Il coinvolgimento dei subresponsabili da parte di Google come descritto nella Sezione 11 (Subresponsabili);

B. Il Cliente inoltrerà al titolare del trattamento pertinente tempestivamente e senza indebito ritardo qualsiasi avviso fornito da Google ai sensi della Sezione 7.2.1 (Notifica dell'incidente), 9.2.1 (Responsabilità per le richieste) o 11.4 (Opportunità di opporsi ai subresponsabili del trattamento); E

C. Il Cliente può rendere disponibile al titolare del trattamento in questione qualsiasi altra informazione resa disponibile da Google ai sensi della presente Appendice sull'ubicazione dei data center di Google o sui nomi, le ubicazioni e le attività dei Subresponsabili.

5.2 *Rispetto delle istruzioni del cliente* . Il Cliente richiede a Google di elaborare i dati del cliente in conformità al Contratto applicabile (inclusa la presente Appendice) e alla legge applicabile solo come segue:

UN. fornire, proteggere e monitorare i Servizi e TSS; E

B. come ulteriormente specificato tramite:

io. Utilizzo dei Servizi da parte del Cliente (anche tramite la Console di amministrazione) e TSS; E

ii. qualsiasi altra istruzione scritta fornita dal Cliente e riconosciuta da Google come costituente istruzione ai sensi del presente Addendum

(collettivamente, le " *Istruzioni* ").

Google rispetterà le Istruzioni a meno che non sia vietato dalla legge europea, dove si applica la legge europea sulla protezione dei dati, o proibito dalla legge applicabile, dove si applica qualsiasi altra legge sulla privacy applicabile.

## 6. Cancellazione dei dati

6.1 *Cancellazione da parte del Cliente* . Google consentirà al Cliente di eliminare i Dati del Cliente durante il Periodo in modo coerente con la funzionalità dei Servizi. Se il Cliente utilizza i Servizi per eliminare eventuali Dati del cliente durante il Periodo e tali Dati del cliente non possono essere recuperati dal Cliente, tale utilizzo costituirà un'istruzione a Google di eliminare i Dati del cliente pertinenti dai sistemi di Google in conformità con la legge applicabile. Google rispetterà le presenti Istruzioni non appena ragionevolmente possibile ed entro un periodo massimo di 180 giorni, a meno che la legge europea non richieda l'archiviazione, laddove si applica la legge europea sulla protezione dei dati, o la legge applicabile richieda l'archiviazione, laddove si applichi qualsiasi altra legge sulla privacy applicabile.

6.2 *Restituzione o cancellazione alla scadenza del termine* . Se il Cliente desidera conservare i propri Dati dopo la scadenza del Periodo, può dare istruzioni a Google in conformità alla 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 restanti Dati del Cliente (incluse le copie esistenti) dai sistemi di Google alla scadenza del Periodo in conformità con la legge applicabile. Dopo un periodo di recupero massimo di 30 giorni a partire da tale data, Google si atterrà alle presenti Istruzioni non appena ragionevolmente possibile ed entro un periodo massimo di 180 giorni, a meno che la legge europea non richieda la conservazione, laddove si applica la legge europea

sulla protezione dei dati, o la legge applicabile richieda archiviazione, laddove si applichi qualsiasi altra legge sulla privacy applicabile.

6.3. *Istruzioni per la cancellazione differita* . Nella misura in cui vengono elaborati anche i Dati del cliente coperti dall'istruzione di eliminazione descritta nella Sezione 6.2 (Restituzione o eliminazione alla scadenza del Periodo), alla scadenza del Periodo applicabile ai sensi della Sezione 6.2, in relazione a un Contratto con una Durata continua, tale istruzione di eliminazione verrà avranno effetto rispetto a tali Dati del Cliente solo alla scadenza del Periodo continuativo. Per maggiore 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 accidentale o illegale, divulgazione o accesso non autorizzati, come descritto nell'Appendice 2 (Misure di sicurezza) ( " *Misure di sicurezza ")* . Le Misure di Sicurezza includono misure per crittografare i Dati del Cliente; per contribuire a garantire la riservatezza, l'integrità, la disponibilità e la resilienza continue 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 periodici 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:

UN. autorizzare i propri dipendenti, collaboratori e Subresponsabili ad accedere ai Dati del Cliente solo nella misura strettamente necessaria per rispettare le Istruzioni;

B. adottare misure adeguate per garantire il rispetto delle Misure di Sicurezza da parte dei propri dipendenti, appaltatori e Subresponsabili 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 *Controlli di sicurezza aggiuntivi* . Google metterà a disposizione controlli di sicurezza aggiuntivi per:

UN. 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 suoi obblighi (o, qualora il cliente sia un responsabile del trattamento, del relativo titolare del trattamento) relativi alla sicurezza e alle violazioni dei dati personali. ai sensi della legge sulla privacy applicabile, da:

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

B. rendere disponibili Controlli di Sicurezza Aggiuntivi in conformità alla Sezione 7.1.3 (Controlli di Sicurezza Aggiuntivi);

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

D. rendere disponibile la Documentazione di Sicurezza in conformità alla Sezione 7.5.1 (Revisioni della Documentazione di Sicurezza) e fornire le informazioni contenute nel Contratto applicabile (incluso il presente Addendum); E

e. se le sottosezioni (a)-(d) di cui sopra non sono sufficienti affinché il Cliente (o il relativo titolare del trattamento) rispetti tali obblighi, su richiesta del Cliente, fornendo al Cliente ulteriore ragionevole cooperazione e assistenza.

7.2 *Incidenti relativi ai dati* .

7.2.1 *Notifica dell'incidente* . Google informerà il Cliente tempestivamente e senza indebito ritardo dopo essere venuta a conoscenza di un Incidente relativo ai 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 di un Incidente relativo ai dati descriverà: la natura dell'Incidente relativo ai dati, comprese le risorse del Cliente interessate; le misure che Google ha adottato, o prevede di adottare, per affrontare l'Incidente relativo ai dati e mitigarne il potenziale rischio; le eventuali misure che Google consiglia al Cliente di adottare per affrontare l'Incidente relativo ai dati; e i dettagli di un punto di contatto dove è possibile ottenere maggiori informazioni. Se non è possibile fornire tutte queste informazioni contemporaneamente, la notifica iniziale di Google conterrà le informazioni allora disponibili e ulteriori informazioni verranno fornite senza indebito ritardo non appena saranno disponibili.

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

7.2.4 *Nessun 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 verrà interpretata come un riconoscimento da parte di Google di qualsiasi colpa o responsabilità in relazione all'Incidente con i 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 di eventuali copie dei Dati del Cliente all'esterno 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 utilizzati dal Cliente per accedere ai Servizi; E

C. eseguire il backup o conservare copie dei dati del cliente, a seconda dei casi.

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

7.4 *Certificazioni di conformità e rapporti SOC* . Google manterrà almeno quanto segue affinché i Servizi controllati possano verificare la continua efficacia delle Misure di sicurezza:

UN. certificati ISO 27001 ed eventuali certificazioni aggiuntive descritte nell'Appendice 4 (Prodotti specifici) (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* ").

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 *Esami e controlli di conformità* .

7.5.1 *Revisioni della documentazione di sicurezza* . Per dimostrare il rispetto da parte di Google degli obblighi previsti dalla presente Appendice, Google renderà la Documentazione sulla sicurezza disponibile per la revisione da parte del Cliente e, se il Cliente è un responsabile del trattamento, consentirà al Cliente di richiedere l'accesso ai Report SOC per il titolare del trattamento pertinente in conformità alla Sezione 7.5. 3 (Termini commerciali aggiuntivi per revisioni e audit).

7.5.2 *Diritti di revisione del cliente* .

UN. *Controllo del cliente* . Google, se richiesto dalla Legge sulla privacy applicabile, consentirà al Cliente o a un revisore indipendente nominato dal Cliente di condurre controlli (comprese ispezioni) per verificare la conformità di Google agli obblighi previsti dal presente Addendum in conformità con la Sezione 7.5.3 (Termini commerciali aggiuntivi per recensioni e Audit). Durante un controllo, Google collaborerà ragionevolmente con il Cliente o il suo revisore come descritto nella presente Sezione 7.5 (Revisioni e controlli di conformità).

