Profilo Commerciale

TIM MULTICLOUD Infrastrutturale Google Cloud Platform

1. L'OFFERTA TIM MULTICLOUD

TIM Multicloud è l'offerta di TIM che risponde alle esigenze di Cloud Transformation dei propri clienti. Con tale offerta TIM, già leader del mercato Cloud italiano, integra la famiglia di servizi Cloud proprietari e di hosting nei propri Data Center con le migliori soluzioni di Public Cloud dei principali Provider.

L'offerta TIM Multicloud si propone come soluzione completa di architetture Hybrid & Multicloud in grado di offrire al cliente architetture ibride su misura basate su Private Cloud, TIM Cloud e sul best-in-class dei Public Cloud Provider disponibili sul mercato. Tale offerta permette una migrazione dei propri servizi su diversi Cloud Provider, armonizzando le singole logiche di business per sfruttare al massimo le caratteristiche dei singoli cloud e dei propri server.

TIM offre soluzioni Managed Services su architetture Multicloud, Hybrid e On Premise utilizzando sia servizi del proprio Cloud, contrattualizzabili attraverso la documentazione contrattuale dello specifico Servizio, sia Public Cloud.

Mediante la presente offerta (di seguito "Offerta"), il Cliente acquista il Servizio TIM Multicloud comprendente Risorse Cloud sull'infrastruttura erogata da Google (nel seguito anche "Cloud Service Provider") e fornita da TIM, denominata "Google Cloud Platform", nel seguito anche "GCP", in associazione al bundle di Managed Services erogato da TIM e indicato nella Scheda tecnica, che insieme compongono il "Servizio".

L'Offerta, una volta sottoscritta, consente al Cliente di richiedere l'erogazione di servizi professionali.

Di seguito una descrizione dei servizi previsti nell'offerta, eventualmente dettagliati nell'Allegato tecnico, se presente, e selezionati nella Scheda Tecnica.

2. DESCRIZIONE DEL SERVIZIO

a. RISORSE CLOUD

L'offerta TIM Multicloud mette a disposizione del Cliente le Risorse infrastrutturali di Public Cloud della Google Cloud Platform.

Ai fini del presente Profilo commerciale, per "Tenant" si intende l'istanza Cliente specifica (ove il Cliente può acquistare SaaS, PaaS e IaaS nel mondo Google) riservata da TIM al Cliente sull'infrastruttura Google Cloud Platform e per "Sottoscrizione" il raggruppamento delle Risorse Cloud associate ad una fattura a consumo.

Il Cliente può richiedere a TIM un nuovo Tenant oppure può richiedere a TIM di importare il tenant di cui sia già in possesso ("On Boarding") sotto l'Organization di TIM ("TIM Organization" o "TIM Root") o, ancora, richiedere a TIM la creazione di una nuova Sottoscrizione associata ad un Tenant già esistente.

In caso di On Boarding, al Cliente è richiesto di indicare nella Scheda tecnica la provenienza della Sottoscrizione, se direttamente dal Cloud Service Provider o da altro Partner o da TIM stessa, poiché le procedure di on-boarding possono variare notevolmente. È inoltre richiesto di specificare se l'infrastruttura sia già esistente o se sia da creare a cura TIM.

Per una descrizione delle Risorse Cloud previste nell'Offerta si rimanda all'Allegato tecnico, se presente, e al catalogo dei Prodotti del Cloud Service Provider consultabile sul sito https://cloud.google.com.

a. TIM MANAGED SERVICES

I Managed Services sono una componente fondamentale dell'offerta Multicloud di TIM e vengono erogati da figure professionali di alto livello specialistico. Si tratta di servizi continuativi di gestione operativa end-to end di tutta l'infrastruttura del Cliente, che vengono offerti anche a clienti che non sono in "TIM Root" (vale a dire che non rientrano nella Organization TIM). In questo caso resta a cura del Cliente fornire a TIM le opportune utenze e credenziali.

I Managed Services sono strutturati in tre raggruppamenti di attività ("bundle") di seguito descritti sinteticamente. Per maggiori dettagli si rimanda all'Allegato tecnico.

Specifici SLA possono essere concordati all'interno dei singoli contratti.

Il servizio di **Customer Support** erogato da TIM è compreso in tutti i bundle ed è erogabile sia tramite Numero verde 800199477 pin 1124 sia in modalità Self Ticketing dalla Console di Gestione dei Servizi, sezione Assistenza.

