# Termini per il trattamento dei dati di Google Ads

Google e la controparte che accetta i presenti termini (il "**Cliente**") hanno stipulato un contratto per la prestazione dei Servizi del Titolare del trattamento (come di volta in volta modificati, il "**Contratto**").

I Termini per il trattamento dei dati di Google Ads (incluse le appendici, "**Termini per il trattamento dei dati**") sono stipulati tra Google e il Cliente e sono parte integrante del Contratto. I presenti Termini per il trattamento dei dati entreranno in vigore a decorrere dalla Data di efficacia degli stessi e sostituiranno qualsiasi accordo precedentemente applicabile (inclusi eventuali emendamenti o allegati sul trattamento dei dati relativi ai Servizi del Titolare del trattamento).

In caso di accettazione dei presenti Termini per il trattamento dei dati per conto del Cliente, la parte che accetta garantisce di: (a) disporre dei poteri legali necessari per vincolare il Cliente ai presenti Termini per il trattamento dei dati; (b) avere letto e compreso i presenti Termini per il trattamento dei dati; e (c) accettare i presenti Termini per il trattamento dei dati per conto del Cliente. Qualora la parte che accetta non fosse titolare dei poteri necessari a vincolare il Cliente, dovrà astenersi dall'accettare i presenti Termini contrattuali per il trattamento dei dati.

## 1. Introduzione

I presenti Termini per il trattamento dei dati riflettono l'accordo tra le parti in relazione ai termini che regolano il trattamento di determinati dati con riferimento alla Normativa europea sulla Protezione dei Dati e a determinate Normative non europee sulla Protezione dei Dati.

## 2. Definizioni e interpretazione

2.1 Nei presenti Termini per il trattamento dei dati:

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

Per "**CCS**" si intendono le Clausole Contrattuali Standard del Cliente e/o le Clausole Contrattuali Standard(da responsabile a responsabile, esportatore Google), a seconda dei casi.

Per "**CCS (da responsabile a responsabile)**" si intendono i termini indicati all'indirizzo business.safety.google/adsprocessorterms/sccs/p2p.

Per "**CCS (da responsabile a responsabile, esportatore Google)**" si intendono i termini indicati all'indirizzo business.safety.google/adsprocessorterms/sccs/p2p-intra-group.

Per "**CCS (da responsabile a titolare)**" si intendono i termini indicati all'indirizzo business.safety.google/adsprocessorterms/sccs/p2c.

Per "**CCS (da titolare a responsabile)**" si intendono i termini indicati all'indirizzo business.safety.google/adsprocessorterms/sccs/c2p.

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

Per "**Certificazione ISO 27001**" si intende la certificazione ISO/IEC 27001:2013 o una certificazione equivalente relativa ai Servizi del Responsabile del trattamento.

Per "**Data di efficacia dei Termini**" si intende, a seconda dei casi:

(a) Il 25 maggio 2018, se il Cliente ha selezionati l'opzione "accettare" o le parti hanno accettato in altra sede i presenti Termini per il trattamento dei dati in tale data o precedentemente; oppure

(b) La data in cui il Cliente ha selezionati l'opzione "accettare" o le parti hanno accettato in altra sede i presenti Termini per il trattamento dei dati, qualora tale data sia successiva al 25 maggio 2018.

Per "**Dati personali del Cliente**" si intendono i dati personali trattati da Google per conto del Cliente nell'ambito della prestazione, da parte di Google, dei Servizi del Responsabile del trattamento.

Per "**Documentazione in materia di sicurezza**" si intendono i certificati relativi alla Certificazione ISO 27001 e qualsiasi altra certificazione o documentazione in materia di sicurezza messa a disposizione da Google in relazione ai Servizi del Responsabile del trattamento.

Per "**FDPA svizzero**" si intende la Legge federale sulla protezione dei dati del 19 giugno 1992 (Svizzera).

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

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

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

Per "**Google**" si intende la Società di Google parte del Contratto.

Per "**Incidente relativo ai dati**" si intende una violazione del sistema di sicurezza di Google che comporta la distruzione accidentale o dolosa, la perdita, l'alterazione, la divulgazione non autorizzata o l'accesso ai Dati personali del cliente presenti nei sistemi gestiti o altrimenti controllati da Google. Gli "Incidenti relativi ai dati" non includono le attività o i tentativi falliti di compromettere la sicurezza dei Dati personali del Cliente, tra cui tentativi di accesso falliti, ping, scansioni delle porte, attacchi denial-of-service e altri tipi di attacchi di rete su firewall o sistemi di rete.

Per "**Indirizzo email di notifica**" si intende l'indirizzo email indicato dal Cliente, tramite l'interfaccia utente dei Servizi del Responsabile del trattamento o altri mezzi simili forniti da Google, per la ricezione di determinate notifiche concernenti i presenti Termini per il trattamento dei dati trasmesse da Google.

Il termine "**Istruzioni**" ha il significato descritto nella Sezione 5.2 (Istruzioni del Cliente).

Per “**Leggi europee**” si intendono, a seconda dei casi: (a) la normativa UE o di uno Stato Membro dell'UE (se il GDPR dell'Unione Europea è applicabile al trattamento dei Dati personali del Cliente); e (b) le leggi del Regno Unito o di una parte del Regno Unito (se il GDPR del Regno Unito è applicabile al trattamento dei Dati personali del Cliente).

Il termine “**Misure di sicurezza**” ha il significato descritto nella Sezione 7.1.1 (Misure di sicurezza di Google).

Per “**Normativa europea sulla Protezione dei Dati**” si intendono, a seconda dei casi: (a) il GDPR; e/o (b) l'FDPA svizzero.

Per “**Normativa non europea sulla Protezione dei Dati**” si intendono le leggi sulla protezione dei dati o sulla privacy in vigore al di fuori dello SEE, della Svizzera e del Regno Unito.

Il termine “**Nuovo Sub-responsabile**” ha il significato descritto nella Sezione 11.1 (Consenso per l'incarico del Sub-responsabile).

Per “**Paese Adeguato**”si intende:

(a) Per i dati trattati soggetti al GDPR dell'Unione Europea: i paesi SEE o un paese o territorio che sia stato riconosciuto come garante di un livello adeguato di protezione dei dati ai sensi del GDPR dell'Unione Europea;

(b) Per i dati trattati soggetti al GDPR del Regno Unito: il Regno Unito o un paese o territorio che sia stato riconosciuto come garante di un livello adeguato di protezione dei dati ai sensi del GDPR del Regno Unito e del Data Protection Act del 2018; e/o

(c) Per i dati trattati soggetti all'FDPA svizzero: la Svizzera o un paese o territorio che sia (i) incluso nell'elenco degli stati la cui legislazione garantisce una protezione adeguata come pubblicato dall'Incaricato federale della protezione dei dati e della trasparenza svizzero o (ii) riconosciuto come garante di un livello adeguato di protezione dei dati da parte del Consiglio federale svizzero ai sensi dell'FDPA svizzero, in ogni caso, oltre che sulla base di un accordo quadro facoltativo relativo alla protezione dei dati.

Per “**Periodo di validità**” si intende il periodo che va dalla Data di efficacia dei termini fino all’interruzione della fornitura da parte di Google dei Servizi del Responsabile ai sensi del Contratto.

Per “**Prodotto aggiuntivo**” si intende un prodotto, servizio o applicazione fornito da Google o da terze parti, che: (a) non fa parte dei Servizi del Titolare del trattamento; e (b) è accessibile e utilizzabile dall'interfaccia utente dei Servizi del Titolare del trattamento oppure è integrato in altro modo ai Servizi del Titolare.

Per “**SEE**” si intende lo Spazio Economico Europeo.

Per “**Servizi del Responsabile del trattamento**” si intendono i servizi applicabili elencati all'indirizzo business.safety.google/adsservices.

Per “**Società Google**” si intendono Google LLC (precedentemente nota come Google Inc.), Google Ireland Limited o qualsiasi altra o qualsiasi altra entità che direttamente o indirettamente controlla, è controllata da, o è soggetta a controllo comune con Google LLC.

Per “**Soluzione alternativa di trasferimento**” si intende una soluzione diversa dalle CCS che consente il trasferimento legittimo di dati personali a un paese terzo in conformità con la Legislazione europea sulla protezione dei dati, come ad esempio un accordo quadro sulla protezione dei dati in relazione al quale le realtà che ne fanno parte garantiscono una protezione adeguata.