B. *Revisione indipendente dal cliente* . Il Cliente può condurre un controllo per verificare la conformità di Google agli obblighi previsti dalla presente Appendice esaminando la Documentazione sulla sicurezza (che riflette l'esito dei controlli condotti dal Revisore di terze parti di Google).

7.5.3 *Termini commerciali aggiuntivi per revisioni e audit* .

UN. Il cliente deve contattare il team di protezione dei dati cloud di Google per richiedere:

io. accesso ai rapporti SOC per un titolare del trattamento pertinente ai sensi della Sezione 7.5.1 (Revisioni della documentazione di sicurezza); O

ii. un audit ai sensi della Sezione 7.5.2(a) (Audit del cliente).

B. A seguito di una richiesta del Cliente ai sensi della Sezione 7.5.3(a), Google e il Cliente discuteranno e concorderanno in anticipo su:

io. controlli di sicurezza e riservatezza applicabili a qualsiasi accesso ai Rapporti SOC da parte di un responsabile del trattamento pertinente ai sensi della Sezione 7.5.1 (Revisioni della documentazione di sicurezza); E

ii. la data di inizio ragionevole, l'ambito e la durata dei controlli di sicurezza e riservatezza applicabili a qualsiasi audit ai sensi della Sezione 7.5.2(a) (Audit del cliente).

C. Google può addebitare una tariffa (basata sui costi ragionevoli di Google) per qualsiasi controllo ai sensi della Sezione 7.5.2(a) (Controllo del cliente). Google fornirà al Cliente ulteriori dettagli su eventuali tariffe applicabili 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 audit.

D. Google può opporsi per iscritto a un revisore nominato dal Cliente per condurre qualsiasi verifica ai sensi della Sezione 7.5.2(a) (Verifica del cliente) se il revisore non è, secondo la ragionevole opinione di Google, adeguatamente qualificato o indipendente, un concorrente di Google o altrimenti manifestamente inadatto. Qualsiasi obiezione di questo tipo da parte di Google richiederà al Cliente di nominare un altro revisore o di condurre lui stesso la verifica.

e. Qualsiasi richiesta del Cliente ai sensi dell'Appendice 3 (Leggi specifiche sulla privacy) o dell'Appendice 4 (Prodotti specifici) per l'accesso a qualsiasi report SOC per un controller pertinente o per controlli sarà soggetta anche alla presente Sezione 7.5.3 (Termini commerciali aggiuntivi per revisioni e controlli) .

## 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 suoi obblighi (o, nel caso in cui il Cliente sia un responsabile del trattamento, del relativo titolare del trattamento) relativi alle valutazioni della protezione dei dati, alle valutazioni dei rischi, ai precedenti regolamenti normativi consultazioni o procedure equivalenti ai sensi della normativa privacy applicabile, da parte di:

UN. rendere disponibili i Controlli di Sicurezza Aggiuntivi in conformità alla Sezione 7.1.3 (Controlli di Sicurezza Aggiuntivi) e la Documentazione di Sicurezza a disposizione in conformità alla Sezione 7.5.1 (Revisioni della Documentazione di Sicurezza);

B. fornire le informazioni contenute nel Contratto applicabile (incluso il presente Addendum); E

C. se le sottosezioni (a) e (b) di cui sopra non sono sufficienti affinché il Cliente (o il relativo titolare del trattamento) rispetti tali obblighi, su richiesta del Cliente, fornendo al Cliente ulteriore ragionevole cooperazione e assistenza.

9. Accesso; 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 il trattamento 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 che i suoi dati personali sono inaccurati o obsoleti, sarà responsabile dell'utilizzo di tale funzionalità per rettificare o eliminare tali dati se richiesto dalla legge sulla privacy applicabile.

9.2 *Richieste dell'interessato* .

9.2.1 *Responsabilità per le richieste* . Nel corso della Durata, se il team di protezione dei dati cloud di Google riceve una richiesta da un interessato relativa ai dati personali del cliente e identifica il cliente, Google:

UN. consigliare all'interessato di presentare 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, l'utilizzo della funzionalità dei Servizi.

9.2.2 *Assistenza per la richiesta di assistenza da parte dell'interessato di Google* . Google (tenendo conto della natura del trattamento dei dati personali del cliente) assisterà il cliente nell'adempimento dei suoi obblighi (o, nel caso in cui il cliente sia un responsabile del trattamento, del relativo titolare del trattamento) ai sensi della legge sulla privacy applicabile per rispondere alle richieste di esercizio dei diritti dell'interessato da parte di :

UN. rendere disponibili Controlli di Sicurezza Aggiuntivi in conformità alla 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 affinché il Cliente (o il relativo titolare del trattamento) rispetti tali obblighi, su richiesta del Cliente, fornendo al Cliente ulteriore ragionevole cooperazione e assistenza.

10. Luoghi di trattamento dei dati

10.1 *Strutture di archiviazione ed elaborazione dei dati.* Fatti salvi gli impegni di Google sulla localizzazione dei dati ai sensi dei Termini specifici del servizio e gli impegni sul trasferimento dei dati ai sensi dell'Appendice 3 (Leggi specifiche sulla privacy), se applicabile, i dati del cliente possono essere trattati in qualsiasi paese in cui Google o i suoi sub-responsabili del trattamento hanno strutture.

10.2 *Informazioni sul centro dati* . Le ubicazioni dei data center di Google sono descritte nell'Appendice 4 (Prodotti specifici).

11. Subresponsabili del trattamento

11.1 *Consenso all'incarico del sub-responsabile* . Il Cliente autorizza specificamente l'impegno di Google in qualità di Subresponsabili delle entità indicate come descritto nella Sezione 11.2 (Informazioni sui Subresponsabili) a partire dalla Data di entrata in vigore dell'Addendum. Inoltre, fatta salva la Sezione 11.4 (Opportunità di opporsi ai subresponsabili), il Cliente autorizza generalmente l'assunzione da parte di Google di altre terze parti come subresponsabili (“ *Nuovi subresponsabili* ”).

11.2 *Informazioni sui subresponsabili* . Nomi, sedi e attività dei Subresponsabili sono descritti nell'Appendice 4 (Prodotti specifici).

11.3 *Requisiti per l'incarico di sub-responsabile* . Quando coinvolge qualsiasi sub-responsabile, Google:

UN. garantire tramite contratto scritto che:

io. il Subresponsabile accede e utilizza i Dati del Cliente solo nella misura necessaria per eseguire gli obblighi ad esso subappaltati e lo fa in conformità con il Contratto applicabile (incluso il presente Addendum); E

ii. se richiesto dalle Leggi sulla privacy applicabili, gli obblighi di protezione dei dati descritti nel presente Addendum sono imposti al Subresponsabile (come può essere ulteriormente descritto nell'Appendice 3 (Leggi specifiche sulla privacy)); E

B. rimanere pienamente responsabile per tutti gli obblighi subappaltati e per tutti gli atti e le omissioni del Subresponsabile.

11.4 *Opportunità di opporsi ai subresponsabili del trattamento* .

UN. Quando Google assume un Nuovo Subresponsabile durante il Periodo, Google, almeno 30 giorni prima che il Nuovo Subresponsabile inizi a elaborare i Dati del Cliente, notificherà al Cliente l'incarico (compreso il nome, l'ubicazione e le attività del Nuovo Subresponsabile).

B. Il Cliente può, entro 90 giorni dalla notifica dell'assunzione di un Nuovo Subresponsabile, opporsi risolvendo immediatamente il Contratto applicabile per comodità:

io. in conformità con la disposizione di risoluzione per convenienza di tale Contratto; O

ii. se non esiste tale disposizione, avvisando 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 per la protezione dei dati nel cloud di Google fornirà assistenza tempestiva e ragionevole per qualsiasi domanda del cliente relativa al trattamento dei dati del cliente ai sensi del contratto applicabile e potrà essere contattato come descritto nella sezione Avvisi del contratto applicabile o nell'Appendice 4 (Prodotti specifici).

