Cloud Data Processing Addendum (clienti)

Il presente Cloud Data Processing Addendum (comprese le sue appendici, l'"*Addendum*") viene incorporato nel Contratto (come definito di seguito) tra Google e il Cliente. Il presente Addendum era precedentemente noto come "Termini per il trattamento e la sicurezza dei dati" ai sensi di un Contratto per Google Cloud Platform, Looker (original), i Servizi Google SecOps o Google Cloud Skills Boost per le Organizzazioni; l'"Emendamento sul trattamento dei dati" ai sensi di un Contratto per Google Workspace o Cloud Identity; e l'"Data Processing Addendum" ai sensi di un Contratto per Mandiant Consulting Services e Managed Services.

Termini generali

1. Panoramica

Il presente Addendum descrive le obbligazioni delle parti, anche ai sensi delle leggi applicabili in materia di privacy, sicurezza e 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 validità dell'Addendum (come definita di seguito) e sostituirà qualsiasi termine precedentemente applicabile al trattamento e alla sicurezza dei Dati del Cliente. I termini con l'iniziale maiuscola utilizzati nel presente Addendum hanno il significato a loro attribuito nel Contratto.

2. Definizioni

2.1 Nel presente Addendum:

- Per "*Data di validità dell'Addendum*" si intende la data in cui il Cliente accetta, oppure le parti altrimenti concordano, il presente Addendum.
- Per "*Controlli di sicurezza aggiuntivi*" si intendono risorse, caratteristiche, funzionalità e controlli relativi alla sicurezza che il Cliente può utilizzare a propria scelta e discrezione, inclusi la Console di amministrazione, la crittografia, il logging e il monitoraggio, la gestione di identità e accessi, l'analisi della 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, per quanto riguarda il trattamento dei Dati personali del Cliente, qualsiasi legge o regolamento nazionale, federale, dell'Unione Europea, statale. provinciale o altro in materia di privacy, sicurezza dei dati e protezione dei dati.

- Per "*Servizi controllati*" si intendono i Servizi attualmente rientranti nell'ambito di applicazione della certificazione o del report pertinente all'indirizzo https://cloud.google.com/security/compliance/services-in-scope. Google non potrà rimuovere alcun Servizio da questo URL a meno che non sia più disponibile in conformità con il Contratto vigente.

- Per "*Certificazioni di conformità*" si intende il significato indicato alla Sezione 7.4 (Certificazioni di conformità e Report SOC).

- Per "*Dati del Cliente*", se non definito nel Contratto, si intende quanto indicato nell'Appendice 4 (Prodotti specifici).

- Per "*Dati personali del Cliente*" si intendono i dati personali presenti all'interno dei dati del Cliente, inclusa qualsiasi categoria speciale di dati personali o dati sensibili definiti ai sensi della legge vigente sulla privacy.

- Per "*Incidente relativo ai dati*" si intende una violazione dei sistemi di sicurezza di Google che comporta la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso accidentali o illeciti ai Dati del Cliente presenti nei sistemi gestiti o controllati in altro modo da Google.

- Per "*EMEA*" si intendono Europa, Medio Oriente e Africa.

- Per "*GDPR dell'Unione Europea*" si intende il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 sulla protezione delle persone fisiche in merito al trattamento dei dati personali, nonché alla libera circolazione di questi dati e che abroga la direttiva 95/46/CE.

- Per "*Legge europea sulla protezione dei dati*" si intendono, a seconda dei casi: (a) il GDPR; o (b) il FADP svizzero.

- Per "*Legge europea*" si intendono, a seconda dei casi: (a) le leggi dell'Unione Europea o di uno Stato Membro dell'Unione Europea (se il GDPR dell'Unione Europea è applicabile al trattamento dei Dati personali del Cliente); (b) le leggi del Regno Unito o di una parte del Regno Unito (se il GDPR del Regno Unito è applicabile al trattamento dei Dati personali del Cliente); o (c) le leggi della Svizzera (se il FADP svizzero è applicabile al trattamento dei Dati personali del Cliente).

- Per "*GDPR*" si intende, a seconda dei casi: (a) il GDPR dell'Unione Europea; o (b) il GDPR del Regno Unito.

- Per "*Revisore di terze parti di Google*" si intende un revisore di terze parti qualificato e indipendente incaricato da Google, la cui identità attuale verrà divulgata da Google al Cliente.

- Per "*Disposizioni*" si intende il significato descritto nella Sezione 5.2 (Conformità con le Disposizioni del Cliente).

- Per "*Indirizzo email di notifica*" si intendono l'indirizzo o gli indirizzi email indicati dal Cliente nella Console di amministrazione o nel Modulo d'ordine per la ricezione di determinate notifiche inviate da Google.

- Per "*Documentazione sulla sicurezza*" si intendono le Certificazioni di conformità e i Report SOC.

- Per "*Misure di sicurezza*" si intende il significato descritto nella Sezione 7.1.1 (Misure di sicurezza di Google).

- Per "*Servizi*" si intendono i servizi applicabili descritti nell'Appendice 4 (Prodotti specifici).

- Per "*Report SOC*" si intende il significato indicato alla Sezione 7.4 (Certificazioni di conformità e Report SOC).

- Per "*Sub-responsabile*" si intende una terza parte autorizzata, in qualità di responsabile aggiuntivo ai sensi del presente Addendum, a trattare i Dati del Cliente allo scopo di fornire parti dei Servizi e dei Servizi di assistenza tecnica (se applicabile).

- Per "*Autorità di controllo*" si intende, a seconda dei casi: (a) un'"autorità di controllo" come definita nel GDPR dell'Unione Europea; o (b) il "Commissioner" come definito nel GDPR del Regno Unito o nel FADP svizzero.

- Per "*FADP svizzero*" si intende, a seconda dei casi, la Legge federale sulla protezione dei dati del 19 giugno 1992 (Svizzera) (con l'Ordinanza alla Legge federale sulla protezione dei dati del 14 giugno 1993) o la Legge federale sulla protezione dei dati modificata del 25 settembre 2020 (Svizzera) (con l'Ordinanza alla Legge federale sulla protezione dei dati del 31 agosto 2022).

- Per "*Periodo di validità*" si intende il periodo di tempo che va dalla Data di validità dell'Addendum fino alla conclusione della fornitura da parte di Google dei Servizi, incluso, se applicabile, qualsivoglia periodo di tempo durante il quale i Servizi possono essere stati sospesi e qualsivoglia periodo di tempo successivo al recesso durante il quale Google può aver continuato a fornire i Servizi allo scopo di consentire una transizione.

- Per "*GDPR del Regno Unito*" si intende il GDPR dell'Unione Europea come emendato e integrato nelle normative del Regno Unito ai sensi del UK European Union (Withdrawal) Act 2018 e dalla legislazione secondaria vigente promulgata ai sensi di questa legge.

2.2 I termini "dati personali", "interessato", "trattamento", "titolare" e "responsabile", come utilizzati nel presente Addendum, hanno i significati descritti dalla Legge vigente sulla privacy o, in assenza di questo significato o legge, dal GDPR dell'Unione Europea.

2.3 I termini "interessato", "titolare" e "responsabile" includono "consumatori", "aziende" e "fornitori di servizi", rispettivamente, come previsto dalla Legge vigente sulla privacy.

3. Durata

Indipendentemente dal fatto che il Contratto vigente sia stato oggetto di recesso o sia scaduto, il presente Addendum resterà in vigore fino a quando Google non avrà eliminato tutti i Dati del Cliente, come descritto nel presente Addendum, momento in cui quest'ultimo scadrà automaticamente.

4. Ruoli; Conformità legale

4.1 *Ruoli delle parti.* Google è responsabile e il Cliente è titolare o responsabile, 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 dati).

4.3 *Conformità alla legge*. Le parti si atterranno alle rispettive obbligazioni relative 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 come descritto nell'Appendice 3 (Leggi specifiche sulla privacy), i termini corrispondenti dell'Appendice 3 si applicheranno in aggiunta ai presenti Termini generali e prevarranno come descritto nella Sezione 14.1 (Precedenza).

5. Trattamento dei dati

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

a. Il Cliente garantisce su base continuativa che il titolare pertinente ha autorizzato:

i. le disposizioni;

ii. il coinvolgimento di Google da parte del Cliente come ulteriore responsabile del trattamento; e

iii. il coinvolgimento di sub-responsabili da parte di Google come descritto nella Sezione 11 (Sub-responsabili);

b. Il Cliente inoltrerà al titolare in questione tempestivamente e senza ritardi ingiustificati eventuali notifiche fornite da Google ai sensi della Sezione 7.2.1 (Notifica degli incidenti), 9.2.1 (Responsabilità per le richieste), o 11.4 (Facoltà di opporsi a modifiche relative ai Sub-responsabili); e

c. Il Cliente può rendere disponibili al titolare pertinente tutte le altre informazioni rese disponibili da Google ai sensi dell'Addendum in merito all'ubicazione dei data center di Google o ai nomi, alle ubicazioni e alle attività dei Sub-responsabili.

5.2 *Conformità con le Disposizioni del Cliente*. Il Cliente istruisce Google circa il trattamento dei Dati del Cliente ai sensi del Contratto vigente (incluso il presente Addendum) esclusivamente come segue:

a. per fornire, proteggere e monitorare i Servizi e i TSS (se applicabile); e

b. come ulteriormente specificato mediante:

i. L'uso da parte del Cliente dei Servizi (anche mediante la Console di amministrazione) e dei TSS (se applicabile); e

ii. Qualsiasi altra disposizione scritta fornita al Cliente e riconosciuta da Google come disposizione costitutiva ai sensi del presente Addendum

(collettivamente, le "*Disposizioni*").

Google agirà in maniera conforme alle Disposizioni, salvo se vietato dalle Leggi europee, nel caso in cui si applichi la Legge europea sulla protezione dei dati, o se proibito dalla legge vigente, nel caso in cui si applichi qualsiasi altra legge sulla privacy applicabile.

6. Eliminazione dei dati

6.1 *Eliminazione da parte del Cliente*. Durante il Periodo di validità, Google consentirà al Cliente di eliminare i Dati del Cliente in modo conforme alle funzionalità dei Servizi. Se, durante il Periodo di validità, il Cliente utilizza i Servizi per eliminare Dati del Cliente e questi non possono essere recuperati dal Cliente, questo utilizzo costituirà una Disposizione che richiede l'eliminazione da parte di Google dei Dati del Cliente pertinenti dai sistemi di Google. Google adempirà a questa Disposizione non appena ragionevolmente possibile ed entro un periodo massimo di 180 giorni, a meno che la Legge europea non richieda l'archiviazione dei dati, qualora si applicasse la Legge europea sulla protezione dei dati, o a meno che la legge applicabile non richieda l'archiviazione, qualora si applicasse qualsiasi altra legge sulla privacy.

6.2 *Restituzione o eliminazione alla fine del Periodo di validità*. Se il Cliente desidera conservare i Dati del Cliente dopo la scadenza del Periodo di validità, durante questo Periodo può dare a Google disposizioni affinché i dati gli vengano restituiti, in conformità con la Sezione 9.1 (Accesso, rettifica, trattamento limitato, portabilità). Ai sensi della Sezione 6.3 (Disposizione relativa all'eliminazione differita), il Cliente dà a Google disposizioni affinché tutti i Dati del Cliente rimanenti (incluse le copie esistenti) vengano eliminati dai sistemi Google. Trascorso un periodo di recupero di massimo 30 giorni da questa data, Google ottempererà a questa disposizione non appena ragionevolmente possibile ed entro un periodo massimo di 180 giorni, a meno che la Legge europea non richieda l'archiviazione dei dati, qualora si applicasse la Legge europea sulla protezione dei dati, o a meno che la legge applicabile non richieda l'archiviazione, qualora si applicasse qualsiasi altra legge sulla privacy.

6.3. *Disposizione relativa all'eliminazione differita*. Nella misura in cui i Dati del Cliente interessati dalla disposizione di eliminazione descritta nella Sezione 6.2 (Restituzione o eliminazione alla scadenza del Periodo di validità) siano anche soggetti a trattamento, alla scadenza del Periodo di validità applicabile ai sensi della Sezione 6.2 riguardi un Contratto con un Periodo di validità la cui scadenza sia successiva, tale disposizione relativa all’eliminazione avrà effetto rispetto ai Dati del Cliente in questione soltanto al termine del Periodo di validità la cui scadenza è più lontana. Per maggiore chiarezza: il presente Addendum continuerà ad applicarsi a tali Dati del Cliente fino alla loro eliminazione da parte di Google.

7. Sicurezza dei dati

7.1 *Misure, controlli e assistenza in materia di sicurezza da parte di Google*.

7.1.1 *Misure di sicurezza di Google*. Google attuerà e manterrà misure tecniche, organizzative e fisiche per evitare che i Dati personali del Cliente vengano, accidentalmente o illecitamente, distrutti, persi o modificati e impedirne la divulgazione e l'accesso non autorizzati come descritto nell'Allegato 2 (Misure di sicurezza) **(**le ***Misure di sicurezza*****")**. Le Misure di sicurezza includono provvedimenti finalizzati a criptare i Dati del Cliente; a contribuire ad assicurare il mantenimento su base continuativa della riservatezza, dell'integrità, della disponibilità e della resilienza dei sistemi e dei servizi di Google; a contribuire al ripristino tempestivo dell'accesso ai Dati del Cliente in seguito a un incidente e a eseguire test di efficienza regolari. Google potrà periodicamente aggiornare le Misure di sicurezza, a condizione che tali i aggiornamenti non comportino un deterioramento sostanziale della sicurezza dei Servizi.

7.1.2 *Accesso e conformità*. Google:

a. autorizzerà i propri dipendenti, appaltatori e Sub-responsabili ad accedere ai Dati del Cliente esclusivamente nella misura necessaria ad adempiere alle Disposizioni;

b. adotterà misure appropriate per garantire la conformità con le Misure di sicurezza da parte dei propri dipendenti, appaltatori e Sub-responsabili in base alla portata delle rispettive prestazioni; e

c. garantirà che tutte le persone autorizzate al trattamento dei Dati del Cliente siano vincolate da un obbligo di riservatezza.

