Google Cloud

Modifica del trattamento dei dati a G Suite e / o Accordo sul prodotto complementare (Versione 2.2)

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

1. **Inizio** .

La presente modifica all'elaborazione dei dati a G Suite e / o all'accordo sui prodotti complementari, comprese le relative appendici (la " **modifica dell'elaborazione dei dati** ") sarà efficace e sostituirà qualsiasi termine di elaborazione dei dati precedentemente applicabile e termini di sicurezza a partire dalla data di efficacia della modifica (come definita di seguito).

Questa modifica al trattamento dei dati integra l'accordo applicabile. Laddove tale Accordo sia stato stipulato offline con Google Ireland Limited, la presente Modifica sull'elaborazione dei dati sostituisce la clausola "Privacy" nel Contratto (se applicabile).

2. **Definizioni**

2.1 I termini in maiuscolo definiti nell'accordo applicabile si applicano alla presente modifica al trattamento dei dati. Inoltre, in questa modifica al 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'uso 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 decide, tra cui Admin Console, crittografia, registrazione e monitoraggio, gestione delle identità e degli accessi, scansione della sicurezza e firewall.

" **Pubblicità** " indica gli annunci pubblicitari online visualizzati da Google per gli Utenti finali, ad esclusione di tutti gli annunci pubblicitari che il Cliente sceglie espressamente di visualizzare Google o uno dei suoi Affiliati in relazione ai Servizi in base a un accordo separato (ad esempio, gli annunci pubblicitari Google AdSense implementati dal Cliente su un sito Web creato dal Cliente utilizzando qualsiasi funzionalità di Google Sites all'interno dei Servizi).

" **Affiliato** " indica qualsiasi entità che controlla, controllata da o sotto controllo comune con una parte, in cui il "controllo" è definito come: (a) la proprietà di almeno il cinquanta percento (50%) del patrimonio netto o degli interessi benefici dell'entità ; (b) il diritto di voto o di nomina della maggioranza del consiglio di amministrazione o di 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 del contratto tipo, che consente il trasferimento legale di dati personali in un paese terzo in conformità con la legge europea sulla protezione dei dati (ad esempio, Privacy Shield).

" **Data di** entrata in **vigore della modifica** " indica la data in cui il cliente ha accettato, o le parti hanno diversamente concordato, la presente modifica al trattamento dei dati.

" **Servizi certificati** " significa:

un. quei servizi G Suite Core indicati come nell'ambito della relativa certificazione o relazione all'indirizzo 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 l'Accordo applicabile; e

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

" **Contratto di prodotto complementare** " indica: un Contratto di identità cloud o altro accordo in base al quale Google accetta di fornire servizi di identità in quanto tali al Cliente; Contratto di noleggio; o altri accordi che incorporano questo emendamento sull'elaborazione dei dati per riferimento o affermano che si applicherà se accettato dal cliente.

" **Riepilogo dei servizi di prodotti complementari** " indica la descrizione attuale dei servizi forniti ai sensi di un Accordo sui prodotti complementari, come indicato nell'Accordo 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, divulgazione non autorizzata o accesso ai Dati del cliente su sistemi gestiti da o altrimenti controllati da Google.

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

" **Data di attivazione completa** " indica: (a) se la presente Modifica di elaborazione dei dati viene automaticamente incorporata nell'Accordo applicabile, la Data di efficacia della modifica; o (b) se il Cliente ha accettato o le parti hanno concordato diversamente con la presente Modifica sull'elaborazione dei dati, l'ottavo giorno successivo alla Data di efficacia della modifica.

" **GDPR dell'UE** " indica il regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali e alla libera circolazione di tali dati e che abroga la direttiva 95/46 / CE.

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

" **Diritto europeo o nazionale** " indica, a seconda dei casi: (a) il diritto dell'UE o degli Stati membri dell'UE (se il GDPR dell'UE si applica al trattamento dei dati personali dei clienti); e / o (b) la legge del Regno Unito o parte di il Regno Unito (se il GDPR del Regno Unito si applica al trattamento dei dati personali dei clienti).

" **GDPR** " indica, a seconda dei casi: (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, qualificato e indipendente nominato da Google, la cui identità di quel momento che Google rivelerà al Cliente.

" **Accordo G Suite** " indica un Accordo G Suite; un accordo G Suite for Education; un Contratto master di Google Cloud con il programma dei servizi di G Suite; o qualsiasi altro accordo in base al quale Google accetta di fornire qualsiasi servizio descritto nel Riepilogo dei servizi di G Suite al Cliente.

