Cloud Data Processing Addendum (Partner)

Il presente Cloud Data Processing Addendum (comprese le sue appendici, l'"*Addendum*") viene incorporato nel Contratto (come definito di seguito) tra Google e il Partner. Il presente Addendum era precedentemente noto come "Termini per il trattamento e la sicurezza dei dati" per Google Cloud Platform e come "Data Processing Addendum" o "Termini per il trattamento e la sicurezza dei dati" per i Servizi Looker (original) o Google SecOps.

Termini generali

1. Panoramica

Il presente Addendum descrive le obbligazioni delle parti, anche ai sensi delle leggi applicabili in materia di privacy, sicurezza dei dati e protezione dei dati, in relazione al trattamento e alla sicurezza dei dati del Partner. Il presente Addendum entrerà in vigore alla Data di validità dell'Addendum (come definita di seguito) e sostituirà tutti i termini precedentemente applicabili al trattamento e alla sicurezza dei dati del Partner. I termini con iniziali maiuscole 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 Partner ha accettato, oppure le parti hanno altrimenti concordato, il presente Addendum.
- Per "*Controlli di Sicurezza Aggiuntivi*" si intendono risorse, caratteristiche, funzionalità e controlli relativi alla sicurezza che il Partner può utilizzare a propria scelta e discrezione, tra cui Console di amministrazione, crittografia, logging e monitoraggio, gestione di identità e accessi, analisi della sicurezza e firewall.
- Per "*Contratto*" si intende il contratto in base al quale Google ha accettato di fornire al Partner i Servizi applicabili.
- Per "*Legge sulla privacy applicabile*" si intende, per quanto riguarda il trattamento dei Dati personali del Partner, qualsiasi legge o regolamento nazionale, federale, dell'Unione Europea, statale, provinciale o di altro tipo in materia di privacy, sicurezza dei dati o protezione dei dati.

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

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

- Per "*Incidente relativo ai dati*" si intende una violazione della sicurezza di Google che, in modo accidentale o illegale, comporti la distruzione, la perdita, la modifica, la divulgazione non autorizzata dei, o l'accesso ai, dati del Partner presenti nei sistemi gestiti o altrimenti controllati 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 Partner); (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 Partner); o (c) le leggi della Svizzera (se il FADP svizzero è applicabile al trattamento dei Dati personali del Partner).

- 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 corrente verrà comunicata al Partner da Google.

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

- Per "*Indirizzo email di notifica*" si intende l'indirizzo o gli indirizzi email che il Partner ha indicato nella Console di amministrazione o nel Modulo d'ordine per la ricezione di determinate notifiche da Google.

- Per "*Utente finale del Partner*" si intende il significato indicato nel Contratto o, qualora non sia specificato, si intende il significato indicato nel Contratto per "Utente finale".

- Per "*Dati personali del Partner*" si intendono i dati personali inclusi nei dati del Partner, comprese tutte le categorie speciali di dati personali o dati sensibili definiti ai sensi della legge vigente sulla privacy.

- 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 Partner per fornire parti dei Servizi e dei TSS.

- 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 dei Servizi da parte di Google, 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 dell'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 loro assenza, quelli descritti dal GDPR dell'Unione Europea.

2.3 I termini "interessato", "titolare" e "responsabile" includono rispettivamente "consumatore", "azienda" e "fornitore di servizi", come previsto dalla Legge vigente sulla privacy.

3. Durata

Indipendentemente dal fatto che il Contratto sia stato risolto o sia scaduto, il presente Addendum resterà in vigore fino a quando Google non avrà eliminato tutti i dati del Partner, come descritto nel presente Addendum, e scadrà automaticamente in quel momento.

4. Ruoli; Conformità legale

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

4.2 *Riepilogo del trattamento*. L'oggetto e i dettagli del trattamento dei Dati personali del Partner 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 Partner ai sensi della Legge vigente sulla privacy.

4.4 *Termini legali aggiuntivi*. Nella misura in cui il trattamento dei Dati personali del Partner 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 *Partner responsabili*. Se il Partner è un responsabile:

a. Il Partner garantisce su base continuativa che il Cliente e titolare in questione ha autorizzato:

i. le disposizioni;

ii. l'incarico a Google da parte del Partner come ulteriore responsabile del trattamento; e

iii. l'incarico di Sub-responsabili da parte di Google come descritto nella Sezione 11 (Sub-responsabili);

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

c. Il Partner può mettere a disposizione del Cliente e titolare in questione qualsiasi altra informazione resa disponibile da Google ai sensi del presente Addendum in merito all'ubicazione dei data center di Google oppure a nomi, ubicazioni e attività dei Sub-responsabili.