7.1.3 *Controlli di Sicurezza aggiuntivi*. Google metterà a disposizione Controlli aggiuntivi per la sicurezza per:

a. consentire al Cliente di adottare misure necessarie per la protezione dei Dati del Cliente; e

b. fornire al Cliente informazioni sulla protezione, l'accesso e l'utilizzo dei Dati del Cliente.

7.1.4 *Assistenza di Google in materia di sicurezza*. Google (tenendo presente la natura del trattamento dei Dati personali del Cliente) fornirà assistenza al Cliente per garantire la conformità con le sue (o, se il Cliente è un responsabile, quelle del titolare in questione) obbligazioni in relazione alla sicurezza e alle violazioni dei dati personali ai sensi della legge sulla privacy applicabile:

a. implementare e mantenendo delle Misure di sicurezza di cui alla Sezione 7.1.1 (Misure di sicurezza di Google);

b. fornendo Controlli di Sicurezza aggiuntivi, in conformità con quanto indicato nella Sezione 7.1.3 (Controlli di Sicurezza aggiuntivi);

c. rispettando i termini di cui alla Sezione 7.2 (Incidenti relativi ai dati);

d. mettendo a disposizione la Documentazione sulla sicurezza in conformità con la Sezione 7.5.1 (Revisioni della Documentazione sulla sicurezza) e fornendo le informazioni contenute nel Contratto vigente (compreso il presente Addendum); e

e. se le sottosezioni (a)-(d) riportate sopra non sono sufficienti affinché il Cliente (o il titolare del trattamento pertinente) possa ottemperare a queste obbligazioni, fornendo al Cliente, su richiesta di quest'ultimo, ragionevoli collaborazione e assistenza aggiuntive.

7.2 *Incidenti relativi ai dati.*.

7.2.1 *Notifica degli incidenti*. Nel momento in cui Google viene a conoscenza di un Incidente relativo ai dati, ne informerà il Cliente tempestivamente e senza ingiustificato ritardo e adotterà prontamente misure ragionevoli per ridurre al minimo i danni e salvaguardare i Dati del Cliente.

7.2.2 *Dettagli dell'Incidente relativo ai dati*. La notifica inviata da Google in relazione a un Incidente relativo ai dati descriverà: la natura dell'Incidente relativo ai dati, incluse le risorse del Cliente interessate; i provvedimenti che Google ha adottato, o prevede di adottare, per gestire l'Incidente relativo ai dati e mitigare i potenziali rischi; le eventuali misure che Google consiglia al Cliente di adottare per gestire l'Incidente relativo ai dati, nonché i dettagli di un punto di contatto presso il quale è possibile ottenere ulteriori informazioni. Se non è possibile fornire tutte queste informazioni contemporaneamente, la notifica iniziale di Google conterrà le informazioni disponibili al momento e informazioni ulteriori verranno comunicate senza ingiustificato ritardo non appena diventino disponibili.

7.2.3 *Nessuna valutazione dei Dati del Cliente da parte di Google.*. Google non ha alcuna obbligazione di valutare i Dati del Cliente allo scopo di identificare informazioni soggette a qualsivoglia requisito legale specifico.

7.2.4 *Nessuna ammissione di colpa da parte di Google*. La notifica o la risposta di Google concernente un Incidente relativo ai dati ai sensi della presente Sezione 7.2 (Incidenti relativi ai dati) non dovrà essere interpretata come un'ammissione di colpa o responsabilità da parte di Google in merito all'Incidente relativo ai dati.

7.3 Responsabilità e valutazione del Cliente in materia di sicurezza.

7.3.1 Responsabilità del Cliente in materia di sicurezza. Fatti salvi gli obblighi di Google indicati nelle sezioni 7.1 (Misure, controlli e assistenza in materia di sicurezza da parte di Google) e 7.2 (Incidenti relativi ai dati), nonché altrove nel Contratto vigente, il Cliente è responsabile per il proprio utilizzo dei Servizi e l'archiviazione di qualsiasi copia dei Dati del Cliente al di fuori dei sistemi di Google o dei sub-responsabili di Google, inclusi:

a. L'utilizzo dei Servizi e dei Controlli di Sicurezza aggiuntivi per assicurare un livello di sicurezza adeguato ai rischi a cui sono esposti i Dati del Cliente;

b. La protezione delle credenziali di autenticazione degli account, dei sistemi e dei dispositivi utilizzati dal Cliente per accedere ai Servizi; e

c. Il backup o la conservazione di copie dei propri Dati del Cliente, ove appropriato.

7.3.2 *Valutazione della sicurezza da parte del Cliente*. Il Cliente conviene che i Servizi, le Misure di sicurezza, i Controlli di Sicurezza aggiuntivi per la sicurezza e gli impegni assunti da Google ai sensi della presente Sezione 7 (Sicurezza dei dati) forniscono un livello di sicurezza appropriato ai rischi a cui sono esposti i Dati del Cliente (tenuto conto del livello di sviluppo della tecnologia, dei costi di implementazione, della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento dei Dati del Cliente, nonché dei rischi a cui sono esposte le persone fisiche).

7.4 *Conformità, certificazioni e Report SOC*. In relazione ai Servizi controllati, Google provvederà a mantenere almeno quanto segue, allo scopo di verificare la continua efficacia delle Misure di sicurezza:

a. Le certificazioni relative agli standard ISO 27001 e qualsiasi altra certificazione descritta nell'Appendice 4 (Prodotti specifici) (le "*Certificazioni di conformità*"); e

b. I report SOC 2 e SOC 3 elaborati dal Revisore di terze parti di Google e aggiornati ogni anno in base a controlli eseguiti almeno una volta ogni 12 mesi (i "*Report SOC*").

Google potrebbe aggiungere altri standard di volta in volta. Google ha facoltà di sostituire una Certificazione di conformità o un Report SOC con un'alternativa equivalente o migliore.

7.5 *Revisioni e Audit di conformità*.

7.5.1 *Revisioni della Documentazione sulla sicurezza*. Al fine di provare la conformità ai suoi obblighi ai sensi del presente Addendum, Google metterà a disposizione del Cliente, per la sua revisione, la Documentazione sulla sicurezza e, se il Cliente è un responsabile, permetterà al Cliente di richiedere accesso ai Report SOC per il titolare in questione ai sensi della Sezione 7.5.3 (Termini commerciali aggiuntivi per le revisioni e gli audit).

7.5.2 *Diritti di Audit del Cliente*.

a. *Audit del Cliente*. Google, se richiesto dalla Legge sulla privacy applicabile, consentirà al Cliente o a un revisore indipendente nominato dal Cliente di condurre controlli (incluse le ispezioni) per verificare il rispetto da parte di Google delle obbligazioni previste dal presente Addendum, in conformità con la Sezione 7.5.3 (Termini commerciali aggiuntivi per le revisioni e i controlli). Durante un controllo, Google collaborerà ragionevolmente con il Cliente o con il suo revisore, come descritto nella presente Sezione 7.5 (Revisioni e controlli di conformità).

b. *Valutazione indipendente del Cliente*. Il Cliente ha facoltà di eseguire controlli per verificare la conformità di Google alle sue obbligazioni ai sensi del presente Addendum mediante la revisione della Documentazione in materia di sicurezza, che riflette i risultati dei controlli eseguiti dal Revisore di terze parti di Google.

7.5.3 *Termini commerciali aggiuntivi per le revisioni e gli audit*.

a. Il Cliente deve contattare il team di Google dedicato alla protezione dei dati cloud e richiedere:

i. accesso ai Report SOC per un determinato titolare ai sensi della Sezione 7.5.1 (Revisioni della Documentazione sulla sicurezza); o

ii. un controllo ai sensi della Sezione 7.5.2(a) (Audit del Cliente).

b. In seguito al ricevimento della richiesta del Cliente di cui alla Sezione 7.5.3(a), Google e il Cliente si confronteranno e converranno in anticipo su:

i. i controlli sulla sicurezza e sulla riservatezza applicabili a qualsiasi accesso ai Report SOC da parte di un determinato titolare ai sensi della Sezione 7.5.1 (Revisioni della Documentazione sulla sicurezza); e

ii. la ragionevole data di inizio, l'ambito, la durata e le verifiche applicabili in materia di sicurezza e riservatezza dei controlli di cui alla Sezione 7.5.2(a) (Audit del Cliente).

c. Google può addebitare una commissione (basata sulle spese ragionevolmente sostenute da Google) per eventuali controlli di cui alla Sezione 7.5.2(a) (Controlli del Cliente). Google fornirà al Cliente ulteriori dettagli su eventuali commissioni applicabili e i relativi criteri di calcolo, prima di questi controlli. Il Cliente si farà carico di eventuali commissioni addebitate dai revisori incaricati dal Cliente per l'esecuzione di tale audit.

d. Google può opporsi in forma scritta alla nomina di un revisore da parte del Cliente per l'esecuzione di un audit di cui alla Sezione 7.5.2(a) (Audit del Cliente) qualora questo revisore, in base alla ragionevole opinione di Google, non disponesse dei requisiti necessari o non fosse indipendente, fosse un concorrente di Google o fosse palesemente inadatto per altri motivi. Qualora Google sollevi una di dette obiezioni, il Cliente dovrà nominare un altro revisore o eseguire il controllo per proprio conto.

e. Qualsiasi richiesta da parte del Cliente ai sensi dell'Appendice 3 (Leggi specifiche sulla privacy) o dell'Appendice 4 (Prodotti specifici) di accesso a dei Report SOC per un determinato titolare o nell'ambito di un controllo sarà soggetto anche alla presente Sezione 7.5.3 (Termini commerciali aggiuntivi per le revisioni e i controlli).

8. Valutazioni dell'impatto e consultazioni

Google (tenendo presente la natura del trattamento e le informazioni a disposizione di Google) fornirà assistenza al Cliente al fine di garantire la conformità con i propri (o, nel caso in cui il Cliente sia un responsabile, quelle del titolare in questione) obblighi relativi alle valutazioni della protezione dei dati, alle analisi del rischio, alle precedenti consultazioni normative o a procedure analoghe ai sensi della legge sulla privacy applicabile:

a. mettendo a disposizione Controlli aggiuntivi per la sicurezza in conformità con la Sezione 7.1.3 (Controlli aggiuntivi per la sicurezza) e la Documentazione sulle sicurezza in conformità con la Sezione 7.5.1 (Revisioni della Documentazione sulla sicurezza); e

b. fornendo le informazioni contenute nel Contratto vigente (incluso il presente Addendum); e

c. Se le sottosezioni (a) e (b) riportate sopra non sono sufficienti affinché il Cliente (o il titolare del trattamento pertinente) possa ottemperare a tali obbligazioni, fornendo al Cliente, su richiesta di quest'ultimo, ragionevoli collaborazione e assistenza aggiuntive.

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

9.1 *Accesso, rettifica, trattamento limitato, portabilità*. Durante il Periodo di validità, Google consentirà al Cliente, in modo coerente con le funzionalità dei Servizi, di accedere, rettificare e limitare il trattamento dei Dati del Cliente, anche attraverso la funzionalità di eliminazione fornita da Google di cui alla Sezione 6.1 (Eliminazione da parte del Cliente), nonché di esportare i Dati del Cliente. Se il Cliente viene a conoscenza del fatto che i Dati personali del Cliente sono imprecisi o obsoleti, sarà sua responsabilità utilizzare tali funzionalità per rettificare o eliminare tali dati, qualora richiesto dalla Legge sulla privacy applicabile.

9.2 *Richieste degli interessati*.

9.2.1 *Responsabilità per le richieste*. Se, durante il Periodo di validità, il team di Google dedicato alla protezione dei dati cloud riceve una richiesta da un interessato in relazione ai Dati personali del Cliente e identifica il Cliente, Google:

a. inviterà l'interessato a inviare la richiesta al Cliente;

b. avviserà tempestivamente il Cliente; e

c. non risponderà in altro modo alla richiesta dell'interessato senza l'autorizzazione del Cliente.

Il Cliente sarà responsabile di rispondere a queste richieste anche, ove necessario, tramite l'utilizzo delle funzionalità dei Servizi.

9.2.2 *Assistenza di Google in merito alla richiesta dell'interessato*. Google (tenendo presente la natura del trattamento dei Dati personali del Cliente) fornirà assistenza al Cliente nell'adempimento delle sue obbligazioni (o, nel caso in cui il Cliente sia un responsabile del trattamento, delle obbligazioni del titolare in questione) ai sensi della legge sulla privacy applicabile per quanto riguarda la risposta a richieste relative all'esercizio dei propri diritti da parte degli interessati:

a. fornendo Controlli di Sicurezza aggiuntivi, in conformità con quanto indicato nella Sezione 7.1.3 (Controlli di Sicurezza aggiuntivi);

b. ottemperando a quanto disposto nelle Sezioni 9.1 (Accesso, rettifica, trattamento limitato, portabilità) e 9.2.1 (Responsabilità per le richieste) e .

c. Qualora le sottosezioni (a) e (b) riportate sopra non siano sufficienti affinché il Cliente (o il titolare del trattamento pertinente) possa ottemperare a tali obbligazioni, fornendo al Cliente, su richiesta di quest'ultimo, ragionevoli collaborazione e assistenza aggiuntive.

10. Località del trattamento dati

10.1 *Sedi di archiviazione e trattamento dei dati*. In conformità con quanto previsto dagli impegni assunti da Google in relazione alla posizione dei dati ai sensi dei Termini di Servizio specifici e con quanto disposto nell'Appendice 3 (Leggi specifiche sulla privacy), ove applicabile, i dati del Cliente possono essere trattati in uno qualsiasi dei paesi in cui Google o i suoi Sub-responsabili dispongono di strutture.

10.2 *Informazioni relative ai data center*. Le sedi dei data center di Google sono descritte nell'Appendice 4 (Prodotti specifici).