Per “**Sub-responsabili**” si intendono terze parti autorizzate, ai sensi dei presenti Termini per il trattamento dei dati, a eseguire l'accesso logico e al trattamento dei Dati personali del Cliente al fine di fornire parte dei Servizi del Responsabile e la relativa assistenza tecnica.

Per “**Termini aggiuntivi relativi alla Normativa non europea sulla Protezione dei Dati**” si intendono i Termini aggiuntivi a cui si fa riferimento nell'Allegato 3, che riflettono l'accordo tra le parti sui termini che regolano il trattamento di determinati dati in relazione a determinate Normative non europee sulla protezione dei dati.

Per “**Tool per gli interessati**” si intende uno strumento (se esistente) messo a disposizione degli interessati da una Società Google, e che permette a Google di rispondere in modo diretto e standardizzato a determinate richieste provenienti dagli interessati relative ai Dati personali del Cliente (per esempio, le impostazioni relative alla pubblicità online o un plug-in del browser per la disattivazione).

2.2 I termini “**titolare**”, “**interessato**”, “**dati personali**”, “**trattamento**” e “**responsabile**” sono utilizzati nei presenti Termini per il trattamento dei dati con il significato loro attribuito nel GDPR mentre i termini “**importatore di dati**” ed “**esportatore di dati**” hanno il significato specificato nelle CCS applicabili.

2.3 Il verbo “**includere**” ed espressioni quali “**tra cui**” hanno il significato di “a titolo esemplificativo”. Gli esempi contenuti nei presenti Termini per il trattamento dei dati sono a scopo illustrativo e non si intendono esaustivi rispetto a un determinato concetto.

2.4 Qualsiasi riferimento a quadri normativi, leggi scritte o altri atti legislativi riguarda questi ultimi così come di volta in volta emendati o ripromulgati.

2.5 Qualora qualsiasi versione tradotta dei presenti Termini per il trattamento dei dati non fosse coerente con la versione in lingua inglese, prevarrà quest'ultima.

## 3. Durata dei presenti Termini per il trattamento dei dati

I presenti Termini per il trattamento dei dati entreranno in vigore a decorrere dalla Data di efficacia degli stessi. A prescindere dal fatto che il Contratto sia risolto o scaduto, i presenti Termini per il trattamento dei dati resteranno in vigore fino alla cancellazione da parte di Google di tutti i Dati personali del Cliente come descritto nei presenti Termini per il trattamento dei dati, momento in cui scadranno automaticamente.

## 4. Applicazione dei presenti Termini per il trattamento dei dati

4.1 **Applicazione della Normativa europea sulla Protezione dei Dati**. Le Sezioni dalla 5 (Trattamento dei dati) alla 12 (Contattare Google; Registri relativi al trattamento) (incluse) si applicheranno esclusivamente nella misura prevista dalla Normativa europea sulla Protezione dei Dati in materia di trattamento dei Dati personali del Cliente, incluse le eventualità in cui:

(a) il trattamento è svolto nel contesto delle attività di una sede del Cliente stabilita all'interno dello SEE o del Regno Unito; e/o

(b) i Dati personali del Cliente sono Dati personali relativi agli interessati che si trovano all'interno dello SEE o del Regno Unito e il trattamento implica l'offerta di beni o servizi o il monitoraggio del loro comportamento nello SEE o nel Regno Unito.

4.2 **Applicazione ai Servizi del Responsabile**. I presenti Termini per il trattamento dei dati si applicano esclusivamente ai Servizi del Responsabile del trattamento, come stabilito dalle parti nell'ambito dei presenti Termini per il trattamento dei dati, ad esempio: (a) i Servizi forniti dal Responsabile selezionati dal Cliente al momento dell’accettazione dei presenti Termini per il trattamento dei dati; oppure (b) qualora il Contratto includa per riferimento i presenti Termini per il trattamento dei dati, i Servizi forniti dal Responsabile del trattamento oggetto del Contratto.

4.3 **Inclusione di Termini aggiuntivi relativi alla Normativa non europea sulla Protezione dei Dati**. I Termini aggiuntivi relativi alla Normativa non europea sulla

Protezione dei Dati integrano i presenti Termini per il trattamento dei dati.

# 5. Trattamento dei dati

5.1 **Ruoli e conformità normativa; autorizzazioni**.

5.1.1 **Responsabilità del Titolare e del Responsabile**. Le parti prendono atto e accettano che:

(a) l'Allegato 1 descrive l'oggetto e i dettagli relativi al trattamento dei Dati personali del Cliente;

(b) Google è responsabile dei Dati personali del Cliente ai sensi della Normativa europea sulla Protezione dei Dati;

(c) il Cliente è, a seconda dei casi, titolare o responsabile dei Dati personali del Cliente ai sensi della Normativa europea sulla Protezione dei Dati; e

(d) ciascuna parte si conformerà ai relativi obblighi ad essa applicabili ai sensi della Normativa europea sulla Protezione dei Dati in merito al trattamento dei Dati personali del Cliente.

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

(a) il Cliente garantisce, su base continuativa, che il titolare del trattamento competente ha autorizzato: (i) le Istruzioni, (ii) la nomina di Google, da parte del Cliente, come altro responsabile del trattamento, e (iii) l'assegnazione dell'incarico, da parte di Google, a dei Sub-responsabili come descritto nella Sezione 11 (Sub-responsabili);

(b) il Cliente trasmetterà immediatamente al titolare del trattamento competente qualsiasi comunicazione fornita da Google ai sensi delle Sezioni 5.4 (Notifiche relative alle Istruzioni), 7.2.1 (Notifica dell'incidente), 11.4 (Facoltà di opporsi alla sostituzione del Sub-responsabile) o correlata a qualsiasi CCS; e

(c) il Cliente potrà mettere a disposizione del titolare del trattamento competente qualsiasi informazione messa a disposizione da Google ai sensi delle Sezioni 7.4 (Certificazione di sicurezza), 10.5 (Informazioni sui data center) e 11.2 (Informazioni sui Sub-responsabili).

5.2 **Istruzioni del Cliente**. Con la stipula dei presenti Termini per il trattamento dei dati, il Cliente dà incarico a Google di trattare i Dati personali del Cliente in assoluta conformità con le leggi in vigore, ossia: (a) di fornire i Servizi del Responsabile del trattamento e la relativa assistenza tecnica; (b) come ulteriormente specificato in merito all'utilizzo da parte del Cliente dei Servizi del Responsabile (incluse le impostazioni e altre funzionalità dei Servizi del Responsabile) e della relativa assistenza tecnica; (c) come documentato nel modulo del Contratto (inclusi i presenti Termini per il trattamento dei dati); e (d) come ulteriormente documentato in ogni altra istruzione scritta fornita dal Cliente e riconosciuta da Google come istruzione ai fini dei presenti Termini per il trattamento dei dati (collettivamente le "**Istruzioni**").

5.3 **Conformità di Google alle Istruzioni**. Google agirà in maniera conforme alle Istruzioni, salvo il caso in cui ciò fosse vietato dalle Leggi europee.

5.4 **Notifiche relative alle Istruzioni**. Google invierà immediatamente una notifica al Cliente nel caso in cui Google ritenga che: (a) le Leggi europee impediscono a Google di agire in conformità con un'Istruzione; (b) un'Istruzione non è conforme alla Normativa europea sulla Protezione dei Dati; o (c) Google non è altrimenti in grado di rispettare un'Istruzione, salvo che tale notifica non sia proibita dalle Leggi europee. La presente Sezione 5.4 (Notifiche relative alle Istruzioni) non limita i diritti e gli obblighi delle parti descritti altrove nel Contratto.

5.5 **Prodotti aggiuntivi**. Se il Cliente utilizza Prodotti aggiuntivi, i Servizi del Responsabile del trattamento potrebbero consentire l'accesso di tali Prodotti aggiuntivi ai Dati personali del Cliente, secondo quanto richiesto ai fini dell'interoperabilità tra i Prodotti aggiuntivi e i Servizi del Responsabile del trattamento. Per maggiore chiarezza, i presenti Termini per il trattamento dei dati non si applicano al trattamento dei dati personali correlati alla fornitura dei Prodotti aggiuntivi utilizzati dal Cliente, inclusi i dati personali inviati o ricevuti dai Prodotti aggiuntivi.

