Emendamento sull'elaborazione dei dati a G Suite e / o contratto di prodotto complementare (versione 2.3)

Il cliente accetta questi termini (" **Cliente** ") e Google LLC, Google Ireland Limited, Google Asia Pacific Pte. Ltd., o qualsiasi altra entità che direttamente o indirettamente controlla, è controllata da o è sotto il controllo comune di Google LLC (a seconda dei casi, " **Google** "), ha stipulato uno o più Accordi G Suite (come definito di seguito) e / o Accordi sui prodotti complementari (come definiti di seguito) (ciascuno, come modificato di volta in volta, un " **Accordo** ").

1. **Inizio** .

   Questo Emendamento sul trattamento dei dati a G Suite e / o al Contratto di prodotto complementare, comprese le sue appendici (l '" **Emendamento sul trattamento dei dati** "), entrerà in vigore e sostituirà qualsiasi termine di elaborazione e sicurezza dei dati precedentemente applicabile a partire dalla Data di entrata in vigore della modifica (come definita di seguito).
   Questo Emendamento sul trattamento dei dati integra il Contratto applicabile. Laddove tale Contratto sia stato stipulato offline con Google Ireland Limited, questo Emendamento sul trattamento dei dati sostituisce la clausola "Privacy" del Contratto (se applicabile).

2. **Definizioni**

   2.1 I termini in maiuscolo definiti nel Contratto applicabile si applicano a questo Emendamento sul trattamento dei dati. Inoltre, in questo Emendamento sul trattamento dei dati:

   " **Prodotti aggiuntivi** " indica prodotti, servizi e applicazioni che non fanno parte dei Servizi ma che possono essere accessibili, tramite la Console di amministrazione o in altro modo, per l'utilizzo con i Servizi.

   " **Controlli di sicurezza aggiuntivi** " indica risorse, caratteristiche, funzionalità e / o controlli di sicurezza che il Cliente può utilizzare a sua discrezione e / o come determina, inclusa la Console di amministrazione, crittografia, registrazione e monitoraggio, gestione di identità e accessi, scansione di sicurezza e firewall.

   " **Pubblicità** " indica annunci pubblicitari online visualizzati da Google agli Utenti finali, esclusa qualsiasi pubblicità che il Cliente sceglie espressamente di visualizzare Google o qualsiasi delle sue Affiliate in relazione ai Servizi in base a un contratto separato (ad esempio, annunci pubblicitari di Google AdSense implementati dal Cliente su un sito web creato dal Cliente utilizzando qualsiasi funzionalità di Google Sites all'interno dei Servizi).

   " **Affiliata** " indica qualsiasi entità che controlla, controllata da o è sotto il controllo comune di una parte, dove "controllo" è definito come: (a) la proprietà di almeno il cinquanta per cento (50%) del capitale proprio o degli interessi beneficiari dell'entità ; (b) il diritto di votare o di nominare la maggioranza del consiglio di amministrazione o altro organo di governo dell'entità; o (c) il potere di esercitare un'influenza di controllo sulla gestione o sulle politiche dell'entità.

   " **Limite di responsabilità concordato** " indica l'importo massimo monetario o basato sul pagamento al quale la responsabilità di una parte è limitata ai sensi del Contratto applicabile.

   " **Soluzione di trasferimento alternativa** " indica una soluzione, diversa dalle clausole contrattuali tipo, che consente il trasferimento legale di dati personali a un paese terzo in conformità con la legge europea sulla protezione dei dati.

   " **Data di** entrata in **vigore della modifica** " indica la data in cui il Cliente ha accettato, o le parti hanno altrimenti concordato, questo Emendamento sul trattamento dei dati.

   " **Servizi controllati** " significa:

      un. quei servizi G Suite Core indicati come nell'ambito della relativa certificazione o rapporto su https://cloud.google.com/security/compliance/services-in-scope/ , a condizione che Google possa rimuovere solo un servizio G Suite Core da tale URL interrompendo tale Servizio in conformità con il Contratto applicabile; e

      b. tutti gli altri Servizi, a meno che il Riepilogo dei servizi di G Suite o il Riepilogo dei servizi dei prodotti complementari non indichi diversamente o le parti concordino espressamente diversamente per iscritto.

   " **Contratto di prodotto complementare** " indica: un Contratto di Cloud Identity o altro contratto in base al quale Google accetta di fornire servizi di identità in quanto tali al Cliente; Contratto di noleggio; o altro accordo che incorpora questo Emendamento sul trattamento dei dati per riferimento o afferma che si applicherà se accettato dal Cliente.

   " **Riepilogo dei servizi del prodotto complementare** " indica la descrizione corrente dei servizi forniti in base a un Contratto di prodotto complementare, come stabilito nel Contratto applicabile.

   " **Dati del cliente** " indica i dati inviati, archiviati, inviati o ricevuti tramite i Servizi dal Cliente o dagli Utenti finali.

   " **Dati personali del cliente** " indica i dati personali contenuti nei Dati del cliente.

" **Incidente di dati** " indica una violazione della sicurezza di Google che porta alla distruzione, perdita, alterazione accidentale o illegale, divulgazione non autorizzata o accesso ai Dati del cliente su sistemi gestiti o altrimenti controllati da Google.

" **SEE** " indica lo Spazio economico europeo.

" **Data di attivazione completa** " significa: (a) se questo Emendamento sul trattamento dei dati è automaticamente incorporato nel Contratto applicabile, la Data di efficacia della modifica; o (b) se il Cliente ha accettato o le parti hanno altrimenti concordato questo Emendamento sul trattamento dei dati, l'ottavo giorno dopo la Data di entrata in vigore della modifica.

" **EU GDPR** " indica il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio, del 27 aprile 2016, sulla protezione delle persone fisiche con riguardo al trattamento dei dati personali e sulla libera circolazione di tali dati, e che abroga la Direttiva 95/46 / CE.

" **Legge europea sulla protezione dei dati** " indica, se applicabile: (a) il GDPR; e / o (b) la legge federale sulla protezione dei dati del 19 giugno 1992 (Svizzera).

" **Legge europea o nazionale** " indica, a seconda dei casi: (a) la legge dell'UE o di uno Stato membro dell'UE (se il GDPR dell'UE si applica al trattamento dei Dati personali del cliente); e / o (b) la legge del Regno Unito o parte di Regno Unito (se il GDPR del Regno Unito si applica al trattamento dei dati personali del cliente).

" **GDPR** " indica, se applicabile: (a) il GDPR dell'UE; e / o (b) il GDPR del Regno Unito.

" **Revisore di terze parti di Google** " indica un revisore di terze parti nominato da Google, qualificato e indipendente, la cui identità allora attuale sarà rivelata da Google al Cliente.

" **Contratto G Suite** " indica un Contratto G Suite; un contratto G Suite for Education; un contratto principale di Google Cloud con la pianificazione dei servizi G Suite; o qualsiasi altro contratto in base al quale Google accetta di fornire al Cliente i servizi descritti nel Riepilogo dei servizi di G Suite.