11. Sub-responsabili

11.1 *Consenso per l'incarico del Sub-responsabile*. Il Cliente autorizza espressamente Google ad assegnare l'incarico di Sub-responsabili alle persone giuridiche indicate come descritto nella Sezione 11.2 (Informazioni sui Sub-responsabili) a partire dalla data di validità dell'Addendum. Inoltre, fatto salvo quanto disposto dalla Sezione 11.4 (Facoltà di opporsi ai Sub-responsabili), il Cliente autorizza in via

generale Google ad assegnare l'incarico di Sub-responsabili ad altre terze parti ("*Nuovi Sub-responsabili*").

11.2 *Informazioni sui Sub-responsabili*. I nomi, le sedi e le attività dei Sub-responsabili sono descritti nell'Appendice 4 (Prodotti specifici).

11.3 *Requisiti per l'incarico del Sub-responsabile*. Al momento di assegnare l'incarico a un qualsiasi Sub-responsabile, Google:

a. Garantirà tramite un contratto scritto che:

i. Il Sub-responsabile acceda e utilizzi i Dati del Cliente esclusivamente nella misura necessaria ad adempiere alle obbligazioni assegnategli e in conformità con il Contratto (incluso il presente Addendum); e

ii. Se previsto dalle leggi sulla privacy applicabili, si impongono le obbligazioni in materia di protezione dei dati descritte nel presente Addendum al Sub-responsabile (come descritto in maggiore dettaglio nell'Appendice 3 (Leggi specifiche sulla privacy)); e

b. Si assumerà la piena responsabilità per tutte le obbligazioni assegnate al Sub-responsabile, così come per tutti i suoi atti e le sue omissioni.

11.4 *Facoltà di opporsi a modifiche relative ai Sub-responsabili*.

a. Qualora Google incarichi un nuovo Sub-responsabile durante il Periodo di validità, almeno 30 giorni prima che il nuovo Sub-responsabile inizi il trattamento dei dati del Cliente, Google comunicherà al Cliente questo incarico (compresi il nome, la sede e le attività del nuovo Sub-responsabile).

b. Il Cliente, entro 90 giorni dalla notifica dell'assegnazione dell'incarico a un Nuovo sub-responsabile, ha facoltà di opporsi tramite recesso, con effetto immediato e senza addurre motivazioni:

i. in conformità con le disposizioni del recesso libero del Contratto; o

ii. in caso di assenza di queste disposizioni, dando notifica a Google.

12. Team dedicato alla protezione dei dati cloud; Registri relativi al trattamento

12.1 *Team di Google dedicato alla protezione dei dati cloud*. Il team di Google dedicato alla protezione dei dati cloud fornirà tempestivamente ragionevole assistenza in relazione a qualsiasi richiesta del Cliente correlata al trattamento dei Dati del Cliente ai sensi del Contratto e può essere contattato come descritto nella sezione Comunicazioni del Contratto vigente o nell'Appendice 4 (Prodotti specifici).

12.2 *Registri relativi al trattamento di Google*. Google conserverà la documentazione appropriata relativa alle proprie attività di trattamento secondo quanto richiesto dalla legge sulla privacy applicabile. Nella misura in cui una legge sulla privacy applicabile richieda a Google di raccogliere e conservare i registri di determinate informazioni relative al Cliente, il Cliente utilizzerà la Console di amministrazione o altri mezzi riportati nell'Appendice 4 (Prodotti specifici) per fornire queste informazioni e far sì che siano sempre accurate e aggiornate. Google può mettere queste informazioni a

disposizione delle autorità di regolamentazione competenti, tra cui l'Autorità di controllo, se richiesto dalla legge sulla privacy applicabile.

12.3 *Richieste del titolare*. Se, durante il Periodo di validità, il team di Google dedicato alla protezione dei dati cloud riceve una richiesta o un'istruzione da una terza parte che sostiene di essere titolare del trattamento dei Dati personali del Cliente, Google inviterà tale terza parte a contattare il Cliente.

13. Comunicazioni

Le Comunicazioni ai sensi del presente Addendum (tra cui le notifiche circa eventuali incidenti relativi ai dati) verranno inviate all'indirizzo email di notifica. Il Cliente è tenuto a usare la Console di amministrazione, o a informare Google in altro modo, per far sì che il suo indirizzo email di notifica sia valido e aggiornato.

14. Interpretazione

14.1 *Precedenza*. In caso di conflitto tra:

a. Appendice 3 (Leggi specifiche sulla privacy) e la parte restante dell'Addendum (compresa l'Appendice 4 (Prodotti specifici)), prevarrà l'Appendice 3; e

b. Appendice 4 (Prodotti specifici) e la parte restante dell'Addendum (a esclusione dell'Appendice 3), prevarrà l'Appendice 4; e

c. Il presente Addendum e la parte restante del Contratto, prevarrà il presente Addendum.

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

14.2 *Riferimenti alle sezioni*. Salvo quanto diversamente specificato, i riferimenti alle sezioni di un'Appendice al presente Addendum si riferiscono alle sezioni dei Termini Generali dell'Addendum.

Appendice 1: Oggetto e dettagli del trattamento dei dati

Oggetto

La fornitura al Cliente dei Servizi e dei TSS (Servizi di assistenza tecnica) da parte di Google (se applicabile).

Durata del trattamento

Il Periodo di validità più il periodo compreso tra la scadenza del Periodo di validità e l'eliminazione di tutti i dati del Partner da parte di Google, in conformità con il presente Addendum.

Natura e scopo del trattamento

Google tratterà i Dati personali del Cliente al fine di fornire al Cliente i Servizi e i TSS (se applicabile) in conformità con il presente Addendum.

Categorie di dati

Dati correlati a privati forniti a Google tramite i Servizi dal Cliente o dagli Utenti finali, o su indicazione del Cliente.

Soggetti interessati

Per soggetti interessati si intendono i privati i cui dati vengono forniti a Google tramite i Servizi dal Cliente o dagli Utenti finali, o su indicazioni del Cliente.

Appendice 2: Misure di sicurezza

A partire dalla Data di validità 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 possiede data center distribuiti in diverse aree geografiche. I data center in cui Google archivia tutti i dati di produzione sono fisicamente sicuri.

Ridondanza. I sistemi dell'infrastruttura sono stati concepiti per eliminare i single point of failure e ridurre al minimo l'impatto dei rischi ambientali prevedibili. Circuiti doppi, switch, reti o altri dispositivi necessari contribuiscono alla realizzazione della ridondanza. I Servizi sono concepiti per consentire a Google di attuare determinate tipologie di manutenzione preventiva e correttiva senza interruzione dell'attività. Tutte le attrezzature e le strutture ambientali dispongono di procedure di manutenzione preventiva documentate che descrivono in dettaglio il processo e la frequenza di esecuzione in conformità con le specifiche interne o del produttore. La manutenzione preventiva e correttiva delle attrezzature dei data center è programmata per mezzo di un procedimento di modifica standard conforme alle procedure documentate.

Alimentazione. I sistemi di alimentazione elettrica del data center sono concepiti per offrire ridondanza e manutenibilità senza impatto sulla continuità delle operazioni 24 ore su 24, 7 giorni su 7. Nella maggior parte dei casi, per i componenti critici dell'infrastruttura dei data center, vengono fornite una fonte di alimentazione primaria e una fonte di alimentazione alternativa, entrambe con pari capacità. Una fonte di alimentazione di riserva è fornita attraverso vari meccanismi, quali batterie di gruppi di continuità (UPS), che forniscono una protezione dell'alimentazione altamente affidabile durante cali di tensione della rete, blackout, eventi di sovratensione o sottotensione e condizioni di frequenza fuori dai parametri di tolleranza. Se l'alimentazione di rete viene interrotta, l'alimentazione di riserva è concepita per fornire temporaneamente energia al data center, al pieno della capacità, per un massimo di dieci minuti, fino a quando non subentrano i sistemi dei generatori di riserva. I generatori di riserva sono in grado di avviarsi automaticamente in pochi secondi per fornire una quantità di energia elettrica di emergenza sufficiente a far funzionare il data center al pieno delle proprie capacità, generalmente per una durata di diversi giorni.

Sistemi operativi server. I server di Google utilizzano un'implementazione basata su Linux personalizzata per l'ambiente applicativo. I dati vengono archiviati utilizzando algoritmi di proprietà al fine di accrescerne la sicurezza e la ridondanza.

Qualità del codice. Google impiega un procedimento di revisione del codice per aumentare la sicurezza del codice utilizzato per fornire i Servizi e migliorare i prodotti dedicati alla sicurezza negli ambienti di produzione.

Continuità operativa. Google ha sviluppato programmi per la pianificazione della continuità aziendale e il disaster recovery che vengono rivisti e testati regolarmente.

(*b) Reti e trasmissione*.

Trasmissione dei dati. I data center sono generalmente connessi tramite connessioni private ad alta velocità per garantire il trasferimento rapido e sicuro dei dati. Questa configurazione è stata concepita per prevenire la lettura, la copia, l'alterazione o la rimozione dei dati non autorizzate durante il trasferimento o trasporto elettronico oppure durante la copia su supporti di archiviazione dei dati. Google trasferisce i dati impiegando protocolli internet standard.

Superficie di attacco esterna. Google impiega livelli multipli di dispositivi di rete e rilevamento delle intrusioni per proteggere la propria superficie di attacco esterna. Google valuta i potenziali vettori di attacco e integra tecnologie appropriate, progettate allo scopo, nei sistemi rivolti all'esterno.

Rilevamento delle intrusioni. Il rilevamento delle intrusioni mira a fornire insight relativi alle attività di attacco in corso e informazioni adeguate per poter reagire agli incidenti. Il rilevamento delle intrusioni di Google prevede: (i) rigidi controlli sulla dimensione e sulla composizione della superficie di attacco della rete di Google attraverso una serie di misure preventive, (ii) l'impiego di controlli di rilevamento intelligente in tutti i punti di immissione dati e (iii) l'uso di tecnologie per la correzione automatica di determinate situazioni pericolose.

Risposta agli incidenti. Google monitora una varietà di canali di comunicazione per gli incidenti che interessano la sicurezza e il personale addetto alla sicurezza di Google reagisce tempestivamente agli incidenti noti.

Tecnologie di crittografia. Google offre la crittografia HTTPS (nota anche come connessione SSL o TLS). I server di Google supportano lo scambio di chiavi di crittografia Diffie Hellman a curva ellittica temporanee firmato con RSA ed ECDSA. Questi metodi di Perfect Forward Secrecy (PFS) contribuiscono a proteggere il traffico di dati e riducono al minimo l'impatto in caso di compromissione di una chiave o di violazione della crittografia.

2. Accesso e verifica delle sedi

(a) Verifica delle sedi.

Unità operativa di sicurezza dei data center in loco. I data center di Google dispongono di un'unità operativa di sicurezza in loco responsabile di tutte le funzioni di sicurezza fisica dei data center 24 ore su 24, 7 giorni su 7. Il personale dell'unità operativa di sicurezza in loco esegue il monitoraggio delle telecamere a circuito chiuso ("CCTV") e di tutti i sistemi di allarme. Il personale dell'unità operativa di sicurezza in loco esegue regolarmente perlustrazioni interne ed esterne dei data center.

Procedure di accesso ai data center. Google mantiene procedure di accesso formali per consentire l'accesso fisico ai data center. I data center sono ospitati in strutture munite di accesso mediante

scheda magnetica e di sistemi di allarme collegati all'unità operativa di sicurezza in loco. Tutti coloro che accedono al data center devono identificarsi e mostrare un documento d'identità all'unità operativa di sicurezza in loco. L'ingresso ai data center è consentito soltanto ai dipendenti, ai appaltatori e ai visitatori autorizzati. Solo i dipendenti e i appaltatori autorizzati possono richiedere una scheda magnetica di accesso a tali strutture. Le richieste delle schede magnetiche di accesso devono essere inoltrate in anticipo via email e richiedono l'approvazione del responsabile del richiedente e del direttore del data center. Le altre persone che richiedono un accesso temporaneo al data center devono: (i) ottenere la previa approvazione dei responsabili del data center in questione per lo specifico dato center e le specifiche aree interne che intendono visitare; (ii) registrarsi presso l'unità operativa di sicurezza in loco e (iii) fare riferimento a un registro ufficiale di accesso al data center che permetta di stabilire se la persona è approvata.

Dispositivi di sicurezza dei data center presenti in loco. I data center di Google impiegano un sistema di controllo degli accessi a doppia autenticazione collegato a un allarme di sistema. Il sistema di controllo degli accessi monitora e registra le schede magnetiche di ogni persona e il momento in cui accede alle porte perimetrali, alle aree di spedizione e ricezione e ad altre aree sensibili. Le attività non autorizzate e i tentativi di accesso non riusciti vengono registrati dal sistema di controllo degli accessi e sono oggetto di verifica, come del caso. L'accesso autorizzato a tutte le aree operative e ai data center aziendali è limitato in base alle zone e alle responsabilità professionali della persona che lo effettua. Le porte antincendio dei data center sono dotate di allarme. Le telecamere CCTV sono in funzione all'interno e all'esterno dei data center. Il posizionamento delle telecamere è stato progettato per coprire le aree strategiche, tra cui il perimetro, le porte di accesso agli edifici dei data center e le aree di spedizione/ricezione. Il personale delle operazioni di sicurezza in loco gestisce le attrezzature di monitoraggio, registrazione e controllo del sistema CCTV. Un sistema di cablaggio sicuro connette le attrezzature CCTV in tutti i data center. Le telecamere effettuano registrazioni in loco 24 ore su 24, 7 giorni su 7 tramite videoregistratori digitali. Le registrazioni di sorveglianza vengono conservate per almeno 30 giorni, a seconda dell'attività.

(b) Controllo degli accessi.

Personale preposto alla sicurezza dell'infrastruttura. Google attua e mantiene una politica di sicurezza per il proprio personale, il cui pacchetto formativo viene obbligatoriamente integrato da programmi di formazione in materia di sicurezza. Il personale preposto alla sicurezza dell'infrastruttura di Google è responsabile del monitoraggio costante della sicurezza delle infrastrutture di Google, della verifica dei Servizi e della risposta agli incidenti relativi alla sicurezza.