12.2 *Dati di elaborazione di Google* . Google conserverà la documentazione adeguata delle proprie attività di trattamento come richiesto dalla normativa sulla privacy applicabile. Nella misura in cui qualsiasi Legge sulla privacy applicabile richiede a Google di raccogliere e conservare registrazioni di determinate informazioni relative al Cliente, il Cliente utilizzerà la Console di amministrazione o altri mezzi identificati nell'Appendice 4 (Prodotti specifici) per fornire tali informazioni e mantenerle accurate e aggiornate -data. Google può rendere tali informazioni disponibili alle autorità di regolamentazione competenti, inclusa un'autorità di vigilanza, se richiesto dalla legge sulla privacy applicabile.

12.3 *Richieste del controllore* . Durante il Periodo, se il Team per la 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. Avvisi

Le comunicazioni ai sensi del presente Addendum (comprese le notifiche di eventuali Incidenti relativi ai dati) verranno recapitate all'Indirizzo e-mail di notifica. Il Cliente è responsabile dell'utilizzo della Console di amministrazione per garantire che il proprio indirizzo e-mail di notifica rimanga aggiornato e valido.

## 14. Interpretazione

14.1 *Precedenza* . Nella misura di qualsiasi conflitto tra:

UN. L'Appendice 3 (Norme specifiche sulla privacy) e il resto dell'Addendum (inclusa l'Appendice 4 (Prodotti specifici)), l'Appendice 3 prevarrà; E

B. L'Appendice 4 (Prodotti specifici) e il resto dell'Addendum (esclusa l'Appendice 3), prevarrà l'Appendice 4; E

C. presente Addendum e il resto del Contratto, il presente Addendum prevarrà.

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

14.2 *Riferimenti alle sezioni* . Salvo diversa indicazione, i riferimenti alle sezioni presenti in qualsiasi Appendice del presente Addendum si riferiscono alle sezioni delle Condizioni Generali dell'Addendum.

## Allegato 1: Oggetto e dettagli del trattamento dei dati

*Argomento*

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

*Durata del Trattamento*

La Durata più il periodo che va dalla fine della Durata fino alla cancellazione di tutti i Dati del Cliente da parte di Google in conformità con la presente Appendice.

*Natura e finalità del trattamento*

Google tratterà i Dati personali del Cliente allo scopo di fornire i Servizi e i TSS al Cliente in conformità alla presente Appendice.

*Categorie di dati*

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

*Interessati*

Gli interessati includono le persone di cui i dati vengono forniti a Google tramite i Servizi da (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.*

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

*Ridondanza* . I sistemi infrastrutturali sono stati progettati per eliminare i singoli punti di guasto e ridurre al minimo l'impatto dei rischi ambientali previsti. Doppi circuiti, interruttori, reti o altri dispositivi necessari contribuiscono a fornire questa ridondanza. I Servizi sono progettati per consentire a Google di eseguire determinati tipi di manutenzione preventiva e correttiva senza interruzione. Tutte le attrezzature e le strutture ambientali dispongono di 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. La manutenzione preventiva e correttiva delle apparecchiature del data center è programmata attraverso un processo di modifica standard secondo procedure documentate.

*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, per i componenti critici dell'infrastruttura del data center viene fornita una fonte di alimentazione primaria e una alternativa, ciascuna con la stessa capacità. 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 abbassamenti di tensione, blackout, sovratensione,

sottotensione e condizioni di frequenza fuori tolleranza. Se l'alimentazione di rete viene interrotta, l'alimentazione di backup è progettata per fornire energia transitoria al data center, a piena capacità, per un massimo di 10 minuti fino a quando i sistemi di generatori 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 a 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 applicativo. I dati vengono archiviati utilizzando algoritmi proprietari per aumentare la sicurezza e la ridondanza dei dati.

*Qualità del codice* . 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, 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 generalmente collegati tramite collegamenti privati ad alta velocità per fornire un trasferimento dati sicuro e veloce tra 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 dati. Google trasferisce i dati tramite protocolli standard Internet.

*Superficie di attacco esterna* . Google utilizza più livelli di dispositivi di rete e rilevamento delle intrusioni per proteggere la propria superficie di attacco esterna. Google prende in considerazione i potenziali vettori di attacco e incorpora tecnologie appropriate appositamente sviluppate nei sistemi rivolti verso l'esterno.

*Rilevamento delle 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 prevede: (i) un controllo rigoroso delle dimensioni e della composizione della superficie di attacco di Google attraverso misure preventive; (ii) impiegando controlli di rilevamento intelligenti nei punti di immissione dei dati; e (iii) impiegare tecnologie che risolvono automaticamente determinate situazioni pericolose.

*Risposta agli incidenti* . Google monitora una serie di canali di comunicazione per rilevare eventuali incidenti di sicurezza e il personale di sicurezza di Google reagirà tempestivamente agli incidenti noti.

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

**2. Accesso e controlli del sito**

*(a) Controlli del sito.*

*Operazione di sicurezza del data center in loco* . I data center di Google mantengono un'unità 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 addetto alla 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 al funzionamento della sicurezza in loco. Tutti gli ingressi 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 collaboratori autorizzati possono richiedere l'accesso a tali strutture con chiave elettronica. Le richieste di accesso con chiave elettronica al 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 necessitano di un accesso temporaneo al data center devono: (i) ottenere preventivamente l'approvazione da parte dei gestori del data center per lo specifico data center 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 degli accessi a doppia autenticazione collegato a un allarme di sistema. 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 indagati, ove opportuno. L'accesso autorizzato alle 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 gli altri, 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 CCTV. Le telecamere registrano sul posto tramite videoregistratori digitali 24 ore al giorno, 7 giorni alla settimana. I registri di sorveglianza vengono conservati fino a 30 giorni in base all'attività.

*(b) Controllo degli accessi.*

*Personale addetto alla sicurezza delle infrastrutture* . Google dispone e mantiene una politica di sicurezza per il proprio personale e richiede 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 Single Sign On per poter utilizzare i Servizi.

*Processi e politiche di accesso ai dati interni – Politica di accesso* . I processi e le politiche di accesso ai dati interni di Google sono progettati per impedire a persone e sistemi non autorizzati di accedere ai sistemi utilizzati per elaborare i dati del cliente. Google progetta i propri 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'utilizzo e dopo la registrazione. I sistemi sono progettati per rilevare eventuali accessi inappropriati. 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 garantire solo i 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 rischio di utilizzo non autorizzato dell'account. La concessione o la modifica dei diritti di accesso si basa: sulle responsabilità lavorative del personale autorizzato; requisiti di mansione lavorativa necessari per svolgere i compiti autorizzati; e la necessità di conoscere le basi. La concessione o la modifica dei diritti di accesso deve inoltre essere conforme alle politiche di accesso ai dati interni e alla formazione di Google. Le approvazioni sono gestite da strumenti del flusso di lavoro che mantengono registrazioni di controllo di tutte le modifiche. L'accesso ai sistemi viene registrato per creare una traccia

di controllo per la responsabilità. Laddove vengono utilizzate password per l'autenticazione (ad esempio per l'accesso alle postazioni di lavoro), vengono implementate politiche relative alle 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 esempio i dati delle carte di credito), Google utilizza token hardware.

**3. Dati**

(a) *Archiviazione, isolamento e registrazione dei dati* . Google archivia i dati in un ambiente multi-tenant su server di proprietà di Google. Fatte salve eventuali istruzioni contrarie (ad esempio sotto forma di selezione della posizione dei dati), Google replica i dati del cliente tra più data center geograficamente dispersi. Google inoltre isola logicamente i dati dei clienti. Al cliente verrà dato 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 dei dischi* . I dischi contenenti dati potrebbero presentare problemi di prestazioni, errori o guasti hardware che ne comportano la disattivazione ("Disco disattivato"). Ogni disco disattivato è soggetto a una serie di processi di distruzione dei dati ("Norme 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 fasi e verificati come completi da almeno due validatori indipendenti. I risultati della cancellazione vengono registrati tramite il numero di serie del disco dismesso 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 dismesso 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 aziendali in materia di riservatezza, etica aziendale, utilizzo appropriato e standard professionali. Google conduce controlli dei precedenti ragionevolmente appropriati nella misura consentita dalla legge e in conformità con le leggi locali sul lavoro e le normative statutarie applicabili.