# 6. Cancellazione dei dati

6.1 **Cancellazione durante il Periodo di validità**.

6.1.1 **Servizi del Responsabile con funzionalità di cancellazione**. Durante il Periodo di validità, se:

(a) la funzionalità dei Servizi del Responsabile comprende l'opzione per il Cliente di cancellare i Dati personali del Cliente;

(b) il Cliente utilizza i Servizi del Responsabile per cancellare determinati Dati personali del Cliente; e

(c) i Dati personali del Cliente cancellati non possono essere recuperati dal Cliente (ad esempio, dal "cestino"),

Google cancellerà i Dati personali del Cliente dai propri sistemi non appena ragionevolmente possibile ed entro un periodo massimo di 180 giorni, salvo che le Leggi europee ne richiedano la conservazione.

6.1.2 **Servizi del Responsabile senza funzionalità di cancellazione**. Durante il Periodo di validità, se la funzionalità dei Servizi del Responsabile non comprende l'opzione che consente al Cliente di cancellare i Dati personali del Cliente, Google si conformerà:

(a) a qualsiasi richiesta, purché ragionevole, del Cliente di facilitare tale cancellazione, per quanto ciò sia possibile, tenuto conto della natura e della funzionalità dei Servizi del Responsabile del trattamento e salvo che le Leggi europee ne richiedano la conservazione; e

(b) alle pratiche di conservazione dei dati descritte alla pagina policies.google.com/technologies/ads.

Google potrebbe addebitare una commissione (basata sulle spese ragionevolmente sostenute da Google) per gli interventi di cancellazione dei dati ai sensi della Sezione 6.1.2 (a). Google fornirà al Cliente ulteriori dettagli sulle commissioni applicabili e i relativi criteri di calcolo, prima di ogni intervento di cancellazione.

6.2 **Cancellazione alla scadenza del Periodo di validità**. Alla scadenza del Periodo di validità del Contratto, il Cliente richiederà a Google di cancellare tutti i Dati personali del Cliente (incluse le copie esistenti) dai sistemi di Google, ai sensi delle leggi vigenti. Google adempirà a tale richiesta in tempi ragionevolmente brevi ed entro un periodo massimo di 180 giorni, salvo che le Leggi europee ne richiedano la conservazione.

# 7. Sicurezza dei dati

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

7.1.1 **Misure di sicurezza di Google**. Google attuerà e manterrà misure tecniche e organizzative per prevenire la distruzione, accidentale o dolosa, la perdita, l'alterazione, la divulgazione e l'accesso non autorizzato ai Dati personali del Cliente, come descritto nell'Allegato 2 ("**Misure di sicurezza**"). Come descritto

nell'Allegato 2, le Misure di sicurezza includono misure: (a) per criptare i dati personali; (b) che contribuiscono al mantenimento della riservatezza, dell'integrità, della disponibilità e della capacità di recupero su base continua dei sistemi e servizi di Google; (c) che contribuiscono al ripristino tempestivo dell'accesso ai dati personali in seguito a un incidente; e (d) volte all'esecuzione regolare di test di efficienza. Google potrà di volta in volta aggiornare o modificare le Misure di sicurezza, sempre che tali interventi di aggiornamento o modifica non comportino un deterioramento della sicurezza generale dei Servizi del Responsabile del trattamento.

7.1.2 **Accesso e conformità**. Google: (a) autorizzerà i propri dipendenti, collaboratori e Sub-responsabili ad accedere ai Dati personali del Cliente solo nella misura strettamente necessaria a rispettare le Istruzioni; (b) adotterà tutti i provvedimenti necessari per garantire la conformità alle Misure di sicurezza da parte dei propri dipendenti, collaboratori e Sub-responsabili in base alla portata delle rispettive prestazioni; e (c) garantirà che tutte le persone autorizzate al trattamento dei Dati personali del Cliente si siano impegnate alla riservatezza o siano vincolate a un adeguato obbligo di riservatezza previsto dalla legge.

7.1.3 **Assistenza di Google in materia di sicurezza**. Google (tenendo conto della natura del trattamento dei Dati personali del Cliente e delle informazioni a cui Google ha accesso) fornirà assistenza al Cliente nel garantire l'adempimento degli obblighi del Cliente (o, nel caso in cui il Cliente sia un responsabile, del titolare competente) relativamente alla sicurezza dei dati personali e alla violazione degli stessi inclusi gli obblighi del Cliente (o, nel caso in cui il Cliente sia un responsabile, del titolare competente) ai sensi degli Articoli da 32 a 34 (inclusi) del GDPR, mediante:

(a) l'attuazione e il mantenimento delle Misure di sicurezza di cui alla Sezione 7.1.1 (Misure di sicurezza di Google);

(b) il rispetto dei termini di cui alla Sezione 7.2 (Incidenti relativi ai dati); e

(c) la fornitura al Cliente della Documentazione in materia di sicurezza di cui alla Sezione 7.5.1 (Revisioni della Documentazione in materia di sicurezza) e delle informazioni contenute nei presenti Termini per il trattamento dei dati.

7.2 **Incidenti relativi ai dati**.

7.2.1 **Notifica dell'Incidente**. Qualora Google venisse a conoscenza di un Incidente relativo ai dati, provvederà a: (a) comunicarlo al Cliente tempestivamente e senza ingiustificato ritardo; e (b) adottare tempestivamente i provvedimenti necessari a minimizzare i danni e salvaguardare i Dati personali del Cliente.

7.2.2 **Dettagli dell'Incidente relativo ai dati**. Le notifiche di cui alla Sezione 7.2.1 (Notifica dell'Incidente) descriveranno: la natura dell'Incidente relativo ai dati, incluse le risorse del Cliente coinvolte; i provvedimenti che Google ha adottato, o intende adottare, per risolvere l'Incidente relativo ai dati e mitigare i potenziali rischi; le eventuali misure che Google consiglia al Cliente di adottare per risolvere l'Incidente relativo ai dati; e il recapito di un referente dal quale è possibile ottenere ulteriori informazioni. Se non è possibile fornire tutte queste informazioni contemporaneamente, la notifica iniziale di Google conterrà le informazioni disponibili al momento e le successive informazioni verranno comunicate senza ingiustificato ritardo non appena disponibili.

7.2.3 **Metodo di notifica**. Google farà pervenire la notifica di eventuali Incidenti relativi ai dati all'Indirizzo email di notifica o, a discrezione di Google (anche qualora il Cliente non abbia fornito a Google un Indirizzo email di notifica), mediante altra comunicazione diretta (ad esempio, per telefono o in occasione di una riunione di persona). È esclusivamente responsabilità del Cliente fornire un Indirizzo email di notifica e assicurarsi che tale Indirizzo email di notifica sia valido.

7.2.4 **Notifiche a terze parti**. Il Cliente è il solo responsabile dell'osservanza delle leggi ad esso applicabili in relazione alla notifica degli Incidenti e dell'adempimento di obblighi di notifica a terze parti concernenti eventuali Incidenti relativi ai dati.

7.2.5 **Responsabilità di Google**. La notifica o la risposta di Google che riguarda un Incidente relativo ai dati ai sensi della presente Sezione 7.2 (Incidenti relativi ai dati) non dovrà essere in alcun modo intesa come un riconoscimento di responsabilità da parte di Google in merito all'Incidente relativo ai dati.

7.3 **Responsabilità del Cliente in materia di sicurezza e analisi**.

7.3.1 **Responsabilità del Cliente in materia di sicurezza**. Il Cliente accetta che, fermi restando gli obblighi di Google di cui alle Sezioni 7.1 (Misure e assistenza in materia di sicurezza da parte di Google) e 7.2 (Incidenti relativi ai dati):

(a) Il Cliente è responsabile dell'uso dei Servizi del Responsabile del trattamento, inclusi:

(i) l'uso adeguato dei Servizi del Responsabile del trattamento per garantire un livello di sicurezza proporzionato al rischio legato ai Dati personali del Cliente; e

(ii) la protezione delle credenziali di autenticazione dell'account, dei sistemi e dei dispositivi utilizzati dal Cliente per accedere ai Servizi del Responsabile del trattamento; e

(b) Google non ha l'obbligo di tutelare i Dati personali del Cliente che quest'ultimo decide di archiviare o trasferire al di fuori dei sistemi di Google e dei suoi Sub-responsabili.