" **Riepilogo dei servizi di G Suite** " indica la descrizione corrente dei servizi di G Suite (comprese le edizioni correlate), come indicato su https://gsuite.google.com/terms/user_features.html (come potrebbe essere aggiornato da Google da di volta in volta in conformità con il contratto G Suite).

" **Clausole contrattuali tipo** " o "MCC" indicano le clausole standard di protezione dei dati per il trasferimento di dati personali a responsabili del trattamento stabiliti in paesi terzi che non garantiscono un livello adeguato di protezione dei dati, come descritto nell'articolo 46 del GDPR dell'UE e stabilito a https://gsuite.google.com/terms/mcc_terms.html .

" **Legge non europea sulla protezione dei dati** " indica le leggi sulla protezione dei dati o sulla privacy in vigore al di fuori del SEE, della Svizzera e del Regno Unito.

" **Indirizzo e-mail di notifica** " indica gli indirizzi e-mail designati dal Cliente nella Console di amministrazione o nel Modulo d'ordine o nel Documento d'ordine (a seconda dei casi), per ricevere determinate notifiche da Google. Il Cliente è responsabile dell'utilizzo della Console di amministrazione per garantire che il proprio indirizzo e-mail di notifica rimanga aggiornato e valido.

" **Documentazione sulla sicurezza** " indica tutti i documenti e le informazioni resi disponibili da Google nella Sezione 7.5.1 (Revisioni della documentazione sulla sicurezza).

" **Misure di sicurezza** " ha il significato indicato nella Sezione 7.1.1 (Misure di sicurezza di Google).

" **Termini specifici del servizio** " ha il significato indicato nel Contratto G Suite o nel Contratto del prodotto complementare, a seconda dei casi, oppure, se il Contratto G Suite del Cliente non definisce i "Termini specifici del servizio", indica i termini correnti specifici per uno o più Core I servizi per G Suite sono disponibili su https://gsuite.google.com/terms/service-terms/ .

" **Servizi** " indica i seguenti servizi, a seconda dei casi:

un. i servizi principali per G Suite, come descritti nel riepilogo dei servizi di G Suite;

b. gli Altri servizi per G Suite, come descritto nel Riepilogo dei servizi di G Suite; e /

o c. i servizi descritti nel Riepilogo servizi prodotti complementari.

" **Sub-** responsabile del trattamento" indica una terza parte autorizzata come altro responsabile del trattamento ai sensi del presente Emendamento sul trattamento dei dati ad avere accesso logico ed elaborare i Dati del cliente al fine di fornire parti dei Servizi e dei TSS.

" **Autorità di controllo** " indica, a seconda dei casi: (a) una "autorità di controllo" come definita nel GDPR dell'UE; e / o (b) il "Commissario" come definito nel GDPR del Regno Unito.

" **Durata** " indica il periodo dalla Data di efficacia della modifica fino alla fine della fornitura dei Servizi da parte di Google ai sensi del Contratto applicabile, incluso, se applicabile, qualsiasi periodo durante il quale la fornitura dei Servizi può essere sospesa e qualsiasi periodo successivo alla risoluzione durante il quale Google può continuare a fornire i Servizi a fini transitori.

" **UK GDPR** " indica il GDPR dell'UE come modificato e incorporato nel diritto del Regno Unito ai sensi della legge del 2018 sull'Unione europea (recesso) del Regno Unito, se in vigore.

2.2. I termini "dati personali", "soggetto dei dati", "elaborazione", "responsabile del trattamento" e "responsabile del trattamento" utilizzati in questo Emendamento sull'elaborazione dei dati hanno il significato indicato nel GDPR, indipendentemente dal fatto che la legge europea sulla protezione dei dati o dati non europei Si applica la legge sulla protezione.

3. **Durata** . Il presente Emendamento sull'elaborazione dei dati, nonostante la scadenza del Periodo, rimarrà in vigore fino all'eliminazione di tutti i Dati del cliente da parte di Google e scadrà automaticamente al momento della cancellazione di tutti i Dati del cliente da parte di Google come descritto in

questo Emendamento sull'elaborazione dei dati.

4. **Campo di applicazione della legge sulla protezione dei dati** .

4.1 Applicazione della legge europea . Le parti riconoscono che la legge europea sulla protezione dei dati si applicherà al trattamento dei dati personali del cliente se, ad esempio:

un. il trattamento è effettuato nell'ambito delle attività di uno stabilimento del Cliente nel territorio del SEE o del Regno Unito; e / o

b. i Dati personali del cliente sono dati personali relativi agli interessati che si trovano nel SEE o nel Regno Unito e il trattamento si riferisce all'offerta loro di beni o servizi nel SEE o nel Regno Unito, o al monitoraggio del loro comportamento nel SEE o nel UK.

4.2 Applicazione della legge non europea . Le parti riconoscono che la legge non europea sulla protezione dei dati può essere applicata anche al trattamento dei dati personali del cliente.

4.3 Applicazione dell'emendamento sul trattamento dei dati . Salvo nella misura in cui questo Emendamento sul trattamento dei dati stabilisce diversamente, i termini di questo Emendamento sul trattamento dei dati si applicheranno indipendentemente dal fatto che la legge europea sulla protezione dei dati o la legge non europea sulla protezione dei dati si applichi al trattamento dei dati personali del cliente.

5. **Trattamento dei dati** .

5.1 **ruoli e conformità normativa; Autorizzazione** .

5.1.1. Responsabilità del processore e del titolare . Se la legge europea sulla protezione dei dati si applica al trattamento dei dati personali del cliente:

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

b. Google è un elaboratore di tali Dati personali del cliente ai sensi della legge europea sulla protezione dei dati;

c. Il Cliente è titolare del trattamento o responsabile del trattamento, a seconda dei casi, dei Dati personali del Cliente ai sensi della Legge europea sulla protezione dei dati; e

d. ciascuna parte rispetterà gli obblighi ad essa applicabili ai sensi della legge europea sulla protezione dei dati in relazione al trattamento dei dati personali del cliente.

5.1.2. Autorizzazione da parte del titolare del trattamento di terze parti . Se la legge europea sulla protezione dei dati si applica al trattamento dei dati personali del cliente e il cliente è un responsabile del trattamento, il cliente garantisce che le sue istruzioni e azioni in relazione a tali dati personali del cliente, inclusa la sua nomina di Google come altro responsabile del trattamento, sono state autorizzate dal responsabile del trattamento pertinente .

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

5.2 **Scopo del trattamento** .