5.2 *Conformità con le Disposizioni del Partner*. Il Partner dà disposizione a Google di trattare i dati del Partner in conformità con il Contratto (incluso il presente Addendum) esclusivamente nelle modalità di seguito descritte:

a. per fornire, proteggere e monitorare i Servizi e i TSS; e

b. come ulteriormente specificato mediante:

i. l'uso dei Servizi (anche mediante la Console di amministrazione) e dei TSS da parte del Partner; e

ii. qualsiasi altra disposizione scritta fornita al Partner e riconosciuta da Google come tale ai fini del presente Addendum

(collettivamente, le "*Disposizioni*").

Google agirà in maniera conforme alle Disposizioni, a meno che non sia vietato dalle Leggi europee, laddove si applichi la Legge europea sulla protezione dei dati, o dalle leggi vigenti, laddove si applichi qualsiasi altra legge sulla privacy applicabile.

6. Eliminazione dei dati

6.1 *Eliminazione da parte del Partner*. Google consentirà al Partner di eliminare i dati del Partner durante il Periodo di validità coerentemente con la funzionalità dei Servizi. Se il Partner utilizza i Servizi per eliminare i dati del Partner durante il Periodo di validità e questi dati del Partner non possono essere recuperati dal Partner, questo utilizzo costituirà una Disposizione nei confronti di Google affinché elimini i dati del Partner in questione dai sistemi di Google. Google ottempererà a questa Disposizione non appena ragionevolmente possibile ed entro un periodo massimo di 180 giorni, a meno che la Legge europea non imponga la conservazione, laddove si applichi la Legge europea sulla protezione dei dati, o che la legge vigente non imponga la conservazione, laddove si applichi qualsiasi altra legge sulla privacy applicabile.

6.2 *Restituzione o eliminazione alla fine del Periodo di validità*. Se il Partner desidera conservare i dati del Partner dopo la fine del Periodo di validità, può dare disposizione a Google di restituire quei dati durante il Periodo di validità, in conformità con la Sezione 9.1 (Accesso; Rettifica; Trattamento limitato; Portabilità). Il Partner dà disposizione a Google di eliminare tutti i restanti dati del Partner (comprese le copie esistenti) dai sistemi di Google al termine del Periodo di validità. Trascorso il periodo di recupero massimo di 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 imponga la conservazione, laddove si applichi la Legge europea sulla protezione dei dati, o che la legge vigente non imponga la conservazione, laddove si applichi qualsiasi altra legge sulla privacy applicabile.

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 del Partner vengano accidentalmente o illegalmente distrutti, persi o modificati e per impedirne la divulgazione e l'accesso non autorizzati come descritto nell'Appendice 2 (le "*Misure di sicurezza*"). Le Misure di sicurezza includono misure finalizzate a criptare i dati del Partner; a contribuire ad assicurare la riservatezza, l'integrità, la disponibilità e la resilienza su base continuativa dei sistemi e dei servizi di Google; a contribuire al ripristino tempestivo dell'accesso ai dati del Partner in seguito a un incidente; e ad eseguire test di efficienza regolari. Google potrà periodicamente aggiornare queste Misure di sicurezza, a condizione che tali 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 Partner esclusivamente nella misura strettamente necessaria per ottemperare alle Disposizioni;

b. adotterà misure appropriate per garantire il rispetto delle Misure di sicurezza da parte dei propri dipendenti, appaltatori e Sub-responsabili nella misura applicabile all'ambito delle rispettive prestazioni; e

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

7.1.3 *Controlli di Sicurezza Aggiuntivi*. Google metterà a disposizione Controlli di Sicurezza Aggiuntivi per:

a. consentire al Partner di adottare le misure necessarie per proteggere i Dati del Partner; e

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

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

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

b. fornire Controlli di Sicurezza Aggiuntivi, in conformità con la Sezione 7.1.3 (Controlli di Sicurezza Aggiuntivi);

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

d. rendere disponibile la Documentazione sulla sicurezza in conformità con la Sezione 7.5.1 (Revisioni della Documentazione sulla sicurezza) e fornire le informazioni contenute nel Contratto (compreso il presente Addendum); e

e. fornire al Partner, su richiesta di quest'ultimo, collaborazione e assistenza aggiuntive in misura ragionevole, qualora le sottosezioni (a)-(d) sopra riportate non siano sufficienti affinché il Partner (o il titolare del trattamento in questione) possa ottemperare a queste obbligazioni.

7.2 *Incidenti relativi ai dati*.