Il personale di Google è tenuto a sottoscrivere un accordo di riservatezza e deve confermare di aver ricevuto e rispettato le norme sulla riservatezza e sulla privacy di Google. Il personale riceve una formazione sulla sicurezza. Il personale che tratta i Dati del Cliente è tenuto a completare ulteriori requisiti adeguati al proprio ruolo (ad esempio certificazioni). Il personale di Google non tratterà i Dati del Cliente senza autorizzazione.

**5. Sicurezza del sub-responsabile**

Prima di assumere i Subresponsabili, Google conduce un controllo delle pratiche di sicurezza e privacy dei Subresponsabili per garantire che i Subresponsabili 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, soggetti ai requisiti descritti nella Sezione 11.3 (Requisiti per l'ingaggio del Subresponsabile), il Subresponsabile è tenuto a stipulare termini contrattuali adeguati in materia di sicurezza, riservatezza e privacy.

Appendice 3: Leggi specifiche sulla privacy

I termini di ciascuna sottosezione della presente Appendice 3 si applicano solo laddove la legge corrispondente si applica al trattamento dei Dati personali del Cliente.

Legge europea sulla protezione dei dati

**1. Definizioni aggiuntive.**

- Per " *Paese adeguato* " si intende:

(a) per i dati trattati soggetti al GDPR dell'UE: lo Spazio economico europeo, 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; O

(c) per i dati trattati soggetti alla LPD svizzera: la Svizzera o un Paese o territorio che: (i) figura nell'elenco degli Stati la cui legislazione garantisce una protezione adeguata, come pubblicato dall'Incaricato federale svizzero della protezione dei dati e della trasparenza, se applicabile; oppure (ii) riconosciuti come idonei a garantire una protezione adeguata dal Consiglio federale svizzero ai sensi della LPD svizzera;

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

- Per " *Soluzione di trasferimento alternativa* " si intende una soluzione, diversa dalle SCC, che consente il trasferimento legittimo di dati personali verso un paese terzo in conformità con la legge europea sulla protezione dei dati, ad esempio un quadro di protezione dei dati riconosciuto come atto a garantire che le entità partecipanti forniscano una protezione adeguata.
- Per " *SCC del cliente* " si intendono le SCC (da controller a processore), le SCC (da processore a processore) o le SCC (da processore a controller), a seconda dei casi.
- Per " *SCC* " si intendono le SCC del cliente o le SCC (da processore a processore, esportatore di Google), a seconda dei casi.
- " *SCC (da controller a processore)* " indica i termini su: https://cloud.google.com/terms/sccs/eu-c2p
- Per " *SCC (processore-controllore)* " si intendono i termini presenti all'indirizzo: https://cloud.google.com/terms/sccs/eu-p2c
- Per " *SCC (da processore a processore)* " si intendono i termini presenti all'indirizzo: https://cloud.google.com/terms/sccs/eu-p2p
- Per " *SCC (processore a processore, Google Exporter)* " si intendono i termini disponibili all'indirizzo: https://cloud.google.com/terms/sccs/eu-p2p-google-exporter

**2. Notifiche di istruzioni.** Fatti salvi gli obblighi di Google ai sensi della Sezione 5.2 (Conformità alle istruzioni del Cliente) o qualsiasi altro diritto o obbligo di entrambe le parti ai sensi del Contratto applicabile, Google informerà immediatamente il Cliente se, a suo avviso:

UN. La Legge Europea vieta a Google di rispettare un'Istruzione;

B. un'Istruzione non è conforme alla normativa europea sulla protezione dei dati; O

C. In caso contrario Google non è in grado di rispettare un'Istruzione,

in ogni caso, a meno che tale avviso non sia vietato dalla legge europea.

Se il Cliente è un responsabile del trattamento, inoltrerà immediatamente al titolare del trattamento pertinente qualsiasi notifica fornita da Google ai sensi della presente sezione.

**3. Diritti di revisione del cliente.** Google consentirà al Cliente o a un revisore indipendente nominato dal Cliente di condurre controlli (incluse ispezioni) come descritto nella Sezione 7.5.2(a) (Verifica del cliente). Durante tale audit, Google renderà disponibili tutte le informazioni necessarie per dimostrare la conformità ai propri obblighi ai sensi della presente Appendice e contribuirà all'audit come descritto nella Sezione 7.5 (Revisioni e controlli di conformità) e in questa sezione.

**4. Trasferimenti di dati.**

4.1 *Trasferimenti 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 possano essere trattati 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 nella sezione 4.2 (Certificazione da parte di clienti non EMEA) dei presenti termini della legge europea sulla protezione dei dati, se il suo indirizzo di fatturazione è al di fuori dell'area EMEA ) (“ *Trasferimenti limitati* ”), quindi:

UN. se Google ha adottato una Soluzione di trasferimento alternativa per eventuali Trasferimenti limitati, Google informerà il Cliente della soluzione pertinente e garantirà che tali Trasferimenti limitati vengano effettuati in conformità con essa; O

B. se Google non ha adottato una Soluzione di trasferimento alternativa per eventuali Trasferimenti limitati, o informa il Cliente che Google non sta più adottando, una Soluzione di trasferimento alternativa per eventuali Trasferimenti limitati (senza adottare una Soluzione di trasferimento alternativa sostitutiva):

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

A. le SCC (da responsabile a responsabile, esportatore di Google) si applicheranno in relazione a tali Trasferimenti limitati da Google ai subresponsabili; E

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

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

4.2 *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, a meno che l'Appendice 4 (Prodotti specifici) del presente Addendum indichi diversamente, il Cliente certificherà come tale e identificherà la propria Autorità di vigilanza competente tramite il Console di amministrazione per i servizi applicabili.

4.3 *Informazioni sui trasferimenti limitati* . Google fornirà al Cliente informazioni relative ai trasferimenti limitati, ai controlli di sicurezza aggiuntivi e ad altre misure di protezione supplementari:

UN. come descritto nella Sezione 7.5.1 (Revisioni della documentazione di sicurezza);

B. in eventuali ulteriori luoghi descritti nell'Appendice 4 (Prodotti specifici); E

C. in relazione all'adozione da parte di Google di una soluzione di trasferimento alternativa, all'indirizzo https://cloud.google.com/terms/alternative-transfer-solution .

4.4 *Audit SCC* . Se si applicano le SCC del Cliente come descritto nella Sezione 4.1 (Trasferimenti limitati) dei presenti termini della Legge europea sulla protezione dei dati, 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, sia in conformità con la Sezione 7.5.3 (Termini commerciali aggiuntivi per revisioni e audit).

4.5 *Avvisi SCC* . Il Cliente inoltrerà al titolare del trattamento competente tempestivamente e senza indebito ritardo qualsiasi avviso che faccia riferimento a eventuali SCC.

4.6 *Risoluzione a causa del rischio di trasferimento dei dati* . Se il Cliente conclude, in base all'uso attuale o previsto dei Servizi, che non sono previste garanzie adeguate per i Dati personali del Cliente trasferiti, allora il Cliente potrà risolvere immediatamente il Contratto applicabile in conformità con la disposizione di risoluzione per comodità di tale Contratto o, se non vi è alcuna tale provvedimento, dandone comunicazione a Google.

4.7 *Nessuna modifica delle SCC* . Nessuna disposizione dell'Accordo (incluso il presente Addendum) è intesa a modificare o contraddire le clausole contrattuali tipo o a pregiudicare i diritti o le libertà fondamentali degli interessati ai sensi della normativa europea sulla protezione dei dati.

4.8 *Precedenza delle SCC* . Nella misura di qualsiasi conflitto o incoerenza tra le SCC del Cliente (incorporate per riferimento nel presente Addendum) e il resto del Contratto (incluso il presente Addendum), prevarranno le SCC del Cliente.

**5. Requisiti per l'assunzione del sub-responsabile.** La legge europea sulla protezione dei dati impone a Google di garantire tramite un contratto scritto che gli obblighi di protezione dei dati descritti nel presente Addendum, di cui all'articolo 28, paragrafo 3, del GDPR, se applicabile, siano imposti a qualsiasi sub-responsabile incaricato da Google.