5.2.1 Istruzioni del cliente . Il Cliente ordina a Google di elaborare i Dati personali del cliente solo in conformità con la legge applicabile: (a) per fornire i Servizi e TSS; (b) come ulteriormente specificato tramite l'utilizzo dei Servizi da parte del Cliente e degli Utenti finali (inclusa la Console di amministrazione e altre funzionalità dei Servizi) e TSS; (c) come documentato nella forma dell'Accordo applicabile, incluso il presente Emendamento sul trattamento dei dati; e (d) come ulteriormente documentato in altre istruzioni scritte fornite dal Cliente e riconosciute da Google come istruzioni costituenti ai fini del presente Emendamento sul trattamento dei dati.

5.2.2 Conformità di Google con le istruzioni . A partire dalla Data di attivazione completa (al più tardi), Google rispetterà le istruzioni descritte nella Sezione 5.2.1 (Istruzioni del cliente) (anche in relazione ai trasferimenti di dati) a meno che la legge europea o nazionale a cui è soggetta Google non richieda un altro trattamento di Dati personali del cliente da parte di Google, nel qual caso Google informerà il Cliente (a meno che tale legge non vieti a Google di farlo per importanti motivi di interesse pubblico) prima di tale altra elaborazione. Per chiarezza, Google non elaborerà i dati personali del cliente per scopi pubblicitari né fornirà pubblicità nei servizi.

5.3. **Prodotti aggiuntivi**. Se Google, a sua discrezione, mette a disposizione del Cliente Prodotti aggiuntivi in conformità con i Termini dei prodotti aggiuntivi e se il Cliente sceglie di installare o utilizzare tali Prodotti aggiuntivi, i Servizi possono consentire a tali Prodotti aggiuntivi di accedere ai Dati personali del Cliente come richiesto per l'interoperabilità di i Prodotti aggiuntivi con i Servizi. Per chiarezza, questo Emendamento sul trattamento dei dati non si applica al trattamento dei dati personali in relazione alla fornitura di qualsiasi Prodotto aggiuntivo installato o utilizzato dal Cliente, inclusi i dati personali trasmessi ao da tali Prodotti aggiuntivi. Il Cliente può utilizzare la funzionalità dei Servizi per abilitare o disabilitare Prodotti aggiuntivi,

6. **Cancellazione dei dati**

6.1 **Cancellazione durante il periodo**. Google consentirà al Cliente e agli Utenti finali di eliminare i Dati del cliente durante il Periodo applicabile in modo coerente con la funzionalità dei Servizi. Se il Cliente o un Utente finale utilizza i Servizi per eliminare i Dati del cliente durante il Periodo applicabile e tali Dati del cliente non possono essere recuperati dal Cliente o da un Utente finale (ad esempio dal "cestino"), tale utilizzo costituirà un'istruzione per Google a eliminare i Dati del cliente pertinenti dai sistemi di Google in conformità con la legge applicabile. Google si atterrà a questa istruzione non appena ragionevolmente possibile ed entro un periodo massimo di 180 giorni, a meno che la legge europea o nazionale non richieda l'archiviazione.

6.2 **Cancellazione alla scadenza del termine** . In base alla Sezione 6.3 (Istruzioni per l'eliminazione differita), alla scadenza del Periodo applicabile, il Cliente ordina a Google di eliminare tutti i Dati del cliente (comprese le copie esistenti) dai sistemi di Google in conformità con la /

legge applicabile. Google rispetterà queste istruzioni non appena ragionevolmente possibile ed entro un periodo massimo di 180 giorni, a meno che la legge europea o nazionale non richieda l'archiviazione. Fatta salva la Sezione 9.1 (Accesso; Rettifica; Elaborazione limitata; Portabilità), il Cliente è responsabile dell'esportazione, prima della scadenza del Periodo applicabile, dei Dati del cliente che desidera conservare.

6.3 **Istruzione di cancellazione differita** . Nella misura in cui vengono elaborati anche i Dati del cliente coperti dalle istruzioni di cancellazione descritte nella Sezione 6.2 (Cancellazione alla scadenza del termine), alla scadenza del Periodo applicabile di cui alla Sezione 6.2, in relazione a un Contratto con un Periodo di validità, tale istruzione di cancellazione effetto rispetto a tali Dati del cliente alla scadenza del Periodo di validità. Per chiarezza, questo Emendamento sul trattamento dei dati continuerà ad applicarsi a tali Dati del cliente fino alla sua eliminazione da parte di Google.

7. **Protezione 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 e organizzative per proteggere i Dati del cliente da distruzione, perdita, alterazione, divulgazione o accesso accidentale o illegale come descritto nell'Appendice 2 (le " **Misure di sicurezza**"). Le misure di sicurezza includono misure per crittografare i dati personali; per contribuire a garantire la riservatezza, l'integrità, la disponibilità e la resilienza costanti dei sistemi e dei servizi di Google; per aiutare a ripristinare l'accesso tempestivo ai dati personali a seguito di un incidente; e per testare regolarmente l'efficacia. Google può aggiornare periodicamente le Misure di sicurezza a condizione che tali aggiornamenti non comportino il degrado della sicurezza complessiva dei Servizi.

7.1.2 Conformità alla sicurezza da parte del personale di Google . Google: (a) adotterà le misure appropriate per garantire la conformità con le Misure di sicurezza da parte dei suoi dipendenti, appaltatori e Sub-responsabili nella misura applicabile al loro ambito di prestazione, e (b) assicurerà che tutte le persone autorizzate a trattare i Dati personali del cliente siano obbligo di riservatezza.

7.1.3 Controlli di sicurezza aggiuntivi . Google metterà a disposizione Controlli di sicurezza aggiuntivi per: (a) consentire al Cliente di adottare misure per proteggere i Dati del cliente; e (b) fornire al Cliente informazioni sulla protezione, l'accesso e l'utilizzo dei Dati del cliente.

7.1.4 Assistenza per la sicurezza di Google . Google (tenendo conto della natura del trattamento dei Dati personali del Cliente e delle informazioni a disposizione di Google) assisterà il Cliente nel garantire il rispetto dei propri obblighi ai sensi degli articoli da 32 a 34 del GDPR, tramite:

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

b. rendere disponibili al Cliente Controlli di sicurezza aggiuntivi in conformità con la Sezione 7.1.3 (Controlli di sicurezza aggiuntivi);

c. rispettare i termini della Sezione 7.2 (Incidenti di dati);

d. fornire al Cliente la Documentazione sulla sicurezza in conformità con la Sezione 7.5.1 (Revisioni della documentazione sulla sicurezza) e le informazioni contenute nel Contratto applicabile, incluso questo Emendamento sul trattamento dei dati; e

e. se le sottosezioni (a) - (d) di cui sopra non sono sufficienti per consentire al Cliente di adempiere a tali obblighi, su richiesta del Cliente, fornendo ulteriore ragionevole assistenza.

7.2 **Incidenti di dati**

7.2.1 Notifica dell'incidente . Google informerà il Cliente tempestivamente e senza indebito ritardo dopo essere venuto a conoscenza di un Incidente con i dati e adotterà prontamente misure ragionevoli per ridurre al minimo i danni e proteggere i Dati del cliente.