7.2.1 *Notifica degli incidenti*. Qualora Google venisse a conoscenza di un Incidente relativo ai dati, lo comunicherà tempestivamente e senza ingiustificato ritardo al Partner e adotterà prontamente misure ragionevoli per ridurre al minimo i danni e proteggere i dati del Partner.

7.2.2 *Dettagli dell'Incidente relativo ai dati*. La notifica di un Incidente relativo ai dati inviata da Google descriverà: la natura dell'Incidente relativo ai dati, incluse le risorse del Partner 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 Partner di adottare per gestire l'Incidente relativo ai dati; i dettagli di un punto di contatto a cui è possibile rivolgersi per 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 Partner da parte di Google*. Non esiste alcuna obbligazione per Google di valutare i Dati del Partner per 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 Partner in materia di sicurezza*.

7.3.1 *Responsabilità del Partner in materia di sicurezza*. Fatti salvi gli obblighu di Google indicate 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 tra Google e il Partner, il Partner è responsabile per il proprio utilizzo dei Servizi e per l'utilizzo da parte dei suoi Clienti e per la conservazione da parte sua di qualsiasi copia dei dati del Partner 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 Partner;

b. la protezione delle credenziali di autenticazione degli account, dei sistemi e dei dispositivi utilizzati dal Partner e dai suoi Clienti per accedere ai Servizi; e

c. l'esecuzione di backup dei dati del Partner come appropriato.

7.3.2 *Valutazione della sicurezza del Partner*. Il Partner conviene che i Servizi, le Misure di sicurezza, i Controlli di Sicurezza Aggiuntivi e gli impegni di Google ai sensi della presente Sezione 7 (Sicurezza dei dati) forniscono un livello di sicurezza adeguato al rischio per i dati del Partner (tenendo conto dello stato dell'arte, dei costi di implementazione e della natura, dell'ambito, del contesto e delle finalità del trattamento dei dati del Partner, nonché dei rischi per i privati).

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. i certificati relativi 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 in qualsiasi momento. 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*. Per dimostrare la conformità di Google alle sue obbligazioni previste dal presente Addendum, Google metterà la Documentazione sulla sicurezza a disposizione del Partner per la revisione e, se il Partner è un responsabile, permetterà al Partner di richiedere accesso ai Report SOC per il Cliente e 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 Partner*.

a. *Audit del Partner*. Google, se richiesto dalla Legge sulla privacy applicabile, consentirà al Partner o a un revisore indipendente nominato dal Partner di condurre controlli (incluse 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 Partner o con il suo revisore, come descritto nella presente Sezione 7.5 (Revisioni e controlli di conformità).

b. *Revisione indipendente del Partner*. Il Partner può eseguire controlli per verificare la conformità di Google alle proprie obbligazioni ai sensi del presente Addendum mediante la revisione della Documentazione sulla 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 i audit*.

a. il Partner 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 e Audit di conformità); o

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

b. A seguito di una richiesta del Partner ai sensi della Sezione 7.5.3(a), Google e il Partner discuteranno 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. data di inizio, ambito e durata ragionevoli dei controlli di sicurezza e riservatezza applicabili in conformità alla Sezione 7.5.2(a) (Audit del Partner).

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

d. Google può opporsi in forma scritta alla nomina di un revisore da parte del Partner per l'esecuzione di un audit di cui alla Sezione 7.5.2(a) (Audit del Partner) 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 queste obiezioni, il Partner dovrà nominare un altro revisore o eseguire il controllo per proprio conto.

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

8. Valutazioni dell'impatto e consultazioni

Google (tenendo conto della natura del trattamento e le informazioni a disposizione di Google) fornirà assistenza al Partner al fine di garantire la conformità con i propri obblighi (o, se il Partner è un responsabile, quelle del titolare in questione) relativi alle valutazioni della protezione dei dati, alle analisi del rischio, alle consultazioni normative preventive o a procedure analoghe ai sensi della legge vigente sulla privacy:

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 sulla sicurezza in conformità con la Sezione 7.5.1 (Revisioni della Documentazione sulla sicurezza);

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

c. fornendo al Partner collaborazione e assistenza aggiuntive in misura ragionevole su richiesta del Partner, quando le sottosezioni (a) e (b) sopra riportate non sono sufficienti perché il Partner (o il titolare in questione) possa ottemperare a queste obbligazioni.