" **Riepilogo dei servizi di G Suite** " indica la descrizione attuale dei servizi di G Suite (comprese le edizioni correlate), come indicato in https://gsuite.google.com/terms/user_features.html (che può essere aggiornato da Google da di volta in volta in conformità con l'accordo G Suite).

Per " **clausole contrattuali tipo** " o "MCC" si intendono le clausole standard di protezione dei dati per il trasferimento di dati personali a processori stabiliti in paesi terzi che non garantiscono un livello adeguato di protezione dei dati, come descritto nell'articolo 46 del GDPR dell'UE.

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

" **Indirizzo e-mail di notifica** " indica l'indirizzo o gli indirizzi e-mail designati dal Cliente nell'Admin Console, o nel Modulo d'ordine o nel Documento d'ordine (come applicabile), per ricevere determinate notifiche da Google. Il cliente è responsabile dell'utilizzo dell'Admin Console per garantire che il suo indirizzo e-mail di notifica rimanga aggiornato e valido.

" **Scudo per la privacy** " indica, ove applicabile, il quadro giuridico per lo scudo per la privacy UE-USA, il quadro giuridico per lo scudo per la privacy svizzero-americano e qualsiasi quadro giuridico equivalente applicabile tra il Regno Unito e gli Stati Uniti.

" **Documentazione sulla sicurezza** " indica tutti i documenti e le informazioni resi disponibili da Google ai sensi della Sezione 7.5.1 (Recensioni 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 nell'Accordo G Suite o nell'Accordo sul prodotto complementare, a seconda dei casi, oppure, se l'Accordo G Suite del Cliente non definisce "Termini specifici del servizio", si intendono i termini attuali specifici di uno o più Core I servizi per G Suite sono disponibili all'indirizzo https://gsuite.google.com/terms/service-terms/ .

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

un. i Servizi principali per G Suite, come descritto nel Riepilogo dei servizi G Suite;

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

c. i servizi descritti nel Riepilogo dei servizi di prodotti complementari.

" **Sottoprocessore** " indica una terza parte autorizzata come altro elaboratore ai sensi della presente Modifica sull'elaborazione dei dati per avere accesso logico ed elaborare i dati del cliente al fine di fornire parti dei Servizi e TSS.

" **Autorità di vigilanza** " indica, a seconda dei casi: (a) un'autorità di vigilanza 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 post-terminazione durante il quale Google può continuare a fornire i Servizi a fini transitori.

" **GDPR del Regno Unito** " indica il GDPR dell'UE modificato e incorporato nella legge britannica ai sensi del UK European Union (Prelievo) Act 2018, se in vigore.

2.2. I termini "dati personali", "soggetto dei dati", "elaborazione", "responsabile del trattamento" e "responsabile del trattamento" utilizzati nella presente modifica al trattamento dei dati hanno i significati indicati nel GDPR, indipendentemente dal fatto che la legge europea sulla protezione dei dati o i dati non europei Si applica la legge sulla protezione.

3. **Durata** . La presente modifica al trattamento dei dati, nonostante la scadenza del termine, rimarrà in vigore fino a quando, e automaticamente scadrà, la cancellazione di tutti i dati dei clienti da parte di Google come descritto nella presente modifica al trattamento dei dati.

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

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

un. il trattamento è effettuato nel contesto 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 a soggetti 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 del diritto non europeo . Le parti riconoscono che la legge non europea sulla protezione dei dati può applicarsi anche al trattamento dei dati personali dei clienti.

4.3 Applicazione dell'emendamento sull'elaborazione dei dati . Salvo quanto diversamente indicato da questa modifica al trattamento dei dati, i termini di questa modifica al 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 controller . Se la legge europea sulla protezione dei dati si applica al trattamento dei dati personali dei clienti:

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

b. Google è responsabile del trattamento dei dati personali del cliente ai sensi della legge europea sulla protezione dei dati;

c. Il Cliente è un controllore o elaboratore, a seconda dei casi, di tali 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 di tali 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 elaboratore, il cliente garantisce che le sue istruzioni e azioni in relazione a tali dati personali del cliente, inclusa la nomina di Google come altro elaboratore, sono state autorizzate dal responsabile del trattamento .

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

5.2 **Ambito di elaborazione** .

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 dall'uso 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 questo Emendamento sul trattamento dei dati; e (d) come ulteriormente documentato in qualsiasi altra istruzione scritta fornita dal Cliente e riconosciuto da Google come istruzioni per l'uso ai fini della presente Modifica sull'elaborazione dei dati.

5.2.2 Conformità di Google alle 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 merito ai trasferimenti di dati) a meno che la legge europea o nazionale alla quale Google è soggetto 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 dei clienti a fini pubblicitari né pubblicizzerà i Servizi.