7.2.2 Dettagli dell'incidente di dati . La notifica di Google di un Incidente di dati descriverà, per quanto possibile, la natura dell'Incidente di dati, le misure adottate per mitigare i potenziali rischi e le misure che Google consiglia al Cliente di adottare per affrontare l'Incidente di dati.

7.2.3 Consegna della notifica . Le notifiche di qualsiasi Incidente di dati verranno inviate all'indirizzo e-mail di notifica o, a discrezione di Google, tramite comunicazione diretta (ad esempio, telefonata o incontro di persona).

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

7.2.5 Nessun riconoscimento di colpa da parte di Google . La notifica o la risposta di Google a un Incidente con i dati ai sensi della presente Sezione 7.2 (Incidenti con i dati) non sarà interpretata come un riconoscimento da parte di Google di alcuna colpa o responsabilità in relazione all'Incidente di dati.

7.3. **Responsabilità e valutazione della sicurezza del cliente** .

7.3.1 Responsabilità del cliente in materia di sicurezza . Fatti salvi gli obblighi di Google ai sensi delle Sezioni 7.1 (Misure di sicurezza, controlli e assistenza di Google) e 7.2 (Incidenti sui dati) e altrove nel Contratto applicabile, il Cliente è responsabile dell'utilizzo dei Servizi e dell'archiviazione di eventuali copie dei Dati del cliente all'esterno Sistemi di Google o dei subprocessori di Google, tra cui:

un. utilizzare i Servizi e Controlli di sicurezza aggiuntivi per garantire un livello di sicurezza adeguato al rischio in relazione ai Dati del cliente;

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

e c. conservare le copie dei dati del cliente come appropriato.

7.3.2 Valutazione della sicurezza del cliente . Il Cliente accetta, in base al suo uso corrente e previsto dei Servizi, 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): (a) soddisfano le esigenze del Cliente, anche in relazione a eventuali obblighi di sicurezza del Cliente ai sensi della legge europea sulla protezione dei dati e / o della legge non europea sulla protezione dei dati, a seconda dei casi, e (b) fornire un livello di sicurezza appropriato al rischio in relazione ai dati del cliente.

7.4 **Certificazioni di conformità e rapporti SOC** . Google manterrà almeno quanto segue per i Servizi controllati al fine di valutare la continua efficacia delle Misure di sicurezza:

un. certificati per ISO 27001, ISO 27017 e ISO 27018 e

b. Rapporti SOC 2 e SOC 3 prodotti dal revisore di terze parti di Google e aggiornati annualmente in base a un controllo eseguito almeno una volta ogni 12 mesi (i " **Rapporti SOC** "). Google può aggiungere standard in qualsiasi momento. Google può sostituire un rapporto SOC con un'alternativa equivalente o migliorata.

7.5 **Revisioni e verifiche di conformità**

7.5.1 Revisioni della documentazione di sicurezza . Google renderà i rapporti SOC disponibili per la revisione da parte del Cliente per dimostrare la conformità da parte di Google ai propri obblighi ai sensi del presente Emendamento sul trattamento dei dati.

7.5.2 Diritti di revisione del cliente .

un. Se la legge europea sulla protezione dei dati si applica al trattamento dei dati personali del cliente, Google consentirà al cliente oa un revisore indipendente nominato dal cliente di condurre controlli (comprese le ispezioni) per verificare la conformità di Google ai suoi obblighi ai sensi del presente emendamento sul trattamento dei dati in conformità con la sezione 7.5. 3 (Termini commerciali aggiuntivi per revisioni e audit). Google contribuirà a tali controlli come descritto nella Sezione 7.4 (Certificazioni di conformità e rapporti SOC) e in questa Sezione 7.5 (Revisioni e controlli di conformità).

b. Se il Cliente ha stipulato le Clausole contrattuali tipo come descritto nella Sezione 10.2 (Trasferimento di dati), Google consentirà al Cliente oa un revisore indipendente nominato dal Cliente di condurre verifiche come descritto nelle Clausole contrattuali tipo in conformità alla Sezione 7.5.3 (Termini commerciali aggiuntivi per revisioni e audit).

c. Il Cliente può condurre una verifica per verificare la conformità di Google ai propri obblighi ai sensi del presente Emendamento sul trattamento dei dati esaminando la Documentazione sulla sicurezza (che riflette i risultati delle verifiche condotte dal revisore di terze parti di Google).

7.5.3 Termini commerciali aggiuntivi per revisioni e audit .

un. Il Cliente deve inviare qualsiasi richiesta di revisione del rapporto SOC 2 ai sensi della Sezione 7.5.1 o di audit ai sensi della Sezione 7.5.2 (a) o 7.5.2 (b) al Cloud Data Protection Team di Google come descritto nella Sezione 12 (Cloud Data Protection Team ; Elaborazione record).

b. In seguito alla ricezione da parte di Google di una richiesta ai sensi della Sezione 7.5.3 (a), Google e il Cliente discuteranno e concorderanno in anticipo: (i) le date ragionevoli e i controlli di sicurezza e riservatezza applicabili a qualsiasi revisione del SOC 2 rapporto di cui alla sezione 7.5.1; e (ii) la data di inizio ragionevole, l'ambito e la durata e i controlli di sicurezza e riservatezza applicabili a qualsiasi audit ai sensi della Sezione 7.5.2 (a) o 7.5.2 (b).

c. Google può addebitare una commissione (basata sui costi ragionevoli di Google) per qualsiasi verifica ai sensi della Sezione 7.5.2 (a) o 7.5.2 (b). Google fornirà al Cliente ulteriori dettagli su qualsiasi commissione applicabile e la base del suo calcolo prima di tale verifica. Il Cliente sarà responsabile di qualsiasi commissione addebitata da qualsiasi revisore incaricato dal Cliente per eseguire tale verifica.

d. Google può opporsi per iscritto a un revisore incaricato dal Cliente di condurre qualsiasi verifica ai sensi della Sezione 7.5.2 (a) o 7.5.2 (b) se il revisore non è, a giudizio ragionevole di Google, non adeguatamente qualificato o indipendente, un concorrente di Google , o altrimenti manifestamente inadatto. Qualsiasi obiezione di questo tipo da parte di Google richiederà al Cliente di nominare un altro revisore o di condurre la verifica stessa.

7.5.4 Nessuna modifica degli MCC . Nulla nella presente Sezione 7.5 (Revisioni e verifiche di conformità) varia o modifica i diritti o gli obblighi del Cliente o di Google LLC ai sensi delle Clausole contrattuali tipo stipulate come descritto nella Sezione 10.2 (Trasferimento di dati).