CCPA

**1. Definizioni aggiuntive.**

- Per " *CCPA* " si intende il California Consumer Privacy Act del 2018, come modificato, incluso quanto modificato dal California Privacy Rights Act del 2020, insieme a tutti i regolamenti di attuazione.
- I " *Dati personali del cliente* " includono le "informazioni personali".
- I termini "azienda", "scopo commerciale", "consumatore", "informazioni personali", "elaborazione", "vendita", "vendita", "fornitore di servizi" e "condivisione" hanno il significato indicato nel CCPA.

**2. Divieti.** Fatti salvi gli obblighi di Google ai sensi della Sezione 5.2 (Conformità alle istruzioni del cliente), in relazione al trattamento dei dati personali del cliente in conformità al CCPA, Google non potrà, salvo diversamente consentito dal CCPA:

UN. vendere o condividere i dati personali del cliente;

B. conservare, utilizzare o divulgare i dati personali del cliente:

io. se non per scopi commerciali ai sensi del CCPA per conto del Cliente e per lo scopo specifico di eseguire i Servizi e i TSS; O

ii. al di fuori del rapporto commerciale diretto tra Google e il Cliente; O

C. combinare o aggiornare i dati personali del cliente con le informazioni personali che Google riceve da o per conto di terzi o raccoglie dalle proprie interazioni con il consumatore.

**3. Conformità.** Fatti salvi gli obblighi di Google ai sensi della Sezione 5.2 (Conformità alle istruzioni del Cliente) o qualsiasi altro diritto o obbligo di entrambe le parti ai sensi del Contratto applicabile, Google informerà il Cliente se, a suo avviso, Google non è in grado di soddisfare i propri obblighi ai sensi del CCPA, a meno che tale avviso è vietato dalla legge applicabile.

**4. Intervento del cliente.** Se Google notifica al Cliente qualsiasi utilizzo non autorizzato dei Dati personali del Cliente, anche ai sensi della Sezione 3 (Conformità) di questa sottosezione o della Sezione 7.2.1 (Notifica dell'incidente), il Cliente può adottare misure ragionevoli e appropriate per interrompere o rimediare a tale utilizzo non autorizzato:

UN. adottare eventuali misure consigliate da Google ai sensi della Sezione 7.2.2 (Dettagli sull'incidente relativo ai dati), se applicabile; O

B. esercitare i propri diritti ai sensi della Sezione 7.5.2(a) (Controllo del cliente) o 9.1 (Accesso; Rettifica; Trattamento limitato; Portabilità).

Tacchino

**1. Trasferimenti di dati.**

1.1 Se l'indirizzo di fatturazione del Cliente è in Turchia e il Cliente accetta eventuali termini aggiuntivi resi disponibili separatamente da Google in relazione ai trasferimenti dei dati personali del Cliente ai sensi della legge turca sulla protezione dei dati personali n. 6698 del 7 aprile 2016, tali termini integreranno questo Addendum.

1.2 Se il Cliente conclude, sulla base dell'uso attuale o previsto dei Servizi, che non sono previste garanzie adeguate per i Dati personali del Cliente trasferiti, allora il Cliente può risolvere immediatamente

il Contratto applicabile in conformità con la disposizione di risoluzione di tale Contratto per comodità o, se vi è tale disposizione, avvisando Google.

Israele

**1. Definizione aggiuntiva.**

- Per " *Legge israeliana sulla protezione della privacy* " si intende la legge israeliana sulla protezione della privacy del 1981 e tutti i regolamenti promulgati ai sensi della stessa.

**2. Termini equivalenti.** Qualsiasi termine equivalente a “responsabile del trattamento”, “dati personali”, “trattamento” e “responsabile del trattamento”, come utilizzato nel presente Addendum, ha il significato indicato nella legge israeliana sulla protezione della privacy.

**3 . Diritti di revisione del cliente.** Google consentirà al Cliente o a un revisore indipendente nominato dal Cliente di condurre controlli (incluse ispezioni) come descritto nella Sezione 7.5.2(a) (Verifica del cliente).

Appendice 4: Prodotti specifici

I termini di ciascuna sottosezione della presente Appendice 4 si applicano esclusivamente in relazione al trattamento dei dati del cliente da parte del/i servizio/i corrispondente/i.

Piattaforma cloud di Google

**1. Definizioni aggiuntive.**

- Per " *Account* ", se non definito nel Contratto, si intende l'account Google Cloud Platform del Cliente.
- Per " *Dati del cliente* ", se non definiti nel Contratto, si intendono i dati forniti a Google dal Cliente o dagli Utenti finali tramite Google Cloud Platform nell'ambito dell'Account e i dati che il Cliente o gli Utenti finali ricavano da tali dati attraverso il loro utilizzo di Google Cloud Platform.
- Per " *Google Cloud Platform* " si intendono i servizi Google Cloud Platform descritti all'indirizzo https://cloud.google.com/terms/services , escluse eventuali offerte di terze parti.
- Per " *Offerte di terze parti* ", se non definito nel Contratto, si intendono (a) servizi, software, prodotti e altre offerte di terze parti che non sono incorporati in Google Cloud Platform o nel Software, (b) offerte identificate nella sezione "Offerte di terze parti" -Termini delle parti" dei Termini specifici del servizio del Contratto e (c) sistemi operativi di terze parti.

**2. Certificazioni di conformità.** Le certificazioni di conformità per i servizi controllati di Google Cloud Platform includeranno anche i certificati ISO 27017 e ISO 27018 e un'attestazione di conformità PCI DSS.

**3. Posizioni dei data center.** Le posizioni dei data center di Google Cloud Platform sono descritte su https://cloud.google.com/about/locations/ .

**4. Informazioni sui Subresponsabili.** Nomi, posizioni e attività dei sub-responsabili di Google Cloud Platform sono descritti su https://cloud.google.com/terms/subprocessors .

**5. Team per la protezione dei dati nel cloud.** Il team di protezione dei dati per Google Cloud Platform può essere contattato all'indirizzo https://support.google.com/cloud/contact/dpo .

**6. Informazioni sui trasferimenti limitati** . Ulteriori informazioni relative ai trasferimenti limitati, ai controlli di sicurezza aggiuntivi e ad altre misure di protezione supplementari sono disponibili all'indirizzo cloud.google.com/privacy/ .

**7. Termini specifici del servizio.**

**Soluzione bare metal (Google Cloud Platform)**

La soluzione Bare Metal fornisce accesso non virtualizzato alle risorse dell'infrastruttura sottostante e, in base alla progettazione, presenta alcune caratteristiche distinte.

**1. Emendamenti.** Il presente Addendum è modificato come segue rispetto alla Soluzione Bare Metal:

- La definizione di "Revisore esterno di Google" è sostituita dalla seguente:
- Per " *Revisore dei conti di terze parti di Google* " si intende un revisore dei conti di terze parti qualificato e indipendente nominato da Google o da un sub-responsabile della soluzione Bare Metal, la cui identità attuale Google rivelerà al Cliente su richiesta.
- Vengono cancellati i seguenti termini:
- Dalla Sezione 7.1.1 (Misure di sicurezza di Google), la frase "crittografare i dati personali";
- Dall'Appendice 2 (Misure di sicurezza), le sottosezioni della Sezione 1(a) intitolate "Sistemi operativi server" e "Continuità aziendale";
- Dall'Appendice 2, le sottosezioni della Sezione 1(b) intitolate "Superficie di attacco esterna", "Rilevamento delle intrusioni" e "Tecnologie di crittografia"; E
- Dall'Appendice 2, le seguenti frasi della Sezione 3(a):
- Google archivia i dati in un ambiente multi-tenant su server di proprietà di Google. Fatte salve eventuali istruzioni contrarie del Cliente (ad esempio, sotto forma di selezione della posizione dei dati), Google replica i Dati del Cliente tra più data center geograficamente dispersi.