5.3. **Prodotti aggiuntivi**. Se Google, a sua discrezione, rende disponibili al Cliente eventuali Prodotti aggiuntivi in conformità con i Termini di prodotto 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, la presente modifica al trattamento dei dati non si applica al trattamento dei dati personali in relazione alla fornitura di eventuali prodotti aggiuntivi installati o utilizzati dal cliente, compresi i dati personali trasmessi da o verso tali prodotti aggiuntivi. Il Cliente può utilizzare la funzionalità dei Servizi per abilitare o disabilitare Prodotti aggiuntivi,

6. **Data Deletion**

6.1 **Deletion During Term**. Google will enable Customer and End Users to delete Customer Data during the applicable Term in a manner consistent with the functionality of the Services. If Customer or an End User uses the Services to delete any Customer Data during the applicable Term and that Customer Data cannot be recovered by Customer or an End User (such as from the "trash"), this use will constitute an instruction to Google to delete the relevant Customer Data from Google's systems in accordance with applicable law. Google will comply with this instruction as soon as reasonably practicable and within a maximum period of 180 days, unless European or National Law requires storage.

6.2 **Deletion on Term Expiry**. Subject to Section 6.3 (Deferred Deletion Instruction), on expiry of the applicable Term, Customer instructs Google to delete all Customer Data (including existing copies) from Google's systems in accordance with applicable law. Google will comply with this instruction as soon as reasonably practicable and within a maximum period of 180 days, unless European or National Law requires storage. Without prejudice to Section 9.1 (Access; Rectification; Restricted Processing; Portability), Customer is responsible for exporting, before the applicable Term expires, any Customer Data it wishes to retain.

6.3 **Deferred Deletion Instruction**. To the extent any Customer Data covered by the deletion instruction described in Section 6.2 (Deletion on Term Expiry) is also processed, when the applicable Term under Section 6.2 expires, in relation to an Agreement with a continuing Term, such deletion instruction will only take effect with respect to such Customer Data when the continuing Term expires. For clarity, this Data Processing Amendment will continue to apply to such Customer Data until its deletion by Google.

7. **Data Security**.

7.1 **Google's Security Measures, Controls and Assistance**.

7.1.1 Google's Security Measures. Google will implement and maintain technical and organizational measures to protect Customer Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access as described in Appendix 2 (the "**Security Measures**"). The Security Measures include measures to encrypt personal data; to help ensure ongoing confidentiality, integrity, availability and resilience of Google's systems and services; to help restore timely access to personal data following an incident; and for regular testing of effectiveness. Google may update the Security Measures from time to time provided that such updates do not result in the degradation of the overall security of the Services.

7.1.2 Security Compliance by Google Staff. Google will: (a) take appropriate steps to ensure compliance with the Security Measures by its employees, contractors and Subprocessors to the extent applicable to their scope of performance, and (b) ensure that all persons authorized to process Customer Personal Data are under an obligation of confidentiality.

7.1.3 Additional Security Controls. Google will make Additional Security Controls available to: (a) allow Customer to take steps to secure Customer Data; and (b) provide Customer with information about securing, accessing and using Customer Data.

7.1.4 Google's Security Assistance. Google will (taking into account the nature of the processing of Customer Personal Data and the information available to Google) assist Customer in ensuring compliance with its obligations pursuant to Articles 32 to 34 of the GDPR, by:

a. implementing and maintaining the Security Measures in accordance with Section 7.1.1 (Google's Security Measures);

b. making Additional Security Controls available to Customer in accordance with Section 7.1.3 (Additional Security Controls);

c. complying with the terms of Section 7.2 (Data Incidents);

d. providing Customer with the Security Documentation in accordance with Section 7.5.1 (Reviews of Security Documentation) and the information contained in the applicable Agreement including this Data Processing Amendment; and

e. if subsections (a)-(d) above are insufficient for Customer to comply with such obligations, upon Customer's request, providing additional reasonable assistance.

7.2 **Data Incidents**

7.2.1 Incident Notification. Google will notify Customer promptly and without undue delay after becoming aware of a Data Incident, and promptly take reasonable steps to minimize harm and secure Customer Data.

7.2.2 Details of Data Incident. Google's notification of a Data Incident will describe, to the extent possible, the nature of the Data Incident, the measures taken to mitigate the potential risks and the measures Google recommends Customer take to address the Data Incident.

7.2.3 Delivery of Notification. Notification(s) of any Data Incident(s) will be delivered to the Notification Email Address or, at Google's discretion, by direct communication (for example, by phone call or an in-person meeting).

