Ministero dell'Istruzione e del Merito
**ISTITUTO COMPRENSIVO STATALE DI MOLTENO**
Piazza don Biffi, 1 – 23847 Molteno ( LC)
Tel. 031 850358 - C.F. 92058790137
e-mail uffici: lcic822006@istruzione.it – lcic822006@pec.istruzione.it
sito web: www.icsmolteno.edu.it

# Addendum sull'elaborazione dei dati nel cloud (clienti)

Il presente Addendum sull'elaborazione dei dati nel cloud (inclusi i relativi allegati, l'" *Addendum* ") è incorporato nel/nei Contratto/i (come definito/i di seguito) tra Google e il Cliente. Il presente Addendum era precedentemente noto come "Termini di elaborazione e sicurezza dei dati" nell'ambito di un Contratto per Google Cloud Platform, Looker (originale), Google SecOps Services o Google Skills for Organizations; "Emendamento sull'elaborazione dei dati" nell'ambito di un Contratto per Google Workspace o Cloud Identity; e "Addendum sull'elaborazione dei dati" nell'ambito di un Contratto per i Servizi di consulenza e i Servizi gestiti di Mandiant.

# *Termini generali*

## 1. Panoramica

Il presente Addendum descrive gli obblighi 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 Cliente (come definiti di seguito). Il presente Addendum entrerà in vigore alla Data di Entrata in Vigore dell'Addendum (come definita di seguito) e sostituirà qualsiasi termine precedentemente applicabile al trattamento e alla sicurezza dei Dati del Cliente. I termini in maiuscolo utilizzati ma non definiti nel presente Addendum hanno il significato loro attribuito nel Contratto.

## 2. Definizioni

2.1 Nel presente Addendum:

- Per " *Data di entrata in vigore dell'Addendum* " si intende la data in cui il Cliente ha accettato, o le parti hanno altrimenti concordato, il presente Addendum.
- Per " *Controlli di sicurezza aggiuntivi* " si intendono le risorse, le funzionalità e i controlli di sicurezza che il Cliente può utilizzare a sua discrezione e secondo le proprie esigenze, tra cui la Console di amministrazione, la crittografia, la registrazione e il monitoraggio, la gestione delle identità e degli accessi, la scansione di sicurezza e i firewall.
- Per " *Accordo* " 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, ove applicabile al trattamento dei Dati personali del Cliente, 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. A titolo di chiarezza, le Leggi sulla privacy applicabili includono, a titolo esemplificativo ma non esaustivo, le leggi menzionate nell'Appendice 3 (Leggi specifiche sulla privacy).
- Per " *Servizi sottoposti ad audit* " si intendono i Servizi attualmente in vigore indicati come rientranti nell'ambito della relativa certificazione o del relativo report all'indirizzo https://cloud.google.com/security/compliance/services-in-scope . Google non può rimuovere alcun Servizio da questo URL a meno che non sia stato interrotto in conformità con l'Accordo applicabile.
- " *Certificazioni di conformità* " ha il significato attribuito nella Sezione 7.4 (Certificazioni di conformità e report SOC).

- “ *Dati del Cliente* ”, se non definiti nel Contratto, hanno il significato loro attribuito nell’Allegato 4 (Prodotti Specifici).
- Per “ *Dati personali del cliente* ” si intendono i dati personali contenuti nei Dati del cliente, comprese le categorie particolari di dati personali o i dati sensibili definiti dalla normativa applicabile in materia di privacy.
- Per " *Incidente dei dati* " si intende una violazione della sicurezza di Google che comporti la distruzione, la perdita, l'alterazione, la divulgazione non autorizzata o l'accesso non autorizzato, accidentali o illeciti, ai Dati del Cliente sui sistemi gestiti o comunque controllati da Google.
- “ *EMEA* ” significa Europa, Medio Oriente e Africa.
- “ *GDPR UE* ” indica il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE.
- « *Legge europea sulla protezione dei dati* » significa, a seconda dei casi: (a) il GDPR; o (b) la Legge federale sulla protezione dei dati svizzera.
- Per “ *Legge europea* ” si intende, a seconda dei casi: (a) la legge dell’UE o dello Stato membro dell’UE (se il GDPR dell’UE si applica al trattamento dei Dati personali del Cliente); (b) la legge del Regno Unito o di una parte del Regno Unito (se il GDPR del Regno Unito si applica al trattamento dei Dati personali del Cliente); o (c) la legge della Svizzera (se la LPDA svizzera si applica al trattamento dei Dati personali del Cliente).
- “ *GDPR* ” significa, a seconda dei casi: (a) il GDPR dell’UE; o (b) il GDPR del Regno Unito.
- Per " *Revisore dei Conti di Google* " si intende un revisore dei conti terzo, qualificato e indipendente, nominato da Google, la cui identità, al momento della verifica, Google comunicherà al Cliente.
- “ *Istruzioni* ” ha il significato indicato nella Sezione 5.2 (Conformità alle Istruzioni del Cliente).
- Per " *Indirizzo e-mail di notifica* " si intende l'indirizzo o gli indirizzi e-mail indicati dal Cliente nella Console di amministrazione o nel Modulo d'ordine per ricevere determinate notifiche da Google.
- Per “ *Documentazione di sicurezza* ” si intendono le Certificazioni di conformità e i Report SOC.

- Per “ *Misure di sicurezza* ” si intende quanto definito nella Sezione 7.1.1 (Misure di sicurezza di Google).
- Per “ *Servizi* ” si intendono i servizi applicabili descritti nell’Appendice 4 (Prodotti specifici).
- “ *Report SOC* ” ha il significato attribuito nella Sezione 7.4 (Certificazioni di conformità e report SOC).
- Per “ *Sub-responsabile del trattamento* ” si intende una terza parte autorizzata come ulteriore responsabile del trattamento ai sensi del presente Addendum a trattare i Dati del Cliente al fine di fornire parti dei Servizi e del TSS (ove applicabile).
- « *Autorità di controllo* » significa, a seconda dei casi: (a) un'«autorità di controllo» come definita nel GDPR dell'UE; o (b) il «Commissario» come definito nel GDPR del Regno Unito o nella legge svizzera sulla protezione dei dati personali (FADP).
- Per “ Legge *federale svizzera* sulla protezione dei dati” si intende, a seconda dei casi, la Legge federale sulla protezione dei dati del 19 giugno 1992 (Svizzera) (con l’ordinanza di adeguamento della Legge federale sulla protezione dei dati del 14 giugno 1993) o la Legge federale sulla protezione dei dati rivista del 25 settembre 2020 (Svizzera) (con l’ordinanza di adeguamento della Legge federale sulla protezione dei dati del 31 agosto 2022).
- Per “ *Durata* ” si intende il periodo che intercorre tra la Data di entrata in vigore dell’Addendum e la fine della fornitura dei Servizi da parte di Google, inclusi, se del caso, eventuali periodi durante i quali la fornitura dei Servizi potrebbe essere sospesa e qualsiasi periodo successivo alla cessazione durante il quale Google potrebbe continuare a fornire i Servizi a fini transitori.
- Per " *GDPR del Regno Unito* " si intende il GDPR dell'UE, come modificato e incorporato nella legislazione del Regno Unito ai sensi dell'UK European Union (Withdrawal) Act 2018, e della relativa legislazione secondaria emanata in virtù di tale legge.

2.2 I termini “dati personali”, “interessato”, “trattamento”, “titolare del trattamento” e “responsabile del trattamento”, come utilizzati nel presente Addendum, hanno il significato attribuito dalla Legge applicabile in materia di privacy o, in mancanza di tale significato o legge, dal GDPR dell'UE.

2.3 I termini “interessato”, “titolare del trattamento” e “responsabile del trattamento” includono rispettivamente “consumatore”, “impresa” e “fornitore di servizi”, come richiesto dalla normativa applicabile in materia di privacy.

**3. Durata**

Indipendentemente dal fatto che l'Accordo applicabile sia stato risolto o sia scaduto, il presente Addendum rimarrà in vigore fino a quando Google non eliminerà tutti i Dati del Cliente come descritto nel presente Addendum e scadrà automaticamente quando ciò avverrà.

**4. Ruoli; Conformità legale**

4.1 *Ruoli delle parti.* Google agisce in qualità di responsabile del trattamento e il Cliente agisce in qualità di titolare o responsabile del trattamento, a seconda dei casi, dei Dati personali del Cliente.

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

4.3 *Conformità alla legge.* Ciascuna parte si impegna a rispettare i propri obblighi relativi al trattamento dei Dati Personali del Cliente ai sensi della Legge sulla Privacy applicabile.

4.4 *Disposizioni legali aggiuntive* . Nella misura in cui il trattamento dei Dati personali del Cliente sia soggetto a una Legge sulla privacy applicabile descritta nell'Appendice 3 (Leggi specifiche sulla privacy), le corrispondenti disposizioni dell'Appendice 3 si applicheranno in aggiunta alle presenti Condizioni generali e prevarranno come descritto nella Sezione 14.1 (Precedenza).

**5. Elaborazione dei dati**

5.1 *Clienti che fungono da elaboratori di dati* . Se il cliente è un elaboratore di dati:

a. Il cliente garantisce in modo continuativo che il titolare del trattamento terzo competente ha autorizzato:

i. le Istruzioni;

ii. Il coinvolgimento del cliente di Google come ulteriore responsabile del trattamento; e.

iii. L'impiego da parte di Google di sub-responsabili del trattamento come descritto nella Sezione 11 (Sub-responsabili del trattamento);

b. Il Cliente inoltrerà tempestivamente e senza indebito ritardo al titolare del trattamento terzo qualsiasi comunicazione fornita da Google ai sensi della Sezione 7.2.1 (Notifica dell'incidente), 9.2.1 (Responsabilità per le richieste) o 11.4 (Opportunità di opposizione ai subappaltatori); e

c. Il Cliente può mettere a disposizione del titolare del trattamento terzo qualsiasi altra informazione resa disponibile da Google ai sensi del presente Addendum in merito all'ubicazione dei data center di Google o ai nomi, all'ubicazione e alle attività dei subappaltatori.

5.2 *Conformità alle istruzioni del Cliente* . Il Cliente incarica Google di elaborare i Dati del Cliente in conformità con l'Accordo applicabile (incluso il presente Addendum) esclusivamente come segue:

a. fornire, proteggere e monitorare i Servizi e il TSS (ove applicabile); e

b. come ulteriormente specificato tramite:

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

ii. qualsiasi altra istruzione scritta fornita dal Cliente e riconosciuta da Google come parte integrante delle istruzioni previste dal presente Addendum

(collettivamente, le " *Istruzioni* ").

Google si conformerà alle Istruzioni, salvo ove proibito dalla legge europea, laddove si applichi la normativa europea sulla protezione dei dati, o dalla legge applicabile, laddove si applichi qualsiasi altra legge applicabile in materia di privacy.

**6. Eliminazione dei dati**

6.1 *Cancellazione da parte del Cliente* . Google consentirà al Cliente di cancellare i Dati del Cliente durante il Periodo di validità del Contratto in modo coerente con le funzionalità dei Servizi. Se il Cliente utilizza i Servizi per cancellare i Dati del Cliente durante il Periodo di validità del Contratto e tali Dati del Cliente non possono essere recuperati dal Cliente, tale utilizzo costituirà un'Istruzione a Google per la cancellazione dei relativi Dati del Cliente dai sistemi di Google. Google si conformerà a tale Istruzione non appena ragionevolmente possibile e comunque 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 la legge applicabile non imponga la conservazione, laddove si applichi qualsiasi altra Legge applicabile sulla privacy.

6.2 *Restituzione o cancellazione al termine del Contratto* . Se il Cliente desidera conservare i Dati del Cliente dopo la scadenza del Contratto, può richiedere a Google, in conformità con la Sezione 9.1 (Accesso; Rettifica; Trattamento limitato; Portabilità), la restituzione di tali dati durante il Contratto. Fatto salvo quanto

previsto dalla Sezione 6.3 (Istruzioni per la cancellazione differita), il Cliente richiede a Google di cancellare tutti i Dati del Cliente rimanenti (incluse le copie esistenti) dai sistemi di Google al termine del Contratto. Dopo un periodo di recupero fino a 30 giorni da tale data, Google si conformerà a tale Istruzione non appena ragionevolmente possibile e comunque 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 la legge applicabile non imponga la conservazione, laddove si applichi qualsiasi altra Legge applicabile sulla privacy.