**2. Certificazioni di conformità e rapporti SOC.** Google o il suo Subresponsabile manterranno almeno quanto segue (o un'alternativa equivalente o migliorata) affinché Bare Metal Solution possa verificare la continua efficacia delle Misure di sicurezza:

UN. un certificato ISO 27001 e un attestato di conformità PCI DSS (le " *Certificazioni di conformità BMS* "); E

B. Report SOC 1 e SOC 2 aggiornati annualmente sulla base di un audit eseguito almeno una volta ogni 12 mesi (i " *Report SOC BMS* ").

**3. Revisioni della documentazione di sicurezza.** Per dimostrare la conformità da parte di Google agli obblighi previsti dal presente Addendum, Google renderà le certificazioni di conformità BMS e i report SOC BMS disponibili per la revisione da parte del Cliente e, se il Cliente è un responsabile del trattamento, consentirà al Cliente di richiedere l'accesso per il titolare del trattamento pertinente ai Report SOC BMS in conformità con la Sezione 7.5.3 (Termini commerciali aggiuntivi per revisioni e audit).

**4. Obblighi del cliente.** Senza limitare gli obblighi espliciti di Google relativi alla Soluzione Bare Metal, il Cliente adotterà misure ragionevoli per proteggere e mantenere la sicurezza dei Dati del Cliente e di qualsiasi altro contenuto archiviato o elaborato tramite la Soluzione Bare Metal.

**5. Dichiarazione di non responsabilità.** Nonostante quanto diversamente stabilito nel Contratto (inclusa la presente Appendice), Google non è responsabile di quanto segue in relazione alla Soluzione Bare Metal:

UN. sicurezza non fisica, come controlli di accesso, crittografia, firewall, protezione antivirus, rilevamento delle minacce e scansione di sicurezza;

B. registrazione e monitoraggio;

C. manutenzione o supporto non hardware;

D. backup dei dati, inclusa qualsiasi configurazione di ridondanza o alta disponibilità; O

e. politiche o procedure di continuità aziendale e ripristino di emergenza.

Il Cliente è l'unico responsabile della protezione (ad eccezione della sicurezza fisica dei server Bare Metal Solution), della registrazione, del monitoraggio, della manutenzione, del supporto e del backup di qualsiasi sistema operativo, dato del cliente, software e applicazione che il Cliente utilizza, carica su o ospita su Soluzione in metallo nudo.

**Google Distributed Cloud Edge (Google Cloud Platform)**

Google Distributed Cloud Edge (" *GDCE* ") non è distribuito in un data center di Google e, in base alla progettazione, presenta alcune caratteristiche distinte.

**1. Emendamenti.** Il presente Addendum è modificato come segue rispetto al GDCE:

- I riferimenti ai "sistemi di Google" vengono sostituiti con "l'Attrezzatura".
- La Sezione 6.2 (Restituzione o cancellazione alla scadenza del termine) è sostituita con la seguente:
- 6.2 *Restituzione o Cancellazione alla scadenza del Termine* . Il Cliente dà istruzioni a Google di eliminare tutti i restanti Dati del Cliente (comprese le copie esistenti) dall'Apparecchiatura alla scadenza del Periodo in conformità con la legge applicabile. Se il Cliente desidera conservare i Dati del Cliente dopo la fine del Periodo, può esportare o fare copie di tali dati prima della fine del Periodo. Google rispetterà le Istruzioni contenute nella presente Sezione 6.2 non appena ragionevolmente possibile ed entro un periodo massimo di 180 giorni, a meno che la legge europea non richieda l'archiviazione, laddove si applica la legge europea sulla protezione dei dati, o la legge applicabile richieda l'archiviazione, laddove si applichi qualsiasi altra legge sulla privacy applicabile. .
- Alla fine della Sezione 10.1 (Strutture di archiviazione ed elaborazione dei dati) vengono aggiunte le seguenti parole: "o dove si trova la sede del cliente".
- La Sezione 1 (Data Center e Sicurezza della Rete) dell'Appendice 2 (Misure di Sicurezza) è sostituita con la seguente:
- **1. Macchine locali e sicurezza di rete**

*Macchine locali* . I dati del cliente vengono archiviati esclusivamente sull'apparecchiatura da distribuire in una sede del cliente.

*Sistemi operativi per server* . I server di Google utilizzano un'implementazione basata su Linux personalizzata per l'ambiente applicativo. Google utilizza un processo di revisione del codice per aumentare la sicurezza del codice utilizzato per fornire GDCE e migliorare i prodotti di sicurezza negli ambienti di produzione GDCE.

*Tecnologie di crittografia* . Google mette a disposizione la crittografia HTTPS (nota anche come connessione SSL o TLS) e consente la crittografia dei dati in transito. I server di Google supportano lo scambio di chiavi crittografiche effimere con curva ellittica Diffie-Hellman firmate con RSA ed ECDSA. Questi metodi PFS (Perfect Forward Secrecy) aiutano a proteggere il traffico e a ridurre al minimo l'impatto di una chiave compromessa o di una svolta crittografica. Google rende disponibile anche la crittografia dei dati inattivi, utilizzando almeno AES128 o simili. GDCE ha un'integrazione CMEK; ulteriori informazioni sono disponibili all'indirizzo https://cloud.google.com/kms/docs/cmek .

*Connessione a Cloud VPN* . Google consente al Cliente di abilitare e configurare un'interconnessione potente e crittografata tra l'Apparecchiatura e il Virtual Private Cloud del Cliente utilizzando Cloud VPN tramite una connessione VPN IPSEC.

*Deposito vincolato* . L'archiviazione dei dati del cliente è vincolata al server. Se un disco viene rubato o copiato mentre è inattivo, il contenuto di tale disco sarà irrecuperabile al di fuori del server.

- Le sezioni 2 (Accessi e controlli del sito) e 3 (Dati) dell'Appendice 2 (Misure di sicurezza) sono cancellate.

**2. Disposizioni inapplicabili.** Eventuali obblighi di Google contenuti nel Contratto (incluso il presente Addendum) o dichiarazioni nella documentazione di sicurezza associata (inclusi i white paper) che dipendono dal funzionamento di un data center di Google da parte di Google non si applicano al GDCE.

**Multi-cloud gestito da Google (Google Cloud Platform)**

I servizi multi-cloud gestiti da Google coinvolgono infrastrutture di terze parti e, in base alla progettazione, presentano alcune caratteristiche distinte.

**1. Definizione aggiuntiva.**

- Per " *Emendamento sull'elaborazione dei dati MCS gestito da Google* " si intendono i termini disponibili all'indirizzo https://cloud.google.com/terms/mcs-data-processing-terms .

**2. Termini per il trattamento dei dati multi-cloud.** L'Emendamento sull'elaborazione dei dati MCS gestito da Google integra e modifica la presente Appendice in relazione ai servizi multi-cloud gestiti da Google per Google Cloud Platform.

**Google Cloud VMware Engine (Google Cloud Platform)**

Google potrebbe non avere accesso all'ambiente VMware del Cliente o essere in grado di crittografare i dati personali nell'ambiente VMware del Cliente.

**Volumi NetApp (Google Cloud Platform)**

**1. Emendamenti.** Il presente Addendum viene modificato come segue rispetto ai Volumi NetApp:

- La definizione di "Revisore esterno di Google" è sostituita dalla seguente:
- Per " *Revisore dei conti di terze parti di Google* " si intende un revisore dei conti di terze parti qualificato e indipendente nominato da Google o da un sub-responsabile del trattamento di NetApp Volumes, la cui identità attuale Google rivelerà al Cliente su richiesta.
- La sezione 3(a) (Archiviazione, isolamento e registrazione dei dati) dell'Appendice 2 (Misure di sicurezza) è sostituita dalla seguente:
- (a) *Archiviazione, isolamento e registrazione dei dati* . Google memorizza i dati in un ambiente multi-tenant su server di proprietà di NetApp, Inc. Salvo eventuali istruzioni contrarie (ad esempio sotto forma di selezione della posizione dei dati), Google replica i dati del cliente tra più data center geograficamente dispersi. Google inoltre isola logicamente i dati dei clienti. Al cliente verrà dato 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.

**2. Certificazioni di conformità e rapporti SOC** . Google o il suo Subresponsabile otterranno almeno quanto segue (o un'alternativa equivalente o migliorata) per NetApp Volumes:

UN. un certificato ISO 27001 e un attestato di conformità PCI DSS (le " *Certificazioni di conformità NetApp* "); E

B. Report SOC 1 e SOC 2 aggiornati annualmente sulla base di un audit eseguito almeno una volta ogni 12 mesi (i " *Report SOC NetApp* ").