7.2.4 No Assessment of Customer Data by Google. Google has no obligation to assess Customer Data in order to identify information subject to any specific legal requirements.

7.2.5 No Acknowledgement of Fault by Google. Google's notification of or response to a Data Incident under this Section 7.2 (Data Incidents) will not be construed as an acknowledgement by Google of any fault or liability with respect to the Data Incident.

7.3. **Customer's Security Responsibilities and Assessment**.

7.3.1 Customer's Security Responsibilities. Without prejudice to Google's obligations under Sections 7.1 (Google's Security Measures, Controls and Assistance) and 7.2 (Data Incidents), and elsewhere in the applicable Agreement, Customer is responsible for its use of the Services and its storage of any copies of Customer Data outside Google's or Google's Subprocessors' systems, including:

a. using the Services and Additional Security Controls to ensure a level of security appropriate to the risk in respect of the Customer Data;

b. securing the account authentication credentials, systems and devices Customer uses to access the Services; and

c. retaining copies of its Customer Data as appropriate.

7.3.2 Customer's Security Assessment. Customer agrees, based on its current and intended use of the Services, that the Services, Security Measures, Additional Security Controls and Google's commitments under this Section 7 (Data Security): (a) meet Customer's needs, including with respect to any security obligations of Customer under European Data Protection Law and/or Non-European Data Protection Law, as applicable, and (b) provide a level of security appropriate to the risk in respect of the Customer Data.

7.4 **Compliance Certifications and SOC Reports**. Google will maintain at least the following for the Audited Services in order to evaluate the continued effectiveness of the Security Measures:

a. certificates for ISO 27001, ISO 27017 and ISO 27018, and

b. SOC 2 and SOC 3 reports produced by Google's Third Party Auditor and updated annually based on an audit performed at least once every 12 months (the "**SOC Reports**"). Google may add standards at any time. Google may replace a SOC Report with an equivalent or enhanced alternative.

7.5 **Reviews and Audits of Compliance**

7.5.1 Reviews of Security Documentation. Google will make the SOC Reports available for review by Customer to demonstrate compliance by Google with its obligations under this Data Processing Amendment.

7.5.2 Customer's Audit Rights.

a. If European Data Protection Law applies to the processing of Customer Personal Data, Google will allow Customer or an independent auditor appointed by Customer to conduct audits (including inspections) to verify Google's compliance with its obligations under this Data Processing Amendment in accordance with Section 7.5.3 (Additional Business Terms for Reviews and Audits). Google will contribute to such audits as described in Section 7.4 (Compliance Certifications and SOC Reports) and this Section 7.5 (Reviews and Audits of Compliance).

b. If Customer has entered into Model Contract Clauses as described in Section 10.2 (Transfers of Data), Google will, allow Customer or an independent auditor appointed by Customer to conduct audits as described in the Model Contract Clauses in accordance with Section 7.5.3 (Additional Business Terms for Reviews and Audits).

c. Customer may conduct an audit to verify Google's compliance with its obligations under this Data Processing Amendment by reviewing the Security Documentation (which reflects the outcome of audits conducted by Google's Third Party Auditor).

7.5.3 Additional Business Terms for Reviews and Audits.

a. Customer must send any requests for reviews of the SOC 2 report under Section 7.5.1 or audits under Section 7.5.2(a) or 7.5.2(b) to Google's Cloud Data Protection Team as described in Section 12 (Cloud Data Protection Team; Processing Records).

b. Following receipt by Google of a request under Section 7.5.3(a), Google and Customer will discuss and agree in advance on: (i) the reasonable date(s) of and security and confidentiality controls applicable to any review of the SOC 2 report under Section 7.5.1; and (ii) the reasonable start date, scope and duration of and security and confidentiality controls applicable to any audit under Section 7.5.2(a) or 7.5.2(b).

c. Google may charge a fee (based on Google's reasonable costs) for any audit under Section 7.5.2(a) or 7.5.2(b). Google will provide Customer with further details of any applicable fee, and the basis of its calculation, in advance of any such audit. Customer will be responsible for any fees charged by any auditor appointed by Customer to execute any such audit.

d. Google may object in writing to an auditor appointed by Customer to conduct any audit under Section 7.5.2(a) or 7.5.2(b) if the auditor is, in Google's reasonable opinion, not suitably qualified or independent, a competitor of Google, or otherwise manifestly unsuitable. Any such objection by Google will require Customer to appoint another auditor or conduct the audit itself.

7.5.4 No Modification of MCCs. Nothing in this Section 7.5 (Reviews and Audits of Compliance) varies or modifies any rights or obligations of Customer or Google LLC under any Model Contract Clauses entered into as described in Section 10.2 (Transfers of Data).