9. Accesso, ecc.; Diritti dell'interessato; esportazione dei dati

9.1 *Accesso, rettifica, trattamento limitato, portabilità*. Durante il Periodo di validità, Google consentirà al Partner, in modo coerente con le funzionalità dei Servizi, di accedere, rettificare e limitare il trattamento dei dati del Partner, anche attraverso la funzionalità di eliminazione fornita da Google di cui alla Sezione 6.1 (Eliminazione da parte del Partner), nonché di esportare i dati del Partner. Qualora il Partner venisse a conoscenza del fatto che i Dati personali del Partner sono imprecisi o obsoleti, il Partner sarà responsabile dell'utilizzo di questa funzionalità per rettificare o eliminare questi dati, se previsto 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 Partner e identifica il Partner, Google:

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

b. avviserà tempestivamente il Partner; e

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

Il Partner sarà responsabile di rispondere a queste richieste anche, ove necessario, utilizzando 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 Partner) fornirà assistenza al Partner nell'adempimento delle sue obbligazioni (o, nel caso in cui il Partner 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. fornendo al Partner collaborazione e assistenza aggiuntive in misura ragionevole su richiesta del Partner, qualora le sottosezioni (a) e (b) sopra riportate non siano sufficienti affinrché il Partner (o il titolare in questione) possa ottemperare a questi obblighi.

10. Posizioni del trattamento dei dati

10.1 *Strutture 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 Partner 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 dei Sub-responsabili*. Il Partner 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 Partner 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 dei Sub-responsabili*. Al momento di assegnare l'incarico a un qualsiasi Sub-responsabile, Google:

a. garantirà tramite un contratto scritto che:

i. il Sub-responsabile acceda ai dati del Partner e li utilizzi esclusivamente nella misura necessaria per ottemperare alle obbligazioni derivanti dal suo incarico e in conformità con il Contratto (incluso il presente Addendum); e

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

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

11.4 *Facoltà di opporsi ai Sub-responsabili*.

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

b. Il Partner, 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, tramite notifica a Google.

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

12.1 *Team 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 Partner correlata al trattamento dei dati del Partner ai sensi del Contratto e può essere contattato come descritto nella sezione Comunicazioni del Contratto o nell'Appendice 4 (Prodotti specifici).

12.2 *Registri di Google relativi al trattamento*. 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 Partner o ai suoi Clienti, il Partner 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 regolamentazionei 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 una disposizione da una terza parte che sostiene di essere titolare del trattamento dei Dati personali del Partner, Google inviterà questa terza parte a contattare il Partner.

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 Partner è tenuto a informare Google utilizzando la

Console di amministrazione o in altro modo per garantire che il suo Indirizzo email di notifica sia valido e aggiornato.

14. Interpretazione

14.1 *Precedenza*. In caso di conflitto tra:

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

b. l'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.

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.

14.3 *Clienti*. A scanso di dubbi, i Clienti non sono beneficiari terzi del presente Addendum.

Appendice 1: Oggetto e dettagli del trattamento dei dati

Oggetto

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

Durata del trattamento

Il Periodo di validità più il periodo compreso tra la fine 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 Partner al fine di fornire al Partner i Servizi e i TSS in conformità con il presente Addendum.

Categorie di dati

Dati relativi a privati forniti a Google tramite i Servizi dal Partner (o su sua indicazione) o dai suoi Clienti o dagli Utenti finali del Partner.

Interessati

Per interessati si intendono i privati i cui dati vengono forniti a Google tramite i Servizi dal Partner (o su sua indicazione) o dai suoi Clienti o dagli Utenti finali del Partner.

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. Google archivia tutti i dati di produzione in data center 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 dei 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 dell'infrastruttura critica dei data center vengono fornite una fonte di alimentazione primaria e una alternativa, 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 in 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 del 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 operativa e il disaster recovery che vengono rivisti e testati regolarmente.

(*b) Reti e trasmissione.*

Trasmissione dei dati. I data center sono generalmente collegati 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 registrazione 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 dati approfonditi 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 di Google attraverso misure preventive, (ii) l'impiego di controlli di rilevamento intelligente in tutti i punti di immissione dati e (iii) l'uso di tecnologie per rimediare automaticamente di determinate situazioni pericolose.

Risposta agli incidenti. Google monitora una varietà di canali di comunicazione per gli incidenti di 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 tramite chiave elettronica 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 a dipendenti, appaltatori e visitatori autorizzati. Solo i dipendenti e i appaltatori autorizzati possono richiedere l'accesso tramite chiave elettronica a queste strutture. Le richieste di accesso tramite chiave elettronica ai data center devono essere inoltrate 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 preventivamente l'approvazione dei responsabili del data center per lo specifico data 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 il privato è approvato.