**3. Revisioni della documentazione di sicurezza** . Per dimostrare la conformità da parte di Google agli obblighi previsti dal presente Addendum, Google renderà disponibili le certificazioni di conformità NetApp e i report SOC NetApp per la revisione da parte del Cliente e, se il Cliente è un responsabile del trattamento, consentirà al Cliente di richiedere l'accesso per il titolare del trattamento pertinente ai Report SOC NetApp in conformità con la Sezione 7.5.3 (Termini commerciali aggiuntivi per revisioni e audit).

Google Workspace e Cloud Identity

**1. Definizioni aggiuntive.**

- Per " *Account* ", se non definito nel Contratto, si intende l'account Google Workspace o Cloud Identity del Cliente.
- Per " *Cloud Identity* " se acquistato ai sensi di un Contratto autonomo e non come parte di Google Cloud Platform o Google Workspace, si intendono i Servizi Cloud Identity descritti all'indirizzo https://cloud.google.com/terms/identity/user-features .

- Per " *Dati del cliente* ", se non definiti nel Contratto, si intendono i 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.
- Per " *Google Workspace* " si intendono i servizi Google Workspace o Google Workspace for Education descritti all'indirizzo https://workspace.google.com/terms/user_features.html , a seconda dei casi.

**2. 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 i Prodotti aggiuntivi tramite la Console di amministrazione e non dovrà utilizzare i Prodotti aggiuntivi per utilizzare Google Workspace o Cloud Identity; E

B. se il Cliente sceglie di installare Prodotti aggiuntivi o di utilizzarli con Google Workspace o Cloud Identity, i Prodotti aggiuntivi potranno accedere ai Dati del cliente come richiesto per interagire con Google Workspace o Cloud Identity, a seconda dei casi.

Per chiarezza, la presente Appendice non si applica al trattamento dei dati personali in relazione alla fornitura di eventuali Prodotti aggiuntivi installati o utilizzati dal Cliente, compresi i dati personali trasmessi a o da tali Prodotti aggiuntivi.

**3. Certificazioni di conformità.** Le certificazioni di conformità per Google Workspace e Cloud Identity Audited Services includeranno anche i certificati ISO 27017 e ISO 27018.

**4. Posizioni dei data center.** Le posizioni dei data center di Google Workspace e Cloud Identity sono descritte all'indirizzo https://www.google.com/about/datacenters/locations/ .

**5. Informazioni sui Subresponsabili.** Nomi, posizioni e attività dei sub-responsabili di Google Workspace e Cloud Identity sono descritti all'indirizzo https://workspace.google.com/intl/en/terms/subprocessors.html .

**6. Team per la protezione dei dati nel cloud.** Il team di protezione dei dati per Google Workspace e Cloud Identity (mentre gli amministratori hanno effettuato l'accesso al proprio account amministratore) può essere contattato all'indirizzo https://support.google.com/a/contact/googlecloud_dpr .

**7. Misure di sicurezza aggiuntive.** Per Google Workspace e Cloud Identity:

UN. Google separa logicamente i dati di ciascun Utente finale dai dati di altri Utenti finali; E

B. i dati di un Utente finale autenticato non verranno visualizzati da un altro Utente finale (a meno che l'ex Utente finale o un Amministratore non consenta la condivisione dei dati).

**8 . Informazioni sui trasferimenti limitati** . Ulteriori informazioni relative ai trasferimenti limitati, ai controlli di sicurezza aggiuntivi e ad altre misure di protezione supplementari sono disponibili all'indirizzo cloud.google.com/privacy/ .

**9. Addendum sui dati di servizio.** Se Google rende disponibile per l'accettazione da parte del Cliente un Addendum sui dati di servizio facoltativo in relazione al presente Addendum, la disponibilità di tale addendum facoltativo costituirà un "Aggiornamento DPA" se tale termine è definito in qualsiasi Addendum sui dati di servizio precedentemente stipulato dal Cliente.

**10. Termini specifici del servizio.**

**AppSheet (Google Workspace)**

**1. Emendamenti.** Il presente Addendum è modificato come segue rispetto ad AppSheet:

- Il paragrafo intitolato "Sistemi operativi del server" nella Sezione 1(a) dell'Appendice 2 (Misure di sicurezza) è sostituito con il seguente:
- *Sistemi operativi per server* . I server di Google utilizzano un'implementazione basata su Linux personalizzata per l'ambiente applicativo.

**2. Posizioni aggiuntive dei data center.** Ulteriori posizioni dei data center per AppSheet sono descritte all'indirizzo https://cloud.google.com/about/locations/ .

Guardatore (originale)

**1. Definizioni aggiuntive.**

- Per " *Console di amministrazione* " si intende qualsiasi console di amministrazione applicabile a ciascuna Istanza.
- Per " *Emendamento sull'elaborazione dei dati MCS gestito da Google* " si intendono, se applicabili, i termini disponibili all'indirizzo https://cloud.google.com/terms/mcs-data-processing-terms .
- Per " *Servizi multi-cloud gestiti da Google* " si intendono, se applicabili, i servizi, i prodotti e le funzionalità Google specificati ospitati sull'infrastruttura di un fornitore cloud di terze parti.
- Per " *Looker (originale)* " si intende una piattaforma integrata (inclusa l'infrastruttura basata su cloud, se applicabile, e i componenti software, comprese eventuali API associate) che consente alle aziende di analizzare dati e definire metriche aziendali su più origini dati rese disponibili da Google al Cliente ai sensi del Accordo. Looker (originale) esclude le Offerte di terze parti.
- " *Fornitore* di terze parti *di servizi multi-cloud* " ha il significato indicato nell'Emendamento sull'elaborazione dei dati MCS gestito da Google.
- " *Modulo d'ordine* " ha il significato indicato nel Contratto, a meno che il Cliente non abbia acquistato tramite un rivenditore o un mercato online o utilizzi Looker solo a scopo di prova o di valutazione nell'ambito di un contratto di prova o di valutazione, nel qual caso Modulo d'ordine può indicare un'altra forma scritta ( email o altro mezzo elettronico consentito) come autorizzato da Google.

**2. Emendamenti.** Il presente Addendum è modificato come segue rispetto a Looker (originale):

- La definizione di “Indirizzo email di notifica” è sostituita dalla seguente:
- "Indirizzo email di notifica" indica gli indirizzi email indicati dal Cliente nel Modulo d'ordine o tramite Looker (a seconda dei casi) per ricevere determinate notifiche da Google.
- Le definizioni di "SCC (da controller a processore)", "SCC (da processore a controller)", "SCC (da processore a processore)" e "SCC (da processore a processore, esportatore di Google)" in L'Appendice 3 (Norme specifiche sulla privacy) è sostituita dalla seguente:
- Per " *SCC (da controller a processore)* " si intendono i termini presenti all'indirizzo: https://cloud.google.com/terms/looker/legal/sccs/eu-c2p ;
- Per " *SCC (processore-controllore)* " si intendono i termini presenti all'indirizzo: https://cloud.google.com/terms/looker/legal/sccs/eu-p2c ;
- Per " *SCC (processore a processore)* " si intendono i termini presenti all'indirizzo: https://cloud.google.com/terms/looker/legal/sccs/eu-p2p ; E
- Per " *SCC (processore a processore, Google Exporter)* " si intendono i termini disponibili all'indirizzo: https://cloud.google.com/terms/looker/legal/sccs/eu-p2p-intra-group .
- Alla fine della Sezione 10.1 (Strutture di archiviazione ed elaborazione dei dati) vengono aggiunte le seguenti parole: "o laddove eventuali fornitori di servizi multi-cloud di terze parti mantengano strutture".

**3. Ulteriori responsabilità in materia di sicurezza del cliente.** Il Cliente è responsabile della sicurezza del proprio ambiente, dei database e della configurazione di Looker (originale), esclusi i sistemi gestiti e controllati da Google.