8. **Valutazioni e consultazioni d'impatto** . Google (tenendo conto della natura del trattamento e delle informazioni a disposizione di Google) assisterà il Cliente nel garantire il rispetto dei suoi obblighi ai sensi degli articoli 35 e 36 del GDPR, tramite:

un. fornire Controlli di sicurezza aggiuntivi in conformità con la Sezione 7.1.3 (Controlli di sicurezza aggiuntivi) e la Documentazione di sicurezza in conformità con la Sezione 7.5.1 (Revisioni della documentazione di sicurezza);

b. fornire le informazioni contenute nel Contratto applicabile, incluso questo Emendamento sul trattamento dei dati; e

c. se le sottosezioni (a) e (b) di cui sopra non sono sufficienti per consentire al Cliente di adempiere a tali obblighi, su richiesta del Cliente, fornendo ulteriore ragionevole assistenza.

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

9.1 **Accesso; Rettifica; Elaborazione limitata; Portabilità** . Durante il Periodo applicabile, Google consentirà al Cliente, in modo coerente con la funzionalità dei Servizi, di accedere, rettificare e limitare l'elaborazione dei Dati del Cliente, anche tramite la funzionalità di eliminazione fornita

da Google come descritto nella Sezione 6.1 (Eliminazione durante il Periodo di validità) e per esportare i dati del cliente.

9.2 **Richieste dell'interessato** .

9.2.1 Responsabilità del cliente per le richieste . Durante il periodo applicabile, se il team per la protezione dei dati nel cloud di Google riceve una richiesta da un soggetto interessato in relazione ai dati personali del cliente e la richiesta identifica il cliente, Google avviserà l'interessato di inviare la richiesta al cliente. Il Cliente sarà responsabile di rispondere a qualsiasi richiesta di questo tipo, incluso, ove necessario, l'utilizzo della funzionalità dei Servizi.

9.2.2 Richiesta di assistenza da parte dell'interessato di Google . Google (tenendo conto della natura del trattamento dei Dati personali del Cliente) assisterà il Cliente nell'adempimento dei propri obblighi ai sensi del Capitolo III del GDPR per rispondere alle richieste di esercizio dei diritti dell'interessato:

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

b. rispettare le Sezioni 9.1 (Accesso; Rettifica; Trattamento limitato; Portabilità) e 9.2.1 (Responsabilità del cliente per le richieste); e

c. se le sottosezioni (a) e (b) di cui sopra non sono sufficienti per consentire al Cliente di adempiere a tali obblighi, su richiesta del Cliente, fornendo ulteriore ragionevole assistenza.

10. **Trasferimento dei dati**

10.1 **Conservazione dei dati e strutture di elaborazione** . Google può archiviare ed elaborare i Dati del cliente ovunque Google o i suoi sub-responsabili abbiano strutture, soggetto a:

un. Sezione 10.2 (Trasferimento dei dati) in relazione alle Clausole contrattuali tipo o alla Soluzione di trasferimento alternativa;

e b. i Termini specifici del servizio applicabili (se presenti) in relazione alla posizione dei dati.

10.2 **Trasferimenti di dati** . Se l'archiviazione e / o l'elaborazione dei Dati personali del cliente comporta trasferimenti di Dati personali del cliente dallo SEE, dalla Svizzera o dal Regno Unito a qualsiasi paese terzo che non garantisce un livello adeguato di protezione ai sensi della legge europea sulla protezione dei dati e si applica la legge europea sulla protezione dei dati a quei trasferimenti, quindi:

un. se il Cliente (in qualità di esportatore di dati) stipula le Clausole contrattuali tipo con Google LLC (in qualità di importatore di dati) all'interno della Console di amministrazione, allora:

io. i trasferimenti saranno soggetti alle clausole contrattuali tipo; e

ii. Google garantirà che Google LLC rispetti i propri obblighi ai sensi delle clausole contrattuali tipo in relazione a tali trasferimenti;

o b. se il Cliente non stipula le Clausole contrattuali tipo come descritto nella Sezione 10.2 (a), allora:

io. se Google mette a disposizione una Soluzione di trasferimento alternativa: (A) si riterrà che il Cliente la utilizzi e intraprenderà qualsiasi azione (che può includere l'esecuzione di documenti) strettamente necessaria per dargli pieno effetto; e (B) Google garantirà che i trasferimenti siano effettuati in conformità con tale Soluzione di trasferimento alternativa; o

ii. se una Soluzione di trasferimento alternativa non è resa disponibile da Google: (A) il Cliente (in qualità di esportatore di dati) si riterrà che abbia stipulato le Clausole contrattuali tipo con Google LLC (in qualità di importatore di dati); (B) i trasferimenti saranno soggetti alle clausole contrattuali tipo; e (C) Google garantirà che Google LLC rispetti i propri obblighi ai sensi delle Clausole contrattuali tipo in relazione a tali trasferimenti; e

c. se il Cliente ha stipulato le clausole contrattuali tipo ma successivamente determina ragionevolmente che non forniscono un livello di protezione adeguato, allora:

io. se una Soluzione di trasferimento alternativa è resa disponibile da Google, il Cliente può, notificando a Google LLC tramite il Cloud Data Protection Team di Google in conformità con la Sezione 12.1 (Cloud Data Protection Team di Google), risolvere qualsiasi Clausola contrattuale tipo applicabile ai sensi della Sezione 10.2 (a), in modo tale che si applichi la Sezione 10.2 (b) (i); o

ii. se una Soluzione di trasferimento alternativa non è resa disponibile da Google, il Cliente può risolvere immediatamente il Contratto dandone notifica a Google.

10.3 **Informazioni sul data center** . Le informazioni sull'ubicazione dei data center di Google sono disponibili all'indirizzo: https://www.google.com/about/datacenters/inside/locations/index.html (come può essere aggiornato da Google di volta in volta).

10.4 **Divulgazione di informazioni riservate contenenti dati personali** . Se il Cliente ha stipulato clausole contrattuali tipo come descritto nella Sezione 10.2 (Trasferimento di dati), Google, nonostante qualsiasi termine contrario nel Contratto applicabile, garantirà che qualsiasi divulgazione delle Informazioni riservate del Cliente contenenti dati personali e qualsiasi notifica relativa a qualsiasi divulgazione di questo tipo, sarà effettuata in conformità con tali clausole contrattuali tipo.

11. **Subprocessori**

11.1 **Consenso all'incarico del sub-responsabile** . Il Cliente autorizza specificamente l'incarico in qualità di Subprocessori di: (a) quelle entità elencate alla Data di entrata in vigore della Modifica all'URL specificato nella Sezione 11.2 (Informazioni sui Subprocessori); e (b) tutti gli altri affiliati di Google di volta in volta. Inoltre, fatta salva la Sezione 11.4 (Opportunità di opporsi a modifiche di subprocessori), il Cliente generalmente autorizza l'incarico come Subprocessors di qualsiasi altra terza parte (" **New Third Party Subprocessors**"). Se il Cliente ha stipulato clausole contrattuali tipo come descritto nella Sezione 10.2 (Trasferimento di dati), le autorizzazioni di cui sopra costituiscono il previo consenso scritto del Cliente al subappalto da parte di Google LLC del trattamento dei Dati del cliente.