8. **Impact Assessments and Consultations**. Google will (taking into account the nature of the processing and the information available to Google) assist Customer in ensuring compliance with its obligations pursuant to Articles 35 and 36 of the GDPR, by:

a. providing Additional Security Controls in accordance with Section 7.1.3 (Additional Security Controls) and the Security Documentation in accordance with Section 7.5.1 (Reviews of Security Documentation);

b. providing the information contained in the applicable Agreement including this Data Processing Amendment; and

c. if subsections (a) and (b) above are insufficient for Customer to comply with such obligations, upon Customer's request, providing additional reasonable assistance.

9. **Access etc.; Data Subject Rights; Data Export**

9.1 **Access; Rectification; Restricted Processing; Portability**. During the applicable Term, Google will enable Customer, in a manner consistent with the functionality of the Services, to access, rectify and restrict processing of Customer Data, including via the deletion functionality provided by Google as described in Section 6.1 (Deletion During Term), and to export Customer Data.

9.2 **Data Subject Requests**.

9.2.1 Customer's Responsibility for Requests. During the applicable Term, if Google's Cloud Data Protection Team receives a request from a data subject in relation to Customer Personal Data, and the request identifies Customer, Google will advise the data subject to submit their request to Customer. Customer will be responsible for responding to any such request including, where necessary, by using the functionality of the Services.

9.2.2 Google's Data Subject Request Assistance. Google will (taking into account the nature of the processing of Customer Personal Data) assist Customer in fulfilling its obligations under Chapter III of the GDPR to respond to requests for exercising the data subject's rights by:

a. providing Additional Security Controls in accordance with Section 7.1.3 (Additional Security Controls);

b. complying with Sections 9.1 (Access; Rectification; Restricted Processing; Portability) and 9.2.1 (Customer's Responsibility for Requests); and

c. if subsections (a) and (b) above are insufficient for Customer to comply with such obligations, upon Customer's request, providing additional reasonable assistance.

10. **Data Transfers**

10.1 **Data Storage and Processing Facilities**. Google may store and process Customer Data anywhere Google or its Subprocessors maintain facilities, subject to Google's obligations under:

a. Section 10.2 (Transfers of Data) with respect to Model Contract Clauses or an Alternative Transfer Solution; and

b. the applicable Service Specific Terms (if any) with respect to data location.

10.2 **Transfers of Data**.

10.2.1 Google's Transfer Obligations. If the storage and/or processing of Customer Personal Data involves transfers of Customer Personal Data out of the EEA, Switzerland or the UK, and European Data Protection Law applies to the transfers of such data ("**Transferred Personal Data**") under any Agreement, Google will, in relation to Transferred Personal Data under all Agreements:

a. ensure that Google LLC enters into Model Contract Clauses with Customer as the exporter of such data if requested to do so by Customer, and ensure that the transfers are made in accordance with such Model Contract Clauses; and/or

b. offer an Alternative Transfer Solution in respect of such data, ensure that the transfers are made in accordance with such Alternative Transfer Solution, and make information available to Customer about such Alternative Transfer Solution.

10.2.2 Customer's Transfer Obligations. In respect of Transferred Personal Data under any Agreement, Customer will:

a. enter into Model Contract Clauses as the exporter of such data, if under European Data Protection Law Google reasonably requires Customer to do so; and

b. use an Alternative Transfer Solution offered by Google in respect of such data and take any action (which may include execution of documents) strictly required to give full effect to such solution if under European Data Protection Law Google reasonably requires Customer to do so.

10.3 **Data Center Information**. Information about the locations of Google data centers is available at: https://www.google.com/about/datacenters/inside/locations/index.html (as may be updated by Google from time to time).

10.4 **Disclosure of Confidential Information Containing Personal Data**. If Customer has entered into Model Contract Clauses as described in Section 10.2 (Transfers of Data), Google will, notwithstanding any term to the contrary in the applicable Agreement, ensure that any disclosure of Customer's Confidential Information containing personal data, and any notifications relating to any such disclosures, will be made in accordance with such Model Contract Clauses.

11. **Subprocessors**

11.1 **Consent to Subprocessor Engagement**. Customer specifically authorizes the engagement as Subprocessors of: (a) those entities listed as of the Amendment Effective Date at the URL specified in Section 11.2 (Information about Subprocessors); and (b) all other Google Affiliates from time to time. In addition, without prejudice to Section 11.4 (Opportunity to Object to Subprocessor Changes), Customer generally authorizes the engagement as Subprocessors of any other third parties ("**New Third Party Subprocessors**"). If Customer has entered into Model Contract Clauses as described in Section 10.2 (Transfers of Data), the above authorizations constitute Customer's prior written consent to the subcontracting by Google LLC of the processing of Customer Data.