**4. Certificazioni di conformità e rapporti SOC.** Le certificazioni di conformità e i report SOC per i servizi controllati da Looker (originale) possono variare in base all'ambiente di hosting in cui vengono utilizzati i servizi pertinenti. Su richiesta, Google fornirà i dettagli delle certificazioni di conformità e dei rapporti SOC disponibili per ambienti di hosting specifici.

**5. Posizioni dei data center.** Le ubicazioni dei data center Looker (originali) saranno descritte nel Modulo d'ordine applicabile o altrimenti identificate da Google.

**6. Nessuna certificazione da parte di clienti non EMEA.** Il Cliente non è obbligato a certificare o identificare la propria Autorità di controllo competente come descritto nella Sezione 4.2 (Certificazione da parte di clienti non EMEA) dei termini europei sulla protezione dei dati nell'Appendice 3 (Leggi specifiche sulla privacy) per Looker (originale).

**7. Informazioni sui trasferimenti limitati.** Ulteriori informazioni relative ai trasferimenti limitati, ai controlli di sicurezza aggiuntivi e ad altre misure di protezione supplementari per Looker (originale) sono disponibili all'indirizzo https://docs.looker.com .

**8. Informazioni sui Subresponsabili.** Nomi, sedi e attività dei subresponsabili di Looker (originale) sono descritti all'indirizzo:

UN. https://cloud.google.com/terms/looker/privacy/lookeroriginal-subprocessors e

B. https://cloud.google.com/terms/subprocessors .

**9. Multi-cloud gestito da Google (Looker (originale))**

I servizi multi-cloud gestiti da Google coinvolgono infrastrutture di terze parti e, in base alla progettazione, presentano alcune caratteristiche distinte.

9.1 *Termini per il trattamento dei dati multi-cloud* . L'Emendamento sull'elaborazione dei dati MCS gestito da Google integra e modifica la presente Appendice rispetto ai servizi multi-cloud gestiti da Google per Looker (originale).

**10. Team per la protezione dei dati nel cloud.** Il team per la protezione dei dati di Looker (originale) può essere contattato all'indirizzo https://support.google.com/cloud/contact/dpo .

**11. Dati di elaborazione di Google.** Nella misura in cui qualsiasi Legge sulla privacy applicabile richiede a Google di raccogliere e conservare registrazioni di determinate informazioni relative al Cliente, il Cliente fornirà tali informazioni a Google su richiesta e notificherà a Google eventuali aggiornamenti necessari per mantenere tali informazioni accurate e aggiornate, a meno che Google non richieda al Cliente di fornire e aggiornare tali informazioni tramite altri mezzi.

**12. Ulteriori misure di sicurezza dell'applicazione.** Google implementerà e manterrà le misure di sicurezza aggiuntive descritte di seguito per Looker (originale):

UN. Google segue almeno le pratiche standard del settore per l'architettura di sicurezza. I server proxy utilizzati per le applicazioni di Google aiutano a proteggere l'accesso a Looker fornendo un unico punto per filtrare gli attacchi tramite la lista nera IP e la limitazione della velocità di connessione.

B. Gli amministratori del cliente controllano l'accesso alle applicazioni da parte del personale Google per fornire il supporto tecnico richiesto dal cliente o dagli utenti finali.

Servizi SecOps

**1. Definizioni aggiuntive.**

- Per " *Account* ", se non definito nel Contratto, si intende l'account dei Servizi SecOps o di Google Cloud Platform del Cliente, a seconda dei casi.
- Per " *Dati del cliente* ", se non definiti nel Contratto, si intendono i dati forniti a Google dal Cliente o dagli Utenti finali tramite i Servizi SecOps nell'Account.
- Per " *Servizi SecOps* " si intendono Chronicle SIEM, Chronicle SOAR e Mandiant Solutions, ciascuno come descritto all'indirizzo https://cloud.google.com/terms/secops/services , escluse eventuali Offerte di terze parti. A scanso di equivoci, i servizi SecOps escludono i servizi gestiti Mandiant e i servizi di consulenza Mandiant.

- Per " *Offerte di terze parti* ", se non definito nel Contratto, si intendono (a) servizi, software, prodotti e altre offerte di terze parti che non sono incorporati nei Servizi o nel Software SecOps e (b) sistemi operativi di terze parti.

**2. Emendamenti.** Il presente Addendum è modificato come segue rispetto ai servizi SecOps:

- La definizione di “Controlli di Sicurezza Aggiuntivi” è sostituita con la seguente:
- *Per "Controlli di sicurezza aggiuntivi"* si intendono le risorse di sicurezza, le caratteristiche, le funzionalità e/o i controlli (se presenti) che il Cliente può utilizzare a sua discrezione e/o come determina, inclusi (se presenti) crittografia, registrazione e monitoraggio, gestione dell'identità e degli accessi, e scansione di sicurezza.
- La definizione di “Servizi sottoposti a revisione” è sostituita dalla seguente:
- Per " *Servizi controllati* " si intendono i servizi SecOps allora attuali indicati come rientranti nell'ambito della certificazione o del rapporto pertinente all'indirizzo https://cloud.google.com/security/compliance/secops/services-in-scope . Google non può rimuovere alcun servizio SecOps da questo URL a meno che non sia stato interrotto in conformità al contratto applicabile.
- Le definizioni di "SCC (da controller a processore)", "SCC (da processore a controller)", "SCC (da processore a processore)" e "SCC (da processore a processore, esportatore di Google)" in L'Appendice 3 (Norme specifiche sulla privacy) è sostituita dalla seguente:
- "SCC (da controller a processore)" indica i termini su: https://cloud.google.com/terms/secops/sccs/eu-c2p
- Per "SCC (processore-controllore)" si intendono i termini disponibili all'indirizzo: https://cloud.google.com/terms/secops/sccs/eu-p2c .
- Per "SCC (da processore a processore)" si intendono i termini presenti all'indirizzo: https://cloud.google.com/terms/secops/sccs/eu-p2p
- Per "SCC (processore a processore, Google Exporter)" si intendono i termini presenti all'indirizzo: https://cloud.google.com/terms/secops/sccs/eu-p2p-google-exporter
- La sezione 7.4 (Certificazioni di conformità e rapporti SOC) dell'Addendum viene modificata come segue:
- 7.4 *Certificazioni di conformità e rapporti SOC* . Google manterrà almeno le certificazioni e i report identificati all'indirizzo https://cloud.google.com/security/compliance/secops/services-in-scope per i Servizi controllati al fine di verificare la continua efficacia delle Misure di sicurezza ("Conformità" Certificazioni” e “Rapporti SOC”).

  Google può aggiungere standard in qualsiasi momento. Google può sostituire una certificazione di conformità o un rapporto SOC con un'alternativa equivalente o migliorata.

**3. Posizioni dei data center.** Le ubicazioni dei data center dei servizi SecOps sono descritte all'indirizzo https://cloud.google.com/terms/secops/data-residency .

**4. Nessuna certificazione da parte di clienti non EMEA.** Il Cliente non è obbligato a certificare o identificare la propria Autorità di vigilanza competente come descritto nella Sezione 4.2 (Certificazione da parte di clienti non EMEA) dei termini europei sulla protezione dei dati nell'Appendice 3 (Leggi specifiche sulla privacy) per i Servizi SecOps.

**5. Informazioni sui Subresponsabili.** Nomi, posizioni e attività dei subresponsabili dei servizi SecOps sono descritti all'indirizzo https://cloud.google.com/terms/secops/subprocessors .

**6. Team per la protezione dei dati nel cloud.** Il team di protezione dei dati per i servizi SecOps può essere contattato all'indirizzo https://support.google.com/cloud/contact/dpo (e/o tramite altri mezzi che Google può fornire di volta in volta).

**7. Dati di elaborazione di Google.** Nella misura in cui qualsiasi Legge sulla privacy applicabile richiede a Google di raccogliere e conservare registrazioni di determinate informazioni relative al Cliente, il Cliente fornirà tali informazioni a Google su richiesta e notificherà a Google eventuali aggiornamenti necessari per mantenere tali informazioni accurate e aggiornate, a meno che Google non richieda al Cliente di fornire e aggiornare tali informazioni tramite altri mezzi.