Controllo dell'accesso e gestione dei privilegi. Per poter usare i Servizi, gli Amministratori e gli Utenti finali del Cliente devono eseguire l'autenticazione per mezzo di un sistema di autenticazione centrale o di un sistema Single Sign-On.

Norme e procedimenti per l'accesso ai dati interni - Norme di accesso. Le norme e i procedimenti interni di Google relativi all'accesso ai dati sono concepiti per impedire l'accesso di persone e sistemi non autorizzati ai sistemi utilizzati per il trattamento dei Dati del Cliente. I sistemi di Google sono progettati per: (i) consentire esclusivamente alle persone autorizzate di accedere ai dati per i quali dispongono dell'autorizzazione e (ii) assicurare che, durante il trattamento, l'utilizzo e dopo la registrazione, i Dati del Cliente non possano essere letti, copiati, alterati o rimossi senza autorizzazione.

I sistemi sono stati progettati per rilevare ogni tipo di accesso illecito. Google impiega un sistema di gestione centralizzato per controllare gli accessi del personale ai server di produzione e fornisce l'accesso solo a un numero limitato di membri del personale autorizzati. I sistemi di autenticazione e autorizzazione di Google utilizzano certificati SSH e token di sicurezza e sono progettati per fornire a Google meccanismi di accesso sicuri e flessibili. Tali meccanismi sono progettati per concedere solo diritti di accesso approvati a host di siti, log, dati e informazioni di configurazione. Google richiede l'uso di ID utente univoci, password efficaci, autenticazione a due fattori ed elenchi degli accessi attentamente monitorati per ridurre al minimo l'eventualità di un uso non autorizzato degli account. La concessione o la modifica dei diritti di accesso si basa: sulle responsabilità professionali del personale autorizzato; sulle esigenze legate alle mansioni lavorative necessarie all'esecuzione dei compiti autorizzati e sulla limitazione alle persone che "devono esserne a conoscenza". La concessione o la modifica dei diritti di accesso deve inoltre essere conforme alle norme interne di Google sull'accesso ai dati e alla relativa formazione. Le approvazioni sono gestite da strumenti di workflow che mantengono registri di controllo per ogni modifica. L'accesso ai sistemi viene registrato per creare un audit trail per le responsabilità. Qualora le password vengano impiegate per l'autenticazione (ad esempio per accedere a delle workstation), per queste password saranno adottati dei criteri che quanto meno seguano le pratiche standard di settore. Questi standard includono restrizioni relative al riutilizzo delle password e un livello di sicurezza della password adeguato. Per l'accesso a informazioni estremamente sensibili (ad esempio i dati sulle carte di credito), Google utilizza token hardware.

3. Dati

(a) *Archiviazione, isolamento e logging dei dati*. Google archivia i dati su server di sua proprietà in un ambiente multi-tenant. Fatte salve eventuali disposizioni contrarie (ad esempio, sotto forma di selezione di una posizione per i dati), i Dati del Cliente vengono replicati da Google tra più data center distribuiti in diverse aree geografiche. Inoltre Google isola logicamente i Dati del Cliente. Al Cliente viene dato il controllo di criteri di condivisione dei dati specifici. Questi criteri, in conformità con le funzionalità dei Servizi, consentono al Cliente di determinare le impostazioni di condivisione dei prodotti applicabili agli Utenti finali del Cliente per scopi specifici. Il Cliente può scegliere di utilizzare le funzionalità di logging che Google mette a sua disposizione tramite i Servizi.

(b) *Norme relative alla dismissione dei dischi e alla cancellazione dei relativi dati*. Alcuni dischi contenenti dati potrebbero venire dismessi ("Dischi dismessi") a causa di errori, problemi di prestazioni o guasti hardware. Prima di abbandonare le sedi di Google per essere riutilizzato o distrutto, ogni Disco dismesso viene sottoposto a una serie di procedure per la distruzione dei dati (le "Norme relative alla cancellazione dei dati dei dischi"). I Dischi dismessi vengono cancellati mediante un procedimento composto da varie fasi, la cui compiutezza viene verificata da almeno due ispettori indipendenti. I risultati della cancellazione vengono registrati mediante il numero di serie del Disco ritirato ai fini della tracciabilità. Infine, il Disco dismesso viene reinserito nell'inventario per essere riutilizzato o distribuito nuovamente. Qualora i dati presenti sul Disco dismesso non possano essere cancellati a causa di guasti hardware, il disco verrà conservato in un luogo sicuro fino a quando non potrà essere distrutto. Tutte le strutture vengono sottoposte regolarmente a controlli al fine di monitorare la conformità con le Norme relative alla cancellazione dei dati dei dischi.

4. Sicurezza del personale

Google richiede al proprio personale di adottare una condotta coerente con le linee guida della società in materia di riservatezza, etica aziendale, uso appropriato e standard professionali. Google esegue controlli del background ragionevolmente consoni nella misura consentita dalla legge e ai sensi delle leggi e dei regolamenti locali sul lavoro.

Il personale di Google è tenuto a sottoscrivere un accordo di riservatezza, nonché a dare conferma di ricezione delle norme sulla privacy e sulla riservatezza di Google, e della propria conformità con queste norme. Il personale riceve una formazione in materia di sicurezza. Il personale incaricato della gestione dei dati del Cliente deve soddisfare requisiti aggiuntivi inerenti al proprio ruolo (ad esempio, certificazioni). Il personale di Google non tratterà i Dati del Cliente senza autorizzazione.

5. Sicurezza dei Sub-responsabili

Prima di eseguire l'onboarding di nuovi Sub-responsabili, Google conduce un controllo delle prassi relative alla sicurezza e delle norme di tutela della privacy adottate dai Sub-responsabili per assicurare che questi forniscano un livello di sicurezza e privacy consono all'accesso ai dati e alla portata dei servizi per cui vengono incaricati. Una volta che Google ha sottoposto a valutazione i rischi presentati dal Sub-responsabile, fatti salvi i requisiti descritti nella Sezione 11.3 (Requisiti per l'incarico del Sub-responsabile), il Sub-responsabile deve stipulare termini contrattuali appropriati in materia di sicurezza, riservatezza e tutela della privacy.

Appendice 3: Leggi specifiche sulla privacy

I termini di ciascuna sottosezione della presente Appendice 3 si applicano solo se 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 ai sensi del GDPR dell'Unione Europea: lo Spazio economico europeo o un paese o territorio riconosciuto come in grado di assicurare una protezione adeguata ai sensi del GDPR dell'Unione Europea;

(b) per i dati trattati ai sensi del GDPR del Regno Unito: il Regno Unito o un paese o territorio riconosciuto come in grado di assicurare una protezione adeguata ai sensi del GDPR del Regno Unito e del Data Protection Act del 2018; o

(c) per i dati trattati ai sensi dell'FADP svizzero: la Svizzera o un paese o territorio che (i) è incluso nell'elenco degli stati la cui legislazione garantisce un livello adeguato di protezione come pubblicato dall'Incaricato federale della protezione dei dati e della trasparenza svizzero, ove applicabile, o (ii) è riconosciuto come in grado di assicurare una protezione adeguata dal Consiglio federale svizzero ai sensi dell'FADP svizzero;

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

- Per "*Soluzione di trasferimento alternativa*" si intende una soluzione diversa dalle SCC (Standard Contractual Clauses, Clausole contrattuali tipo) che consente il trasferimento legittimo di dati personali in un paese terzo in conformità con la Legge europea sulla protezione dei dati, ad esempio un framework sulla protezione dei dati per garantire che le persone giuridiche partecipanti forniscano un livello di protezione adeguato.

- Per "*SCC del Cliente*" si intendono le SCC (da titolare a responsabile), le SCC (da responsabile a responsabile) o le SCC (da responsabile a titolare), a seconda dei casi.

- Per "*SCC*" si intendono le SCC del Cliente o le SCC (da responsabile a responsabile, Esportatore Google), a seconda dei casi.

- Per "*SCC (da titolare a responsabile)*" si intendono i termini riportati all'indirizzohttps://cloud.google.com/terms/sccs/eu-c2p

- Per "*SCC (da responsabile a titolare)*" si intendono i termini riportati all'indirizzo https://cloud.google.com/terms/sccs/eu-p2c

- Per "*SCC (da responsabile a responsabile)*" si intendono i termini riportati all'indirizzo https://cloud.google.com/terms/sccs/eu-p2p

- Per "*SCC (da responsabile a responsabile, Esportatore Google)*" si intendono i termini riportati all'indirizzo https://cloud.google.com/terms/sccs/eu-p2p-google-exporter

2. Notifiche relative alle Disposizioni. Fatto salvo quanto disposto dalla Sezione 5.2 (Conformità con le Disposizioni del Cliente) o qualsiasi altro diritto o obbligazione di una delle parti ai sensi del Contratto vigente, Google informerà immediatamente il Cliente se, a giudizio di Google:

a. la Legge europea impedisce a Google di ottemperare a una Disposizione;

b. una Disposizione non è conforme alla Legge europea sulla protezione dei dati; o

c. Google non è altrimenti in grado di ottemperare a una Disposizione, in ciascun caso purché questa comunicazione non sia proibita dalla Legge europea.

Se il Cliente è un responsabile, il Cliente inoltrerà immediatamente al titolare competente qualsiasi comunicazione fornita da Google ai sensi della presente sezione.

3. Diritti di Audit del Cliente. Google può consentire al Cliente o a un revisore indipendente nominato dal Cliente di eseguire audit, incluse ispezioni, come descritto nella Sezione 7.5.2(a) (Audit del Cliente). Durante questo controllo, Google renderà disponibili tutte le informazioni necessarie al fine di dimostrare la conformità con le sue obbligazioni ai sensi del presente Addendum e contribuirà al controllo come descritto nella presente Sezione 7.5 (Revisioni e audit di conformità) e in questa sezione.

4. Trasferimenti di dati.

4.1 *Trasferimenti limitati.* Le parti riconoscono che, ai sensi della Legge europea sulla protezione dei dati, non sono necessarie 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 la Legge europea sulla protezione dei dati si applica ai trasferimenti (come certificato dal Cliente ai sensi della Sezione 4.2 (Certificazione da parte di Cliente non appartenenti all'area EMEA) dei presenti termini della Legge europea sulla protezione dei dati, se il suo indirizzo di fatturazione si trova al di fuori dell'area EMEA) ("*Trasferimenti limitati*"):

a. Se Google non ha adottato una Soluzione di trasferimento alternativa per eventuali Trasferimenti limitati, Google informerà il Cliente circa la soluzione e garantirà che questi Trasferimenti limitati avvengano in conformità con la stessa; o

b. Se Google non ha adottato una Soluzione di trasferimento alternativa per eventuali Trasferimenti limitati, o informa il Cliente che Google ha smesso di adottare una Soluzione di trasferimento alternativa per eventuali Trasferimenti limitati (senza adottare una sostituzione alla Soluzione di trasferimento alternativa):

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

Le SCC (da responsabile a responsabile nell'Unione Europea, esportatore Google) si applicheranno a questi Trasferimenti limitati da Google ai Sub-responsabili; e

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

ii. Inoltre, se l'indirizzo di Google non si trova in un Paese adeguato, le SCC (da titolare a responsabile) o le SCC (da responsabile a responsabile) si applicheranno ai Trasferimenti limitati tra Google e il Cliente (a prescindere dal fatto che il Cliente sia un titolare o un responsabile).

4.2 *Certificazione da parte di Clienti non appartenenti all'area EMEA*. Se l'indirizzo di fatturazione del Cliente si trova al di fuori dell'area EMEA e i dati personali del Cliente sono soggetti alla Legge europea sulla protezione dei dati, a condizione che l'Appendice 4 (Prodotti specifici) del presente Addendum non preveda diversamente, il Cliente certificherà e identificherà la propria Autorità di controllo mediante la Console di amministrazione per i Servizi in questione.

4.3 *Informazioni sui Trasferimenti limitati*. Google fornirà al Cliente le informazioni pertinenti ai Trasferimenti limitati, ai Controlli aggiuntivi per la sicurezza e ad altre misure supplementari di protezione:

a. Nella Sezione 7.5.1 (Revisioni della Documentazione in materia di sicurezza);

b. In altre sedi come descritto 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 delle SCC*. Qualora si applichino 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 audit come descritto in queste SCC e, durante i controlli, metterà a disposizione tutte le informazioni necessarie per queste SCC, sia in conformità con la Sezione 7.5.3 (Termini commerciali aggiuntivi per le revisioni e i controlli).

4.5 *Comunicazioni sulle SCC*. Il Cliente inoltrerà al titolare in questione tempestivamente e senza ritardi ingiustificati eventuali notifiche relative alle SCC.

4.6 *Recesso per rischio di trasferimento dei dati*. Qualora il Cliente stabilisse, in base all'uso corrente o previsto dei Servizi, che non siano state fornite le misure di protezione appropriate per i dati personali del Cliente trasferiti, il Cliente potrà recedere con effetto immediato dal Contratto in questione in conformità con la disposizione sul recesso libero del Contratto o, qualora non vi sia questa disposizione, inviandone notifica a Google.

4.7 *Immodificabilità delle SCC*. Nessuna disposizione nel Contratto (incluso il presente Addendum) è intesa a modificare o contraddire le SCC o pregiudicare i diritti o le libertà fondamentali degli interessati ai sensi della Legge europea sulla protezione dei dati.

4.8 *Precedenza delle SCC*. Per quanto concerne qualsiasi conflitto tra le SCC del Cliente (le quali vengono incorporate per citazione al presente Addendum) e la parte restante del Contratto (incluso il presente Addendum), prevarranno le SCC del Cliente.

5. Requisiti per l'incarico del Sub-responsabile. Ai sensi della Legge europea sulla protezione dei dati, Google ha l'obbligo di garantire mediante un contratto per iscritto che le obbligazioni sulla protezione dei dati descritte nel presente Addendum, come definito nell'Articolo 28(3) del the GDPR, ove applicabile, vengano imposte su qualsiasi Sub-responsabile incaricato da Google.