11.2 **Informazioni sui subprocessori** . Le informazioni sui subprocessori, comprese le loro funzioni e ubicazioni, sono disponibili su https://gsuite.google.com/intl/en/terms/subprocessors.html (come può essere aggiornato da Google di volta in volta in conformità con questo Emendamento sul trattamento dei dati).

11.3 **Requisiti per l'incarico del sub-responsabile** . Quando coinvolge un subprocessore, Google:

un. garantire tramite un contratto scritto che:

io. il Sub-responsabile accede e utilizza i Dati del cliente solo nella misura necessaria per adempiere agli obblighi a lui subappaltati, e lo fa in conformità con il Contratto (incluso questo Emendamento sull'elaborazione dei dati) e le Clausole contrattuali tipo o la Soluzione di trasferimento alternativa, come applicabile ai sensi della Sezione 10.2 (Trasferimento di dati); e

ii. se il GDPR si applica al trattamento dei dati personali del cliente, gli obblighi di protezione dei dati descritti nell'articolo 28, paragrafo 3, del GDPR, come descritto in questo emendamento sul trattamento dei dati, sono imposti al sub-responsabile del trattamento; e

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

11.4 **Opportunità di opporsi alle modifiche del subprocessore** .

un. Quando un nuovo sub-responsabile del trattamento di terze parti viene assunto durante il periodo applicabile, Google, almeno 30 giorni prima che il nuovo sub-responsabile del trattamento di terze parti inizi a elaborare i dati del cliente, informerà il cliente dell'impegno (inclusi il nome e l'ubicazione del relativo sub-responsabile del trattamento e le attività si esibirà).

b. Il Cliente può, entro 90 giorni dalla notifica dell'impegno di un nuovo sub-responsabile del trattamento di terze parti, opporsi risolvendo immediatamente il contratto applicabile mediante notifica a Google. Questo diritto di recesso è l'unico ed esclusivo rimedio del Cliente se il Cliente si oppone a qualsiasi nuovo sub-responsabile del trattamento di terze parti.

12. **Cloud Data Protection Team; Elaborazione dei record**

12.1 **Cloud Data Protection Team di Google** . Il team per la protezione dei dati nel cloud di Google può essere contattato dagli amministratori del cliente all'indirizzo https://support.google.com/a/contact/googlecloud_dpr (mentre gli amministratori hanno eseguito l'accesso al proprio account amministratore) e / o dal cliente fornendo una notifica a Google come descritto nell'Accordo applicabile.

12.2. **Record di elaborazione di Google** . Nella misura in cui il GDPR richiede a Google di raccogliere e conservare registrazioni di determinate informazioni relative al Cliente, il Cliente, ove richiesto, utilizzerà la Console di amministrazione per fornire tali informazioni e mantenerle accurate e aggiornate. Google può rendere disponibili tali informazioni alle Autorità di controllo se richiesto dal GDPR.

13. **Responsabilità**

13.1 Limite di **responsabilità** . Se le Clausole del contratto tipo sono state stipulate come descritto nella Sezione 10.2 (Trasferimenti di dati), soggetta alla Sezione 13.2 (Esclusioni del limite di responsabilità), la responsabilità totale combinata di una delle parti e delle sue Affiliate nei confronti dell'altra parte e delle sue Affiliate ai sensi o in connessione con l'Accordo applicabile e tali Clausole di contratto tipo combinate saranno limitate al Limite di responsabilità concordato per la parte interessata.

13.2 **Esclusioni del** limite di **responsabilità** . Nulla nella Sezione 13.1 (Limite di responsabilità) influenzerà i restanti termini dell'Accordo applicabile in materia di responsabilità (comprese eventuali esclusioni specifiche da qualsiasi limitazione di responsabilità).

14. **Terzo beneficiario**

Nonostante qualsiasi disposizione contraria nel Contratto applicabile, dove Google LLC non è una parte di tale Contratto, Google LLC sarà una terza parte beneficiaria delle Sezioni 7.5 (Revisioni e controlli di conformità), 10.2 (Trasferimento di dati), 11.1 (Consenso Incarico del sub-responsabile) e 13 (Responsabilità).

15 **Effetto della modifica**

Nonostante qualsiasi disposizione contraria nel Contratto applicabile, nella misura di qualsiasi conflitto o incoerenza tra i termini di questo Emendamento sul trattamento dei dati e il resto del Contratto applicabile, prevarrà questo Emendamento sul trattamento dei dati. Per chiarezza, se il Cliente ha stipulato più di un Accordo, questo Emendamento sul trattamento dei dati modificherà ciascuno degli Accordi separatamente.

Appendice 1: Oggetto e dettagli del trattamento dei dati

Argomento

Fornitura da parte di Google dei Servizi e dei Servizi di assistenza tecnica al Cliente.

Durata del trattamento

Il Periodo applicabile più il periodo dalla scadenza di tale Periodo fino alla cancellazione di tutti i Dati del cliente da parte di Google in conformità con l'Emendamento sull'elaborazione dei dati.

Natura e finalità del trattamento

Google elaborerà i Dati personali del cliente allo scopo di fornire i Servizi e i TSS al Cliente in conformità con l'Emendamento sull'elaborazione dei dati.

Categorie di dati

Dati relativi a persone fisiche fornite a Google tramite i Servizi, dal (o su indicazione del) Cliente o Utenti finali.

Soggetti interessati

Gli interessati includono le persone su cui vengono forniti i dati a Google tramite i Servizi da (o su indicazione del) Cliente o Utenti finali.

Appendice 2: misure di sicurezza

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

1. Data Center e sicurezza di rete

(a) Data Center.

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

Ridondanza. I sistemi infrastrutturali sono stati progettati per eliminare i singoli punti di guasto e ridurre al minimo l'impatto dei rischi ambientali previsti. Doppi circuiti, interruttori, reti o altri dispositivi necessari aiutano a fornire questa ridondanza. I Servizi sono progettati per consentire a Google di eseguire determinati tipi di manutenzione preventiva e correttiva senza interruzioni. Tutte le apparecchiature e le strutture ambientali hanno documentato procedure di manutenzione preventiva che descrivono in dettaglio il processo e la frequenza delle prestazioni in conformità con le specifiche del produttore o interne.

Energia. I sistemi di alimentazione elettrica del data center sono progettati per essere ridondanti e manutenibili senza impatto sulle operazioni continue, 24 ore al giorno, 7 giorni alla settimana. Nella maggior parte dei casi, viene fornita una fonte di alimentazione primaria e alternativa, ciascuna con la stessa capacità, per i componenti dell'infrastruttura critica nel data center. L'alimentazione di backup è fornita da vari meccanismi come le batterie UPS (Uninterruptible Power Supply), che forniscono una protezione dell'alimentazione costantemente affidabile durante le interruzioni di corrente, i blackout, la sovratensione, la sottotensione e le condizioni di frequenza fuori tolleranza. Se l'alimentazione di rete viene interrotta, l'alimentazione di backup è progettata per fornire alimentazione transitoria al data center, a piena capacità, per un massimo di 10 minuti fino a quando i sistemi del generatore diesel non prendono il sopravvento. I generatori diesel sono in grado di avviarsi automaticamente in pochi secondi per fornire energia elettrica di emergenza sufficiente per far funzionare il data center a piena capacità in genere per un periodo di giorni.