6.3. *Istruzioni di cancellazione differita* . Nella misura in cui i Dati del Cliente coperti dalle istruzioni di cancellazione descritte nella Sezione 6.2 (Restituzione o cancellazione alla scadenza del termine) vengano elaborati anche, alla scadenza del termine applicabile ai sensi della Sezione 6.2, in relazione a un Contratto con un termine continuativo, tali istruzioni di cancellazione avranno effetto rispetto a tali Dati del Cliente solo alla scadenza del termine continuativo. Per chiarezza, il presente Addendum continuerà ad applicarsi a tali Dati del Cliente fino alla loro cancellazione da parte di Google.

**7. Sicurezza dei dati**

7.1 *Misure di sicurezza, controlli e assistenza di Google* .

7.1.1 *Misure di sicurezza di Google* . Google implementerà e manterrà misure tecniche, organizzative e fisiche per proteggere i Dati del Cliente da distruzione, perdita, alterazione, divulgazione o accesso non autorizzati, accidentali o illeciti, come descritto nell'Appendice 2 (Misure di sicurezza) **(** le **" *Misure di sicurezza* ")** . Le Misure di sicurezza includono misure per crittografare i Dati del Cliente; per contribuire a garantire la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi di Google; per contribuire a ripristinare tempestivamente l'accesso ai Dati del Cliente a seguito di un incidente; e per testare regolarmente l'efficacia. Google può aggiornare le Misure di sicurezza di volta in volta, a condizione che tali aggiornamenti non comportino una riduzione sostanziale della sicurezza dei Servizi.

7.1.2 *Accesso e conformità* . Google si impegna a:

a. autorizzare i propri dipendenti, appaltatori e subappaltatori ad accedere ai Dati del Cliente solo nella misura strettamente necessaria per conformarsi alle Istruzioni;

b. adottare misure appropriate per garantire la conformità alle Misure di sicurezza da parte dei propri dipendenti, appaltatori e subappaltatori nella misura in cui ciò sia applicabile al loro ambito di prestazione; e

c. garantire che tutte le persone autorizzate a trattare i Dati del Cliente siano soggette a un obbligo di riservatezza.

7.1.3 *Controlli di sicurezza aggiuntivi* . Google renderà disponibili controlli di sicurezza aggiuntivi per:

a. consentire al Cliente di adottare misure per proteggere i Dati del Cliente; e

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

7.1.4 *Assistenza di Google in materia di sicurezza* . Google (tenendo conto della natura del trattamento dei Dati Personali del Cliente e delle informazioni a disposizione di Google) assisterà il Cliente nel garantire il rispetto dei propri obblighi (o, qualora il Cliente sia un responsabile del trattamento, degli obblighi del titolare del trattamento terzo) in materia di sicurezza e violazioni dei dati personali ai sensi della normativa applicabile in materia di privacy, mediante:

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

b. rendere disponibili controlli di sicurezza aggiuntivi conformemente alla Sezione 7.1.3 (Controlli di sicurezza aggiuntivi);

c. rispettare le disposizioni della Sezione 7.2 (Incidenti relativi ai dati);

d. rendere disponibile la Documentazione di Sicurezza in conformità alla Sezione 7.5.1 (Revisioni della Documentazione di Sicurezza) e fornire le informazioni contenute nell'Accordo applicabile (incluso il presente Addendum); e

e. se i paragrafi (a)-(d) di cui sopra non sono sufficienti affinché il Cliente (o il titolare del trattamento terzo) possa adempiere a tali obblighi, su richiesta del Cliente, fornendogli ulteriore ragionevole cooperazione e assistenza.

7.2 *Incidenti relativi ai dati* .

7.2.1 *Notifica degli incidenti* . Google informerà il Cliente tempestivamente e senza indebito ritardo dopo essere venuta a conoscenza di un incidente relativo ai dati e adotterà prontamente misure ragionevoli per ridurre al minimo i danni e proteggere i dati del Cliente.

7.2.2 *Dettagli dell'incidente relativo ai dati* . La notifica di Google relativa a un incidente relativo ai dati descriverà: la natura dell'incidente, comprese le risorse del Cliente interessate; le misure che Google ha adottato o prevede di adottare per affrontare l'incidente relativo ai dati e mitigarne il potenziale rischio; le misure, se del caso, che Google raccomanda al Cliente di adottare per affrontare l'incidente relativo ai dati; e i dettagli di un punto di contatto presso il quale è possibile ottenere ulteriori informazioni. Qualora non sia possibile fornire tutte queste informazioni contemporaneamente, la notifica iniziale di Google conterrà le informazioni disponibili al momento e ulteriori informazioni saranno fornite senza indebito ritardo non appena disponibili.

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

7.2.4 *Nessun riconoscimento di colpa da parte di Google* . La notifica o la risposta di Google a un Incidente relativo ai Dati ai sensi della presente Sezione 7.2 (Incidenti relativi ai Dati) non sarà interpretata come un riconoscimento da parte di Google di alcuna colpa o responsabilità in relazione all'Incidente relativo ai Dati.

7.3 *Responsabilità e valutazione della sicurezza del cliente* .

7.3.1 *Responsabilità del Cliente in materia di sicurezza* . Fermo restando quanto previsto dagli obblighi di Google ai sensi delle Sezioni 7.1 (Misure di sicurezza, controlli e assistenza di Google) e 7.2 (Incidenti relativi ai dati), e altrove nel Contratto applicabile, il Cliente è responsabile del proprio utilizzo dei Servizi e della conservazione di qualsiasi copia dei Dati del Cliente al di fuori dei sistemi di Google o dei Subappaltatori di Google, inclusi:

a. utilizzare i Servizi e i Controlli di Sicurezza Aggiuntivi per garantire un livello di sicurezza adeguato al rischio per i Dati del Cliente;

b. proteggere le credenziali di autenticazione dell'account, i sistemi e i dispositivi che il Cliente utilizza per accedere ai Servizi; e

c. eseguire il backup o conservare copie dei Dati del Cliente, a seconda dei casi.

7.3.2 *Valutazione della sicurezza da parte del Cliente* . Il Cliente accetta che i Servizi, le Misure di sicurezza, i Controlli di sicurezza aggiuntivi e gli impegni di Google ai sensi della presente Sezione 7 (Sicurezza dei dati) forniscano un livello di sicurezza adeguato al rischio per i Dati del Cliente (tenendo conto dello stato dell'arte, dei costi di implementazione e della natura, della portata, del contesto e

delle finalità del trattamento dei Dati del Cliente, nonché dei rischi per le persone fisiche).

7.4 *Certificazioni di conformità e report SOC* . Google manterrà almeno i seguenti elementi per i Servizi sottoposti ad audit al fine di verificare la continua efficacia delle Misure di sicurezza:

a. certificati per ISO 27001 e qualsiasi certificazione aggiuntiva descritta nell'Appendice 4 (Prodotti specifici) (le " *Certificazioni di conformità* "); e

b. Report SOC 2 e SOC 3 prodotti dal revisore esterno di Google e aggiornati annualmente sulla base di una verifica effettuata almeno una volta ogni 12 mesi (i " *Report SOC* ").

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

7.5 *Revisioni e verifiche di conformità* .

7.5.1 *Revisione della documentazione di sicurezza* . Per dimostrare la conformità di Google ai propri obblighi ai sensi del presente Addendum, Google renderà disponibile la documentazione di sicurezza per la revisione da parte del Cliente e, se il Cliente è un responsabile del trattamento, consentirà al Cliente di richiedere l'accesso ai report SOC per il titolare del trattamento terzo in conformità con la Sezione 7.5.3 (Termini commerciali aggiuntivi per revisioni e audit).

7.5.2 *Diritti di verifica 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 audit (incluse ispezioni) per verificare la conformità di Google ai propri obblighi ai sensi del presente Addendum in conformità con la Sezione 7.5.3 (Termini Commerciali Aggiuntivi per Revisioni e Audit). Durante un audit, Google collaborerà ragionevolmente con il Cliente o il suo revisore come descritto nella presente Sezione 7.5 (Revisioni e Audit di Conformità).

b. *Revisione indipendente da parte del cliente* . Il cliente può condurre un audit per verificare la conformità di Google ai propri obblighi ai sensi del presente Addendum esaminando la Documentazione sulla sicurezza (che riflette l'esito degli audit condotti dal revisore esterno di Google).

7.5.3 *Termini commerciali aggiuntivi per revisioni e audit* .

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

i. accesso ai report SOC per un controller di terze parti ai sensi della Sezione 7.5.1 (Revisioni della documentazione di sicurezza); o

ii. una verifica ai sensi della Sezione 7.5.2(a) (Verifica del cliente).

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

i. controlli di sicurezza e riservatezza applicabili a qualsiasi accesso ai Report SOC da parte di un soggetto terzo ai sensi della Sezione 7.5.1 (Revisioni della documentazione di sicurezza); e

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

c. Google può addebitare una commissione (in base ai costi ragionevoli di Google) per qualsiasi verifica ai sensi della Sezione 7.5.2(a) (Verifica del Cliente). Google fornirà al Cliente ulteriori dettagli su qualsiasi commissione applicabile e sulla base del suo calcolo, prima di qualsiasi verifica di questo tipo. Il Cliente sarà responsabile di tutte le commissioni addebitate da qualsiasi revisore nominato dal Cliente per eseguire tale verifica.

d. Google può opporsi per iscritto alla nomina di un revisore contabile da parte del Cliente per condurre qualsiasi revisione contabile ai sensi della Sezione 7.5.2(a) (Revisione contabile del Cliente) qualora, a ragionevole giudizio di Google, il revisore non sia adeguatamente qualificato o indipendente, sia un concorrente di Google o sia altrimenti manifestamente inadatto. Qualsiasi obiezione di questo tipo da parte di Google richiederà al Cliente di nominare un altro revisore contabile o di condurre la revisione contabile autonomamente.

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

**8. Valutazioni d'impatto e consultazioni**

Google (tenendo conto della natura del trattamento e delle informazioni a disposizione di Google) assisterà il Cliente nel garantire la conformità ai propri

obblighi (o, qualora il Cliente sia un responsabile del trattamento, a quelli del titolare del trattamento terzo) relativi alle valutazioni della protezione dei dati, alle valutazioni del rischio, alle consultazioni preventive con le autorità di controllo o a procedure equivalenti ai sensi della normativa applicabile in materia di privacy, mediante:

a. rendere disponibili i controlli di sicurezza aggiuntivi in conformità alla Sezione 7.1.3 (Controlli di sicurezza aggiuntivi) e la documentazione di sicurezza in conformità alla Sezione 7.5.1 (Revisioni della documentazione di sicurezza);

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

c. qualora i paragrafi (a) e (b) di cui sopra non siano sufficienti affinché il Cliente (o il titolare del trattamento terzo) possa adempiere a tali obblighi, su richiesta del Cliente, fornire al Cliente ulteriore ragionevole cooperazione e assistenza.

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

9.1 *Accesso; Rettifica; Limitazione del trattamento; Portabilità* . Durante il Periodo di validità del Contratto, Google consentirà al Cliente, in modo coerente con le funzionalità dei Servizi, di accedere, rettificare e limitare il trattamento dei Dati del Cliente, anche tramite la funzionalità di cancellazione fornita da Google come descritto nella Sezione 6.1 (Cancellazione da parte del Cliente), e di esportare i Dati del Cliente. Qualora il Cliente venga a conoscenza del fatto che i Dati personali del Cliente siano inesatti o obsoleti, sarà sua responsabilità utilizzare tale funzionalità per rettificare o cancellare tali dati, se richiesto dalla Legge sulla privacy applicabile.

9.2 *Richieste degli interessati* .