CCPA

1. Definizioni aggiuntive.

- Per "*CCPA*" si intende il California Consumer Privacy Act del 2018 e successive modifiche, come emendato dal California Privacy Rights Act del 2020, insieme in applicazione dei regolamenti.
- "*Dati personali del Cliente*" include il termine "informazioni personali".
- I termini "attività commerciale", "scopo commerciale", "consumatore", "informazioni personali", "trattamento", "vendita", "vendere", "fornitore di servizi" e "condivisione" hanno i significati specificati nel CCPA.

2. Divieti. Fatto salvo quanto disposto dalla Sezione 5.2 (Conformità con le Disposizioni del Cliente), in relazione con il trattamento dei dati personali del Cliente in conformità con il CCPA, salvo diversamente consentito ai sensi del CCPA, Google non:

a. venderà o condividerà dati personali del Cliente;

b. tratterrà, userà o divulgherà dati personali del Cliente:

i. se non per uno scopo commerciale ai sensi del CCPA per conto del Cliente e per lo scopo specifico di eseguire i Servizi e i TSS (se applicabile); o

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

c. combinerà o aggiornerà i dati personali del Cliente con le informazioni personali che Google riceve da o per conto di terzi o che raccoglie dalle proprie interazioni con i consumatori.

3. Conformità. A prescindere dalle obbligazioni di Google ai sensi della Sezione 5.2 (Conformità con le Disposizioni del Cliente) o qualsiasi altro diritto o obbligazione di una delle parti ai sensi del Contratto, Google informerà il Cliente se, a suo giudizio, Google non è in grado di adempiere alle proprie obbligazioni ai sensi del CCPA, a meno che la notifica non sia consentita dalla legge vigente.

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) della presente sottosezione o della Sezione 7.2.1 (Notifica degli incidenti), il Cliente potrà adottare misure ragionevoli e appropriate per interrompere o porre rimedio al suddetto utilizzo non autorizzato:

a. adottando una misura raccomandata da Google ai sensi della Sezione 7.2.2 (Dettagli dell'Incidente relativo ai dati), se applicabile; o

b. esercitando i propri diritti ai sensi della Sezione 7.5.2(a) (Audit del Cliente) o 9.1 (Accesso; Rettifica; Trattamento limitato; Portabilità).

Turchia

1. Definizioni aggiuntive.

- Per "*Legge turca sulla protezione dei dati*" si intende la Legge turca sulla protezione dei dati N. 6698 del 7 aprile 2016.
- Per "*Autorità turca competente per la protezione dei dati personali*" si intende il Kişisel Verileri Koruma Kurumu.
- Per "*SCC turche*" si intendono le clausole contrattuali standard ai sensi della legge turca sulla protezione dei dati.

2. Trasferimenti di dati.

2.1 *Termini supplementari*. Qualora l'indirizzo di fatturazione del Cliente si trovi in Turchia e Google renda disponibili per l'accettazione da parte del Cliente eventuali termini aggiuntivi facoltativi (compresi le SCC turche) in relazione al trasferimento dei dati personali del Cliente ai sensi della Legge turca sulla protezione dei dati, questi termini integreranno il presente Addendum a partire dalla data di notifica all'Autorità turca competente per la protezione dei dati personali in conformità con la Sezione 2.2 (Notifica all'Autorità competente) di seguito riportata, come dimostrato dal Cliente a Google.

2.2 *Notifica all'Autorità competente*. Se il Cliente stipula delle SCC turche ai sensi della presente Sezione 2 (Trasferimenti di dati), il Cliente sarà responsabile della notifica all'Autorità turca competente per la protezione dei dati personali dell'uso di SCC turche entro cinque (5) giorni lavorativi dalla firma delle SCC turche, come previsto dalla legge turca sulla protezione dei dati.

2.3 *Audit delle SCC*. Se il Cliente stipula delle SCC turche ai sensi della presente Sezione 2 (Trasferimenti di dati), Google consentirà al Cliente (o a un revisore indipendente nominato dal Cliente) di condurre dei audit come descritto in queste SCC e, durante il controllo, metterà a disposizione tutte le informazioni richieste da queste SCC, sia in conformità con la Sezione 7.5.3 (Termini commerciali aggiuntivi per le revisioni e i controlli).

2.4 *Recesso per rischio di trasferimento dei dati*. Qualora il Cliente stabilisse, in base all'uso corrente o previsto dei Servizi, che non siano state fornite le misure di protezione appropriate per i dati personali del Cliente trasferiti, il Cliente potrà recedere con effetto immediato dal Contratto in questione in conformità con la disposizione sul recesso libero del Contratto o, qualora non vi sia questa disposizione, inviandone notifica a Google.

2.5 *Immodificabilità delle SCC turche*. Nessuna disposizione nel Contratto (incluso il presente Addendum) è intesa a modificare o contraddire le SCC turche o pregiudicare i diritti o le libertà fondamentali degli interessati ai sensi della Legge turca sulla protezione dei dati.

2.6 *Precedenza delle SCC*. Per quanto concerne qualsiasi conflitto o divergenza tra le SCC turche (le quali vengono incorporate per citazione al presente Addendum se stipulato dal Cliente) e la parte restante del Contratto (incluso il presente Addendum) prevarranno le SCC turche.

Israele

1. Definizioni aggiuntive.

- Per "*Legge israeliana sulla protezione della privacy*" si intende la Legge israeliana sulla protezione della privacy del 1981 e qualsiasi altro regolamento promulgato successivamente.

2. Termini equivalenti. Tutti i termini equivalenti a "titolare del trattamento", "dati personali", "trattamento" e "responsabile del trattamento", come utilizzati nel presente Addendum, hanno il significato attribuito dalla Legge israeliana sulla protezione della privacy.

3. Diritti di audit del Cliente di eseguire controlli. Google può consentire al Cliente o a un revisore indipendente nominato dal Cliente di eseguire audit, incluse ispezioni, come descritto nella Sezione 7.5.2(a) (Audit del Cliente).

Appendice 4: Prodotti specifici

I termini di ciascuna sottosezione della presente Appendice 4 si applicano solo in relazione al trattamento dei Dati del Cliente da parte dei Servizi corrispondenti.

Google Cloud Platform

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 definito nel Contratto, si intendono i dati forniti a Google dal Cliente o dagli Utenti finali tramite Google Cloud Platform nell'ambito dell'Account, nonché i dati che il Cliente o gli Utenti finali ricavano da quei dati attraverso l'utilizzo di Google Cloud Platform.
- Per "*Google Cloud Platform*" si intendono i servizi descritti all'indirizzo https://cloud.google.com/terms/services a esclusione delle Offerte di terze parti.
- Per "*Offerte di terze parti*", se non definite nel Contratto, si intendono (a) servizi, software, prodotti e altre offerte di terze parti che non sono incorporate nella piattaforma o nei software Google Cloud, (b) offerte identificate nella sezione "Termini di terze parti" dei Termini specifici dei servizi del Contratto e (c) sistemi operativi di terze parti.

2. Certificazioni di conformità. Le Certificazioni di conformità per i servizi controllati della piattaforma Google Cloud includono anche le certificazioni ISO 27017 e ISO 27018 e un'Attestazione di conformità PCI DSS.

3. Località dei data center. Le località dei data center della piattaforma Google Cloud sono descritte all'indirizzo https://cloud.google.com/about/locations/.

4. Informazioni sui Sub-responsabili. Nomi, sedi e attività dei Sub-responsabili della piattaforma Google Cloud sono descritti all'indirizzo https://cloud.google.com/terms/subprocessors.

5. Team di Google dedicato alla protezione dei dati cloud. È possibile contattare il Team dedicato alla protezione dei dati cloud per la piattaforma Google Cloud all'indirizzo https://support.google.com/cloud/contact/dpo.

6. Informazioni sui Trasferimenti limitati. Ulteriori informazioni pertinenti ai Trasferimenti limitati, ai Controlli aggiuntivi per la sicurezza e ad altre misure supplementari proattive sono disponibili all'indirizzo cloud.google.com/privacy/.

7. Termini specifici dei servizi.

Bare Metal Solution (Google Cloud Platform)

Bare Metal Solution fornisce un accesso non virtualizzato alle risorse infrastrutturali sottostanti e, per sua natura, presenta alcune caratteristiche distinte.

1. Emendamenti. Il presente Addendum viene emendato come segue in relazione a Bare Metal Solution:

- La definizione di "Revisore di terze parti di Google" viene sostituita dalla seguente:

        - Per "*Revisore di terze parti di Google*" si intende un revisore di terze parti qualificato nominato da Google o un Sub-responsabile di Bare Metal Solution, la cui identità attuale verrà divulgata da Google al Cliente su richiesta.

- I seguenti termini vengono eliminati:

    - Dalla Sezione 7.1.1 (Misure di sicurezza di Google), la frase "criptare i dati del Cliente";

    - Dall'Appendice 2 (Misure di sicurezza), Sezione 1(a), le sottosezioni "Sistemi operativi del server" e "Continuità aziendale";

    - Dall'Appendice 2, Sezione 1(b), le sottosezioni "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 su server di sua proprietà in un ambiente multi-tenant. Fatte salve eventuali disposizioni contrarie del Cliente (ad esempio, sotto forma di selezione della sede dei dati), Google replica i dati del Cliente tra più data center in diverse aree geografiche.

2. Conformità, certificazioni e Report SOC. Google o i suoi Sub-responsabili provvederanno a mantenere almeno quanto segue (o un'alternativa analoga o migliore) per Bare Metal Solution allo scopo di verificare la continua efficacia delle Misure di sicurezza: .

a. un certificato per ISO 27001 e un'Attestazione di conformità PCI DSS (le "*Certificazioni di conformità BMS*"); e

b. Report SOC 1 e SOC 2 aggiornati su base annuale sulla base dei controlli svolti almeno una volta ogni 12 mesi (i "*Report SOC BMS*").

3. Revisioni della Documentazione in materia di sicurezza. Al fine di provare la conformità ai suoi obblighi ai sensi del presente Addendum, Google metterà a disposizione del Cliente le Certificazioni di conformità BMS e i Report SOC BMS e, se il Cliente è un responsabile, permetterà al Cliente di richiedere accesso ai Report SOC BMS per il titolare in questione ai sensi della Sezione 7.5.3 (Termini commerciali aggiuntivi per le revisioni e i controlli).

4. Obbligazioni del Cliente. Senza limitare le obbligazioni esplicite di Google relative a Bare Metal Solution, il Cliente adotterà misure ragionevoli per proteggere e mantenere la sicurezza dei dati del Cliente e di qualsiasi altro contenuto memorizzato o elaborato mediante Bare Metal Solution.

5. Limitazione di responsabilità. In deroga a eventuali disposizioni contrarie nel Contratto (compreso il presente Addendum), Google non è responsabile per nessuna delle seguenti circostanze relative a Bare Metal Solution:

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

b. logging e monitoraggio;

c. manutenzione o assistenza non hardware;

d. backup dei dati, comprese eventuali configurazioni di ridondanza o ad alta disponibilità; o

e. norme o procedure per la continuità operativa e disaster recovery.

Il Cliente è l'unico responsabile della protezione (diversa dalla sicurezza fisica dei server Bare Metal Solution), del logging e del monitoraggio, della manutenzione e dell'assistenza, nonché del backup di qualsiasi Sistema operativo, Dati del Cliente, software e applicazioni utilizzati, caricati o ospitati dal Cliente su Bare Metal Solution.

Cloud NGFW (Google Cloud Platform)

L'edizione di Cloud NGFW dal titolo "Cloud NGFW Enterprise" ("CNE") è progettata per mitigare i rischi di cybersicurezza e, in quanto tale, presenta alcune caratteristiche distinte.

1. Emendamenti. L'Addendum viene emendato come segue per quanto riguarda CNE:

- Le Sezioni 6.1 (Eliminazione da parte del Cliente) e 6.2 (Restituzione o eliminazione alla fine del Periodo di validità) non impediranno a Google o ai Sub-responsabili di conservare qualsiasi file o intercettazione di pacchetti di traffico di rete inviati ai fini dei TSS e indicati da CNE come delle minacce per la sicurezza, a condizione che il file o l'intercettazione di pacchetti di traffico di rete non includa i dati personali del Cliente.

Google Distributed Cloud connesso (Google Cloud Platform)

Il deployment di Google Distributed Cloud connesso non viene eseguito presso i data center di Google e presenta volutamente delle caratteristiche distinte.

1. Emendamenti. Il presente Addendum viene emendato come segue in relazione a Google Distributed Cloud connesso:

- I riferimenti ai "sistemi di Google" vengono sostituiti da "le apparecchiature".

- La Sezione 6.2 (Restituzione o eliminazione alla fine del Periodo di validità) viene sostituita da quanto segue:

    - 6.2 *Restituzione o eliminazione alla scadenza del Periodo di validità.*. Alla scadenza del Periodo di validità del contratto, il Cliente richiede a Google di eliminare tutti i Dati del Cliente (incluse le copie esistenti) dall'Apparecchiatura, ai sensi delle leggi vigenti. Se il Cliente desidera conservare i Dati del Cliente dopo la scadenza del Periodo di validità, può esportare o effettuare copie di detti dati prima della scadenza del Periodo di validità. Google agirà in maniera conforme alle Disposizioni della presente Sezione 6.2 come ragionevolmente possibile ed entro un massimo di 180 giorni, a meno che la legge europea non ne preveda l'archiviazione, qualora si applicasse la Legge europea sulla protezione dei dati, o qualsiasi altra legge vigente sulla privacy.

- Alla fine della Sezione 10.1 (Sedi di archiviazione e trattamento 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) viene sostituita da quanto segue:

    - **1. Computer locali e sicurezza di rete**

Computer locali. I Dati del Cliente vengono archiviati esclusivamente sulle Apparecchiature destinate al deployment presso una Sede del Cliente.