Sistemi operativi server . I server di Google utilizzano un'implementazione basata su Linux personalizzata per l'ambiente dell'applicazione. I dati vengono archiviati utilizzando algoritmi proprietari per aumentare la sicurezza e la ridondanza dei dati. Google utilizza un processo di revisione del codice per aumentare la sicurezza del codice utilizzato per fornire i Servizi e migliorare i prodotti di sicurezza negli ambienti di produzione.

Continuità aziendale . Google ha progettato, pianifica e testa regolarmente i propri programmi di pianificazione della continuità operativa / ripristino di emergenza.

(b) Reti e trasmissione .

Trasmissione dei dati . I data center sono generalmente connessi tramite collegamenti privati ad alta velocità per fornire un trasferimento dati sicuro e veloce tra i data center. Questo è progettato per impedire che i dati vengano letti, copiati, alterati o rimossi senza autorizzazione durante il trasferimento elettronico o il trasporto o durante la registrazione su supporti di memorizzazione dati. Google trasferisce i dati tramite protocolli standard di Internet.

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

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

1. controllare strettamente le dimensioni e la composizione della superficie di attacco di Google attraverso misure preventive;
2. impiegando controlli di rilevamento intelligenti nei punti di ingresso dei dati; e
3. impiegando tecnologie che rimediano automaticamente a determinate situazioni pericolose.

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

Tecnologie di crittografia . Google rende disponibile la crittografia HTTPS (denominata anche connessione SSL o TLS). I server di Google supportano lo scambio di chiavi crittografiche Diffie-Hellman con curva ellittica temporanea firmata con RSA ed ECDSA. Questi metodi Perfect Forward Secrecy (PFS) aiutano a proteggere il traffico e riducono al minimo l'impatto di una chiave compromessa o di un'innovazione crittografica.

2. Accesso e controlli del sito.

(a) Controlli del sito.

Operazione di sicurezza del data center in loco . I data center di Google mantengono un'operazione di sicurezza in loco responsabile di tutte le funzioni di sicurezza del data center fisico 24 ore al giorno, 7 giorni alla settimana. Il personale operativo di sicurezza in loco monitora le telecamere TV a circuito chiuso (CCTV) e tutti i sistemi di allarme. Il personale operativo di sicurezza in loco esegue regolarmente pattugliamenti interni ed esterni del data center.

Procedure di accesso al data center. Google mantiene procedure di accesso formali per consentire l'accesso fisico ai data center. I data center sono ospitati in strutture che richiedono l'accesso con chiave elettronica con scheda, con allarmi collegati alle operazioni di sicurezza in loco. Tutti i partecipanti al data center sono tenuti a identificarsi e a mostrare un documento di identità alle operazioni di sicurezza in loco. L'accesso ai data center è consentito solo a dipendenti, appaltatori e visitatori autorizzati. Solo i dipendenti e gli appaltatori autorizzati possono richiedere l'accesso con chiave elettronica a queste strutture. Le richieste di accesso alla chiave della scheda elettronica del data center devono essere effettuate tramite e-mail, e richiedono l'approvazione del manager del richiedente e del direttore del data center. Tutti gli altri entranti che richiedono l'accesso temporaneo al data center devono: (i) ottenere l'approvazione anticipata dai responsabili del data center per il data center specifico e le aree interne che desiderano visitare; (ii) accedere alle operazioni di sicurezza in loco; e (iii) fare riferimento a un record di accesso al data center approvato che identifichi la persona come approvata. (i) ottenere preventivamente l'approvazione dei responsabili del data center per il data center specifico e le aree interne che desiderano visitare; (ii) accedere alle operazioni di sicurezza in loco; e (iii) fare riferimento a un record di accesso al data center approvato che identifichi la persona come approvata. (i) ottenere preventivamente l'approvazione dei responsabili del data center per il data center specifico e le aree interne che desiderano visitare; (ii) accedere alle operazioni di sicurezza in loco; e (iii) fare riferimento a un record di accesso al data center approvato che identifichi la persona come approvata.

Dispositivi di sicurezza per data center in loco. I data center di Google utilizzano una chiave elettronica e un sistema di controllo degli accessi biometrico collegato a un allarme di sistema. Il sistema di controllo accessi monitora e registra la chiave della scheda elettronica di ogni individuo e quando accede alle porte perimetrali, alla spedizione e al ricevimento e ad altre aree critiche. Le attività non autorizzate e i tentativi di accesso non riusciti vengono registrati dal sistema di controllo degli accessi e analizzati, come appropriato. L'accesso autorizzato a tutte le operazioni aziendali e ai data center è limitato in base alle zone e alle responsabilità lavorative dell'individuo. Le porte tagliafuoco dei data center sono allarmate. Le telecamere a circuito chiuso sono in funzione sia all'interno che all'esterno dei data center. Il posizionamento delle telecamere è stato progettato per coprire aree strategiche tra cui, tra le altre, il perimetro, le porte dell'edificio del data center e la spedizione / ricezione. Il personale addetto alle operazioni di sicurezza in loco gestisce le apparecchiature di monitoraggio, registrazione e controllo CCTV. Cavi protetti in tutti i data center collegano le apparecchiature CCTV. Le telecamere registrano sul posto tramite videoregistratori digitali 24 ore al giorno, 7 giorni alla settimana. I record di sorveglianza vengono conservati per un massimo di 30 giorni in base all'attività. Il posizionamento delle telecamere è stato progettato per coprire aree strategiche tra cui, tra le altre, il perimetro, le porte dell'edificio del data center e la spedizione / ricezione. Il personale addetto alle operazioni di sicurezza in loco gestisce le apparecchiature di monitoraggio, registrazione e controllo CCTV. Cavi protetti in tutti i data center collegano le apparecchiature CCTV. Le telecamere registrano sul posto tramite videoregistratori digitali 24 ore al giorno, 7 giorni alla settimana. I record di sorveglianza vengono conservati per un massimo di 30 giorni in base all'attività. Il posizionamento delle telecamere è stato progettato per coprire aree strategiche tra cui, tra le altre, il perimetro, le porte dell'edificio del data center e la spedizione / ricezione. Il personale addetto alle operazioni di sicurezza in loco gestisce le apparecchiature di monitoraggio, registrazione e controllo CCTV. Cavi protetti in tutti i data center collegano le apparecchiature CCTV. Le telecamere registrano sul posto tramite videoregistratori digitali 24 ore al giorno, 7 giorni alla settimana. I record di sorveglianza vengono conservati per un massimo di 30 giorni in base all'attività. Il personale addetto alle operazioni di sicurezza in loco gestisce le apparecchiature di monitoraggio, registrazione e controllo CCTV. Cavi protetti in tutti i data center collegano le apparecchiature CCTV. Le telecamere registrano sul posto tramite videoregistratori digitali 24 ore al giorno, 7 giorni alla settimana. I record di sorveglianza vengono conservati per un massimo di 30 giorni in base all'attività. Il personale addetto alle operazioni di sicurezza in loco gestisce le apparecchiature di monitoraggio, registrazione e controllo CCTV. Cavi protetti in tutti i data center collegano le apparecchiature CCTV. Le telecamere registrano sul posto tramite videoregistratori digitali 24 ore al giorno, 7 giorni alla settimana. I record di sorveglianza vengono conservati per un massimo di 30 giorni in base all'attività.