9.2.1 *Responsabilità per le richieste* . Durante il Periodo di validità, se il team di protezione dei dati di Google Cloud riceve una richiesta da un interessato relativa ai dati personali del Cliente e che identifica il Cliente, Google:

a. consigliare all'interessato di inoltrare la propria richiesta al Cliente;

b. avvisare tempestivamente il Cliente; e

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

Il cliente sarà responsabile di rispondere a qualsiasi richiesta di questo tipo, anche, ove necessario, utilizzando le funzionalità dei Servizi.

9.2.2 *Assistenza di Google alle richieste degli interessati* . Google (tenendo conto della natura del trattamento dei Dati personali del Cliente) assisterà il Cliente nell'adempimento dei propri obblighi (o, qualora il Cliente sia un responsabile del trattamento, degli obblighi del titolare del trattamento terzo) ai sensi della normativa applicabile in materia di privacy per rispondere alle richieste di esercizio dei diritti dell'interessato mediante:

a. rendere disponibili controlli di sicurezza aggiuntivi conformemente alla Sezione 7.1.3 (Controlli di sicurezza aggiuntivi);

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

c. qualora i paragrafi (a) e (b) di cui sopra non siano sufficienti affinché il Cliente (o il titolare del trattamento terzo) possa adempiere a tali obblighi, su richiesta del Cliente, fornire al Cliente ulteriore ragionevole cooperazione e assistenza.

**10. Luoghi di elaborazione dei dati**

10.1 *Strutture di archiviazione ed elaborazione dei dati.* Fatti salvi gli impegni di Google in materia di localizzazione dei dati previsti dai Termini specifici del servizio e gli impegni in materia di trasferimento dei dati previsti dall'Appendice 3 (Leggi specifiche sulla privacy), ove applicabili, i Dati del Cliente possono essere elaborati in qualsiasi Paese in cui Google o i suoi subappaltatori dispongano di strutture.

10.2 *Informazioni sui data center* . L'ubicazione dei data center di Google è descritta nell'Appendice 4 (Prodotti specifici).

**11. Sottoprocessori**

11.1 *Consenso all'incarico di sub-responsabili del trattamento* . Il Cliente autorizza espressamente Google ad avvalersi, in qualità di sub-responsabili del trattamento, delle entità indicate nella Sezione 11.2 (Informazioni sui sub-responsabili del trattamento) a partire dalla Data di entrata in vigore dell'Addendum. Inoltre, fatto salvo quanto previsto dalla Sezione 11.4 (Possibilità di opporsi ai sub-responsabili del trattamento), il Cliente autorizza in generale Google ad avvalersi di altre terze parti in qualità di sub-responsabili del trattamento (" *Nuovi sub-responsabili del trattamento* ").

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

11.3 *Requisiti per l'ingaggio di un sub-responsabile del trattamento* . Quando si incarica un sub-responsabile del trattamento, Google dovrà:

a. garantire tramite un contratto scritto che:

i. il Sub-responsabile del trattamento accede e utilizza i Dati del Cliente solo nella misura necessaria per adempiere agli obblighi subappaltati e lo fa in conformità con l'Accordo applicabile (incluso il presente Addendum); e

ii. se richiesto dalle Leggi sulla Privacy Applicabili, gli obblighi di protezione dei dati descritti nel presente Addendum sono imposti al Sub-responsabile del trattamento (come ulteriormente descritto nell'Appendice 3 (Leggi sulla Privacy Specifiche)); e

b. rimanere pienamente responsabile per tutti gli obblighi subappaltati al Subappaltatore e per tutti gli atti e le omissioni del Subappaltatore.

11.4 *Possibilità di opporsi ai subprocessori* .

a. Qualora Google si avvalga di un Nuovo Sub-responsabile del trattamento durante il Periodo di validità del Contratto, Google informerà il Cliente di tale incarico almeno 30 giorni prima che il Nuovo Sub-responsabile del trattamento inizi a elaborare i Dati del Cliente (indicando nome, sede e attività del Nuovo Sub-responsabile del trattamento).

b. Il Cliente può, entro 90 giorni dalla notifica dell'incarico di un Nuovo Sub-responsabile del trattamento, opporsi risolvendo immediatamente il Contratto applicabile per convenienza:

i. in conformità con la clausola di risoluzione per convenienza di tale Accordo; o

ii. se non esiste tale disposizione, notificandolo a Google.

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

12.1 *Team di protezione dei dati nel cloud* . Il team di protezione dei dati nel cloud di Google fornirà assistenza tempestiva e ragionevole per qualsiasi domanda del Cliente relativa al trattamento dei Dati del Cliente ai sensi del Contratto applicabile e può essere contattato secondo le modalità descritte nella sezione Avvisi del Contratto applicabile o nell'Appendice 4 (Prodotti specifici).

12.2 *Registri di trattamento di Google* . Google manterrà la documentazione appropriata delle proprie attività di trattamento come richiesto dalla Legge sulla privacy applicabile. Nella misura in cui la Legge sulla privacy applicabile richieda a Google di raccogliere e conservare registri di determinate informazioni relative al

Cliente, quest'ultimo utilizzerà la Console di amministrazione o altri mezzi indicati nell'Appendice 4 (Prodotti specifici) per fornire tali informazioni e mantenerle accurate e aggiornate. Google potrà rendere disponibili tali informazioni alle autorità di controllo competenti, inclusa un'Autorità di vigilanza, se richiesto dalla Legge sulla privacy applicabile.

12.3 *Richieste del Titolare del trattamento* . Durante il Periodo di validità, se il team di protezione dei dati di Google Cloud riceve una richiesta o un'istruzione da una terza parte che si dichiara titolare del trattamento dei Dati personali del Cliente, Google consiglierà a tale terza parte di contattare il Cliente.

**13. Avvisi**

Le comunicazioni previste dal presente Addendum (incluse le notifiche relative a eventuali Incidenti di Dati) saranno inviate all'indirizzo e-mail di notifica. Il Cliente è responsabile di utilizzare la Console di Amministrazione, o di informare Google in altro modo, per garantire che il proprio indirizzo e-mail di notifica rimanga aggiornato e valido.

**14. Interpretazione**

14.1 *Precedenza* . Nella misura in cui sussista un conflitto tra:

a. Appendice 3 (Leggi specifiche sulla privacy) e il resto dell'Addendum (inclusa l'Appendice 4 (Prodotti specifici)), l'Appendice 3 prevarrà; e

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

c. In caso di violazione del presente Addendum e del resto dell'Accordo, il presente Addendum prevarrà.

Per maggiore chiarezza, qualora il Cliente disponga di più di un Contratto, il presente Addendum modificherà ciascuno di essi separatamente.

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

## *Appendice 1: Oggetto e dettagli del trattamento dei dati*

*Argomento*

Fornitura da parte di Google dei Servizi e del TSS (ove applicabile) al Cliente.

*Durata dell'elaborazione*

Il Termine più il periodo che va dalla fine del Termine fino alla cancellazione di tutti i Dati del Cliente da parte di Google in conformità con il presente Addendum.

*Natura e finalità del trattamento*

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

*Categorie di dati*

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

*Interessati ai dati*

Per interessati si intendono le persone fisiche i cui dati vengono forniti a Google tramite i Servizi dal Cliente o dai suoi Utenti finali (o su sua indicazione).

## *Appendice 2: Misure di sicurezza*

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

**1. Sicurezza del data center e della rete**

*(a) Centri dati.*

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

*Ridondanza* . I sistemi infrastrutturali sono stati progettati per eliminare i singoli punti di guasto e ridurre al minimo l'impatto dei rischi ambientali previsti. Circuiti, switch, reti o altri dispositivi necessari doppi contribuiscono a fornire questa ridondanza. I Servizi sono progettati per consentire a Google di eseguire determinati tipi di manutenzione preventiva e correttiva senza interruzioni. Tutte le apparecchiature e le strutture ambientali dispongono di procedure di manutenzione preventiva documentate che descrivono in dettaglio il processo e la frequenza di esecuzione in conformità con le specifiche del produttore o interne. La manutenzione preventiva e correttiva delle apparecchiature del data center è programmata tramite un processo di cambio standard secondo procedure documentate.

*Alimentazione* . I sistemi di alimentazione elettrica dei data center sono progettati per essere ridondanti e manutenibili senza interruzioni operative, 24 ore su 24, 7 giorni su 7. Nella maggior parte dei casi, per i componenti critici dell'infrastruttura del data center sono previste sia una fonte di alimentazione primaria che una alternativa, entrambe con pari capacità. L'alimentazione di backup è fornita da diversi meccanismi, come le batterie degli UPS (gruppi di continuità), che

garantiscono una protezione affidabile durante cali di tensione, blackout, sovratensioni, sottotensioni e condizioni di frequenza fuori tolleranza. In caso di interruzione dell'alimentazione di rete, l'alimentazione di backup è progettata per fornire energia transitoria al data center, a piena capacità, per un massimo di 10 minuti, fino all'attivazione dei generatori di backup. Questi ultimi sono in grado di avviarsi automaticamente in pochi secondi per fornire energia elettrica di emergenza sufficiente a far funzionare il data center a piena capacità, in genere per 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 proprietari per rafforzare la sicurezza e la ridondanza dei dati.

*Qualità del codice* . Google adotta un processo di revisione del codice per aumentare la sicurezza del codice utilizzato per fornire i Servizi e per migliorare i prodotti di sicurezza negli ambienti di produzione.

*Continuità aziendale* . Google ha progettato e pianifica e testa regolarmente i propri programmi di continuità aziendale/recupero in caso di disastro.

( *b) Reti e trasmissione.*

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

*Superficie di attacco esterna* . Google utilizza più livelli di dispositivi di rete e sistemi di rilevamento delle intrusioni per proteggere la propria superficie di attacco esterna. Google valuta i potenziali vettori di attacco e integra tecnologie specifiche e appropriate nei sistemi rivolti verso l'esterno.

*Rilevamento delle intrusioni* . Il rilevamento delle intrusioni ha lo scopo di fornire informazioni sulle attività di attacco in corso e di fornire dati adeguati per rispondere agli incidenti. Il sistema di rilevamento delle intrusioni di Google prevede: (i) un controllo rigoroso delle dimensioni e della composizione della superficie di attacco di Google attraverso misure preventive; (ii) l'impiego di controlli di rilevamento intelligenti nei punti di ingresso dei dati; e (iii) l'impiego di tecnologie che risolvono automaticamente determinate situazioni pericolose.

*Risposta agli incidenti* . Google monitora diversi canali di comunicazione per individuare eventuali incidenti di sicurezza e il personale addetto alla sicurezza di Google interviene tempestivamente in caso di incidenti noti.

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

**2. Controllo degli accessi e del sito**

*(a) Controlli del sito.*

*Servizio di sicurezza in loco per i data center* . I data center di Google dispongono di un servizio di sicurezza in loco responsabile di tutte le funzioni di sicurezza fisica del data center, 24 ore su 24, 7 giorni su 7. Il personale addetto alla sicurezza in loco monitora le telecamere a circuito chiuso (CCTV) e tutti i sistemi di allarme. Il personale addetto alla sicurezza in loco effettua regolarmente pattugliamenti interni ed esterni del data center.

*Procedure di accesso ai data center* . Google adotta procedure di accesso formali per consentire l'accesso fisico ai data center. I data center sono ospitati in strutture che richiedono l'accesso tramite badge elettronico, con allarmi collegati al sistema di sicurezza in loco. Tutti coloro che accedono al data center sono tenuti a identificarsi e a mostrare un documento d'identità al personale di sicurezza in loco. Solo i dipendenti, i collaboratori e i visitatori autorizzati possono accedere ai data center. Solo i dipendenti e i collaboratori autorizzati possono richiedere l'accesso tramite badge elettronico a queste strutture. Le richieste di accesso tramite badge elettronico ai data center devono essere inviate via e-mail e richiedono l'approvazione del responsabile del richiedente e del direttore del data center. Tutti gli altri utenti che necessitano di un accesso temporaneo al data center devono: (i) ottenere l'approvazione preventiva dai responsabili del data center per il data center specifico e le aree interne che desiderano visitare; (ii) registrarsi presso il personale di sicurezza in loco; e (iii) fare riferimento a un registro di accesso al data center approvato che identifichi la persona come autorizzata.