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 chiavi elettroniche di ogni privato 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 del privato 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 unità operative 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 norme di sicurezza per i propri dipendenti e richiede che la formazione in materia di sicurezza sia parte integrante del loro pacchetto formativo. 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 Partner devono eseguire l'autenticazione per mezzo di un sistema di autenticazione centrale o di un sistema di 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 Partner. 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 i dati del Partner non possano essere letti, copiati, alterati o rimossi senza autorizzazione durante il trattamento e l'utilizzo e dopo la registrazione. 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 in base al principio della "necessità di sapere". La concessione o la modifica dei diritti di accesso deve inoltre essere conforme alle norme e alla formazione interne di Google in materia di accesso ai dati. Le approvazioni

sono controllate da strumenti di gestione dei workflow che conservano record di controllo per ogni modifica. L'accesso ai sistemi viene registrato per creare un audit trail per la responsabilizzazione. Qualora siano impiegate password per l'autenticazione
(ad esempio per accedere a delle postazioni di lavoro), vengono implementate norme sulle password che seguono almeno 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 della sede dei dati), Google replica i dati del Partner tra più data center in diverse aree geografiche. Inoltre Google isola logicamente i dati del Partner. Al Partner viene dato il controllo dei criteri specifici di condivisione dei dati. Questi criteri, in conformità con le funzionalità dei Servizi, consentono al Partner di determinare le impostazioni di condivisione dei prodotti applicabili agli Utenti finali del Partner per scopi specifici. Il Partner 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 riutilizzati o distrutti, tutti i Dischi dismessi vengono sottoposti 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 validatori indipendenti. I risultati della cancellazione vengono registrati mediante il numero di serie del Disco dismesso 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 finalizzati a 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 in conformità con le leggi e i regolamenti locali vigenti in materia di 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 Partner deve soddisfare requisiti aggiuntivi inerenti al proprio ruolo (ad esempio, certificazioni). Il personale di Google non tratterà i dati del Partner senza autorizzazione.

5. Sicurezza dei Sub-responsabili

Prima di procedere all'onboarding di nuovi Sub-responsabili, Google conduce un controllo delle prassi di sicurezza e delle norme di tutela della privacy adottate dai Sub-responsabili per accertarsi che forniscano un livello di sicurezza e privacy appropriato all'accesso ai dati e alla portata dei servizi per cui vengono incaricati. Una volta che Google ha valutato i rischi presentati dal Sub-responsabile, fatti salvi i requisiti descritti nella Sezione 11.3 (Requisiti per l'incarico dei Sub-responsabili), il Sub-responsabile deve stipulare adeguati termini contrattuali 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 Partner.

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 del 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 del FADP svizzero;

in ogni caso, salvo diversa indicazione in base a un quadro normativo facoltativo sulla protezione dei dati.

- Per "*Soluzione di trasferimento alternativa*" si intende una soluzione diversa dalle SCC 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 quadro normativo sulla protezione dei dati riconosciuto come capace di garantire che le persone giuridiche partecipanti forniscano un livello di protezione adeguato.

- Per "*SCC del Partner*" 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 Partner 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'indirizzo https://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 Partner) o qualsiasi altro diritto o obbligazione di una delle parti ai sensi del Contratto, Google informerà immediatamente il Partner 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, salvo nei casi in cui questa comunicazione è vietata dalla Legge europea.

Se il Partner è un responsabile, comunicherà immediatamente al titolare in questione eventuali notifiche fornite da Google ai sensi della presente sezione.

3. Diritti di audit del Partner. Google consentirà al Partner o a un revisore indipendente nominato dal Partner di eseguire audit, incluse ispezioni, come descritto nella Sezione 7.5.2(a) (Audit del Partner). Durante il 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 Sezione 7.5 (Revisioni e audit di conformità) e nella presente 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 Partner possano essere trattati o trasferiti in un Paese adeguato. Se i Dati personali del Partner vengono trasferiti in qualsiasi altro paese e la Legge europea sulla protezione dei dati si applica ai trasferimenti (come certificato dal Partner ai sensi della Sezione 4.2 (Certificazione da parte di Partner 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 ha adottato una Soluzione di trasferimento alternativa per eventuali Trasferimenti limitati, Google informerà il Partner circa la soluzione pertinente 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 Partner che non sta più adottando una Soluzione di trasferimento alternativa per qualsiasi Trasferimento limitato (senza adottare una Soluzione di trasferimento alternativa sostitutiva):

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

A. le SCC (da responsabile a responsabile, esportatore Google) si applicheranno in relazione a tali Trasferimenti limitati da Google ai Sub-responsabili; e

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

ii. 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 (a prescindere dal fatto che il Partner sia un titolare o un responsabile) in relazione a tali Trasferimenti limitati tra Google e il Partner.