Sistemi operativi server. I server di Google utilizzano un'implementazione basata su Linux personalizzata per l'ambiente applicativo. Google impiega un procedimento di revisione del codice per aumentare la sicurezza del codice utilizzato per fornire Google Distributed Cloud connesso e migliorare i prodotti dedicati alla sicurezza negli ambienti di produzione di Google Distributed Cloud connesso.

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 di crittografia Diffie Hellman a curva ellittica temporanee firmato con RSA ed ECDSA. Questi metodi di Perfect Forward Secrecy (PFS) contribuiscono a proteggere il traffico di dati e riducono al minimo l'impatto in caso di compromissione di una chiave o di violazione della crittografia. Google mette a disposizione anche la crittografia dei dati at-rest usando almeno AES128 o soluzioni analoghe. Google Distributed Cloud connesso presenta 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 attivare e configurare un'interconnessione forte e crittografata tra le Apparecchiature e il Virtual Private Cloud del Cliente utilizzando Cloud VPN attraverso una connessione VPN IPsec.

Archiviazione vincolata. L'archiviazione dei dati del Cliente è vincolata al server. In caso di furto o copia di un disco at-rest, il suo contenuto non sarà recuperabile al di fuori del server.

- Le Sezioni 2 (Accesso e verifica delle sedi) e 3 (Dati) dell'Appendice 2 (Misure di sicurezza) vengono eliminate.

2. Disposizioni non applicabili. Eventuali obbligazioni di Google previste dal Contratto (incluso il presente Addendum) o dichiarazioni contenute nella documentazione di sicurezza associata (inclusi i white paper) che dipendono dalla gestione da parte di Google di un data center Google non si applicano a Google Distributed Cloud connesso.

Multi-cloud gestiti da Google (Google Cloud Platform)

I Servizi per multi-cloud gestiti da Google coinvolgono infrastrutture di terze parti e presentano volutamente delle caratteristiche distinte.

1. Definizioni aggiuntive.

- Per "*Emendamento sul trattamento dei dati per multi-cloud gestiti da Google*" si intedono i termini di cui all'indirizzo https://cloud.google.com/terms/mcs-data-processing-terms.

2. Termini per il trattamento dei dati multi-cloud. L'Emendamento sul trattamento dei dati per multi-cloud gestiti da Google integra e modifica il presente Addendum in relazione ai Servizi multi-cloud gestiti da Google per la Google Cloud Platform.

Google Cloud VMware Engine (Google Cloud Platform)

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

NetApp Volumes (Google Cloud Platform)

1. Emendamenti. Il presente Addendum viene emendato come segue in relazione a NetApp Volumes:

- La definizione di "Revisore di terze parti di Google" viene sostituita dalla seguente:
    - Per "*Revisore di terze parti di Google*" si intende un revisore di terze parti qualificato nominato da Google o un Sub-responsabile di NetApp Volumes, la cui identità attuale verrà divulgata da Google al Cliente su richiesta.
- La Sezione 3(a) (Archiviazione, isolamento e logging dei dati) dell'Appendice 2 (Misure di sicurezza) viene sostituita da quanto segue:
    - (a) *Archiviazione, isolamento e logging dei dati*. Google archivia i dati in un ambiente multi-tenant su server di proprietà di NetApp, Inc. Fatte salve eventuali disposizioni contrarie (ad es. sotto forma di selezione della sede dei dati), Google replica i Dati del Cliente tra più data center situati in diverse aree geografiche. Inoltre Google isola logicamente i Dati del Cliente. Al Cliente viene dato il controllo di criteri di condivisione dei dati specifici. Questi criteri, in conformità con le funzionalità dei Servizi, consentono al Cliente di determinare le impostazioni di condivisione dei prodotti applicabili agli Utenti finali del Cliente per scopi specifici. Il Cliente può scegliere di utilizzare le funzionalità di logging che Google mette a sua disposizione tramite i Servizi.

2. Conformità, certificazioni e Report SOC. Google o i suoi Sub-responsabili otterranno almeno quanto segue (o un'alternativa analoga o migliore) per NetApp Volumes:

a. un certificato per ISO 27001 e un'Attestazione di conformità PCI DSS (le "*Certificazioni di conformità NetApp*"); e

b. Report SOC 1 e SOC 2 aggiornati su base annuale sulla base dei controlli svolti almeno una volta ogni 12 mesi (i "*Report SOC NetApp*").

3. Revisioni della Documentazione in materia di sicurezza. Al fine di provare la conformità ai suoi obblighi ai sensi del presente Addendum, Google metterà a disposizione del Cliente le Certificazioni di conformità NetApp e i Report SOC NetApp e, se il Cliente è un responsabile, permetterà al Cliente di

richiedere accesso ai Report SOC NetApp per il titolare in questione ai sensi della Sezione 7.5.3 (Termini commerciali aggiuntivi per le revisioni e i controlli).

Google Workspace e Cloud Identity

1. Definizioni aggiuntive.

- Per "*Account*", se non definito dal Contratto, si intende l'account Google Workspace o Cloud Identity del Cliente.
- Per "*Cloud Identity*" quando acquistato con un contratto autonomo e non come parte della piattaforma Google Cloud o di Google Workspace, si intendono i Servizi di Cloud Identity descritti all'indirizzo https://cloud.google.com/terms/identity/user-features.
- Per "*Dati del Cliente*", se non definito dal Contratto, si intendono i dati inviati, memorizzati, trasmessi o ricevuti dal Cliente o dai suoi Utenti finali tramite Google Workspace o Cloud Identity nell'ambito dell'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 per i Prodotti aggiuntivi applicabili:

a. il Cliente può attivare o disattivare i Prodotti aggiuntivi tramite la Console di amministrazione e non sarà necessario utilizzare i Prodotti aggiuntivi per utilizzare Google Workspace o Cloud Identity; e

b. se il Cliente decide di installare Prodotti aggiuntivi o di utilizzarli con Google Workspace o Cloud Identity, i Prodotti aggiuntivi potranno accedere ai Dati del Cliente nella misura necessaria per interagire con Google Workspace o Cloud Identity, a seconda dei casi.

Per maggiore chiarezza: il presente Addendum non si applica al trattamento dei dati personali connesso alla fornitura di eventuali Prodotti aggiuntivi installati o utilizzati dal Cliente, inclusi i dati personali trasmessi a o dai Prodotti aggiuntivi.

3. Certificazioni di conformità. Le Certificazioni di conformità per i servizi controllati di Google Workspace e Cloud Identity includono anche i certificati ISO 27017 e ISO 27018.

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

5. Informazioni sui Sub-responsabili. Nomi, sedi e attività dei Sub-responsabili di Google Workspace e Cloud Identity sono descritti all'indirizzo https://workspace.google.com/intl/it/terms/subprocessors.html.

6. Team di Google dedicato alla protezione dei dati cloud. È possibile contattare il Team dedicato alla protezione dei dati per Google Workspace e Cloud Identity (al momento dell'accesso al proprio account amministratore) all'indirizzo https://support.google.com/a/contact/googlecloud_dpr.

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

a. Google applica una separazione logica tra i dati di ciascun Utente finale e quelli degli altri; e

b. i dati di un Utente finale autenticato non possono essere visualizzati da un altro Utente finale (a meno che il primo Utente finale o un Amministratore non consentano la condivisione di detti dati).

8. Informazioni sui Trasferimenti limitati. Ulteriori informazioni pertinenti ai Trasferimenti limitati, ai Controlli aggiuntivi per la sicurezza e ad altre misure supplementari proattive sono disponibili all'indirizzo cloud.google.com/privacy/.

9. Addendum per i dati del servizio. Se Google rende disponibile un Addendum per i dati di servizio opzionale affinché il Cliente lo accetti in relazione al presente Addendum, la disponibilità di suddetto addendum opzionale costituirà un "Aggiornamento DPA" se il termine è definito in qualsiasi Addendum per i dati del servizio precedentemente stipulato dal Cliente.

10. Termini specifici dei servizi.

AppSheet (Google Workspace)

1. Emendamenti. Il presente Addendum viene emendato come segue in relazione ad AppSheet:

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

2. Località dei data center aggiuntive. Le località dei data center aggiuntive per AppSheet sono descritte all'indirizzo https://cloud.google.com/about/locations/.

Looker (original)

1. Definizioni aggiuntive.

- Per "*Console di amministrazione*" si intende qualsiasi console di amministrazione applicabile a qualsiasi istanza.
- Per "*Emendamento sul trattamento dei dati per multi-cloud gestiti da Google*" si intedono, ove applicabile, i termini di cui all'indirizzo https://cloud.google.com/terms/mcs-data-processing-terms.
- Per "*Servizi multi-cloud gestiti da Google*" si intendono, ove applicabile, i servizi, i prodotti e le funzionalità specificati di Google che sono ospitati sull'infrastruttura di un provider cloud di terze parti.

- Per "*Looker (original)*" si intende una piattaforma integrata (compresa l'infrastruttura basata su cloud, ove applicabile, e i componenti software, incluse le API associate) che consente alle aziende di analizzare i dati e definire le metriche aziendali per più fonti di dati, offerta da Google al Cliente ai sensi del Contratto. Looker (original) esclude le Offerte di Terze parti.

- Per "*Provider di servizi multi-cloud di terze parti*" si intende il significato indicato nell'Emendamento sul trattamento dei dati per multi-cloud gestiti da Google.

- Per "*Modulo d'ordine*" si intende il significato indicato nel Contratto, a meno che il Cliente non abbia effettuato l'acquisto tramite un rivenditore o su un marketplace online o stia utilizzando Looker solo per scopi di prova o di valutazione ai sensi di un contratto di prova o di valutazione, nel qual caso per Modulo d'Ordine si può intendere un'altra forma scritta (sono consentite le email o altri mezzi elettronici) come autorizzato da Google.

2. Emendamenti. Il presente Addendum viene emendato come segue in relazione a Looker (original):

- La definizione di "Indirizzo email di notifica" è sostituita dalla seguente:

    - Per "Indirizzo email di notifica" si intendono l'indirizzo o gli indirizzi email indicati dal Cliente nel Modulo d'ordine o mediante Looker (se del caso) per la ricezione di determinate notifiche inviate da Google.

- Le definizioni di "SCC (da titolare a responsabile)", "SCC (da responsabile a titolare)", "SCC (da responsabile a responsabile)" e "SCC (da responsabile a responsabile, Esportatore Google)" nell'Appendice 3 (Leggi specifiche sulla privacy) vengono sostituite come segue:

    - Per "*SCC (da titolare a responsabile)*" si intendono i termini riportati all'indirizzo https://cloud.google.com/terms/looker/legal/sccs/eu-c2p

    - Per "*SCC (da responsabile a titolare)*" si intendono i termini riportati all'indirizzo https://cloud.google.com/terms/looker/legal/sccs/eu-p2c

    - Per "*SCC (da responsabile a responsabile)*" si intendono i termini riportati all'indirizzo https://cloud.google.com/terms/looker/legal/sccs/eu-p2p; e

    - Per "*SCC (da responsabile a responsabile, Esportatore Google)*" si intendono i termini riportati all'indirizzo: https://cloud.google.com/terms/looker/legal/sccs/eu-p2p-intra-group.

- Alla fine della Sezione 10.1 (Sedi di archiviazione e trattamento dei dati) vengono aggiunte le seguenti parole: "o dove i Fornitori di terze parti di servizi multi-cloud mantengono le strutture."

3. Responsabilità aggiuntive del Cliente in materia di sicurezza. Il Cliente è responsabile della sicurezza del proprio ambiente e dei propri database e della configurazione di Looker (original) esclusi i sistemi gestiti e controllati da Google.

4. Conformità, certificazioni e Report SOC. Le Certificazioni di conformità e i Report SOC per i Servizi di Looker (original) sottoposti a controllo possono variare a seconda dell'ambiente di hosting in cui vengono utilizzati i Servizi in questione. Google fornirà su richiesta i dettagli delle Certificazioni di conformità e dei Report SOC disponibili per specifici ambienti di hosting.

5. Località dei data center. L'ubicazione dei centri dati di Looker (original) sarà descritta nel Modulo d'ordine applicabile o altrimenti identificata da Google.

6. Nessuna certificazione da parte di Clienti di paesi che non appartengono all'area EMEA. Il Cliente non è tenuto a certificare o identificare la propria Autorità di controllo competente, come descritto nella Sezione 4.2 (Certificazione da parte di Clienti non appartenenti all'area EMEA) dei termini europei sulla protezione dei dati nell'Appendice 3 (Leggi specifiche sulla privacy) per Looker (original).

7. Informazioni sui Trasferimenti limitati. Ulteriori informazioni pertinenti ai Trasferimenti limitati, ai Controlli aggiuntivi per la sicurezza e ad altre misure supplementari proattive per Looker (original) sono disponibili all'indirizzo https://docs.looker.com.

8. Informazioni sui Sub-responsabili. Nomi, sedi e attività dei Sub-responsabili per Looker (original) sono descritti agli indirizzi:

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

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

9. Multi-cloud gestiti da Google (Looker (original))

I Servizi per multi-cloud gestiti da Google coinvolgono infrastrutture di terze parti e presentano volutamente delle caratteristiche distinte.

9.1 *Termini per il trattamento dei dati multi-cloud*. L'Emendamento sul trattamento dei dati per multi-cloud gestiti da Google integra e modifica il presente Addendum in relazione ai Servizi multi-cloud gestiti da Google per Looker (original).

10. Team di Google dedicato alla protezione dei dati cloud. È possibile contattare il Team dedicato alla protezione dei dati cloud per Looker (original) all'indirizzo https://support.google.com/cloud/contact/dpo.

11. Registri di Google relativi al trattamento. Nella misura in cui una legge vigente sulla privacy richieda a Google di raccogliere e conservare i registri di determinate informazioni relative al Cliente, il Cliente fornirà queste informazioni su richiesta di Google e comunicherà a Google eventuali aggiornamenti necessari per far sì che siano sempre accurate e aggiornate, a meno che Google non richieda al Cliente di fornire e aggiornare queste informazioni secondo un'altra modalità.