*Dispositivi di sicurezza in loco per i data center* . I data center di Google utilizzano un sistema di controllo accessi a doppia autenticazione collegato a un sistema di allarme. Il sistema di controllo accessi monitora e registra la chiave elettronica di ciascun individuo e i suoi accessi alle porte perimetrali, alle aree di carico e scarico

merci e ad altre aree critiche. Le attività non autorizzate e i tentativi di accesso non riusciti vengono registrati dal sistema di controllo accessi e, se necessario, oggetto di indagine. L'accesso autorizzato alle attività aziendali e ai data center è limitato in base alle zone e alle mansioni individuali. Le porte tagliafuoco dei data center sono dotate di allarme. Telecamere a circuito chiuso (CCTV) sono operative sia all'interno che all'esterno dei data center. Il posizionamento delle telecamere è stato progettato per coprire aree strategiche, tra cui, a titolo esemplificativo, il perimetro, le porte dell'edificio del data center e le aree di carico e scarico merci. Il personale addetto alla sicurezza in loco gestisce le apparecchiature di monitoraggio, registrazione e controllo CCTV. Cavi sicuri in tutto il data center collegano le apparecchiature CCTV. Le telecamere registrano in loco tramite videoregistratori digitali 24 ore su 24, 7 giorni su 7. Le registrazioni di sorveglianza vengono conservate per un massimo di 30 giorni, a seconda dell'attività.

*(b) Controllo degli accessi.*

*Personale addetto alla sicurezza dell'infrastruttura* . Google adotta e mantiene una politica di sicurezza per il proprio personale e richiede una formazione in materia di sicurezza come parte integrante del pacchetto formativo. Il personale addetto alla sicurezza dell'infrastruttura di Google è responsabile del monitoraggio continuo dell'infrastruttura di sicurezza di Google, della revisione dei Servizi e della gestione degli incidenti di sicurezza.

*Controllo degli accessi e gestione dei privilegi* . Gli amministratori e gli utenti finali del cliente devono autenticarsi tramite un sistema di autenticazione centralizzato o tramite un sistema di single sign-on per poter utilizzare i Servizi.

*Processi e politiche interne di accesso ai dati – Politica di accesso* . I processi e le politiche interne di accesso ai dati di Google sono progettati per impedire a persone e sistemi non autorizzati di accedere ai sistemi utilizzati per elaborare i Dati del Cliente. Google progetta i suoi sistemi in modo da (i) consentire solo alle persone autorizzate di accedere ai dati a cui sono autorizzate ad accedere; e (ii) garantire che i Dati del Cliente non possano essere letti, copiati, modificati o rimossi senza autorizzazione durante l'elaborazione, l'utilizzo e dopo la registrazione. I sistemi sono progettati per rilevare qualsiasi accesso improprio. Google utilizza un sistema centralizzato di gestione degli accessi per controllare l'accesso del personale ai server di produzione e fornisce l'accesso solo a un numero limitato di personale autorizzato. I sistemi di autenticazione e autorizzazione di Google utilizzano certificati SSH e chiavi di sicurezza e sono progettati per fornire a Google meccanismi di accesso sicuri e flessibili. Questi meccanismi sono progettati per concedere solo diritti di accesso approvati a host del sito, log, dati e informazioni di

configurazione. Google richiede l'utilizzo di ID utente univoci, password complesse, autenticazione a due fattori ed elenchi di accesso attentamente monitorati per ridurre al minimo il potenziale utilizzo non autorizzato dell'account. La concessione o la modifica dei diritti di accesso si basa su: le responsabilità lavorative del personale autorizzato; Requisiti lavorativi necessari per svolgere le mansioni autorizzate; e un principio di necessità di conoscenza. La concessione o la modifica dei diritti di accesso deve inoltre essere conforme alle politiche interne di Google in materia di accesso ai dati e alla formazione ricevuta. Le approvazioni sono gestite da strumenti di workflow che mantengono registri di controllo di tutte le modifiche. L'accesso ai sistemi viene registrato per creare una traccia di controllo a fini di responsabilità. Laddove vengano utilizzate password per l'autenticazione (ad esempio, l'accesso alle workstation), vengono implementate politiche relative alle password che seguono almeno gli standard di settore. Questi standard includono restrizioni sul riutilizzo delle password e requisiti di robustezza sufficienti. Per l'accesso a informazioni estremamente sensibili (ad esempio, dati di carte di credito), Google utilizza token hardware.

**3. Dati**

(a) *Archiviazione, isolamento e registrazione dei dati* . Google archivia i dati in un ambiente multi-tenant su server di proprietà di Google. Salvo diversa indicazione (ad esempio, tramite la selezione della posizione dei dati), Google replica i Dati del Cliente tra più data center geograficamente distribuiti. Google isola inoltre logicamente i Dati del Cliente. Il Cliente avrà il controllo su specifiche politiche di condivisione dei dati. Tali politiche, in conformità con le funzionalità dei Servizi, consentiranno al Cliente di determinare le impostazioni di condivisione dei prodotti applicabili ai propri Utenti finali per scopi specifici. Il Cliente può scegliere di utilizzare le funzionalità di registrazione che Google mette a disposizione tramite i Servizi.

(b) *Dischi dismessi e politica di cancellazione dei dischi* . I dischi contenenti dati possono presentare problemi di prestazioni, errori o guasti hardware che ne comportano la dismissione ("Disco dismesso"). Ogni Disco dismesso è soggetto a una serie di processi di distruzione dei dati (la "Politica di cancellazione dei dischi") prima di lasciare i locali di Google per essere riutilizzato o distrutto. I Dischi dismessi vengono cancellati con un processo in più fasi e la loro completa esecuzione viene verificata da almeno due validatori indipendenti. I risultati della cancellazione vengono registrati tramite il numero di serie del Disco dismesso per consentirne il tracciamento. Infine, il Disco dismesso cancellato viene inserito nell'inventario per il riutilizzo e la ridistribuzione. Se, a causa di un guasto hardware, il Disco dismesso non può essere cancellato, viene conservato in modo sicuro fino

a quando non può essere distrutto. Ogni struttura viene sottoposta a verifiche periodiche per monitorare la conformità con la Politica di cancellazione dei dischi.

**4. Sicurezza del personale**

Il personale di Google è tenuto a comportarsi in modo coerente con le linee guida aziendali in materia di riservatezza, etica aziendale, uso appropriato e standard professionali. Google effettua controlli sui precedenti, nei limiti consentiti dalla legge e in conformità con le leggi sul lavoro e i regolamenti locali applicabili.

Il personale di Google è tenuto a sottoscrivere un accordo di riservatezza e a confermare di aver ricevuto e di rispettare le norme di Google in materia di riservatezza e privacy. Il personale riceve una formazione sulla sicurezza. Il personale che gestisce i Dati dei Clienti è tenuto a soddisfare ulteriori requisiti appropriati al proprio ruolo (ad esempio, certificazioni). Il personale di Google non tratterà i Dati dei Clienti senza autorizzazione.

**5. Sicurezza del sottoprocessore**

Prima di integrare i subappaltatori, Google effettua un audit delle loro pratiche di sicurezza e privacy per garantire che forniscano un livello di sicurezza e privacy adeguato al loro accesso ai dati e alla portata dei servizi che sono incaricati di fornire. Una volta valutati i rischi presentati dal subappaltatore, nel rispetto dei requisiti descritti nella Sezione 11.3 (Requisiti per l'ingaggio dei subappaltatori), quest'ultimo è tenuto a stipulare contratti con termini appropriati in materia di sicurezza, riservatezza e privacy.

## *Appendice 3: Leggi specifiche sulla privacy*

Le disposizioni contenute in ciascuna sottosezione del presente Allegato 3 si applicano solo laddove la legge corrispondente sia applicabile al trattamento dei Dati Personali del Cliente.

***Legge europea sulla protezione dei dati***

**1. Definizioni aggiuntive.**

- " *Paese adeguato* " significa:

(a) per i dati trattati in conformità al GDPR dell'UE: lo Spazio economico europeo o un paese o territorio riconosciuto come in grado di garantire un'adeguata protezione ai sensi del GDPR dell'UE;

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

c) per i dati trattati soggetti alla legge svizzera sulla protezione dei dati personali: la Svizzera, o un paese o territorio che: i) è incluso nell'elenco degli stati la cui legislazione garantisce una protezione adeguata, pubblicato dal Commissario federale svizzero per la protezione dei dati e l'informazione, se applicabile; o ii) è riconosciuto dal Consiglio federale svizzero come garante di una protezione adeguata ai sensi della legge svizzera sulla protezione dei dati personali;

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

- Per " *Soluzione di trasferimento alternativa* " si intende, ai fini delle presenti disposizioni in materia di protezione dei dati personali, una soluzione, diversa dalle clausole contrattuali

standard (SCC), che consenta il trasferimento lecito di dati personali verso un paese terzo in conformità con la normativa europea in materia di protezione dei dati, ad esempio un quadro normativo sulla protezione dei dati riconosciuto come in grado di garantire che le entità partecipanti forniscano una protezione adeguata.

- Per " *Centraline di servizio del cliente* " si intendono le Centraline di servizio (dal controller al processore), le Centraline di servizio (dal processore al processore) o le Centraline di servizio (dal processore al controller), a seconda dei casi.
- Per " *SCC* " si intendono le SCC del Cliente o le SCC (Processor-to-Processor, Google Exporter), a seconda dei casi.
- Per " *SCC (Controller-to-Processor)* " si intendono i termini riportati all'indirizzo https://cloud.google.com/terms/sccs/eu-c2p .
- Per " *SCC (Processor-to-Controller)* " si intendono i termini riportati all'indirizzo https://cloud.google.com/terms/sccs/eu-p2c .
- Per " *SCC (Processor-to-Processor)* " si intendono i termini e le condizioni riportati all'indirizzo https://cloud.google.com/terms/sccs/eu-p2p .
- Per " *SCC (Processor-to-Processor, Google Exporter)* " si intendono i termini e le condizioni riportati all'indirizzo https://cloud.google.com/terms/sccs/eu-p2p-google-exporter .

**2. Notifiche relative alle istruzioni.** Fatto salvo quanto previsto dalla Sezione 5.2 (Conformità alle istruzioni del Cliente) o da qualsiasi altro diritto o obbligo di una delle parti ai sensi del Contratto applicabile, Google informerà immediatamente il Cliente qualora, a suo giudizio:

a. La legge europea vieta a Google di conformarsi a un'Istruzione;

b. un'Istruzione non è conforme alla normativa europea sulla protezione dei dati; o

c. Google non è in grado di conformarsi a un'Istruzione,

in ciascun caso, a meno che tale notifica non sia vietata dal diritto europeo.

Se il Cliente agisce in qualità di responsabile del trattamento, dovrà inoltrare immediatamente al titolare del trattamento terzo qualsiasi comunicazione fornita da Google ai sensi della presente sezione.

**3. Diritti di audit del Cliente.** Google consentirà al Cliente o a un revisore indipendente nominato dal Cliente di condurre audit (incluse ispezioni) come

descritto nella Sezione 7.5.2(a) (Audit del Cliente). Durante tale audit, Google renderà disponibili tutte le informazioni necessarie per dimostrare la conformità ai propri obblighi ai sensi del presente Addendum e contribuirà all'audit 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 la normativa europea sulla protezione dei dati non richiede clausole contrattuali standard (SCC) o una soluzione di trasferimento alternativa affinché i dati personali del Cliente siano trattati o trasferiti in un Paese adeguato. Qualora i dati personali del Cliente vengano trasferiti in un altro Paese e la normativa europea sulla protezione dei dati si applichi ai trasferimenti (come certificato dal Cliente ai sensi della Sezione 4.2 (Certificazione da parte di clienti non EMEA) delle presenti condizioni relative alla normativa europea sulla protezione dei dati, se il suo indirizzo di fatturazione si trova al di fuori dell'area EMEA) (" *Trasferimenti limitati* "), allora:

a. se Google ha adottato una Soluzione di Trasferimento Alternativa per eventuali Trasferimenti Limitati, Google informerà il Cliente della soluzione pertinente e garantirà che tali Trasferimenti Limitati siano effettuati in conformità con essa; oppure

b. se Google non ha adottato una Soluzione di Trasferimento Alternativa per i Trasferimenti Limitati, o informa il Cliente che Google non sta più adottando una Soluzione di Trasferimento Alternativa per i Trasferimenti Limitati (senza adottare una Soluzione di Trasferimento Alternativa sostitutiva):

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

A. le SCC (da processore a processore, Google Exporter) si applicheranno a tali trasferimenti limitati da Google ai subappaltatori; e

B. Inoltre, se l'indirizzo di fatturazione del Cliente non si trova in un Paese adeguato, si applicheranno le Condizioni Generali di Contratto (dal Responsabile del trattamento al Titolare del trattamento) (indipendentemente dal fatto che il Cliente sia un titolare o un responsabile del trattamento) rispetto a tali Trasferimenti Limitati tra Google e il Cliente; oppure

ii. Se l'indirizzo di Google non si trova in un Paese adeguato, si applicheranno le Clausole Contrattuali Standard (dal titolare al responsabile del trattamento) o le Clausole Contrattuali Standard (dal responsabile del trattamento al responsabile del trattamento) (a seconda che il Cliente sia titolare o responsabile del trattamento) in relazione a tali Trasferimenti Limitati tra Google e il Cliente.