7.3.2 **Valutazione sulla sicurezza da parte del Cliente**. Il Cliente riconosce e accetta che le Misure di sicurezza attuate e mantenute da Google secondo quanto previsto nella Sezione 7.1.1 (Misure di sicurezza di Google) forniscono un livello di sicurezza proporzionato al rischio legato ai Dati personali del Cliente, tenuto conto delle tecnologie d'avanguardia, dei costi di attuazione, della natura, dell'ambito di applicazione, del contesto e degli scopi del trattamento dei Dati personali del Cliente, nonché dei rischi per le persone fisiche.

7.4 **Certificazione di sicurezza**. Per valutare e contribuire a garantire la continua efficacia delle Misure di sicurezza, Google manterrà valida la Certificazione ISO 27001.

7.5 **Revisioni e controlli di conformità**.

7.5.1 **Revisioni della Documentazione in materia di sicurezza**. Al fine di provare l'adempimento agli obblighi ai sensi dei presenti Termini per il trattamento dei dati, Google metterà a disposizione del Cliente, per sua revisione, la Documentazione in materia di sicurezza.

7.5.2 **Diritti del Cliente di eseguire audit**.

(a) Google consentirà al Cliente o a un revisore esterno nominato dal Cliente di condurre le procedure di audit (incluse ispezioni) atte a verificare l'adempimento da parte di Google degli obblighi di cui ai presenti Termini per il trattamento dei dati ai sensi della Sezione 7.5.3 (Termini di contratto aggiuntivi per i controlli). Nel corso di un eventuale audit, Google metterà a disposizione tutte le informazioni necessarie per dimostrare tale conformità e parteciperà ai controlli come descritto nella Sezione 7.4 (Certificazione di sicurezza) e nella presente Sezione 7.5 (Revisioni e controlli di conformità).

(b) laddove si applichino le CCS ai sensi della Sezione 10.2 (Trasferimenti europei limitati) Google consentirà al Cliente (o a un revisore esterno nominato dal Cliente) di condurre audit come descritto nelle CCS e, nel corso del controllo, metterà a disposizione tutte le informazioni richieste dalle CCS, ai sensi della Sezione 7.5.3 (Termini di contratto aggiuntivi per i controlli).

(c) Il Cliente potrà inoltre eseguire un audit atto a verificare l'adempimento da parte di Google degli obblighi di cui ai presenti Termini per il trattamento dei dati per mezzo della valutazione del certificato emesso ai fini della Certificazione ISO 27001 (il quale rispecchia l'esito di un controllo eseguito da un revisore di terze parti).

7.5.3 **Termini commerciali aggiuntivi in materia di audit**.

(a) Il Cliente farà pervenire a Google eventuali richieste di audit di cui alla Sezione 7.5.2 (a) o 7.5.2 (b) secondo le modalità descritte nella Sezione 12.1 (Contattare Google).

(b) In seguito al ricevimento da parte di Google della richiesta di cui alla Sezione 7.5.3(a), Google e il Cliente si confronteranno e converranno in anticipo e in modo ragionevole una data di inizio, la portata, la durata e le verifiche applicabili in materia di sicurezza e riservatezza degli audit di cui alle Sezioni 7.5.2 (a) o 7.5.2 (b).

(c) Google potrebbe addebitare una commissione (basata sulle spese ragionevolmente sostenute da Google) per eventuali audit di cui alle Sezioni 7.5.2 (a) o 7.5.2 (b). Google fornirà al Cliente ulteriori dettagli su eventuali commissioni applicabili e i relativi criteri di calcolo, prima di tali audit. Il Cliente si farà carico di eventuali commissioni addebitate dai revisori esterni nominati dal Cliente per l'esecuzione di tali audit.

(d) Google potrà sollevare obiezioni riguardo a qualsiasi revisore esterno nominato dal Cliente per condurre l'audit di cui alle Sezioni 7.5.2 (a) o 7.5.2 (b) qualora il revisore non sia, sulla base di ragioni plausibili addotte da Google, adeguatamente qualificato o indipendente, sia un concorrente di Google o sia palesemente inadatto all'incarico per altri motivi. Qualora Google dovesse sollevare una di tali obiezioni, il Cliente dovrà nominare un altro revisore o eseguire l'audit per proprio conto.

(e) Nulla di quanto disposto dai presenti Termini per il trattamento dei dati presuppone il consenso di Google alla comunicazione al Cliente o al revisore esterno, o all'accesso del Cliente o del revisore esterno a:

(i) dati di eventuali altri clienti di una Società Google;

(ii) dati interni contabili o finanziari di una Società Google;

(iii) segreti commerciali di una Società Google;

(iv) informazioni che, secondo la ragionevole opinione di Google, potrebbero: (A) compromettere la sicurezza di sistemi o uffici di una qualsiasi delle Società Google; o (B) comportare la violazione da parte di una qualsiasi delle Società Google dei propri obblighi, ai sensi della Normativa europea sulla Protezione dei Dati o dei propri obblighi in materia di sicurezza e/o riservatezza nei confronti del Cliente o di terze parti; o

(v) informazioni a cui il Cliente o il revisore esterno da questi nominato cerchino di accedere per ragioni estranee al dovere di buona fede nell'adempimento degli obblighi del Cliente ai sensi della Normativa europea sulla Protezione dei Dati.

# 8. Valutazione dell'impatto e consulenze

Google (tenendo presenti la natura del trattamento e le informazioni a sua disposizione) fornirà assistenza al Cliente al fine di assicurare il rispetto degli obblighi dello stesso(o, nel caso in cui il Cliente sia un responsabile, del titolare competente) con riguardo alle valutazioni di impatto sulla protezione dei dati e alla consulenza preliminare, inclusi (qualora applicabili) gli obblighi del Cliente o del titolare competente ai sensi degli Articoli 35 e 36 del GDPR, fornendo:

(a) la Documentazione in materia di sicurezza di cui alla Sezione 7.5.1 (Revisioni della Documentazione in materia di sicurezza);

(b) le informazioni contenute nel Contratto (inclusi i presenti Termini per il trattamento dei dati); e

(c) mettendo altrimenti a disposizione, secondo le procedure standard di Google, altri materiali attinenti alla natura dei Servizi del Responsabile del trattamento e al trattamento dei Dati personali del Cliente (ad esempio, materiali del Centro assistenza).

# 9. Diritti dell'interessato

9.1 **Risposte alle richieste dell'interessato**. Nel caso in cui Google dovesse ricevere una richiesta da parte di un soggetto interessato relativamente ai Dati personali del Cliente, il Cliente autorizza Google, e Google con la presente informa il Cliente che provvederà a:

(a) rispondere direttamente alla suddetta richiesta, secondo la funzionalità standard del Tool degli interessati (se la richiesta è stata elaborata mediante un Tool degli Interessati); o

(b) suggerire all'interessato di inoltrare la propria richiesta al Cliente, il quale sarà responsabile di evadere tale richiesta (se la richiesta non è stata elaborata mediante un Tool degli interessati).

9.2 **Assistenza di Google in merito alla richiesta dell'interessato**. Google fornirà assistenza al Cliente nell'adempimento dei suoi (o, nel caso in cui il Cliente sia un responsabile, del titolare di riferimento) obblighi ai sensi del Capitolo III del GDPR per quanto riguarda la risposta alle richieste in applicazione dei diritti dell'interessato, in ogni caso tenendo conto della natura del trattamento dei Dati personali del Cliente e, qualora applicabile, dell'Articolo 11 del GDPR, tramite:

(a) la fornitura della funzionalità dei Servizi del Responsabile del trattamento;

(b) l'adempimento degli impegni fissati dalla Sezione 9.1 (Risposte alle richieste dell'interessato); e

(c) se applicabile ai Servizi del Responsabile del trattamento, la messa a disposizione dei Tool per gli interessati.