12. Misure di sicurezza aggiuntive dell'applicazione. Google implementerà e manterrà le Misure di sicurezza aggiuntive per Looker (original) descritte di seguito:

a. Google segue le pratiche standard di 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 attraverso le liste bloccate degli IP e la limitazione di frequenza delle connessioni.

b. Gli amministratori del Cliente controllano l'accesso alle applicazioni da parte del personale di Google per fornire assistenza tecnica come richiesto dal Cliente o dagli Utenti finali del Cliente.

Servizi SecOps

1. Definizioni aggiuntive.

- Per "*Account*", se non definito nel Contratto, si intende l'account dei Servizi SecOps o della Google Cloud Platform del Cliente.

- Per "*Dati del Cliente*", se non definito nel Contratto, si intendono i dati forniti a Google dal Cliente o dagli Utenti finali tramite i Servizi SecOps nell'ambito dell'Account o, per i Mandiant Consulting Services e Managed Services, in relazione alla ricezione dei Servizi SecOps.

- Per "*Fornitore incaricato dal Cliente*" si intende un fornitore di servizi (che può includere un responsabile o un sub-responsabile del trattamento) direttamente incaricato dal Cliente in base a un accordo separato tra il Cliente e detto fornitore.

- Per "*Servizi SecOps*" si intendono i Servizi SecOps descritti all'indirizzo https://cloud.google.com/terms/secops/services, ad eccezione delle Offerte di terze parti.

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

2. Emendamenti. Il presente Addendum viene emendato come segue in relazione ai Servizi SecOps:

- La definizione di "Controlli aggiuntivi per la sicurezza" è sostituita come segue:

    - Per *"Controlli aggiuntivi per la sicurezza"* si intendono risorse, caratteristiche, funzionalità e/o controlli relativi alla sicurezza che il Cliente può utilizzare a propria scelta e/o discrezione, tra cui (se del caso) la crittografia, il logging e il monitoraggio, la gestione di identità e l'analisi della sicurezza.

- La definizione di "Servizi controllati" viene sostituita come segue:

    - Per "*Servizi controllati*" si intendono i Servizi SecOps attualmente rientranti nell'ambito di applicazione della certificazione o del report pertinente all'indirizzo https://cloud.google.com/security/compliance/secops/services-in-scope. Google non potrà rimuovere alcun Servizio SecOps da questo URL a meno che non sia più disponibile in conformità con il Contratto vigente.

- Le definizioni di "SCC (da titolare a responsabile)", "SCC (da responsabile a titolare)", "SCC (da responsabile a responsabile)" e "SCC (da responsabile a responsabile, Esportatore Google)" nell'Appendice 3 (Leggi specifiche sulla privacy) vengono sostituite come segue:
    - Per "SCC (da titolare a responsabile)" si intendono i intendono i termini riportati all'indirizzo https://cloud.google.com/terms/secops/sccs/eu-c2p;
    - Per "SCC (da responsabile a titolare)" si intendono i termini riportati all'indirizzo https://cloud.google.com/terms/secops/sccs/eu-p2c;
    - Per "SCC (da responsabile a responsabile)" si intendono i termini riportati all'indirizzo https://cloud.google.com/terms/secops/sccs/eu-p2p; e
    - Per SCC (da responsabile a responsabile nell'Unione Europea, Esportatore Google) si intendono i termini riportati all'indirizzo https://cloud.google.com/terms/sccs/eu-p2p-google-exporter.
- La Sezione 6.1 (Eliminazione da parte del Cliente) viene modificata come segue:
    - 6.1 **Eliminazione da parte del Cliente**. Durante il Periodo di validità, Google consentirà al Cliente di eliminare i Dati del Cliente in modo conforme alle funzionalità dei Servizi o su richiesta. Se, durante il Periodo di validità, il Cliente utilizza i Servizi per eliminare Dati del Cliente e questi non possono essere recuperati dal Cliente, o se il Cliente richiede l'eliminazione dei Dati del Cliente durante il Periodo di validità, questo utilizzo o richiesta (a seconda dei casi) costituirà una Disposizione che richiede l'eliminazione da parte di Google dei Dati del Cliente pertinenti dai sistemi di Google, in conformità con le leggi vigenti. Google adempirà a questa Disposizione non appena ragionevolmente possibile ed entro un periodo massimo di 180 giorni, a meno che la Legge europea non richieda l'archiviazione dei dati, qualora si applicasse la Legge europea sulla protezione dei dati, o a meno che la legge vigente non richieda l'archiviazione, qualora si applicasse qualsiasi altra legge sulla privacy.
- La Sezione 7.4 (Certificazioni di conformità e Report SOC) dell'Addendum viene modificata come segue:
    - 7.4 *Conformità, certificazioni e Report SOC*. Google manterrà le certificazioni e i report essenziali specificati 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 (le "**Certificazioni di conformità**" e i "**Report SOC**").

Google potrebbe aggiungere altri standard di volta in volta. Google ha facoltà di sostituire una Certificazione di conformità o un Report SOC con un'alternativa equivalente o migliore.

- La Sezione 9.1 (Accesso, rettifica, trattamento limitato, portabilità) è modificata come segue:

9.1 **Accesso, rettifica, trattamento limitato, portabilità**. Durante il Periodo di validità, Google consentirà al Cliente, in modo coerente con le funzionalità dei Servizi, di accedere, rettificare e limitare il trattamento dei Dati del Cliente, anche nelle modalità descritte nella Sezione 6.1 (Eliminazione da parte del Cliente), nonché di esportare i Dati del Cliente. Se il Cliente viene a conoscenza del fatto che i Dati personali del Cliente sono imprecisi o obsoleti, Il Cliente sarà responsabile di informare Google e Google assisterà il Cliente nella rettifica di quei dati, se richiesto dalla Legge sulla privacy applicabile.

3. Località dei data center. Le località 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 di paesi che non appartengono all'area EMEA. Il Cliente non è tenuto a certificare o identificare la propria Autorità di controllo competente, come descritto nella Sezione 4.2 (Certificazione da parte di Clienti non appartenenti all'area EMEA) dei termini europei sulla protezione dei dati nell'Appendice 3 (Leggi specifiche sulla privacy) per i Servizi SecOps.

5. Informazioni sui Sub-responsabili. I nomi, le sedi e le attività di tutti i Sub-responsabili per i Servizi SecOps sono descritti all'indirizzo https://cloud.google.com/terms/secops/subprocessors.

6. Team di Google dedicato alla protezione dei dati cloud. È possibile contattare il Team dedicato alla protezione dei dati cloud per i Servizi SecOps all'indirizzo https://support.google.com/cloud/contact/dpo (e/o mediante altre modalità che Google potrebbe fornire di volta in volta).

7. Registri di Google relativi al trattamento. Nella misura in cui una legge sulla privacy applicabile richieda a Google di raccogliere e conservare i registri di determinate informazioni relative al Cliente, il Cliente fornirà queste informazioni su richiesta di Google e comunicherà a Google eventuali aggiornamenti necessari per far sì che siano sempre accurate e aggiornate, a meno che Google non richieda al Cliente di fornire e aggiornare queste informazioni secondo un'altra modalità.

8. Termini specifici dei servizi.

Mandiant Consulting Services e Managed Services

Mandiant Consulting Services e Managed Services forniscono servizi di consulenza e implementazione (tra cui risposta agli incidenti, preparazione strategica e garanzia tecnica per mitigare le minacce e ridurre i rischi correlati agli incidenti) e servizi gestiti di rilevamento e risposta e, per loro natura, presentano alcune caratteristiche distintive.

1. Emendamenti. L'Addendum è modificato come segue esclusivamente in relazione a Mandiant Consulting Services e Managed Services:

- La definizione di "Incidente relativo ai dati" è integrata con quanto segue:
    - Per chiarezza, il termine "Incidente relativo ai dati" esclude gli incidenti oggetto dei Mandiant Consulting Services e/o Managed Services, a seconda dei casi.

- La Sezione 5.2(b)(i) (Conformità con le Disposizioni del Cliente) viene sostituita con la sezione seguente:
    - i. Uso dei Servizi da parte del Cliente; e
- La seconda frase della Sezione 7.1.1 (Misure di sicurezza di Google) è modificata come segue:
    - Le Misure di sicurezza possono includere (a seconda dei casi) misure atte a crittografare i Dati del Cliente a garantire la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di Google; a ripristinare tempestivamente l'accesso ai Dati del Cliente a seguito di un incidente; e a verificare regolarmente l'efficacia delle misure adottate.
- La Sezione 7.3.1(b) è modificata come segue:
    - b. amministrare, gestire l'accesso e proteggere le credenziali di autenticazione dell'account, i sistemi, i software, le reti e i dispositivi che il Cliente utilizza per ricevere, o autorizza Google ad accedere al fine di fornire, i Mandiant Consulting Services e/o Managed Services, a seconda dei casi;
- Sono aggiunte le nuove Sezioni 7.3.1(d) ed (e) come segue:
    - d. ridurre al minimo la quantità di Dati del Cliente forniti dal Cliente o per suo conto a Google; e
    - e. nella misura in cui l'accesso di Google ai Dati del Cliente sia sotto il controllo del Cliente, revocare l'accesso una volta che Google abbia completato i Mandiant Consulting Services e/o Managed Services, a seconda dei casi.
- L'Appendice 2 (Misure di sicurezza) viene sostituita con la sezione seguente:
    - Appendice 2: Misure tecniche e organizzative aggiuntive

1. Ambiente controllato dal Cliente. Google accederà e tratterà i Dati del Cliente forniti dal Cliente o per suo conto a Google solo tramite un account o un ambiente controllato o approvato dal Cliente.

2. Norme e procedimenti per l'accesso ai dati - Norme relative all'accesso. Le norme e i procedimenti di Google relativi all'accesso ai dati sono concepiti per impedire l'accesso di persone e/o sistemi non autorizzati ai sistemi utilizzati per il trattamento dei Dati del Cliente. Google (i) consente l'accesso ai dati solo alle persone autorizzate; e (ii) adotta misure per garantire che i dati personali non possano essere letti, copiati, modificati o rimossi senza autorizzazione durante il trattamento e l'utilizzo. La concessione o la modifica dei diritti di accesso da parte di Google si basa sulla fornitura da parte del Cliente a Google dell'accesso dell'utente finale al proprio account o ambiente.

3. Sicurezza del personale. Google richiede al proprio personale di adottare una condotta coerente con le linee guida della società in materia di riservatezza, etica aziendale, uso appropriato e standard

professionali. Google conduce controlli ragionevolmente consoni dei precedenti nella misura consentita dalla legge e ai sensi delle leggi e dei regolamenti locali sul lavoro.

Il personale è tenuto a sottoscrivere un accordo di riservatezza, nonché a dare conferma di ricezione delle norme sulla privacy e sulla riservatezza di Google, e della propria conformità con queste norme. Il personale riceve una formazione in materia di sicurezza. Il personale incaricato della gestione dei Dati del Cliente deve soddisfare requisiti aggiuntivi inerenti al proprio ruolo (ad esempio, certificazioni). Il personale di Google non tratterà i Dati del Cliente senza autorizzazione.

4. Misure di sicurezza aggiuntive. Google e il Cliente possono convenire su misure di sicurezza aggiuntive nel Modulo d'ordine vigente, inclusa qualsiasi Capitolato allegato, per i Mandiant Consulting Services e/o Managed Services, a seconda dei casi.

2. Fornitore incaricato dal Cliente. Per chiarezza, e senza limitare le obbligazioni di Google ai sensi della Sezione 7 (Sicurezza dei dati) o 11 (Sub-responsabili), l'Appendice 2 (Misure di sicurezza) non descrive le misure o i controlli di sicurezza attuati o forniti dal Cliente o dai Fornitori incaricati dal Cliente.

Servizi di implementazione

1. Definizioni aggiuntive.

- Per "*Dati del Cliente*" si intendono i dati ai quali il Cliente autorizza il personale di Google ad accedere sui Sistemi gestiti dal Cliente.
- Per "*Sistemi gestiti dal Cliente*" si intende quanto segue, secondo l'utilizzo da parte del Cliente per ricevere i Servizi di implementazione: (a) istanze gestite dal Cliente di servizi Google Cloud o servizi cloud di terze parti; e (b) qualsiasi hardware o software ospitato o gestito nell'ambiente on-premise del Cliente.
- Per "*Servizi Google Cloud*" si intendono tutti i Servizi descritti nella presente Appendice 4 (Prodotti specifici), ad eccezione dei Servizi di implementazione, dei Mandiant Consulting Services e dei Mandiant Managed Services.
- Per "*Personale di Google*" si intendono i dipendenti e gli appaltatori Google impegnati nella fornitura dei Servizi di implementazione.
- Per "*Servizi di implementazione*" si intendono i servizi di consulenza e implementazione forniti dai dipendenti e dagli appaltatori a supporto dei servizi Google Cloud come descritto nel Contratto, incluso in un Modulo d'ordine o in un Capitolato.

2. Emendamenti. Il presente Addendum viene emendato come segue in relazione ai Servizi di implementazione:

- La definizione di "Controlli aggiuntivi per la sicurezza" è eliminata.
- La definizione di "Incidente relativo ai dati" è sostituita con quanto segue:

    - Per "*Incidente relativo ai dati*" si intende una violazione della Sezione 7.1 (Misure, controlli e assistenza in materia di sicurezza da parte di Google) da parte del personale di Google, che comporti l'eliminazione accidentale o illegale, la perdita, l'alterazione, la divulgazione non autorizzata o l'accesso ai Dati personali del Cliente.

- Fatto salvo il resto della presente sezione, il termine "Dati del Cliente" è sostituito con "Dati personali del Cliente" quando utilizzato (a) nella Sezione 2 (Definizioni) nella definizione di "Sub-responsabile" e (b) in altre sezioni del presente Addendum. Per chiarezza, le altre definizioni contenute nella Sezione 2 (Definizioni) rimangono invariate.