4.2 *Certificazione da parte di clienti extra-EMEA* . Se l'indirizzo di fatturazione del Cliente si trova al di fuori dell'area EMEA e il trattamento dei Dati Personali del Cliente è soggetto alla normativa europea sulla protezione dei dati, salvo quanto diversamente indicato nell'Appendice 4 (Prodotti Specifici) del presente Addendum, il Cliente certificherà tale circostanza e indicherà la propria Autorità di Controllo competente tramite la Console di Amministrazione per i Servizi applicabili.

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

a. come descritto nella Sezione 7.5.1 (Revisione della documentazione di sicurezza);

b. in qualsiasi luogo aggiuntivo descritto nell'Appendice 4 (Prodotti specifici); e

c. in relazione all'adozione da parte di Google di una soluzione di trasferimento alternativa, disponibile 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) delle presenti Condizioni generali di contratto (SCC) in materia di protezione dei dati, Google consentirà al Cliente (o a un revisore indipendente nominato dal Cliente) di effettuare audit come descritto in tali SCC e, durante un audit, di rendere disponibili tutte le informazioni richieste da tali SCC, in conformità con la Sezione 7.5.3 (Termini commerciali aggiuntivi per revisioni e audit).

4.5 *Clausole contrattuali standard (SCC) e titolari del trattamento terzi* . Se il Cliente è un responsabile del trattamento, il Cliente riconosce che Google, in quanto altro responsabile del trattamento, potrebbe non essere in grado di identificare il titolare del trattamento terzo e, di conseguenza, il Cliente inoltrerà tempestivamente e senza indebito ritardo al titolare del trattamento terzo qualsiasi comunicazione che faccia riferimento alle clausole contrattuali standard (SCC).

4.6 *Risoluzione a causa del rischio di trasferimento dei dati* . Se il Cliente conclude, in base all'utilizzo attuale o previsto dei Servizi, che non vengono fornite garanzie adeguate per i Dati personali del Cliente trasferiti, il Cliente può risolvere immediatamente il Contratto applicabile in conformità con la clausola di risoluzione per convenienza prevista dal Contratto stesso o, in mancanza di tale clausola, dandone comunicazione a Google.

4.7 *Nessuna modifica delle Clausole Contrattuali Standard* . Nulla nel presente Contratto (incluso il presente Addendum) è inteso a modificare o contraddire le Clausole Contrattuali Standard né a pregiudicare i diritti o le libertà fondamentali degli interessati ai sensi della normativa europea sulla protezione dei dati.

4.8 *Prevalenza delle Condizioni Generali di Contratto* . In caso di conflitto o incoerenza tra le Condizioni Generali di Contratto del Cliente (che sono incorporate per riferimento nel presente Addendum) e il resto del Contratto (incluso il presente Addendum), prevarranno le Condizioni Generali di Contratto del Cliente.

**5. Requisiti per l'incarico di un subappaltatore.** La normativa europea sulla protezione dei dati impone a Google di garantire, tramite un contratto scritto, che gli obblighi in materia di protezione dei dati descritti nel presente Addendum, come previsto dall'articolo 28(3) del GDPR, ove applicabile, siano imposti a qualsiasi subappaltatore incaricato da Google.

## *Appendice 4: Prodotti specifici*

I termini contenuti in ciascuna sottosezione del presente Appendice 4 si applicano esclusivamente al trattamento dei Dati del Cliente da parte del/dei Servizio/i corrispondente/i.

***Piattaforma Google Cloud***

**1. Definizioni aggiuntive.**

- " *Account* ", se non diversamente specificato nel Contratto, si intende l'account Google Cloud Platform del Cliente.
- Per " *Dati del Cliente* ", se non diversamente 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 tali dati attraverso il loro utilizzo di Google Cloud Platform.
- Per " *Google Cloud Platform* " si intendono i servizi di Google Cloud Platform descritti all'indirizzo https://cloud.google.com/terms/services , ad esclusione di eventuali offerte di terze parti.
- " *Offerte di terze parti* ", se non definite nel Contratto, si intendono (a) servizi, software, prodotti e altre offerte di terze parti non incorporati in Google Cloud Platform o Software, (b) offerte identificate nella sezione "Termini di terze parti" dei Termini specifici del servizio del Contratto e (c) sistemi operativi di terze parti.

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

**3. Ubicazione dei data center.** L'ubicazione dei data center di Google Cloud Platform è descritta all'indirizzo https://cloud.google.com/about/locations/ .

**4. Informazioni sui subprocessori.** I nomi, le sedi e le attività dei subprocessori di Google Cloud Platform sono descritti all'indirizzo https://cloud.google.com/terms/subprocessors .

**5. Team di protezione dei dati per il cloud.** È possibile contattare il team di protezione dei dati di Google Cloud Platform all'indirizzo https://support.google.com/cloud/contact/dpo .

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

**7. Termini specifici del servizio.**

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

La soluzione Bare Metal fornisce accesso non virtualizzato alle risorse infrastrutturali sottostanti e, per sua natura, presenta alcune caratteristiche distintive.

**1. Modifiche.** Il presente Addendum viene modificato come segue per quanto riguarda la soluzione Bare Metal:

- La definizione di “Revisore esterno di Google” viene sostituita con la seguente:
- Per " *Revisore dei Conti di Google* " si intende un revisore dei conti terzo qualificato e indipendente, nominato da Google o da un Sub-processore di soluzioni bare metal, la cui identità, al momento della nomina, Google comunicherà al Cliente su richiesta.
- I seguenti termini vengono eliminati:
- Nella sezione 7.1.1 (Misure di sicurezza di Google), la frase "Crittografa i dati dei clienti";
- Dall'Appendice 2 (Misure di sicurezza), le sottosezioni della Sezione 1(a) intitolate "Sistemi operativi server" e "Continuità operativa";
- Dall'Appendice 2, le sottosezioni della Sezione 1(b) intitolate "Superficie di attacco esterna", "Rilevamento delle intrusioni" e "Tecnologie di crittografia"; e
- Dall'Appendice 2, le seguenti frasi della Sezione 3(a):
- Google archivia i dati in un ambiente multi-tenant su server di proprietà di Google. Salvo diversa indicazione da parte del Cliente (ad esempio, tramite la selezione della posizione dei dati), Google replica i Dati del Cliente tra più data center geograficamente distribuiti.

**2. Certificazioni di conformità e report SOC.** Google o il suo subappaltatore manterranno almeno i seguenti elementi (o un'alternativa equivalente o migliorata) per la soluzione Bare Metal al fine di verificare la continua efficacia delle misure di sicurezza:

a. un certificato ISO 27001 e un'attestazione di conformità PCI DSS (le “ *Certificazioni di conformità BMS* ”); e

b. I report SOC 1 e SOC 2 vengono aggiornati annualmente sulla base di un audit effettuato almeno una volta ogni 12 mesi (i " *Report SOC BMS* ").

**3. Revisione della documentazione di sicurezza.** Per dimostrare la conformità di Google ai propri obblighi ai sensi del presente Addendum, Google renderà disponibili al Cliente le Certificazioni di conformità BMS e i Report SOC BMS per la revisione e, se il Cliente è un responsabile del trattamento, consentirà al Cliente di

richiedere l'accesso del titolare del trattamento terzo ai Report SOC BMS in conformità con la Sezione 7.5.3 (Termini commerciali aggiuntivi per revisioni e audit).

**4. Obblighi del Cliente.** Fermo restando quanto espressamente previsto da Google in relazione alla Soluzione Bare Metal, il Cliente adotterà misure ragionevoli per proteggere e mantenere la sicurezza dei Dati del Cliente e di qualsiasi altro contenuto archiviato o elaborato tramite la Soluzione Bare Metal.

**5. Esclusione di responsabilità.** Nonostante qualsiasi disposizione contraria contenuta nel Contratto (incluso il presente Addendum), Google non è responsabile per nessuno dei seguenti aspetti in relazione alla Soluzione Bare Metal:

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

b. registrazione e monitoraggio;

c. manutenzione o supporto non hardware;

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

e. politiche o procedure di continuità operativa e ripristino in caso di disastro.

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

**NGFW cloud (piattaforma Google Cloud)**

L'edizione di Cloud NGFW denominata "Cloud NGFW Enterprise" ("CNE") è progettata per mitigare i rischi di sicurezza informatica e, come tale, presenta alcune caratteristiche specifiche.

**1. Modifiche.** L'Addendum viene modificato come segue per quanto riguarda il CNE:

- Le sezioni 6.1 (Cancellazione da parte del Cliente) e 6.2 (Restituzione o cancellazione alla scadenza del Contratto) non impediranno a Google o ai Subappaltatori di conservare qualsiasi file o acquisizione di pacchetti di traffico di rete inviata per finalità TSS e

designata da CNE come minaccia alla sicurezza, a condizione che il file o l'acquisizione di pacchetti di traffico di rete non includa Dati Personali del Cliente.

**Connessione al cloud distribuito di Google (Google Cloud Platform)**

Google Distributed Cloud Connected non viene distribuito in un data center di Google e, per sua natura, presenta alcune caratteristiche specifiche.

**1. Modifiche.** Il presente Addendum viene modificato come segue per quanto riguarda Google Distributed Cloud connesso:

- La definizione di “Incidente dei dati” viene sostituita con la seguente:
- *Per "Incidente dei Dati"* si intende una violazione della sicurezza di Google che comporti la distruzione, la perdita, l'alterazione, la divulgazione non autorizzata o l'accesso non autorizzato, accidentali o illeciti, ai Dati del Cliente su sistemi gestiti o comunque controllati da Google, ma, per chiarezza, sono escluse le violazioni connesse ad hardware o infrastrutture gestite, ospitate o operate dal Cliente, o comunque di sua responsabilità.
- I riferimenti ai “sistemi di Google” vengono sostituiti con “l’Attrezzatura”.
- La sezione 6.2 (Restituzione o cancellazione al termine del contratto) è sostituita dalla seguente:
- 6.2 *Restituzione o cancellazione al termine del Contratto* . Il Cliente incarica Google di cancellare tutti i Dati del Cliente rimanenti (incluse le copie esistenti) dall'Apparecchiatura al termine del Contratto, in conformità con la legge applicabile. Qualora il Cliente desideri conservare i Dati del Cliente dopo la scadenza del Contratto, potrà esportarli o farne delle copie prima della scadenza del Contratto. Google si conformerà all'Istruzione di cui alla presente Sezione 6.2 non appena ragionevolmente possibile e comunque 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 la legge applicabile non imponga la conservazione, laddove si applichi qualsiasi altra Legge Applicabile sulla Privacy.
- Alla fine della Sezione 10.1 (Strutture di archiviazione ed elaborazione dati) vengono aggiunte le seguenti parole: "o nel luogo in cui si trova la sede del Cliente".
- La sezione 1 (Sicurezza del data center e della rete) dell'Appendice 2 (Misure di sicurezza) è sostituita dalla seguente:
- **1. Sicurezza delle macchine locali e della rete**

*Macchine locali* . I dati del cliente vengono memorizzati esclusivamente sulle apparecchiature da installare presso la sede del cliente.