9.3 **Rettifica**. Qualora il Cliente dovesse rendersi conto del fatto che i Dati personali del Cliente sono inesatti o non aggiornati, il Cliente avrà la responsabilità di rettificare o cancellare tali dati ove ciò sia richiesto dalla Normativa europea sulla Protezione dei Dati, incluso (ove disponibile) mediante l'utilizzo della funzionalità dei Servizi del Responsabile.

# 10. Trasferimenti di dati

10.1 **Sedi di archiviazione e trattamento dei dati**. In conformità con quanto previsto di seguito dalla presente Sezione 10 (Trasferimenti di dati), Google potrà trattare i Dati personali del Cliente in qualsiasi paese in cui Google o i suoi Sub-responsabili del trattamento dispongano di sedi.

10.2 **Trasferimenti europei limitati**. Le parti riconoscono che la Normativa europea sulla Protezione dei Dati non richiede le CCS o una Soluzione alternativa di trasferimento per trattare i Dati personali del Cliente o trasferirli in un Paese Adeguato. Qualora i Dati personali del Cliente fossero trasferiti presso un altro paese e la Legislazione europea sulla protezione dei dati trovasse applicazione a tali trasferimenti ("**Trasferimenti europei limitati**"), allora:

(a) Se Google adotta una Soluzione alternativa di trasferimento per eventuali Trasferimenti europei limitati, Google informerà il Cliente circa la relativa soluzione e garantirà che tali Trasferimenti europei limitati siano effettuati in conformità con tale Soluzione; e/o

(b) Se Google non ha adottato o non ha informato il Cliente del fatto che non sta più adottando una Soluzione alternativa di trasferimento per eventuali Trasferimenti europei limitati, allora:

(i) Se l'indirizzo di Google si trova in un Paese Adeguato:

(A) Le CCS (da responsabile a responsabile, esportatore Google) si applicheranno a tutti i Trasferimenti europei limitati da Google ai Sub-responsabili; e

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

(ii) Se l'indirizzo di Google non si trova in un Paese Adeguato, le CCS (da titolare a responsabile) e/o le CCS (da responsabile a responsabile) si applicheranno (a seconda che il Cliente sia un titolare e/o un responsabile) a detti Trasferimenti europei limitati tra il Cliente e Google.

10.3 **Informazioni e misure supplementari**. Google fornirà al Cliente le informazioni rilevanti sui Trasferimenti europei limitati, incluse le informazioni relative alle misure supplementari per proteggere i Dati personali del Cliente, come descritto nella Sezione 7.5.1 (Revisioni della Documentazione in materia di sicurezza), nell'Allegato 2 (Misure di sicurezza) e in altro materiale relativo alla natura dei Servizi del Responsabile del trattamento e al trattamento dei Dati personali del Cliente (ad esempio, gli articoli del Centro assistenza).

10.4 **Recesso**. Qualora il Cliente stabilisse, in base all'uso corrente o previsto dei Servizi del Responsabile del trattamento, che la Soluzione alternativa di trasferimento e/o le CCS, a seconda dei casi, non offrono una protezione adeguata ai Dati personali del Cliente, il Cliente potrà recedere liberamente dal Contratto con effetto immediato tramite notifica scritta a Google.

10.5 **Informazioni sui data center**. Le informazioni sulle sedi dei data center di Google sono disponibili all'indirizzo www.google.com/about/datacenters/locations/.

# 11. Sub-responsabili del trattamento

11.1 **Consenso per l'ingaggio di Sub-responsabili**. Il Cliente autorizza espressamente l'assegnazione dell'incarico di Sub-responsabile alle società indicate all'URL specificato nella Sezione 11.2 (Informazioni sui Sub-responsabili), a partire dalla Data di validità dei presenti Termini. Inoltre, fatto salvo quanto indicato nella Sezione 11.4 (Facoltà di opporsi alla sostituzione del Sub-responsabile), il Cliente autorizza l'assegnazione dell'incarico a altre terze parti in qualità di Sub-responsabili ("**Nuovi Sub-responsabili del trattamento**").

11.2 **Informazioni sui Sub-responsabili del trattamento**. Le informazioni sui Sub-responsabili sono disponibili all'indirizzo business.safety.google/adssubprocessors.

11.3 **Requisiti per l'ingaggio dei Sub-responsabili del trattamento**. Qualora dovesse assegnare l'incarico a un qualsiasi Sub-responsabile del trattamento, Google:

(a) garantirà tramite un accordo scritto che:

(i) il Sub-responsabile acceda e utilizzi i Dati personali del Cliente esclusivamente nella misura necessaria a soddisfare gli obblighi allo stesso assegnati e che ciò avvenga in conformità con il Contratto (inclusi i presenti Termini per il trattamento dei dati); e

(ii) ove il trattamento dei Dati personali del Cliente fosse soggetto alla Normativa europea sulla Protezione dei Dati, al Sub-responsabile vengano imposti gli obblighi relativi alla protezione dei dati descritti nei presenti Termini per il trattamento dei dati (ai sensi dell'Articolo 28 (3) del GDPR, se applicabile); e

(b) si assumerà la piena responsabilità per tutti gli obblighi del Sub-responsabile, come definiti nell'accordo tra le parti, così come per tutte le sue azioni ed omissioni.

11.4 **Facoltà di opporsi alla sostituzione del Sub-responsabile**.

(a) Quando viene assegnato un incarico a un Nuovo Sub-responsabile del trattamento nel corso del Periodo di validità, Google ne informerà il Cliente con un preavviso di almeno 30 giorni prima che il Nuovo Sub-responsabile del trattamento tratti i Dati personali del Cliente (comunicando anche il nome e la sede del Sub-responsabile in questione e le attività da questo svolte) tramite l'invio di un'email all'indirizzo email di notifica.

(b) Il Cliente potrà opporsi all'assegnazione dell'incarico a un qualsiasi Nuovo Sub-responsabile del trattamento esterno recedendo liberamente dal Contratto con effetto immediato tramite notifica scritta a Google, sempre che questa sia fatta pervenire entro 90 giorni dalla comunicazione dell'ingaggio del Nuovo Sub-responsabile del trattamento come descritto nella Sezione 11.4 (a).

# 12. Contattare Google; registri relativi al trattamento

12.1 **Contattare Google**. Il Cliente potrà contattare Google in merito all'esercizio dei propri diritti ai sensi dei presenti Termini per il trattamento dei dati avvalendosi delle modalità descritte all'indirizzo privacy.google.com/businesses/processorsupport o di altri strumenti che potranno essere forniti da Google di volta in volta. Google fornirà assistenza rapida e ragionevole alle richieste del Cliente ricevute da Google tramite i suddetti strumenti e relative al trattamento dei Dati personali del Cliente ai sensi del Contratto.

12.2 **Registri relativi al trattamento di Google**. Google conserverà la documentazione necessaria relativa alle sue attività di trattamento secondo quanto richiesto dal GDPR. Il Cliente riconosce che Google è tenuta, ai sensi del GDPR, a: (a) predisporre e conservare un registro di determinati dati, inclusi: (i) il nome e le informazioni di contatto di ogni responsabile e/o titolare del trattamento per conto del quale Google agisce e (se applicabile) del rappresentante locale e del responsabile della protezione dei dati di tale responsabile e/o titolare del trattamento; e (ii), se applicabile ai sensi delle CCS del Cliente, l'Autorità di controllo del Cliente; e (b) mettere tali informazioni a disposizione di qualsiasi Autorità di controllo. Di conseguenza, il Cliente fornirà a Google, laddove gliene venga fatta richiesta e sia applicabile, tali informazioni tramite l'interfaccia utente dei Servizi del Responsabile del trattamento o attraverso altri mezzi eventualmente forniti da Google e utilizzerà la suddetta interfaccia utente e i suddetti mezzi per garantire che tutte le informazioni fornite siano accurate e aggiornate.

12.3 **Richieste del titolare**. Se Google riceve una richiesta o un'indicazione tramite gli strumenti descritti nella Sezione 12.1 (o tramite qualsiasi altro metodo) da una terza parte che sostiene di essere un titolare del trattamento dei Dati personali del Cliente, Google inviterà la terza parte a contattare il Cliente.