4.2 *Certificazione da parte di Partner non appartenenti all'area EMEA*. Se l'indirizzo di fatturazione del Partner si trova al di fuori dell'area EMEA e il trattamento dei Dati personali del Partner è soggetto alla Legge europea sulla protezione dei dati, salvo diversamente specificato nell'Appendice 4 (Prodotti specifici) del presente Addendum, il Partner certificherà tale condizione 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 Partner 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 sulla sicurezza);

b. in altre posizioni 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 Partner, come descritto nella Sezione 4.1 (Trasferimenti limitati) dei presenti termini della Legge europea sulla protezione dei dati, Google consentirà al Partner (o a un revisore indipendente nominato dal Partner) 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 Partner inoltrerà al titolare in questione tempestivamente e senza ritardi ingiustificati eventuali notifiche relative alle SCC.

4.6 *Recesso per rischio di trasferimento dei dati*. Se il Partner giunge alla conclusione, in base all'uso corrente o previsto dei Servizi, che non sono state fornite le misure di protezione appropriate per i Dati personali del Partner trasferiti, il Partner potrà recedere con effetto immediato dal Contratto in

conformità con la disposizione di recesso libero del Contratto o, in assenza di tale disposizione, tramite 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 Partner (che vengono incorporate per citazione al presente Addendum) e la parte restante del Contratto (incluso il presente Addendum), prevarranno le SCC del Partner.

5. Requisiti per l'incarico dei Sub-responsabili. Ai sensi della Legge europea sulla protezione dei dati, Google ha l'obbligo di garantire mediante un contratto scritto che le obbligazioni sulla protezione dei dati descritte nel presente Addendum, come definito nell'Articolo 28, paragrafo 3, del GDPR, ove applicabile, vengano imposte a 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 a tutti i regolamenti di attuazione.

- "*Dati personali del Partner*" include "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 Partner), in relazione con il trattamento dei Dati personali del Partner in conformità con il CCPA, salvo diversamente consentito ai sensi del CCPA, Google non:

a. venderà o condividerà Dati personali del Partner;

b. conserverà, userà o divulgherà Dati personali del Partner:

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

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

c. combinerà o aggiornerà i Dati personali del Partner con le informazioni personali che Google riceve da o per conto di terze parti o che raccoglie dalle proprie interazioni con il consumatore.

3. Conformità. A prescindere dalle obbligazioni di Google ai sensi della Sezione 5.2 (Conformità con le Disposizioni del Partner) o qualsiasi altro diritto o obbligazione di una delle parti ai sensi del Contratto,

Google informerà il Partner se, a suo giudizio, Google non è in grado di adempiere alle proprie obbligazioni ai sensi del CCPA, fatto salvo il caso in cui tale avviso sia vietato dalla legge applicabile.

4. Intervento del Partner. Se Google notifica al Partner un uso non autorizzato dei Dati personali del Partner, anche ai sensi della Sezione 3 (Conformità) della presente sottosezione o della Sezione 7.2.1 (Notifica degli incidenti), il Partner può adottare misure ragionevoli e appropriate per interrompere o porre rimedio a questo uso non autorizzato:

a. adottando tutte le misure raccomandate 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 Partner) 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.* Se l'indirizzo di fatturazione del Partner si trova in Turchia e Google rende disponibili per l'accettazione da parte del Partner eventuali termini aggiuntivi facoltativi (comprese le SCC turche) in relazione al trasferimento dei Dati personali del Partner 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 Partner a Google.

2.2 *Notifica all'Autorità competente.* Se il Partner stipula delle SCC turche ai sensi della presente Sezione 2 (Trasferimenti di dati), il Partner 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 Partner stipula delle SCC turche ai sensi della presente Sezione 2 (Trasferimenti di dati), Google consentirà al Partner (o a un revisore indipendente nominato dal Partner) di condurre audit come descritto in queste SCC e, durante i controlli, metterà a disposizione tutte le informazioni richieste da queste SCC, il tutto 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*. Se il Partner giunge alla conclusione, in base all'uso corrente o previsto dei Servizi, che non sono state fornite le misure di protezione appropriate per i Dati personali del Partner trasferiti, il Partner potrà recedere con effetto immediato dal Contratto in questione in conformità con la disposizione di recesso libero del Contratto o, in assenza di tale disposizione, tramite 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 (che vengono incorporate per citazione al presente Addendum se stipulato dal Partner) 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", "dati personali", "trattamento" e "responsabile", come utilizzati nel presente Addendum, hanno il significato attribuito dalla Legge israeliana sulla protezione della privacy.