(b) Controllo degli accessi.

Personale addetto alla sicurezza dell'infrastruttura . Google dispone e mantiene una politica di sicurezza per il proprio personale e richiede formazione sulla sicurezza come parte del pacchetto di formazione per il proprio personale. Il personale addetto alla sicurezza dell'infrastruttura di Google è responsabile del monitoraggio continuo dell'infrastruttura di sicurezza di Google, dell'analisi dei Servizi e della risposta agli incidenti di sicurezza.

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

Procedure e politiche interne di accesso ai dati - Politica di accesso. I processi e le politiche di accesso ai dati interni di Google sono progettati per impedire a persone e / o sistemi non autorizzati di accedere ai sistemi utilizzati per elaborare i dati personali. Google progetta i suoi sistemi per: (i) consentire solo alle persone autorizzate di accedere ai dati a cui sono autorizzati ad accedere; e (ii) garantire che i dati personali non possano essere letti, copiati, modificati o rimossi senza autorizzazione durante l'elaborazione, l'uso e dopo la registrazione. I sistemi sono progettati per rilevare qualsiasi accesso inappropriato. Google utilizza un sistema di gestione degli accessi centralizzato per controllare l'accesso

del personale ai server di produzione, e fornisce l'accesso solo a un numero limitato di personale autorizzato. I sistemi/

di autenticazione e autorizzazione di Google utilizzano certificati SSH e chiavi di sicurezza e sono progettati per fornire a Google meccanismi di accesso sicuri e flessibili. Questi meccanismi sono progettati per concedere solo i diritti di accesso approvati agli host del sito, ai registri, ai dati e alle informazioni di configurazione. Google richiede l'uso di ID utente univoci, password complesse, autenticazione a due fattori e elenchi di accesso attentamente monitorati per ridurre al minimo il potenziale di utilizzo non autorizzato dell'account. La concessione o la modifica dei diritti di accesso si basa su: responsabilità lavorative del personale autorizzato; requisiti di mansione necessari per eseguire compiti autorizzati; e la necessità di conoscere le basi. Anche la concessione o la modifica dei diritti di accesso deve essere conforme alle politiche interne di accesso ai dati e alla formazione. Le approvazioni sono gestite da strumenti del flusso di lavoro che conservano i record di controllo di tutte le modifiche. L'accesso ai sistemi viene registrato per creare un audit trail per la responsabilità. Laddove le password vengono utilizzate per l'autenticazione (ad esempio, l'accesso alle workstation), vengono implementate politiche per le password che seguono almeno le pratiche standard del settore. Questi standard includono limitazioni al riutilizzo delle password e una sufficiente robustezza della password.

3. Dati

(a) Archiviazione, isolamento e registrazione dei dati.

Google memorizza i dati in un ambiente multi-tenant su server di proprietà di Google. Fatte salve eventuali istruzioni contrarie del Cliente (ad esempio, sotto forma di selezione della posizione dei dati), Google replica i Dati del cliente tra più data center dislocati geograficamente. Google inoltre isola logicamente i dati del cliente e separa logicamente i dati di ciascun utente finale dai dati di altri utenti finali e i dati per un utente finale autenticato non verranno visualizzati a un altro utente finale (a meno che l'ex utente finale o un amministratore non consenta ai dati di essere condiviso).

Al cliente verrà dato il controllo su specifiche politiche di condivisione dei dati. Tali politiche, in conformità con la funzionalità dei Servizi, consentiranno al Cliente di determinare le impostazioni di condivisione del prodotto applicabili agli Utenti finali per scopi specifici. Il Cliente può scegliere di utilizzare la funzionalità di registrazione che Google rende disponibile tramite i Servizi.

(b) Dischi disattivati e politica di cancellazione del disco.

I dischi contenenti dati potrebbero riscontrare problemi di prestazioni, errori o guasti hardware che ne determinano la rimozione ("Disco disattivato"). Ogni disco disattivato è soggetto a una serie di processi di distruzione dei dati (la "politica di cancellazione del disco") prima di lasciare la sede di Google per essere riutilizzato o distrutto. I dischi disattivati vengono cancellati in un processo in più fasi e completati da almeno due validatori indipendenti. I risultati della cancellazione vengono registrati dal numero di serie del disco disattivato per il monitoraggio. Infine, il disco rimosso dalle autorizzazioni cancellato viene rilasciato nell'inventario per il riutilizzo e la ridistribuzione. Se, a causa di un guasto hardware, il disco disattivato non può essere cancellato, viene archiviato in modo sicuro fino a quando non può essere distrutto. Ogni struttura viene controllata regolarmente per monitorare la conformità con la politica di cancellazione del disco.

4. Sicurezza del personale

Il personale di Google è tenuto a comportarsi in modo coerente con le linee guida dell'azienda in materia di riservatezza, etica aziendale, utilizzo appropriato e standard professionali. Google esegue controlli del background ragionevolmente appropriati nella misura consentita dalla legge e in conformità con il diritto del lavoro locale e le normative legali applicabili.

Il personale è tenuto a sottoscrivere un accordo di riservatezza e deve accusare ricevuta e conformità alle norme sulla riservatezza e sulla privacy di Google. Al personale viene fornita formazione sulla sicurezza. Il personale che gestisce i Dati dei clienti è tenuto a completare requisiti aggiuntivi appropriati al proprio ruolo (ad esempio, certificazioni). Il personale di Google non elaborerà i Dati del cliente senza autorizzazione.

5. Protezione del sottoprocessore.

Prima di inserire i subprocessori, Google conduce una verifica delle pratiche di sicurezza e privacy dei subprocessori per garantire che i subprocessori forniscano un livello di sicurezza e privacy appropriato al loro accesso ai dati e all'ambito dei servizi che sono incaricati di fornire. Una volta che Google ha valutato i rischi presentati dal Sub-responsabile, quindi soggetti ai requisiti descritti nella Sezione 11.3 (Requisiti per l'incarico del Sub-responsabile) di questo Emendamento sul trattamento dei dati, il Sub-responsabile è tenuto a stipulare i termini del contratto di sicurezza, riservatezza e privacy appropriati.