11.2 **Information about Subprocessors**. Information about Subprocessors, including their functions and locations, is available at https://gsuite.google.com/intl/en/terms/subprocessors.html (as may be updated by Google from time to time in accordance with this Data Processing Amendment).

11.3 **Requirements for Subprocessor Engagement**. When engaging any Subprocessor, Google will:

a. ensure via a written contract that:

i. the Subprocessor only accesses and uses Customer Data to the extent required to perform the obligations subcontracted to it, and does so in accordance with the Agreement (including this Data Processing Amendment) and any Model Contract Clauses entered into or Alternative Transfer Solution adopted by Google as described in Section 10.2 (Transfers of Data); and

ii. if the GDPR applies to the processing of Customer Personal Data, the data protection obligations described in Article 28(3) of the

GDPR, as described in this Data Processing Amendment, are imposed on the Subprocessor; and

b. remain fully liable for all obligations subcontracted to, and all acts and omissions of, the Subprocessor.

11.4 **Opportunity to Object to Subprocessor Changes**.

a. When any New Third Party Subprocessor is engaged during the applicable Term, Google will, at least 30 days before the New Third Party Subprocessor starts processing any Customer Data, notify Customer of the engagement (including the name and location of the relevant subprocessor and the activities it will perform).

b. Customer may, within 90 days after being notified of the engagement of a New Third Party Subprocessor, object by terminating the applicable Agreement immediately upon written notice to Google. This termination right is Customer's sole and exclusive remedy if Customer objects to any New Third Party Subprocessor.

12. **Cloud Data Protection Team; Processing Records**

12.1 **Google's Cloud Data Protection Team**. Google's Cloud Data Protection Team can be contacted by Customer's Administrators at https://support.google.com/a/contact/googlecloud_dpr (while Administrators are signed in to their Admin Account) and/or by Customer by providing a notice to Google as described in the applicable Agreement.

12.2. **Google's Processing Records**. To the extent the GDPR requires Google to collect and maintain records of certain information relating to Customer, Customer will, where requested, use the Admin Console to supply such information and keep it accurate and up-to-date. Google may make any such information available to the Supervisory Authorities if required by the GDPR.

13. **Liability**

13.1 **Liability Cap**. If Model Contract Clauses have been entered into as described in Section 10.2 (Transfers of Data) then, subject to Section 13.2 (Liability Cap Exclusions), the total combined liability of either party and its Affiliates towards the other party and its Affiliates under or in connection with the applicable Agreement and such Model Contract Clauses combined will be limited to the Agreed Liability Cap for the relevant party.

13.2 **Liability Cap Exclusions**. Nothing in Section 13.1 (Liability Cap) will affect the remaining terms of the applicable Agreement relating to liability (including any specific exclusions from any limitation of liability).

14. **Third Party Beneficiary**

Notwithstanding anything to the contrary in the applicable Agreement, where Google LLC is not a party to such Agreement, Google LLC will be a third party beneficiary of Sections 7.5 (Reviews and Audits of Compliance), 11.1 (Consent to Subprocessor Engagement) and 13 (Liability).

15 **Effect of Amendment**

Notwithstanding anything to the contrary in the applicable Agreement, to the extent of any conflict or inconsistency between the terms of this Data Processing Amendment and the remainder of the applicable Agreement, this Data Processing Amendment will govern. For clarity, if Customer has entered more than one Agreement, this Data Processing Amendment will amend each of the Agreements separately.

Appendix 1: Subject Matter and Details of the Data Processing

Subject Matter

Google's provision of the Services and TSS to Customer.

Duration of the Processing

The applicable Term plus the period from the expiry of such Term until deletion of all Customer Data by Google in accordance with the Data Processing Amendment.

Nature and Purpose of the Processing

Google will process Customer Personal Data for the purposes of providing the Services and TSS to Customer in accordance with the Data Processing Amendment.

Categories of Data

Data relating to individuals provided to Google via the Services, by (or at the direction of) Customer or End Users.

Data Subjects

Data subjects include the individuals about whom data is provided to Google via the Services by (or at the direction of) Customer or End Users.

Appendix 2: Security Measures

As from the Amendment Effective Date, Google will implement and maintain the Security Measures described in this Appendix 2.

1. Data Center and Network Security

(a) Data Centers.

Infrastructure. Google maintains geographically distributed data centers. Google stores all production data in physically secure data centers.