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

Appendice 4: Prodotti specifici

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

Piattaforma Google Cloud

1. Definizioni aggiuntive.

- Per "*Account*", se non definito nel Contratto, si intende l'account Google Cloud Platform del Partner.

- 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 i certificati 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 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 a Trasferimenti limitati, Controlli aggiuntivi per la sicurezza e altre misure protettive supplementari sono disponibili all'indirizzo https://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 volutamente 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 e indipendente nominato da Google o un Sub-responsabile di Bare Metal Solution, la cui identità corrente verrà comunicata al Partner da Google su richiesta.
- I seguenti termini vengono eliminati:
    - Dalla Sezione 7.1.1 (Misure di sicurezza di Google), la frase "criptare i dati del Partner";
    - Dall'Appendice 2 (Misure di sicurezza), Sezione 1(a), le sottosezioni "Sistemi operativi del server" e "Continuità operativa";
    - 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 Partner (ad esempio, sotto forma

di selezione della sede dei dati), Google replica i dati del Partner 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 equivalente 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 con cadenza annuale sulla base di controlli svolti almeno una volta ogni 12 mesi (i "*Report SOC BMS*").

3. Revisioni della Documentazione sulla sicurezza. Per dimostrare la conformità alle proprie obbligazioni ai sensi del presente Addendum, Google metterà a disposizione del Partner le Certificazioni di conformità BMS e i Report SOC BMS e, se il Partner è un responsabile, permetterà al Partner 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 Partner. Senza limitare le obbligazioni esplicite di Google relative a Bare Metal Solution, il Partner adotterà misure ragionevoli per proteggere e mantenere la sicurezza dei dati del Partner e di qualsiasi altro contenuto memorizzato o elaborato mediante Bare Metal Solution.

5. Limitazione di responsabilità. In deroga a qualsiasi disposizione contraria contenuta nel Contratto (compreso il presente Addendum), Google non è responsabile per nessuno dei seguenti aspetti in relazione a Bare Metal Solution:

a. sicurezza non fisica, come controlli dell'accesso, crittografia, firewall, protezione antivirus, rilevamento delle minacce e analisi della 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 il disaster recovery.

Il Partner 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 Partner, software e applicazioni utilizzati, caricati o ospitati dal Partner 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 Partner) 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 Partner.

Google Distributed Cloud Edge (Google Cloud Platform)

Il deployment di Google Distributed Cloud Edge ("*GDCE*") 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 GDCE:

- 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.*. Il Partner dà disposizione a Google di eliminare tutti i restanti dati del Partner (comprese le copie esistenti) dalle Apparecchiature al termine del Periodo di validità in conformità con la legge vigente. Se il Partner desidera conservare i dati del Partner dopo la fine del Periodo di validità, può esportare o fare delle copie dei dati prima della fine del Periodo di validità. Google agirà in maniera conforme alle Disposizioni della presente Sezione 6.2 non appena ragionevolmente possibile ed entro un massimo di 180 giorni, a meno che la Legge europea non ne richieda la conservazione, laddove si applichi la Legge europea sulla protezione dei dati, o la legge vigente ne richieda la conservazione, laddove si applichi 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. Macchine locali e sicurezza di rete**

Macchine locali. I dati del Partner vengono archiviati esclusivamente sulle Apparecchiature destinate al deployment presso una Sede del Cliente.

Sistemi operativi del 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 GDCE e migliorare i prodotti per la sicurezza in negli ambienti di produzione GDCE.

Tecnologie di crittografia. Google mette a disposizione la crittografia HTTPS (nota anche come connessione SSL o TLS) e consente la crittografia dei dati in transito. I server di Google supportano lo

scambio di chiavi 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. GDCE presenta un'integrazione CMEK; ulteriori informazioni sono disponibili all'indirizzohttps://cloud.google.com/kms/docs/cmek.

Connessione a Cloud VPN. Google consente al Partner di attivare e configurare un'interconnessione forte e crittografata tra le Apparecchiature e il Virtual Private Cloud del Partner utilizzando Cloud VPN attraverso una connessione VPN IPsec.

Archiviazione vincolata. L'archiviazione dei dati del Partner 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 GDCE.