# 13. Responsabilità

Se il Contratto è regolato dalle leggi di:

(a) uno Stato degli Stati Uniti d'America, ne consegue che, indipendentemente dalle altre disposizioni del Contratto, la responsabilità totale di una parte verso l'altra, ai sensi dei presenti Termini per il trattamento dei dati o in connessione con questi, sarà limitata al risarcimento monetario o a un importo basato sul pagamento pari al valore massimo entro cui è limitata la responsabilità della parte in questione ai sensi del Contratto (pertanto, l'esclusione di pretese di risarcimento derivanti dalla

limitazione di responsabilità inerente al Contratto non potrà essere applicata alle pretese di risarcimento nell'ambito del Contratto riguardanti la Normativa europea sulla Protezione dei Dati o la Normativa non europea sulla Protezione dei Dati); o

(b) una giurisdizione non appartenente a uno Stato degli Stati Uniti d'America, la responsabilità delle parti derivante dai presenti Termini per il trattamento dei dati o in connessione con questi, sarà soggetta alle esclusioni e alle limitazioni di responsabilità previste dal Contratto.

# 14. Validità dei presenti Termini per il trattamento dei dati

14.1 **Ordine di precedenza**. In caso di conflitto o incoerenza tra le CCS del Cliente, i Termini aggiuntivi relativi alla Normativa non europea sulla Protezione dei Dati, il resto dei presenti Termini per il trattamento dei dati e/o il resto del Contratto, si applicherà il seguente ordine di precedenza:

(a) le CCS del Cliente (se applicabili);

(b) i Termini aggiuntivi relativi alla Normativa non europea sulla Protezione dei Dati (se applicabili);

(c) il resto dei presenti Termini per il trattamento dei dati; e

(d) il resto del Contratto.

Fatti salvi gli emendamenti apportati ai presenti Termini per il trattamento dei dati, il Contratto rimane in vigore a tutti gli effetti.

14.2 **Immodificabilità delle CCS**. Nessuna disposizione del Contratto (inclusi i presenti Termini per il trattamento dei dati) è intesa a modificare o contrastare con le CCS o pregiudicare i diritti o le libertà fondamentali degli interessati ai sensi della Normativa europea sulla Protezione dei Dati.

14.3 **Efficacia sui Termini del Titolare**. I presenti Termini per il trattamento dei dati non influiranno su eventuali altri termini separati negoziati tra Google e il Cliente che riflettano una relazione da titolare a titolare per un servizio diverso dai Servizi del Responsabile del trattamento.

14.4 **CCS preesistenti del Regno Unito**. A partire dal 21 settembre 2022 o dalla data di efficacia del Contratto, se successiva, troveranno applicazione le CCS aggiuntive per i trasferimenti ai sensi del GDPR nel Regno Unito e prevarranno e sostituiranno eventuali clausole contrattuali precedentemente concordate e concluse tra Google e il Cliente ai sensi del GDPR del Regno Unito e del Data Protection Act del 2018 ("**CCS preesistenti del Regno Unito**") La presente Sezione 14.4 (CCS preesistenti del Regno Unito) Inon pregiudicherà i diritti delle parti, o di eventuali soggetti interessati, acquisiti ai sensi delle CCS preesistenti del Regno Unito mentre queste erano in vigore.

# 15. Modifiche ai presenti Termini per il trattamento dei dati

15.1 **Modifiche agli URL**. Google potrà periodicamente modificare gli URL riportati nei presenti Termini per il trattamento dei dati e il contenuto di tali URL, fermo restando che Google potrà modificare esclusivamente:

(a) le CCS in conformità alle Sezioni 15.2 (b) - 15.2 (d) (Modifiche ai Termini per il trattamento dei dati) o integrare eventuali nuove versioni delle CCS che potrebbero essere adottate ai sensi della Normativa europea sulla Protezione dei Dati, in ogni caso purché tali modifiche non incidano sulla validità delle CCS ai sensi della Normativa europea sulla Protezione dei Dati; e

(b) l'elenco dei potenziali Servizi del Responsabile del trattamento all'indirizzo business.safety.google/adsservice per: (i) riflettere una modifica al nome di un servizio; (ii) aggiungere un nuovo servizio; o (iii) rimuovere un servizio (o una caratteristica del servizio) nel caso in cui: (x) tutti i contratti per la fornitura del servizio in questione siano stati risolti; (y) Google disponga del consenso del Cliente; o (z) il servizio o una caratteristica del servizio sia stato riclassificato come un servizio del titolare.

15.2 **Modifiche ai Termini per il trattamento dei dati**. Google potrà modificare i presenti Termini per il trattamento dei dati se la modifica:

(a) è espressamente consentita dai presenti Termini per il trattamento dei dati così come descritto nella Sezione 15.1 (Modifiche agli URL);

(b) riflette una modifica al nome o alla forma di una entità giuridica;

(c) è necessaria al fine di conformarsi a leggi o regolamenti vigenti, ordinanze del tribunale o direttive emesse da un'autorità di regolamentazione o un'agenzia governativa oppure rispecchi l'adozione di una Soluzione alternativa di trasferimento da parte di Google; o

(d) non: (i) determini una diminuzione della sicurezza complessiva dei Servizi del Responsabile del trattamento; (ii) ampli l'ambito di applicazione, o rimuova qualsiasi restrizione su, (x) i diritti di Google a utilizzare o altrimenti trattare i dati nell'ambito dei Termini aggiuntivi relativi alla Normativa non europea sulla Protezione dei Dati in caso di applicazione di questi ultimi; o (y) il trattamento dei Dati personali del Cliente da parte di Google in caso di applicazione del resto dei presenti Termini per il trattamento dei dati, come descritto nella Sezione 5.3 (Conformità di Google alle Istruzioni); e (iii) abbia in altro modo un sostanziale impatto negativo sui diritti del Cliente ai sensi dei presenti Termini per il trattamento dei dati, sulla base di una valutazione ragionevolmente effettuata da Google.

15.3 **Notifica delle modifiche**. Qualora Google intenda modificare i presenti Termini per il trattamento dei dati ai sensi della Sezione 15.2 (c) o (d), Google ne informerà il Cliente con un preavviso di almeno 30 giorni (o inferiore, se così prescritto in adempimento delle leggi o regolamenti vigenti, ordinanze del tribunale o direttive emesse da un'autorità di regolamentazione o un'agenzia governativa) prima dell'entrata in vigore delle modifiche mediante: (a) l'invio di un'email all'Indirizzo email di notifica; o (b) un avviso fatto pervenire al Cliente tramite l'interfaccia utente dei Servizi del Responsabile del trattamento. Qualora il Cliente si opponga alle suddette modifiche, potrà recedere liberamente dal Contratto con effetto immediato trasmettendone comunicazione scritta a Google entro 90 giorni dalla notifica delle stesse da parte di Google.

# Allegato 1: Oggetto e dettagli del trattamento di dati

**Oggetto**

La prestazione, da parte di Google, dei Servizi del Responsabile e della relativa assistenza tecnica al Cliente.

**Durata del trattamento**

Il Periodo di validità più il periodo compreso dalla scadenza dello stesso fino alla cancellazione di tutti i Dati personali del Cliente da parte di Google, ai sensi dei presenti Termini per il trattamento dei dati.

**Natura e scopo del trattamento**

Google tratterà (incluse, se applicabili ai Servizi del Responsabile e alle Istruzioni, le attività di raccolta, registrazione, organizzazione, strutturazione, archiviazione, modifica,

recupero, utilizzo, divulgazione, combinazione, cancellazione e distruzione) i Dati personali del Cliente al fine di fornire i Servizi del Responsabile e la relativa assistenza tecnica al Cliente ai sensi dei presenti Termini per il trattamento dei dati.

**Tipi di dati personali**

I Dati personali del Cliente possono includere le tipologie di dati personali descritte all'indirizzo business.safety.google/adsservices.

**Categorie di interessati**

I Dati personali del Cliente possono riferirsi alle seguenti categorie di interessati:

- Interessati di cui Google raccoglie i dati personali nell'ambito della prestazione dei Servizi del Responsabile; e/o
- Interessati i cui dati personali vengono trasferiti a Google dal Cliente, dietro sue istruzioni o per suo conto, in relazione ai Servizi del Responsabile.

A seconda della natura dei Servizi del Responsabile del trattamento, gli interessati potrebbero includere dei privati: (a) a cui è o sarà rivolta la pubblicità online; (b) che hanno visitato specifici siti web o applicazioni per cui Google fornisce i Servizi del Responsabile; e/o (c) che sono clienti o utenti dei prodotti o servizi del Cliente.