Redundancy. Infrastructure systems have been designed to eliminate single points of failure and minimize the impact of anticipated environmental risks. Dual circuits, switches, networks or other necessary devices help provide this redundancy. The Services are designed to allow Google to perform certain types of preventative and corrective maintenance without interruption. All environmental equipment and facilities have documented preventative maintenance procedures that detail the process for and frequency of performance in accordance with the manufacturer’s or internal specifications. Preventative and corrective maintenance of the data center equipment is scheduled through a standard change process according to documented procedures.

Power. The data center electrical power systems are designed to be redundant and maintainable without impact to continuous operations, 24 hours a day, 7 days a week. In most cases, a primary as well as an alternate power source, each with equal capacity, is provided for critical infrastructure components in the data center. Backup power is provided by various mechanisms such as uninterruptible power supplies (UPS) batteries, which supply consistently reliable power protection during utility brownouts, blackouts, over voltage, under voltage, and out-of-tolerance frequency conditions. If utility power is interrupted, backup power is designed to provide transitory power to the data center, at full capacity, for up to 10 minutes until the diesel generator systems take over. The diesel generators are capable of automatically starting up within seconds to provide enough emergency electrical power to run the data center at full capacity typically for a period of days.

Server Operating Systems. Google servers use a Linux based implementation customized for the application environment. Data is stored using proprietary algorithms to augment data security and redundancy. Google employs a code review process to increase the security of the code used to provide the Services and enhance the security products in production environments.

Businesses Continuity. Google has designed and regularly plans and tests its business continuity planning/disaster recovery programs.

(b) Networks and Transmission.

Data Transmission. Data centers are typically connected via high-speed private links to provide secure and fast data transfer between data centers. This is designed to prevent data from being read, copied, altered or removed without authorization during electronic transfer or transport or while being recorded onto data storage media. Google transfers data via Internet standard protocols.

External Attack Surface. Google employs multiple layers of network devices and intrusion detection to protect its external attack surface. Google considers potential attack vectors and incorporates appropriate purpose built technologies into external facing systems.

Intrusion Detection. Intrusion detection is intended to provide insight into ongoing attack activities and provide adequate information to respond to incidents. Google’s intrusion detection involves:

1. tightly controlling the size and make-up of Google’s attack surface through preventative measures;
2. employing intelligent detection controls at data entry points; and
3. employing technologies that automatically remedy certain dangerous situations.

Incident Response. Google monitors a variety of communication channels for security incidents, and Google’s security personnel will react promptly to known incidents.

Encryption Technologies. Google makes HTTPS encryption (also referred to as SSL or TLS connection) available. Google servers support ephemeral elliptic curve Diffie-Hellman cryptographic key exchange signed with RSA and ECDSA. These perfect forward secrecy (PFS) methods help protect traffic and minimize the impact of a compromised key, or a cryptographic breakthrough.

2. Access and Site Controls.

(a) Site Controls.

On-site Data Center Security Operation. Google’s data centers maintain an on-site security operation responsible for all physical data center security functions 24 hours a day, 7 days a week. The on-site security operation personnel monitor closed circuit TV (CCTV) cameras and all alarm systems. On-site security operation personnel perform internal and external patrols of the data center regularly.

Data Center Access Procedures. Google maintains formal access procedures for allowing physical access to the data centers. The data centers are housed in facilities that require electronic card key access, with alarms that are linked to the on-site security operation. All entrants to the data center are required to identify themselves as well as show proof of identity to on-site security operations. Only authorized employees, contractors and visitors are allowed entry to the data centers. Only authorized employees and contractors are permitted to request electronic card key access to these facilities. Data center electronic card key access requests must be made through e-mail, and require the approval of the requestor’s manager and the data center director. All other entrants requiring temporary data center access must: (i) obtain approval in advance from the data center managers for the specific data center and internal areas they wish to visit; (ii) sign in at on-site security operations; and (iii) reference an approved data center access record identifying the individual as approved.

On-site Data Center Security Devices. Google’s data centers employ an electronic card key and biometric access control system that is linked to a system alarm. The access control system monitors and records each individual’s electronic card key and when they access perimeter doors, shipping and receiving, and other critical areas. Unauthorized activity and failed access attempts are logged by the access control system and investigated, as appropriate. Authorized access throughout the business operations and data centers is restricted based on zones and the individual’s job responsibilities. The fire doors at the data centers are alarmed. CCTV cameras are in operation both inside and outside the data centers. The positioning of the cameras has been designed to cover strategic areas including, among others, the perimeter, doors to the data center building, and shipping/receiving. On-site security operations personnel manage the CCTV monitoring, recording and control equipment. Secure cables throughout the data centers connect the CCTV equipment. Cameras record on site via digital video recorders 24 hours a day, 7 days a week. The surveillance records are retained for up to 30 days based on activity.