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

*Tecnologie di crittografia* . Google offre la crittografia HTTPS (nota anche come connessione SSL o TLS) e consente la crittografia dei dati in transito. I server di Google supportano lo scambio di chiavi crittografiche Diffie-Hellman a curva ellittica effimera firmato con RSA ed ECDSA. Questi metodi di Perfect Forward Secrecy (PFS) contribuiscono a proteggere il traffico e a minimizzare l'impatto di una chiave compromessa o di una violazione crittografica. Google offre anche la crittografia dei dati a riposo, utilizzando almeno AES128 o un algoritmo simile. Google Distributed Cloud Connected integra CMEK; ulteriori informazioni sono disponibili all'indirizzo https://cloud.google.com/kms/docs/cmek .

*Connessione a Cloud VPN* . Google consente al Cliente di abilitare e configurare una connessione sicura e crittografata tra l'apparecchiatura e il cloud privato virtuale del Cliente utilizzando Cloud VPN tramite una connessione VPN IPsec.

*Archiviazione vincolata* . I dati del cliente sono archiviati in modo vincolato al server. Qualora un disco venga rubato o copiato a riposo, il contenuto di tale disco non sarà recuperabile al di fuori del server.

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

**2. Disposizioni non applicabili.** Qualsiasi obbligo di Google previsto nel Contratto (incluso il presente Addendum) o dichiarazione contenuta nella documentazione di sicurezza associata (inclusi i white paper) che dipenda dalla gestione di un data center di Google non si applica a Google Distributed Cloud Connected.

**Multicloud gestito da Google (Google Cloud Platform)**

I servizi multicloud gestiti da Google si basano su infrastrutture di terze parti e, per loro natura, presentano alcune caratteristiche distintive.

**1. Definizione aggiuntiva.**

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

**2. Termini relativi al trattamento dei dati multi-cloud.** L'emendamento relativo al trattamento dei dati MCS gestiti da Google integra e modifica il presente Addendum per quanto riguarda i servizi multi-cloud gestiti da Google per Google Cloud Platform.

**Google Cloud VMware Engine (Piattaforma Google Cloud)**

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

**NetApp Volumes (Google Cloud Platform)**

**1. Modifiche.** Il presente Addendum viene modificato come segue per quanto riguarda NetApp Volumes:

- La definizione di “Revisore esterno di Google” viene sostituita con la seguente:
- Per " *Revisore dei Conti di Google* " si intende un revisore dei conti terzo qualificato e indipendente, nominato da Google o da un Sub-processore di NetApp Volumes, la cui identità, al momento della notifica, Google comunicherà al Cliente su richiesta.
- La sezione 3(a) (Archiviazione, isolamento e registrazione dei dati) dell'Appendice 2 (Misure di sicurezza) è sostituita dalla seguente:
- (a) *Archiviazione, isolamento e registrazione dei dati* . Google archivia i dati in un ambiente multi-tenant su server di proprietà di NetApp, Inc. Salvo diversa indicazione (ad esempio, tramite la selezione della posizione dei dati), Google replica i Dati del Cliente tra più data center geograficamente distribuiti. Google isola inoltre logicamente i Dati del Cliente. Il Cliente avrà il controllo su specifiche politiche di condivisione dei dati. Tali politiche, in conformità con le funzionalità dei Servizi, consentiranno al Cliente di determinare le impostazioni di condivisione del prodotto applicabili ai propri Utenti finali per scopi specifici. Il Cliente può scegliere di utilizzare le funzionalità di registrazione che Google mette a disposizione tramite i Servizi.

**2. Certificazioni di conformità e report SOC** . Google o il suo subappaltatore otterranno almeno quanto segue (o un'alternativa equivalente o migliorata) per i volumi NetApp:

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

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

**3. Revisione della documentazione di sicurezza** . Per dimostrare la conformità di Google ai propri obblighi ai sensi del presente Addendum, Google renderà disponibili al Cliente per la revisione tutte le Certificazioni di conformità NetApp e i Report SOC di NetApp e, se il Cliente è un responsabile del trattamento, consentirà al Cliente di richiedere l'accesso del titolare del trattamento terzo ai Report SOC di NetApp in conformità con la Sezione 7.5.3 (Termini commerciali aggiuntivi per revisioni e audit).

***Google Workspace e identità cloud***

**1. Definizioni aggiuntive.**

- " *Account* ", se non diversamente specificato nel Contratto, si intende l'account Google Workspace o Cloud Identity del Cliente.
- Per " *Cloud Identity* ", se acquistato tramite un Contratto separato e non come parte di Google Cloud Platform o Google Workspace, si intendono i Servizi di identità cloud descritti all'indirizzo https://cloud.google.com/terms/identity/user-features .
- Per " *Dati del Cliente* ", se non diversamente definito nel Contratto, si intendono i dati inviati, archiviati, trasmessi o ricevuti dal Cliente o dai suoi Utenti finali, o per loro conto, 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.** Qualora Google, a sua discrezione, renda disponibili al Cliente Prodotti aggiuntivi da utilizzare con Google Workspace o Cloud Identity, in conformità con i Termini applicabili relativi ai Prodotti aggiuntivi:

a. Il cliente può abilitare o disabilitare i Prodotti aggiuntivi tramite la Console di amministrazione e non avrà bisogno di utilizzare Prodotti aggiuntivi per utilizzare Google Workspace o Cloud Identity; e

b. Qualora il Cliente scelga 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 all'interoperabilità con Google Workspace o Cloud Identity, a seconda dei casi.

A titolo di chiarimento, il presente Addendum non si applica al trattamento dei dati personali in relazione alla fornitura di eventuali Prodotti Aggiuntivi installati o utilizzati dal Cliente, inclusi i dati personali trasmessi da o verso tali Prodotti Aggiuntivi.

**3. Certificazioni di conformità.** Le certificazioni di conformità per i servizi Google Workspace e Cloud Identity sottoposti ad audit includeranno anche i certificati ISO 27017 e ISO 27018.

**4. Ubicazione dei data center.** L'ubicazione dei data center di Google Workspace e Cloud Identity è descritta all'indirizzo https://www.google.com/about/datacenters/locations/ .

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

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

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

a. Google separa logicamente i dati di ciascun Utente finale dai dati degli altri Utenti finali; e

b. I dati relativi a un utente finale autenticato non saranno visualizzati da un altro utente finale (a meno che il precedente utente finale o un amministratore non autorizzino la condivisione dei dati).

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

**9. Addendum sui dati di servizio.** Qualora Google renda disponibile al Cliente un Addendum facoltativo sui dati di servizio in relazione al presente Addendum, la disponibilità di tale addendum facoltativo costituirà un "Aggiornamento del DPA" se tale termine è definito in qualsiasi Addendum sui dati di servizio precedentemente stipulato dal Cliente.

**10. Termini specifici del servizio.**

**AppSheet (Google Workspace)**

**1. Modifiche.** Il presente Addendum viene modificato come segue per quanto riguarda AppSheet:

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

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

***Looker (originale)***

**1. Definizioni aggiuntive.**

- Per " *Console di amministrazione* " si intende qualsiasi console di amministrazione applicabile a ciascuna istanza.
- Per " *Emendamento al trattamento dei dati MCS gestito da Google* " si intendono, ove applicabili, i termini disponibili all'indirizzo https://cloud.google.com/terms/mcs-data-processing-terms .
- Per “ *Servizi multicloud gestiti da Google* ” si intendono, ove applicabile, specifici servizi, prodotti e funzionalità di Google ospitati sull'infrastruttura di un fornitore di servizi cloud di terze parti.
- Per “ *Looker (originale)* ” si intende una piattaforma integrata (inclusa l’infrastruttura basata su cloud, se applicabile, e i componenti software, comprese le API associate) che consente alle aziende di analizzare i dati e definire metriche aziendali su più fonti di dati messe a disposizione da Google al Cliente ai sensi del Contratto. Looker (originale) esclude le Offerte di Terze Parti.
- *Il termine* “ Fornitore *di servizi multicloud di terze parti* ” ha il significato attribuitogli dall’emendamento relativo al trattamento dei dati MCS gestito da Google.
- “ *Modulo d’ordine* ” ha il significato indicato nel Contratto, a meno che il Cliente non abbia effettuato l’acquisto tramite un rivenditore o un marketplace online o stia utilizzando Looker esclusivamente a scopo di prova o valutazione in base a un accordo di prova o valutazione, nel qual caso il Modulo d’ordine può significare un altro modulo scritto (e-mail o altri mezzi elettronici consentiti) autorizzato da Google.

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

- La definizione di “Indirizzo e-mail di notifica” viene sostituita con la seguente:
- Per "Indirizzo e-mail di notifica" si intende l'indirizzo o gli indirizzi e-mail indicati dal Cliente nel Modulo d'ordine o tramite Looker (ove applicabile) per ricevere determinate notifiche da Google.
- Le definizioni di “SCC (dal titolare al responsabile del trattamento)”, “SCC (dal responsabile del trattamento al titolare del trattamento)”, “SCC (dal responsabile del trattamento al responsabile del trattamento)” e “SCC (dal responsabile del trattamento al responsabile del trattamento, esportatore Google)” nell’Appendice 3 (Leggi specifiche sulla privacy) sono sostituite dalle seguenti:
- Per “ *SCC (Controller-to-Processor)* ” si intendono i termini riportati all'indirizzo https://cloud.google.com/terms/looker/legal/sccs/eu-c2p ;
- Per “ *SCC (Processor-to-Controller)* ” si intendono i termini riportati all'indirizzo https://cloud.google.com/terms/looker/legal/sccs/eu-p2c ;
- “ *SCC (Processor-to-Processor)* ” indica i termini riportati all'indirizzo https://cloud.google.com/terms/looker/legal/sccs/eu-p2p ; e
- Per “ *SCC (Processor-to-Processor, Google Exporter)* ” si intendono i termini e le condizioni riportati all'indirizzo https://cloud.google.com/terms/looker/legal/sccs/eu-p2p-intra-group .
- Alla fine della Sezione 10.1 (Strutture di archiviazione ed elaborazione dati) vengono aggiunte le seguenti parole: "o laddove i fornitori terzi di servizi multicloud mantengano le proprie strutture".

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

**4. Certificazioni di conformità e report SOC.** Le certificazioni di conformità e i report SOC per i servizi Looker (originali) sottoposti ad audit possono variare a seconda dell'ambiente di hosting in cui vengono utilizzati i relativi servizi. Google fornirà, su richiesta, i dettagli delle certificazioni di conformità e dei report SOC disponibili per specifici ambienti di hosting.

**5. Ubicazione dei data center.** L'ubicazione dei data center di Looker (originariamente) sarà descritta nell'apposito modulo d'ordine o altrimenti indicata da Google.

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

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

**8. Informazioni sui sub-responsabili del trattamento.** I nomi, le sedi e le attività dei sub-responsabili del trattamento per Looker (originale) sono descritti in:

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

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

**9. Multicloud gestito da Google (Looker (originale))**

I servizi multicloud gestiti da Google si basano su infrastrutture di terze parti e, per loro natura, presentano alcune caratteristiche distintive.

9.1 *Termini relativi al trattamento dei dati multi-cloud* . L'emendamento relativo al trattamento dei dati MCS gestiti da Google integra e modifica il presente Addendum per quanto riguarda i servizi multi-cloud gestiti da Google per Looker (originale).

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

**11. Registri di trattamento di Google.** Nella misura in cui qualsiasi legge applicabile in materia di privacy richieda a Google di raccogliere e conservare registri di determinate informazioni relative al Cliente, quest'ultimo fornirà tali informazioni a Google su richiesta e comunicherà a Google qualsiasi aggiornamento necessario per mantenere tali informazioni accurate e aggiornate, a meno che Google non richieda al Cliente di fornire e aggiornare tali informazioni tramite altri mezzi.