- La Sezione 3 (Durata) viene sostituita con la sezione seguente:

    - **3. Durata** Indipendentemente dal fatto che il Contratto vigente sia stato risolto o sia scaduto, il presente Addendum rimarrà in vigore fino a quando Google non avrà più accesso ai Dati personali del Cliente e scadrà automaticamente in quel momento.

- La Sezione 6 (Eliminazione dei dati) viene sostituita con la sezione seguente:

    - **6. Eliminazione dei dati** Alla fine del Periodo di validità, il Cliente (a) deciderà se eliminare i Dati personali del Cliente e (b) sarà responsabile dell'eliminazione.

- La seconda frase della Sezione 7.1.1 (Misure di sicurezza di Google) è sostituita con la sezione seguente:

    - "Le Misure di sicurezza possono includere (a seconda dei casi) misure atte a crittografare i Dati del Cliente a garantire la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di Google; a ripristinare tempestivamente l'accesso ai Dati del Cliente a seguito di un incidente; e a verificare regolarmente l'efficacia delle misure adottate."

- La Sezione 7.1.3 (Controlli di Sicurezza aggiuntivi) è stata eliminata, insieme a tutti gli altri riferimenti a quella sezione.

- La Sezione 9.1 (Accesso, rettifica, trattamento limitato, portabilità) viene sostituita con la seguente:

    - 9.1 *Accesso, rettifica, trattamento limitato, portabilità*. Il Cliente è responsabile dell'utilizzo delle funzionalità dei Sistemi gestiti dal Cliente per accedere, rettificare e limitare il trattamento dei Dati personali del Cliente, anche nel caso in cui il Cliente venga a conoscenza che alcuni Dati personali del Cliente sono inesatti o non aggiornati e sia tenuto dalla Legge sulla privacy vigente a rettificare o eliminare i suddetti dati.

- La Sezione 11.4 (Facoltà di opporsi a modifiche relative ai Sub-responsabili) è sostituita dal seguente testo:

    - 11.4 *Facoltà di opporsi a modifiche relative ai Sub-responsabili*. Quando viene incaricato un nuovo sub-responsabile nel corso del Periodo di validità, Google

informerà il Cliente dell'incarico del nuovo sub-responsabile prima di trattare i Dati personali del Cliente. Il Cliente può opporsi al nuovo sub-responsabile dandone comunicazione a Google e, in tal caso, le parti collaboreranno in buona fede per individuare un'alternativa reciprocamente accettabile.

- L'Allegato 1 (Oggetto e dettagli del trattamento dati) viene emendata come indicato di seguito:
    - La sezione "Durata del trattamento" viene sostituita con la sezione che segue:
        - *"Durata del trattamento*. Il Periodo di validità più (se applicabile) il periodo dalla fine del Periodo di validità fino alla scadenza dell'accesso di Google ai Dati personali del Cliente.
    - Le parole "forniti a Google tramite i Servizi" nelle sezioni "Categorie di dati" e "Soggetti interessati" sono sostituite con "resi accessibili a Google in relazione ai Servizi".
- L'Appendice 2 (Misure di sicurezza) viene sostituita con la sezione seguente:
    - **Appendice 2: Misure di sicurezza**

1. Sistemi gestiti dal Cliente. Il personale di Google accederà e tratterà i Dati personali del Cliente solo sui Sistemi gestiti dal Cliente. Se questi sistemi includono Servizi Google Cloud, l'utilizzo dei Servizi Google Cloud da parte del cliente rimane regolato dal contratto applicabile ai suddetti servizi.

2. Controllo dell'accesso. Le norme e i procedimenti interni di Google relativi all'accesso ai dati sono concepiti per impedire l'accesso di persone e sistemi non autorizzati ai Servizi Google Cloud utilizzati per il trattamento dei dati personali. Le norme di Google (i) consentono al personale di Google di accedere solo ai dati per i quali è autorizzato; e (ii) richiedono che il personale di Google non legga, copi, modifichi o rimuova i Dati personali del Cliente senza autorizzazione durante il trattamento, l'utilizzo e dopo la registrazione. Il Cliente gestisce la concessione o la modifica dei diritti di accesso degli utenti finali ai Sistemi gestiti dal Cliente. Se questi sistemi includono i servizi Google Cloud, i dettagli relativi agli strumenti di workflow che conservano i registri di audit delle modifiche e i log di accesso al sistema sono trattati nel contratto relativo ai servizi Google Cloud applicabili.

3. Sicurezza del personale. Google richiede al proprio personale di adottare una condotta coerente con le linee guida della società in materia di riservatezza, etica aziendale, uso appropriato e standard professionali. Google conduce controlli ragionevolmente consoni dei precedenti nella misura consentita dalla legge e ai sensi delle leggi e dei regolamenti locali sul lavoro.

Il personale di Google è tenuto a sottoscrivere un accordo di riservatezza, nonché a dare conferma di ricezione delle norme sulla privacy e sulla riservatezza di Google, e della propria conformità con queste norme. Il personale di Google riceve una formazione in materia di sicurezza. Il personale di Google incaricato della gestione dei Dati personali del Cliente deve soddisfare requisiti aggiuntivi inerenti al proprio ruolo (ad esempio, certificazioni).

4. Misure di sicurezza aggiuntive. Google e il Cliente possono concordare misure di sicurezza aggiuntive nel Contratto, incluso in un Modulo d'ordine o in un Capitolato.

5. Sicurezza dei Sub-responsabili. Prima di eseguire l'onboarding di nuovi Sub-responsabili, Google conduce un controllo delle prassi relative alla sicurezza e delle norme di tutela della privacy adottate dai Sub-responsabili per assicurare che questi forniscano un livello di sicurezza e privacy consono all'accesso ai dati e alla portata dei servizi per cui vengono incaricati. Una volta che Google ha sottoposto a valutazione i rischi presentati dal Sub-responsabile, fatti salvi i requisiti descritti nella Sezione 11.3 (Requisiti per l'incarico del Sub-responsabile), il Sub-responsabile deve stipulare termini contrattuali appropriati in materia di sicurezza, riservatezza e tutela della privacy.

3. Responsabilità del Cliente in materia di sicurezza. Oltre alle obbligazioni di cui alla Sezione 7.3.1 (Responsabilità del Cliente in materia di sicurezza), il Cliente è responsabile di quanto segue:

- amministrare, gestire l'accesso e proteggere i Sistemi gestiti dal Cliente, compresa la riduzione al minimo dell'accesso del personale di Google ai Dati personali del Cliente nella misura ragionevolmente praticabile e la cessazione di detto accesso al completamento dei Servizi di implementazione; e

- attuare tutti i consigli di sicurezza forniti per iscritto da Google al Cliente in relazione ai Sistemi gestiti dal Cliente.

4. Certificazioni di conformità. Google manterrà le certificazioni ISO 27001, ISO 27017 e ISO 27018 relative ai servizi di implementazione forniti a supporto della piattaforma Google Cloud e di Google Workspace ("*Certificazioni di conformità dei Servizi di implementazione*"). Google potrebbe aggiungere altri standard di volta in volta. Google potrebbe sostituire una Certificazione di conformità dei Servizi di implementazione con un'alternativa equivalente o migliorata.

5. Revisioni della Certificazione di conformità. Per dimostrare la conformità di Google alle proprie obbligazioni ai sensi del presente Addendum, Google metterà a disposizione del Cliente la Certificazione di conformità dei Servizi di Implementazione affinché possa esaminarla e, se il Cliente è un responsabile del trattamento, consentirà al Cliente di richiedere l'accesso alla Certificazione di conformità dei servizi di implementazione al titolare pertinente.

6. Località del trattamento dati. I Dati personali del Cliente possono essere trattati in qualsiasi Paese in cui Google fornisce Servizi di implementazione o in cui il Cliente gestisce Sistemi gestiti dal Cliente.

7. Nessuna certificazione da parte di Clienti di paesi che non appartengono all'area EMEA. Il Cliente non è tenuto a certificare o identificare la propria Autorità di controllo competente, come descritto nella Sezione 4.2 (Certificazione da parte di Clienti non appartenenti all'area EMEA) dei termini europei sulla protezione dei dati nell'Appendice 3 (Leggi specifiche sulla privacy) per i Servizi di implementazione.

8. Informazioni sui Sub-responsabili. I Sub-responsabili per i Servizi di implementazione saranno identificati (come subappaltatori) in un Modulo d'ordine, in un Capitolato o in un'altra conferma fornita al Cliente prima dell'inizio dei Servizi di implementazione, o saranno identificati nelle Società affiliate di Google. Google metterà inoltre a disposizione del Cliente, su richiesta, i nomi, le sedi e le attività dei Sub-responsabili per i Servizi di implementazione.

9. Registri di Google relativi al trattamento. Nella misura in cui una legge vigente sulla privacy richieda a Google di raccogliere e conservare i registri di determinate informazioni relative al Cliente, il Cliente fornirà queste informazioni su richiesta di Google e comunicherà a Google eventuali aggiornamenti necessari per far sì che siano sempre accurate e aggiornate, a meno che Google non richieda al Cliente di fornire e aggiornare queste informazioni secondo un'altra modalità.

Google Cloud Skills Boost per le Organizzazioni

1. Definizioni aggiuntive.

- Per "*Account*", se non definito dal Contratto, si intende l'Account Cliente di Google Cloud Skills Boost per le Organizzazioni.
- Per "*GCSBO*" si riferisce a servizi e contenuti educativi, formativi e didattici forniti tramite https://www.cloudskillsboost.google/ (o un altro sito web gestito o controllato da Google e utilizzato per gli scopi di Google Cloud Skills Boost per le Organizzazioni).
- Per "*TSS*" si intendono i Servizi di assistenza tecnica che Google, a sua discrezione, può fornire al Cliente.

2. Emendamenti. Il presente Addendum viene emendato come segue in relazione a GCSBO:

- La definizione di "Controlli aggiuntivi per la sicurezza" è sostituita come segue:
    - Per *"Controlli di Sicurezza aggiuntivi"* si intendono risorse, caratteristiche, funzionalità e/o controlli relativi alla sicurezza che il Cliente può utilizzare a propria scelta e/o discrezione, tra cui (se del caso) la crittografia, il logging e il monitoraggio, la gestione di identità e l'analisi della sicurezza.
- Le definizioni di "SCC (da titolare a responsabile)", "SCC (da responsabile a titolare)", "SCC (da responsabile a responsabile)" e "SCC (da responsabile a responsabile, Esportatore Google)" nell'Appendice 3 (Leggi specifiche sulla privacy) vengono sostituite come segue:
    - Per "SCC (da titolare a responsabile)" si intendono i termini riportati all'indirizzo https://cloud.google.com/terms/skillsboost-organizations/sccs/eu-c2p;
    - Per "SCC (da responsabile a titolare)" si intendono i termini riportati all'indirizzo https://cloud.google.com/terms/skillsboost-organizations/sccs/eu-p2c;
    - Per "SCC (da responsabile a responsabile)" si intendono i termini riportati all'indirizzo https://cloud.google.com/terms/skillsboost-organizations/sccs/eu-p2p; e
    - Per "SCC (da responsabile a responsabile, Esportatore Google)" si intendono i termini riportati all'indirizzo: https://cloud.google.com/terms/skillsboost-organizations/sccs/eu-p2p-intra-group.

3. Località dei data center. Le località dei data center di GCSBO sono descritte all'indirizzo https://cloud.google.com/about/locations/.

4. Nessuna certificazione da parte di Clienti di paesi che non appartengono all'area EMEA. Il Cliente non è tenuto a certificare o identificare la propria Autorità di controllo competente, come descritto nella Sezione 4.2 (Certificazione da parte di Clienti non appartenenti all'area EMEA) dei termini europei sulla protezione dei dati nell'Appendice 3 (Leggi specifiche sulla privacy) per GCSBO.

5. Informazioni sui Sub-responsabili. Nomi, sedi e attività dei sub-responsabili di GCSBO sono descritti agli indirizzi:

a. https://cloud.google.com/terms/skillsboost-organizations/subprocessors; e

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

6. Team di Google dedicato alla protezione dei dati cloud. È possibile contattare il Team dedicato alla protezione dei dati cloud per GCSBO all'indirizzo https://support.google.com/qwiklabs (e/o mediante altre modalità che Google potrebbe fornire di volta in volta).

7. Registri di Google relativi al trattamento. Nella misura in cui una legge vigente sulla privacy richieda a Google di raccogliere e conservare i registri di determinate informazioni relative al Cliente, il Cliente fornirà queste informazioni su richiesta di Google e comunicherà a Google eventuali aggiornamenti necessari per far sì che siano sempre accurate e aggiornate, a meno che Google non richieda al Cliente di fornire e aggiornare queste informazioni secondo un'altra modalità.

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

9 aprile 2024 30 giugno 2022 24 settembre 2021 19 agosto 2020 10 agosto 2020 17 luglio 2020 11 ottobre 2019 1 ottobre 2019 25 maggio 2018 13 marzo 2018 9 novembre 2017 11 ottobre 2017 7 febbraio 2017 6 ottobre 2016

Versioni precedenti dell'Emendamento sul trattamento dei dati:

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

Versioni precedenti dell'Addendum per il trattamento dei dati per i Servizi (Clienti) Looker (original):

14 febbraio 2023 4 gennaio 2023 20 settembre 2022 30 giugno 2022 16 marzo 2022 24 settembre 2021 1 aprile 2021 15 gennaio 2021 17 dicembre 2020 28 agosto 2020 1 giugno 2020 9 marzo 2020

Versioni precedenti dei DPST per i Servizi SecOps (Clienti):

6 febbraio 2023 28 novembre 2022 27 settembre 2021 1 ottobre 2020

Versioni precedenti dell'Addendum per il trattamento dei dati per i SecOps Consulting Services e Managed Services:

5 ottobre 2023 19 settembre 2023 15 giugno 2023 22 febbraio 2023 6 febbraio 2023

Versioni precedenti *(Ultima modifica: 15 ottobre 2024)*

26 settembre 2024 9 settembre 2024 5 agosto 2024 23 maggio 2024 9 aprile 2024 8 novembre 2023 15 agosto 2023 20 settembre 2022