(b) Access Control.

Infrastructure Security Personnel. Google has, and maintains, a security policy for its personnel, and requires security training as part of the training package for its personnel. Google’s infrastructure security personnel are responsible for the ongoing monitoring of Google’s security infrastructure, the review of the Services, and responding to security incidents.

Access Control and Privilege Management. Customer’s Administrators and End Users must authenticate themselves via a central authentication system or via a single sign on system in order to use the Services.

Internal Data Access Processes and Policies – Access Policy. Google’s internal data access processes and policies are designed to prevent unauthorized persons and/or systems from gaining access to systems used to process personal data. Google designs its systems to: (i) only allow authorized persons to access data they are authorized to access; and (ii) ensure that personal data cannot be read, copied, altered or removed without authorization during processing, use and after recording. The systems are designed to detect any inappropriate access. Google employs a centralized access management system to control personnel access to production servers, and only provides access to a limited number of authorized personnel. Google's authentication and authorization systems utilize SSH certificates and security keys, and are designed to provide Google with secure and flexible access mechanisms. These mechanisms are designed to grant only approved access rights to site hosts, logs, data and configuration information. Google requires the use of unique user IDs, strong passwords, two factor authentication and carefully monitored access lists to minimize the potential for unauthorized account use. The granting or modification of access rights is based on: the authorized personnel's job responsibilities; job duty requirements necessary to perform authorized tasks; and a need to know basis. The granting or modification of access rights must also be in accordance with Google's internal data access policies and training. Approvals are managed by workflow tools that maintain audit records of all changes. Access to systems is logged to create an audit trail for accountability. Where passwords are employed for authentication (e.g., login to workstations), password policies that follow at least industry standard practices are implemented. These standards include restrictions on password reuse and sufficient password strength. For access to extremely sensitive information (e.g., credit card data), Google uses hardware tokens.

3. Data

(a) Data Storage, Isolation and Logging.

Google stores data in a multi-tenant environment on Google-owned servers. Subject to any Customer instructions to the contrary (for example, in the form of a data location selection), Google replicates Customer Data between multiple geographically dispersed data centers. Google also logically isolates Customer Data, and logically separates each End User's data from the data of other End Users, and data for an authenticated End User will not be displayed to another End User (unless the former End User or an Administrator allows the data to be shared).

Customer will be given control over specific data sharing policies. Those policies, in accordance with the functionality of the Services, will enable Customer to determine the product sharing settings applicable to End Users for specific purposes. Customer may choose to use logging functionality that Google makes available via the Services.

(b) Decommissioned Disks and Disk Erase Policy.

Disks containing data may experience performance issues, errors or hardware failure that lead them to be decommissioned ("Decommissioned Disk"). Every Decommissioned Disk is subject to a series of data destruction processes (the "Disk Erase Policy") before leaving Google's premises either for reuse or destruction. Decommissioned Disks are erased in a multi-step process and verified complete by at least two independent validators. The erase results are logged by the Decommissioned Disk's serial number for tracking. Finally, the erased Decommissioned Disk is released to inventory for reuse and redeployment. If, due to hardware failure, the Decommissioned Disk cannot be erased, it is securely stored until it can be destroyed. Each facility is audited regularly to monitor compliance with the Disk Erase Policy.

4. Personnel Security

Google personnel are required to conduct themselves in a manner consistent with the company's guidelines regarding confidentiality, business ethics, appropriate usage, and professional standards. Google conducts reasonably appropriate backgrounds checks to the extent legally permissible and in accordance with applicable local labor law and statutory regulations.

Personnel are required to execute a confidentiality agreement and must acknowledge receipt of, and compliance with, Google's confidentiality and privacy policies. Personnel are provided with security training. Personnel handling Customer Data are required to complete additional requirements appropriate to their role (e.g., certifications). Google's personnel will not process Customer Data without authorization.

5. Subprocessor Security.

Prima di onboarding dei subprocessori, Google effettua un audit delle pratiche di sicurezza e privacy dei subprocessori per garantire che i subprocessori forniscano un livello di sicurezza e privacy adeguato al loro accesso ai dati e alla portata dei servizi che sono impegnati a fornire. Una volta che Google ha valutato i rischi presentati dal Subprocessore, quindi soggetti ai requisiti descritti nella Sezione 11.3 (Requisiti per l'impegno del subprocessore) della presente Modifica sull'elaborazione dei dati, il Subprocessore è tenuto a stipulare appropriati termini di sicurezza, riservatezza e privacy.