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

a. Google adotta almeno le pratiche standard del settore per l'architettura di sicurezza. I server proxy utilizzati per le applicazioni di Google contribuiscono a proteggere l'accesso a Looker fornendo un unico punto di filtraggio degli attacchi tramite l'inserimento in liste di indirizzi IP non consentiti e la limitazione della frequenza di connessione.

b. Gli amministratori del cliente controllano l'accesso alle applicazioni da parte del personale di Google per fornire l'assistenza tecnica richiesta dal cliente o dagli utenti finali.

***Servizi SecOps***

**1. Definizioni aggiuntive.**

- " *Account* ", se non diversamente definito nel Contratto, indica l'account del Cliente per i Servizi SecOps o per la Piattaforma Google Cloud, a seconda dei casi.
- " *Dati del Cliente* ", se non definiti nel Contratto, si intendono (i) i dati forniti a Google dal Cliente o dagli Utenti finali tramite i Servizi SecOps nell'ambito dell'Account e i dati che il Cliente o gli Utenti finali ricavano da tali dati attraverso il loro utilizzo dei Servizi SecOps, oppure (ii) solo per i Servizi di Consulenza Mandiant e i Servizi Gestiti, i dati forniti a Google dal Cliente o dagli Utenti finali in relazione alla ricezione dei Servizi SecOps.
- Per " *Fornitore incaricato dal Cliente* " si intende un fornitore di servizi (che può includere un responsabile del trattamento o un sub-responsabile del trattamento) incaricato direttamente dal Cliente in base a un accordo separato stipulato tra il Cliente e tale fornitore.
- Per " *Servizi SecOps* " si intendono i Servizi SecOps descritti all'indirizzo https://cloud.google.com/terms/secops/services , ad esclusione di eventuali offerte di terze parti.
- " *Offerte di terze parti* ", se non definite nel Contratto, si intendono (a) servizi, software, prodotti e altre offerte di terze parti che non sono incorporati nei Servizi o nel Software SecOps e (b) sistemi operativi di terze parti.

**2. Modifiche.** Il presente Addendum viene modificato come segue per quanto riguarda i Servizi SecOps:

- La definizione di "Controlli di sicurezza aggiuntivi" viene sostituita con la seguente:
- *Per "Controlli di sicurezza aggiuntivi"* si intendono le risorse, le funzionalità e/o i controlli di sicurezza (ove presenti) che il Cliente può utilizzare a sua discrezione e/o secondo le

proprie decisioni, inclusi (ove presenti) crittografia, registrazione e monitoraggio, gestione delle identità e degli accessi e scansione di sicurezza.

- Le definizioni di “SCC (dal titolare al responsabile del trattamento)”, “SCC (dal responsabile del trattamento al titolare del trattamento)”, “SCC (dal responsabile del trattamento al responsabile del trattamento)” e “SCC (dal responsabile del trattamento al responsabile del trattamento, esportatore Google)” nell’Appendice 3 (Leggi specifiche sulla privacy) sono sostituite dalle seguenti:

- Per “SCC (Controller-to-Processor)” si intendono i termini riportati all'indirizzo https://cloud.google.com/terms/secops/sccs/eu-c2p ;

- Per “SCC (Processor-to-Controller)” si intendono i termini riportati all'indirizzo https://cloud.google.com/terms/secops/sccs/eu-p2c ;

- “SCC (Processor-to-Processor)” indica i termini riportati all’indirizzo https://cloud.google.com/terms/secops/sccs/eu-p2p ; e

- Per “SCC (Processor-to-Processor, Google Exporter)” si intendono i termini e le condizioni riportati all'indirizzo https://cloud.google.com/terms/secops/sccs/eu-p2p-google-exporter .

- La sezione 6.1 (Cancellazione da parte del cliente) viene modificata come segue:

- 6.1 **Cancellazione da parte del Cliente** . Google consentirà al Cliente di cancellare i Dati del Cliente durante il Periodo di validità in modo coerente con le funzionalità dei Servizi o su richiesta. Se il Cliente utilizza i Servizi per cancellare i Dati del Cliente durante il Periodo di validità e tali Dati del Cliente non possono essere recuperati dal Cliente, o se il Cliente richiede la cancellazione dei Dati del Cliente durante il Periodo di validità, tale utilizzo o richiesta (a seconda dei casi) costituirà un'Istruzione a Google per cancellare i relativi Dati del Cliente dai sistemi di Google in conformità con la legge applicabile. Google si conformerà a tale Istruzione non appena ragionevolmente possibile e entro un periodo massimo di 180 giorni, a meno che la legge europea non richieda la conservazione, laddove si applichi la normativa europea sulla protezione dei dati, o la legge applicabile non richieda la conservazione, laddove si applichi qualsiasi altra legge applicabile in materia di privacy.

- La sezione 9.1 (Accesso; Rettifica; Trattamento limitato; Portabilità) è modificata come segue:

  9.1 **Accesso; Rettifica; Limitazione del trattamento; Portabilità** . Durante il Periodo di validità del Contratto, Google consentirà al Cliente, in modo coerente con le funzionalità dei Servizi, di accedere, rettificare e limitare il trattamento dei Dati del Cliente, anche come descritto nella Sezione 6.1 (Cancellazione da parte

del Cliente), e di esportare i Dati del Cliente su richiesta. Qualora il Cliente venga a conoscenza del fatto che i Dati personali del Cliente siano inesatti o obsoleti, sarà sua responsabilità informare Google e Google assisterà il Cliente nella rettifica di tali dati, se richiesto dalla Legge sulla privacy applicabile.

**3. Ubicazione dei data center.** L'ubicazione dei data center di SecOps Services è descritta all'indirizzo https://www.google.com/about/datacenters/locations/ .

**4. Nessuna certificazione da parte di clienti extra-EMEA.** Il cliente non è obbligato a certificare o identificare la propria Autorità di controllo competente come descritto nella Sezione 4.2 (Certificazione da parte di clienti extra-EMEA) delle Condizioni europee sulla protezione dei dati contenute nell'Appendice 3 (Leggi specifiche sulla privacy) per i Servizi SecOps.

**5. Informazioni sui subprocessori.** I nomi, le posizioni e le attività dei subprocessori per i servizi SecOps sono descritti all'indirizzo https://cloud.google.com/terms/secops/subprocessors .

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

**7. Registri di trattamento di Google.** Nella misura in cui qualsiasi legge applicabile in materia di privacy richieda a Google di raccogliere e conservare registri di determinate informazioni relative al Cliente, quest'ultimo fornirà tali informazioni a Google su richiesta e comunicherà a Google qualsiasi aggiornamento necessario per mantenere tali informazioni accurate e aggiornate, a meno che Google non richieda al Cliente di fornire e aggiornare tali informazioni tramite altri mezzi.

**8. Termini specifici del servizio.**

**Servizi di consulenza e servizi gestiti di Mandiant**

I servizi di consulenza e i servizi gestiti di Mandiant offrono 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. Modifiche.** L'Addendum viene modificato come segue, esclusivamente con riferimento a Mandiant Consulting Services e ai Servizi Gestiti:

- La definizione di “Incidente dei dati” è integrata dai seguenti elementi:
- Per chiarezza, la definizione di Incidente sui dati esclude gli incidenti oggetto dei Servizi di consulenza e/o dei Servizi gestiti di Mandiant, a seconda dei casi.
- La sezione 5.2(b)(i) (Conformità alle istruzioni del cliente) è sostituita dalla seguente:
- i. L'utilizzo dei Servizi da parte del Cliente; e
- La seconda frase della Sezione 7.1.1 (Misure di sicurezza di Google) viene modificata come segue:
- Le misure di sicurezza possono includere (ove opportuno) misure per crittografare i Dati del Cliente; per contribuire a garantire la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi di Google; per contribuire a ripristinare tempestivamente l'accesso ai Dati del Cliente in seguito a un incidente; e per test periodici di efficacia.
- La sezione 7.3.1(b) viene 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 a cui autorizza Google ad accedere per fornire, i Servizi di consulenza Mandiant e/o i Servizi gestiti, a seconda dei casi;
- Le nuove sezioni 7.3.1(d) e (e) sono aggiunte come segue:
- d. ridurre al minimo la quantità di Dati del Cliente forniti dal Cliente o per conto del Cliente a Google; e
- e. nella misura in cui l'accesso di Google ai Dati del Cliente rientri nel controllo del Cliente, revocando tale accesso al termine dei Servizi di Consulenza Mandiant e/o dei Servizi Gestiti, a seconda dei casi.
- L'Appendice 2 (Misure di sicurezza) è sostituita dalla seguente:
- Appendice 2: Misure tecniche e organizzative aggiuntive

  1. Ambiente controllato dal cliente. Google accederà ed elaborerà i Dati del Cliente forniti dal Cliente o per conto del Cliente a Google esclusivamente tramite un account o un ambiente controllato o approvato dal Cliente.

  2. Processi e politiche di accesso ai dati – Politica di accesso. I processi e le politiche di accesso ai dati di Google sono progettati per impedire a persone e/o sistemi non autorizzati di accedere ai sistemi utilizzati per elaborare i 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 l'elaborazione 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. Il personale di Google è tenuto a comportarsi in modo coerente con le linee guida aziendali in materia di riservatezza, etica aziendale, utilizzo appropriato e standard professionali. Google effettua controlli sui precedenti penali ragionevolmente appropriati, nei limiti consentiti dalla legge e in conformità con le leggi sul lavoro e i regolamenti locali applicabili.

Il personale è tenuto a sottoscrivere un accordo di riservatezza e a confermare di aver ricevuto e di rispettare le norme di Google in materia di riservatezza e privacy. Il personale riceve una formazione sulla sicurezza. Il personale che gestisce i Dati dei Clienti è tenuto a soddisfare ulteriori requisiti appropriati al proprio ruolo (ad esempio, certificazioni). Il personale di Google non tratterà i Dati dei Clienti senza autorizzazione.

4. Misure di sicurezza aggiuntive. Google e il Cliente possono concordare misure di sicurezza aggiuntive nel modulo d'ordine applicabile, inclusa qualsiasi Dichiarazione di lavoro allegata, per i Servizi di consulenza Mandiant e/o i Servizi gestiti, a seconda dei casi.

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

***Servizi di implementazione***

**1. Definizioni aggiuntive.**

- Per " *Dati del Cliente* " si intendono i dati a cui il Cliente autorizza il personale di Google ad accedere sui Sistemi gestiti dal Cliente.
- Per " *Sistemi gestiti dal Cliente* " si intendono i seguenti, utilizzati dal Cliente per ricevere i Servizi di Implementazione: (a) istanze di Google Cloud Services o di servizi cloud di terze parti gestite dal Cliente; e (b) qualsiasi hardware o software ospitato o gestito nell'ambiente locale del Cliente.

- *Per "Servizi Google Cloud* " si intendono tutti i Servizi descritti nell'Appendice 4 (Prodotti Specifici), ad eccezione dei Servizi di Implementazione, dei Servizi di Consulenza Mandiant e dei Servizi Gestiti Mandiant.
- Per " *Personale Google* " si intendono i dipendenti e i collaboratori di Google impegnati nella fornitura dei Servizi di implementazione.
- Per " *Servizi di implementazione* " si intendono i servizi di consulenza e implementazione forniti da dipendenti e collaboratori di Google a supporto dei Servizi Google Cloud, come descritto nel Contratto, incluso in un Modulo d'ordine o in una Dichiarazione di lavoro.