# Allegato 2: Misure di sicurezza

A partire dalla Data di validità dei Termini, Google attuerà e manterrà le Misure di sicurezza definite nel presente Allegato 2. Google potrà di tanto in tanto aggiornare o modificare tali Misure di sicurezza, sempre che tali interventi di aggiornamento e modifica non comportino un peggioramento del livello di sicurezza generale dei Servizi del Responsabile del trattamento.

**1. Data center e sicurezza della rete**

(a) **Data center**.

**Infrastruttura**. Google possiede dei data center dislocati in diverse aree geografiche. Google archivia tutti i dati di produzione in data center fisici protetti.

**Ridondanza**. L'infrastruttura IT è stata concepita per eliminare i single point of failure e minimizzare l'impatto dei rischi ambientali prevedibili. Circuiti doppi, commutatori, reti o altri dispositivi necessari contribuiscono alla realizzazione della ridondanza. I Servizi del Responsabile sono concepiti per consentire a Google di attuare determinate tipologie di manutenzione preventiva e correttiva su base continua. Tutte le apparecchiature ambientali e le sedi hanno documentato le procedure di manutenzione preventiva che descrivono il processo e la frequenza delle prestazioni in base alle specifiche interne o del produttore. La manutenzione preventiva e correttiva delle attrezzature dei data center è programmata per mezzo di un procedimento standard conforme alle procedure documentate.

**Sistemi di alimentazione**. I sistemi elettrici di alimentazione del data center sono concepiti per essere ridondanti e sostenibili senza avere impatto sulla continua operatività, 24 ore al giorno, sette giorni su sette. Nella maggior parte dei casi, una fonte di alimentazione primaria e una fonte di alimentazione alternativa, entrambe con pari capacità, vengono fornite per i settori sensibili delle infrastrutture dei data center. Una fonte di alimentazione di riserva è fornita da vari meccanismi, quali i gruppi statici di continuità (UPS), che forniscono una protezione energetica altamente affidabile durante sbalzi di tensione della rete, blackout, eventi di sovratensione o sottotensione e condizioni di frequenza fuori dai parametri di tolleranza. Se la fornitura di energia elettrica viene interrotta, l'energia di riserva è concepita per fornire un'alimentazione transitoria al data center, al pieno della capacità, per un massimo di dieci minuti, finché non viene rilevata dai sistemi di generazione di riserva. I generatori di riserva sono in grado di avviarsi automaticamente in pochi secondi per fornire una quantità di energia elettrica di emergenza sufficiente a far funzionare il data center al pieno delle proprie capacità, generalmente per una durata di giorni.

**Sistemi operativi del server**. I server di Google utilizzano sistemi operativi con protezione avanzata e personalizzati in base alle esigenze specifiche dei server dell'attività. I dati vengono archiviati utilizzando algoritmi proprietari al fine di accrescerne la sicurezza e la ridondanza. Google impiega un procedimento di revisione del codice per aumentare la sicurezza del codice utilizzato per fornire i Servizi del Responsabile e potenziare i prodotti di sicurezza negli ambienti di produzione.

**Continuità operativa**. Google replica i dati su più sistemi per favorire la protezione contro le perdite o la distruzione accidentali. Google ha sviluppato dei programmi per la pianificazione della continuità operativa e il ripristino di emergenza che vengono rivisti e testati regolarmente.

**Tecnologie di crittografia**. Le norme sulla sicurezza di Google esigono la crittografia at-rest per tutti i dati utente, inclusi i dati personali. Spesso nei data center i dati vengono criptati a più livelli negli stack di archiviazione di produzione di Google, incluso a livello di hardware, senza richiedere alcuna azione da parte dei clienti. L'utilizzo di più livelli di crittografia aggiunge una protezione dei dati ridondante e consente a Google di scegliere l'approccio ottimale in base ai requisiti dell'applicazione. Tutti i dati personali vengono criptati a livello di archiviazione, in genere usando l'algoritmo AES256. Google utilizza librerie crittografiche comuni che integrano il modulo convalidato FIPS 140-2 di Google per un'implementazione coerente della crittografia nei Servizi del Responsabile.

(b) **Reti e trasmissione**.

**Trasmissione dei dati**. I data center sono generalmente connessi tramite collegamenti privati ad alta velocità per garantire il trasferimento rapido e sicuro dei dati. Inoltre, Google cripta i dati trasmessi tra i data center. Tale trasmissione è stata concepita per prevenire la lettura, copia, modifica o rimozione dei dati senza autorizzazione durante il trasferimento elettronico. Google trasferisce i dati impiegando protocolli di rete standard.

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

**Rilevamento delle intrusioni**. Il rilevamento delle intrusioni mira a fornire una panoramica delle attività di attacco in corso e le informazioni adeguate per poter reagire agli incidenti. Il sistema di rilevamento delle intrusioni di Google prevede:

1. Rigidi controlli sulla dimensione e sulla composizione della superficie di attacco della rete di Google attraverso una serie di misure preventive;
2. L'impiego di controlli di rilevamento intelligente in tutti i punti di immissione dati; e
3. L'impiego di tecnologie per la correzione automatica di determinate situazioni di pericolo.

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

**Tecnologie di crittografia**. Google mette a disposizione la crittografia del protocollo HTTPS (noto anche come connessione TLS). I server di Google supportano lo scambio di chiave di crittografia Diffie Hellman a curva ellittica firmato con RSA ed ECDSA. Tali metodi di Perfect Forward Secrecy (PFS) contribuiscono a proteggere il traffico di dati e minimizzano l'impatto di una chiave compromessa o di una violazione della crittografia.

**2. Accesso e verifica delle sedi**

(a) **Verifica delle sedi**.

**Unità operativa di sicurezza dei data center**. I data center di Google dispongono di un'unità operativa di sicurezza in loco responsabile di tutte le funzioni di

sicurezza dei data center fisici 24 ore al giorno, sette giorni su sette. Il personale dell'unità operativa in loco esegue il monitoraggio delle telecamere a Circuito chiuso ("CCTV") e di tutti i sistemi di allarme. Il personale di sicurezza dell'unità operativa in loco esegue regolarmente perlustrazioni interne ed esterne del data center.

**Procedure di accesso al data center**. Google dispone di procedure formali per consentire l'accesso di persone fisiche ai data center. I data center si trovano in strutture munite di accesso mediante carta magnetica e di sistemi di allarme collegati all'unità operativa di sicurezza in loco. Tutti i visitatori del data center devono identificarsi e mostrare un documento di identità all'unità operativa di sicurezza in loco. Solo ai dipendenti, ai collaboratori e ai visitatori autorizzati è consentito entrare nel data center. Solo i dipendenti autorizzati e i collaboratori possono richiedere una carta elettronica di accesso a tali strutture. La richiesta della carta elettronica di accesso al data center deve essere trasmessa in anticipo e per iscritto, dovendo essere approvata dal personale autorizzato del data center. Gli altri visitatori che richiedono un accesso temporaneo al data center devono: (i) ottenere la previa approvazione del personale autorizzato del data center in questione per le specifiche aree interne che intendono visitare; (ii) registrarsi presso l'unità operativa di sicurezza in loco; e (iii) fare riferimento a un registro ufficiale di accesso al data center che permetta di identificare l'individuo come autorizzato.

**Dispositivi di sicurezza dei data center**. I data center di Google impiegano un sistema di controllo degli accessi mediante carta elettronica e riconoscimento biometrico, collegato al sistema di allarme. Il sistema di controllo degli accessi monitora e registra le carte elettroniche di ogni individuo, l'accesso alle porte perimetrali, di spedizione e ricezione, e ad altre aree sensibili. Le attività non autorizzate e i tentativi di accesso falliti vengono rilevati dal sistema di controllo dell'accesso e opportunamente valutati. Gli accessi autorizzati alle attività aziendali e ai data center è limitato in base alle aree e responsabilità professionali degli individui. Le porte antincendio dei data center sono dotate di allarme. Le telecamere CCTV sono in funzione all'interno e all'esterno del data center. Il posizionamento delle telecamere è stato progettato per coprire le aree strategiche, tra cui il perimetro, le porte di accesso agli edifici del data center e quelle di spedizione/ricezione. Il personale operativo di sicurezza in loco gestisce le attrezzature di monitoraggio, registrazione e controllo del sistema CCTV. Un sistema di cablaggio sicuro connette le attrezzature CCTV in tutto il data center. Le telecamere effettuano registrazioni in loco 24 ore al giorno, sette giorni su sette, tramite videoregistratori digitali. Le registrazioni di sorveglianza vengono conservate per almeno sette giorni, a seconda dell'attività.