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

Google Cloud VMware Engine (Google Cloud Platform)

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

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 e indipendente nominato da Google o un Sub-responsabile di NetApp Volumes, la cui identità corrente verrà comunicata al Partner da Google 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 esempio sotto forma di selezione della sede dei dati), Google replica i dati del Partner tra più data center situati in diverse aree geografiche. Inoltre Google isola logicamente i dati del Partner. Al Partner viene dato il controllo dei criteri specifici di condivisione dei dati. Questi criteri, in conformità con le funzionalità dei Servizi, consentono al Partner di determinare le impostazioni di condivisione dei prodotti applicabili agli Utenti finali del Partner per scopi specifici. Il Partner 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 equivalente 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 con cadenza annuale sulla base di controlli svolti almeno una volta ogni 12 mesi (i "*Report SOC NetApp*").

3. Revisioni della Documentazione sulla sicurezza. Per dimostrare la conformità alle proprie obbligazioni ai sensi del presente Addendum, Google metterà a disposizione del Partner le Certificazioni di conformità NetApp e i Report SOC NetApp e, se il Partner è un responsabile, permetterà al Partner 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).

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 Servizi 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 cloud provider 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 origini dati, offerta da Google al Partner 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 Servizi multi-cloud gestiti da Google.

- Per "*Modulo d'ordine*" si intende il significato indicato nel Contratto, a meno che il Partner 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'altro documento scritto (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 Partner nel Modulo d'ordine o mediante Looker (a seconda dei casi) 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 dalle seguenti:

    - 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 Partner ai fini della sicurezza. Il Partner è responsabile della sicurezza dell'ambiente, dei database e della configurazione di Looker (original) del Partner, a esclusione dei 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 data center di Looker (original) sarà descritta nel Modulo d'ordine applicabile o altrimenti identificata da Google.

6. Nessuna certificazione da parte di Partner non appartenenti all'area EMEA. Il Partner non è tenuto a certificare o identificare la propria Autorità di controllo competente, come descritto nella Sezione 4.2 (Certificazione da parte di Partner 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 a Trasferimenti limitati, Controlli aggiuntivi per la sicurezza e altre misure protettive supplementari 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; and

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 per multi-cloud*. L'Emendamento sul trattamento dei dati per Servizi 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 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 sulla privacy applicabile richieda a Google di raccogliere e conservare i registri di determinate informazioni relative al Partner o ai suoi Clienti, il Partner 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 Partner 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 Partner controllano l'accesso alle applicazioni da parte del personale di Google per fornire assistenza tecnica come richiesto dal Partner o dagli Utenti finali del Partner.

Servizi SecOps

1. Definizioni aggiuntive.

- Per "*Account*", se non definito nel Contratto, si intende l'account dei Servizi SecOps o della piattaforma Google Cloud del Partner, a seconda dei casi.
- Per "*Servizi SecOps*" si intendono Chronicle SIEM, Chronicle SOAR e le soluzioni Mandiant, ciascuna descritta all'indirizzo https://cloud.google.com/terms/secops/services, a esclusione delle Offerte di terze parti. A scanso di dubbi, i Servizi SecOps escludono Mandiant Managed Services e Mandiant Consulting Services.
- 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 o nel software SecOps e (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 dalla seguente:
    - Per *"Controlli aggiuntivi per la sicurezza"* si intendono risorse, caratteristiche, funzionalità e/o controlli di sicurezza (se presenti) che il Partner può utilizzare a propria scelta e/o discrezione, tra cui (se presenti) la crittografia, il logging e il monitoraggio, la gestione di identità e accessi e l'analisi della sicurezza.
- La definizione di "Servizi controllati" viene sostituita con la seguente:
    - Per "*Servizi controllati*" si intendono i Servizi SecOps al momento indicati come compresi 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.
- 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 dalle seguenti:
    - Per "*SCC (da titolare a responsabile)*" si 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

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

- 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 almeno le certificazioni e i report 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 "Report SOC").

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

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 Partner non appartenenti all'area EMEA. Il Partner non è tenuto a certificare o identificare la propria Autorità di controllo competente, come descritto nella Sezione 4.2 (Certificazione da parte di Partner 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 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 vigente sulla privacy richieda a Google di raccogliere e conservare i registri di determinate informazioni relative al Partner, il Partner 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 Partner di fornire e aggiornare queste informazioni secondo un'altra modalità.

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

30 giugno 2022 24 settembre 2021 20 agosto 2020 10 agosto 2020 17 luglio 2020 1 ottobre 2019 28 febbraio 2019 25 maggio 2018 13 marzo 2018

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

6 febbraio 2023 31 ottobre 2022 27 settembre 2021

Versioni precedenti *(ultima modifica: 30 ottobre 2024)*

15 ottobre 2024 26 settembre 2024 9 settembre 2024 9 aprile 2024 8 novembre 2023 15 agosto 2023 20 settembre 2022