**2. Modifiche** . Il presente Addendum viene modificato come segue per quanto riguarda i Servizi di implementazione:

- La definizione di "Controlli di sicurezza aggiuntivi" è stata eliminata.
- La definizione di "Incidente dei dati" viene sostituita con la seguente:
- Per " *Incidente dei dati* " si intende una violazione della Sezione 7.1 (Misure di sicurezza, controlli e assistenza di Google) da parte del personale di Google, che comporti la distruzione, la perdita, l'alterazione, la divulgazione non autorizzata o l'accesso non autorizzato ai Dati personali del Cliente, in modo accidentale o illecito.
- Fatto salvo quanto previsto nel resto della presente sezione, il termine "Dati del Cliente" è sostituito da "Dati Personali del Cliente" quando utilizzato (a) nella Sezione 2 (Definizioni) nella definizione di "Sub-responsabile del trattamento", e (b) in altre sezioni del presente Addendum. Per chiarezza, le altre definizioni nella Sezione 2 (Definizioni) rimangono invariate.
- La sezione 3 (Durata) è sostituita dalla seguente:
- **3. Durata** . Indipendentemente dal fatto che l'Accordo applicabile 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 quando ciò avverrà.
- La sezione 6 (Cancellazione dei dati) viene sostituita dalla seguente:
- **6. Cancellazione dei dati.** Al termine del Periodo di validità, il Cliente (a) deciderà se cancellare i Dati personali del Cliente e (b) sarà responsabile di tale cancellazione.
- La seconda frase della Sezione 7.1.1 (Misure di sicurezza di Google) viene sostituita con la seguente:

- "Le misure di sicurezza possono includere (ove opportuno) misure per crittografare i Dati del Cliente; per contribuire a garantire la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi di Google; per contribuire a ripristinare tempestivamente l'accesso ai Dati del Cliente in seguito a un incidente; e per test periodici di efficacia."
- La sezione 7.1.3 (Controlli di sicurezza aggiuntivi) viene eliminata, insieme a tutti gli altri riferimenti a tale sezione.
- La sezione 9.1 (Accesso; Rettifica; Trattamento limitato; Portabilità) è sostituita dalla seguente:
- 9.1 *Accesso; Rettifica; Limitazione del trattamento; Portabilità* . Il Cliente sarà responsabile dell'utilizzo delle funzionalità dei Sistemi gestiti dal Cliente per accedere, rettificare e limitare il trattamento dei Dati personali del Cliente, anche qualora il Cliente venga a conoscenza del fatto che i Dati personali del Cliente siano inesatti o obsoleti e sia tenuto, ai sensi della Legge sulla privacy applicabile, a rettificare o cancellare tali dati.
- La sezione 11.4 (Opportunità di opporsi ai subprocessori) è sostituita dalla seguente:
- 11.4 *Possibilità di opporsi ai subappaltatori* . Qualora venga incaricato un nuovo subappaltatore durante il Periodo di validità del Contratto, Google informerà il Cliente dell'incarico conferito al nuovo subappaltatore prima che quest'ultimo elabori i Dati personali del Cliente. Il Cliente potrà opporsi al nuovo subappaltatore notificandolo a Google e, in tal caso, le parti collaboreranno in buona fede per individuare un'alternativa reciprocamente accettabile.
- L'Appendice 1 (Oggetto e dettagli del trattamento dei dati) viene modificata come segue:
- La sezione “Durata del trattamento” viene sostituita con la seguente:
- *“Durata del trattamento.* Il periodo di validità del Contratto più (se applicabile) il periodo che intercorre tra la fine del Contratto e la scadenza dell'accesso di Google ai Dati personali del Cliente.”
- Le parole “forniti a Google tramite i Servizi” nelle sezioni “Categorie di dati” e “Interessati” vengono sostituite con “resi accessibili a Google in relazione ai Servizi”.
- L'Appendice 2 (Misure di sicurezza) è sostituita dalla seguente:
- **Appendice 2: Misure di sicurezza**

  **1. Sistemi gestiti dal cliente.** Il personale di Google accederà e tratterà i Dati personali del cliente esclusivamente sui sistemi gestiti dal cliente stesso. Qualora

tali sistemi includano i Servizi Google Cloud, l'utilizzo dei Servizi Google Cloud da parte del cliente rimarrà regolato dall'accordo applicabile a tali servizi.

**2. Controllo degli accessi.** I processi e le politiche interne di Google in materia di accesso ai dati sono progettati per impedire a persone e sistemi non autorizzati di accedere ai Servizi Google Cloud utilizzati per l'elaborazione dei dati personali. Le politiche di Google (i) consentono l'accesso ai dati solo al personale di Google autorizzato; e (ii) impongono al personale di Google di non leggere, copiare, modificare o rimuovere i Dati personali del Cliente senza autorizzazione durante l'elaborazione, l'utilizzo e dopo la registrazione. Il Cliente controlla la fornitura o la modifica dei diritti di accesso degli utenti finali ai Sistemi gestiti dal Cliente. Se tali sistemi includono i Servizi Google Cloud, i dettagli relativi agli strumenti di flusso di lavoro che mantengono registri di controllo delle modifiche e registri di accesso al sistema sono specificati nel contratto per i Servizi Google Cloud applicabili.

**3. Sicurezza del personale.** Il personale di Google è tenuto a comportarsi in modo coerente con le linee guida aziendali in materia di riservatezza, etica aziendale, utilizzo appropriato e standard professionali. Google effettua controlli sui precedenti penali ragionevolmente appropriati, nei limiti consentiti dalla legge e in conformità con le leggi sul lavoro e i regolamenti locali applicabili.

Il personale di Google è tenuto a sottoscrivere un accordo di riservatezza e a confermare di aver ricevuto e di rispettare le norme di Google in materia di riservatezza e privacy. Il personale di Google riceve una formazione sulla sicurezza. Il personale di Google che gestisce i Dati Personali dei Clienti è tenuto a soddisfare ulteriori requisiti appropriati al proprio ruolo (ad esempio, certificazioni).

**4. Misure di sicurezza aggiuntive.** Google e il Cliente possono concordare misure di sicurezza aggiuntive nell'Accordo, incluso in un Modulo d'Ordine o in una Dichiarazione di Lavoro.

**5. Sicurezza dei subappaltatori.** Prima di integrare i subappaltatori, Google esegue un audit delle pratiche di sicurezza e privacy dei subappaltatori per garantire che questi forniscano un livello di sicurezza e privacy adeguato al loro accesso ai dati e alla portata dei servizi che sono incaricati di fornire. Una volta che Google ha valutato i rischi presentati dal subappaltatore, nel rispetto dei requisiti descritti nella Sezione 11.3 (Requisiti per l'ingaggio dei subappaltatori), il subappaltatore è tenuto a stipulare contratti con termini appropriati in materia di sicurezza, riservatezza e privacy.

**3. Responsabilità del Cliente in materia di sicurezza** . Oltre agli obblighi previsti dalla 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 tale accesso al completamento dei servizi di implementazione; e
- Implementare tutte le raccomandazioni di sicurezza fornite per iscritto da Google al Cliente in relazione ai Sistemi gestiti dal Cliente.

**4. Certificazione di conformità.** Google manterrà i certificati ISO 27001, ISO 27017 e ISO 27018 relativi ai Servizi di implementazione forniti a supporto di Google Cloud Platform e Google Workspace (le " *Certificazioni di conformità dei Servizi di implementazione* "). Google può aggiungere standard in qualsiasi momento. Google può sostituire una Certificazione di conformità dei Servizi di implementazione con un'alternativa equivalente o migliorata.

**5. Revisione della Certificazione di Conformità.** Per dimostrare la conformità di Google ai propri obblighi ai sensi del presente Addendum, Google renderà disponibile al Cliente la Certificazione di Conformità dei Servizi di Implementazione per la revisione e, se il Cliente è un responsabile del trattamento, consentirà al Cliente di richiedere l'accesso del titolare del trattamento terzo alla Certificazione di Conformità dei Servizi di Implementazione.

**6. Luoghi di elaborazione dei dati.** I dati personali del Cliente possono essere elaborati in qualsiasi Paese in cui Google fornisce Servizi di implementazione o in cui il Cliente gestisce Sistemi propri.

**7. Nessuna certificazione da parte di clienti extra-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 extra-EMEA) delle Condizioni europee sulla protezione dei dati contenute nell'Appendice 3 (Leggi specifiche sulla privacy) per i Servizi di implementazione.

**8. Informazioni sui subappaltatori.** I subappaltatori per i Servizi di implementazione saranno identificati (come subappaltatori) in un apposito Modulo d'ordine, Dichiarazione di lavoro o altra conferma fornita al Cliente prima dell'inizio dei Servizi di implementazione, oppure saranno affiliati di Google. Google renderà inoltre disponibili al Cliente, su richiesta, i nomi, le sedi e le attività dei subappaltatori per i Servizi di implementazione.

**9. Registri di trattamento di Google.** Nella misura in cui qualsiasi legge applicabile in materia di privacy richieda a Google di raccogliere e conservare registri di determinate informazioni relative al Cliente, quest'ultimo fornirà tali informazioni a Google su richiesta e comunicherà a Google qualsiasi aggiornamento necessario per mantenere tali informazioni accurate e aggiornate, a meno che Google non richieda al Cliente di fornire e aggiornare tali informazioni tramite altri mezzi.

***Competenze Google per le organizzazioni***

**1. Definizioni aggiuntive.**

- " *Account* ", se non diversamente specificato nel Contratto, si intende l'Account cliente di Google Skills for Organizations del Cliente.
- Per " *GSO* " si intendono i servizi e i contenuti di istruzione, formazione e apprendimento forniti tramite https://skills.google (o un altro sito web gestito o controllato da Google e utilizzato per le finalità di Google Skills for Organizations).
- Per " *TSS* " si intendono i servizi di supporto tecnico che Google, a sua discrezione, può fornire al Cliente.

**2. Modifiche.** Il presente Addendum viene modificato come segue per quanto riguarda GSO:

- La definizione di "Controlli di sicurezza aggiuntivi" viene sostituita con la seguente:
- *Per "Controlli di sicurezza aggiuntivi"* si intendono le risorse, le funzionalità e/o i controlli di sicurezza (ove presenti) che il Cliente può utilizzare a sua discrezione e/o secondo le proprie decisioni, inclusi (ove presenti) crittografia, registrazione e monitoraggio, gestione delle identità e degli accessi e scansione di sicurezza.
- Le definizioni di "SCC (dal titolare al responsabile del trattamento)", "SCC (dal responsabile del trattamento al titolare del trattamento)", "SCC (dal responsabile del trattamento al responsabile del trattamento)" e "SCC (dal responsabile del trattamento al responsabile del trattamento, esportatore Google)" nell'Appendice 3 (Leggi specifiche sulla privacy) sono sostituite dalle seguenti:
- Per "SCC (Controller-to-Processor)" si intendono i termini riportati all'indirizzo https://cloud.google.com/terms/skills-for-organizations/sccs/eu-c2p ;
- Per "SCC (Processor-to-Controller)" si intendono i termini riportati all'indirizzo https://cloud.google.com/terms/skills-for-organizations/sccs/eu-p2c ;

- “SCC (Processor-to-Processor)” significa i termini indicati all’indirizzo https://cloud.google.com/terms/skills-for-organizations/sccs/eu-p2p ; e
- Per “SCC (Processor-to-Processor, Google Exporter)” si intendono i termini e le condizioni riportati all'indirizzo https://cloud.google.com/terms/skills-for-organizations/sccs/eu-p2p-intra-group .

**3. Ubicazione dei data center.** L'ubicazione dei data center di GSO è descritta all'indirizzo https://cloud.google.com/about/locations/ .

**4. Nessuna certificazione da parte di clienti extra-EMEA.** Il cliente non è obbligato a certificare o identificare la propria Autorità di controllo competente come descritto nella Sezione 4.2 (Certificazione da parte di clienti extra-EMEA) delle Condizioni europee sulla protezione dei dati nell'Appendice 3 (Leggi specifiche sulla privacy) per GSO.

**5. Informazioni sui subappaltatori.** I nomi, le sedi e le attività dei subappaltatori GSO sono descritti ai seguenti indirizzi:

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

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

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

**7. Registri di trattamento di Google.** Nella misura in cui qualsiasi legge applicabile in materia di privacy richieda a Google di raccogliere e conservare registri di determinate informazioni relative al Cliente, quest'ultimo fornirà tali informazioni a Google su richiesta e comunicherà a Google qualsiasi aggiornamento necessario per mantenere tali informazioni accurate e aggiornate, a meno che Google non richieda al Cliente di fornire e aggiornare tali informazioni tramite altri mezzi.

*Versioni precedenti dei Termini relativi al trattamento e alla 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 della modifica relativa al 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 sul trattamento dei dati per i servizi Looker (originale) (clienti):*

*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 di SecOps Services DPST (Clienti):*

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

*Versioni precedenti dell'Addendum sull'elaborazione dei dati per i servizi di consulenza SecOps e i servizi gestiti:*

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