(b) **Controllo degli accessi**.

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

**Controllo dell'accesso e gestione dei privilegi**. Gli amministratori e gli utenti del Cliente devono identificarsi per mezzo di un sistema di autenticazione centrale o di un sistema di single sign-on per poter usare i Servizi del Responsabile.

**Norme e procedimenti per l'accesso ai dati interni - Norme di accesso**. Le norme e i procedimenti per l'accesso ai dati interni di Google sono concepiti per impedire l'accesso di persone e/o sistemi non autorizzati ai sistemi utilizzati per il trattamento dei dati personali. Google intende concepire sistemi che: (i) consentano l'accesso ai dati solo alle persone autorizzate a tal fine; e (ii) salvaguardino i dati personali dalla lettura, riproduzione, modifica o rimozione non autorizzata durante il trattamento e l'uso, e dopo la registrazione. I sistemi sono stati progettati per rilevare ogni tipo di accesso illecito. Google impiega un sistema di gestione centralizzato per controllare l'accesso del personale ai server di produzione e fornisce l'accesso solo a un numero limitato di membri del personale autorizzato. LDAP, Kerberos e un sistema brevettato che impiega i certificati digitali sono progettati per fornire a Google meccanismi di accesso sicuri e flessibili. Tali meccanismi sono progettati per concedere solo diritti di accesso approvati a ospiti di siti, accessi, dati e informazioni di configurazione. Google richiede l'uso di ID utente unici, password efficaci, autenticazione a due fattori ed elenchi per gli accessi attentamente monitorati per ridurre l'eventualità di un uso non autorizzato degli account. La concessione o la modifica dei diritti di accesso si basa: sulle responsabilità professionali del personale autorizzato; sulle esigenze legate alle mansioni lavorative necessarie all'esecuzione dei compiti autorizzati; e sul principio della "necessità di sapere". La concessione o la modifica dei diritti di accesso deve inoltre essere conforme alle norme di Google sull'accesso ai dati interni e alla relativa formazione. Le approvazioni sono gestite da strumenti del flusso di lavoro che mantengono record di audit per ogni modifica. L'accesso ai sistemi viene registrato per creare un audit trail ai fini della responsabilità. Qualora le password vengano impiegate per l'autenticazione (ad esempio per accedere a delle postazioni di lavoro), per tali password saranno adottati dei criteri che quanto meno seguano le pratiche standard del settore. Tali standard includono restrizioni relative al riutilizzo delle password e un livello di sicurezza della password adeguato.

**3. Dati**

(a) **Archiviazione, isolamento e autenticazione dei dati**.

Google archivia i dati in un ambiente multi-tenant all'interno dei propri server. I dati, i database dei Servizi del Responsabile e l'architettura del file system vengono replicati tra data center dislocati in diverse aree geografiche. Google isola coerentemente i dati di ciascun cliente. Un sistema di autenticazione centrale viene usato per tutti i Servizi del Responsabile al fine di ottenere una maggiore uniformità nella sicurezza dei dati.

(b) **Linee guida per dischi ritirati e distruzione dei dischi**.

Alcuni dischi contenenti dati potrebbero venire ritirati ("**Dischi ritirati**") a causa di errori, problemi di prestazioni o danneggiamento dell'hardware. Ogni Disco ritirato viene sottoposto a una serie di procedure per la distruzione dei dati ("**Linee guida per la distruzione dei dati**") prima di abbandonare le sedi di Google per essere riutilizzato o distrutto. I Dischi ritirati vengono cancellati mediante un procedimento composto da varie fasi, la cui compiutezza viene verificata da almeno due ispettori indipendenti. I risultati della cancellazione vengono registrati mediante il numero di serie del Disco ritirato ai fini della tracciabilità. Infine, il Disco ritirato viene reinserito nell'inventario per essere riutilizzato o distribuito nuovamente. Qualora il Disco ritirato non possa essere cancellato a causa di danneggiamento dell'hardware, verrà conservato in un luogo sicuro fino a quando potrà essere distrutto. Tutte le strutture vengono sottoposte regolarmente a controlli al fine di monitorare la conformità alle Linee guida per la distruzione dei dati.

(c) **Dati pseudonimizzati**.

I dati della pubblicità online generalmente vengono associati a identificatori online che sono considerati "pseudonimizzati" (ovvero non possono essere attribuiti a un individuo specifico senza l'utilizzo di informazioni aggiuntive). Google ha implementato un valido insieme di norme e controlli tecnici e organizzativi per garantire la separazione dei dati pseudonimizzati e le informazioni di identificazione personale degli utenti (ovvero le informazioni che, da sole, potrebbero essere usate per identificare, contattare o localizzare con precisione un privato), come i dati dell'Account Google di un utente. Le policy di Google consentono i flussi di informazioni tra dati pseudonimizzati e dati di identificazione personale solo in circostanze rigorosamente limitate.

(d) **Revisioni del lancio**.

Prima che vengano lanciati i nuovi prodotti e le nuove funzionalità, Google conduce delle revisioni del lancio. Queste includono una revisione della privacy da parte degli ingegneri appositamente formati. Durante le revisioni della privacy, gli ingegneri si assicurano che tutte le norme e le linee guida applicabili di Google vengano seguite, incluse a titolo esemplificativo le norme relative alla pseudonimizzazione e alla conservazione e cancellazione dei dati.

**4. Sicurezza del personale**

Google richiede al proprio personale di adottare una condotta conforme alle linee guida della società in materia di riservatezza, etica aziendale, uso adeguato e standard professionali. Google conduce controlli ragionevolmente appropriati delle referenze nella misura consentita dalla legge e ai sensi delle leggi e dei regolamenti locali in materia di lavoro.

Il personale è tenuto ad attenersi a un accordo di riservatezza, a confermare formalmente l'avvenuta ricezione delle norme sulla privacy e sulla riservatezza di Google, e ad

agire in conformità con tali norme. Il personale riceve una formazione in materia di sicurezza. Il personale incaricato della gestione dei Dati personali del Cliente deve soddisfare dei requisiti aggiuntivi inerenti al proprio ruolo. Il personale di Google non tratterà i Dati personali del Cliente senza autorizzazione.

5. **Sicurezza del Sub-responsabile**

Prima di ingaggiare Sub-responsabili, Google conduce un controllo delle pratiche di sicurezza e delle norme di tutela della privacy adottate dai Sub-responsabili, per garantire che questi forniscano un livello di sicurezza e privacy adeguato all'accesso ai dati e alla portata dei servizi per cui vengono incaricati. Dopo che Google avrà valutato i rischi presentati dal Sub-responsabile, il Sub-responsabile dovrà sottoscrivere degli appositi termini contrattuali in materia di sicurezza, riservatezza e privacy, soggetti ai requisiti definiti nella Sezione 11.3 (Requisiti per l'incarico del Sub-responsabile).

# Allegato 3: Termini aggiuntivi relativi alla Normativa non europea sulla Protezione dei Dati

I seguenti Termini aggiuntivi relativi alla Normativa non europea sulla Protezione dei Dati integrano i presenti Termini per il trattamento dei dati:

- Addendum ai sensi delle leggi statali sulla privacy degli Stati Uniti alla pagina business.safety.google/usaprivacyaddendum (datato 1° luglio 2023)
- Appendice relativa alla LGPD applicabile al responsabile, disponibile all'indirizzo business.safety.google/adsprocessorterms/lgpd/ (del 16 agosto 2020)

*Termini per il trattamento dei dati di Google Ads, versione 6.0*

*1° luglio 2023*

**Versioni precedenti**

- 1° gennaio 2023
- 21 settembre 2022
- 16 agosto 2020
- 12 agosto 2020
- 1° gennaio 2020
- 31 ottobre 2019
- 12 ottobre 2017