Le richieste di intervento saranno prese in carico secondo i profili e le tempistiche indicate nella tabella seguente:

Bundle	PROFILO Customer Support	SLA PRESA IN CARICO NON BLOCCANTE	SLA PRESA IN CARICO BLOCCANTE	DISPONIBILITÀCANALI ASSISTENZA
Base Managed	Standard	entro 24 ore	entro 12 ore	h24 x 365
	Professional	entro 4 ore	entro 2 ore	
	Business	entro 1 ora	entro 30 minuti	
Full Managed	Business	entro 1 ora	entro 30 minuti	
Full Managed Plus	Business	entro 1 ora	entro 30 minuti	

Base Managed

Il Bundle Base Managed è rivolto ai clienti che intendono gestire le Risorse Cloud, ma desiderano affidarsi ad un partner qualificato quale TIM come unico punto di accesso verso il Cloud Service Provider, senza cedere la gestione delle Risorse Cloud. I clienti che scelgono soluzioni Base Managed hanno accesso alle Console di servizio dei Cloud Service provider su Tenant TIM per lavorare in massima autonomia su tutti gli elementi, godendo sempre del supporto della Control Room TIM (Customer Support) e accedendo ai servizi professionali e di consulenza erogati da TIM.

Full Managed

Il cliente che contrattualizza il Bundle Full Manged, oltre a fruire del Customer Support, affida a TIM la gestione sistemistica e middleware della propria infrastruttura Cloud, nonché la configurazione, la gestione e il monitoraggio di servizi presenti sulle piattaforme dei Cloud Service Provider (es: ML, serverless ecc.).

Full Managed Plus

Il Bundle Full Managed Plus prevede l'outsourcing completo a TIM da parte del Cliente del proprio ambiente applicativo, consentendogli di focalizzarsi sui propri contenuti restando responsabile del codice applicativo (Full Platform Operations). Oltre al Customer Support, fanno parte di questo gruppo un insieme di attività dettagliate nell'Allegato tecnico, tra cui:

- Monitoraggio;
- Management;
- Workload management;
- Infrastructure and Cost optimization (opzionale);
- Compliance management;
- Vulnerability & Remediation.

Servizi Professionali a richiesta

I Clienti TIM Multicloud hanno a disposizione un set di ulteriori servizi professionali, che consistono in attività professionali erogate su richiesta e caratterizzate da una assenza di continuità e che possono essere richiesti esclusivamente tramite la Console di Gestione Servizi, lo strumento messo a disposizione da TIM come meglio descritto successivamente.

L'elenco dei Servizi professionali disponibili di cui il Cliente può richiedere la fornitura sulla propria sottoscrizione è riportato nell'Allegato B.

3. CONSOLE DI GESTIONE SERVIZI

La Console di Gestione Servizi (https://servizi.nuvolaitaliana.it) è lo strumento messo a disposizione del Cliente da TIM per inoltrare richieste di assistenza disponibili per il Servizio contrattualizzato relativamente ai Servizi già attivi.

- apre e gestisce ticket per richieste e segnalazioni verso TIM;
- accede ai report relativi al riepilogo degli SLA e dei ticket aperti;
- monitora i consumi delle Risorse Cloud e il relativo corrispettivo;
- richiede l'erogazione dei Servizi professionali opzionali;
- accede a tool e funzionalità previste nel Servizio contrattualizzato.

Nel caso in cui il Cliente abbia aperto un Ticket sulla Console, il Cliente si impegna a fornire riscontro riguardo il buon esito dell'attività svolta da TIM, rispondendo per iscritto entro 2 (due) giorni lavorativi alla comunicazione di chiusura del Ticket inviata da TIM. In mancanza di contestazioni da comunicarsi per iscritto a cura del Cliente entro il suddetto termine, TIM provvederà a chiudere il Ticket decorsi i successivi 5 (cinque) giorni lavorativi.

4. MODALITA' DI ATTIVAZIONE DEL SERVIZIO

Il personale TIM, completata la configurazione del Servizio, ne comunica al Cliente la relativa attivazione tramite l'invio all'indirizzo del Referente tecnico indicato dal Cliente di una e-mail contenente anche le credenziali di accesso al Portale di amministrazione del Cloud Service Provider, se previsto, e l'indirizzo web di accesso alla Console di Gestione Servizi (https://servizi.nuvolaitaliana.it/) e relative chiavi di accesso. Qualora l'Allegato tecnico preveda attività di collaudo, il Servizio si considererà attivato alla data della sottoscrizione del verbale conclusosi con esito positivo.

5. CONDIZIONI ECONOMICHE E FATTURAZIONE

Fatto salvo quanto diversamente pattuito tra le Parti, TIM emetterà le fatture relative ai corrispettivi dovuti per il Servizio con cadenza bimestrale.

Risorse infrastrutturali Cloud fornite da TIM

Le Risorse Cloud contrattualizzate in modalità a consumo verranno fatturate da TIM al Cliente a consuntivo, in ragione dell'effettivo utilizzo da parte del Cliente, sulla base del consumo registrato dal Cloud Service Provider e del listino in vigore al momento dell'utilizzo del Servizio. I corrispettivi e/o i costi unitari di riferimento sono indicati nel listino pubblicato all'indirizzo https://cloud.google.com. Tale listino è suscettibile di variazioni da parte del Cloud Service Provider.

Resta inteso che, nella prima fattura utile, verranno addebitati anche i costi dei consumi di Risorse Cloud utilizzate durante l'eventuale fase di predisposizione dell'ambiente del Cliente da parte di TIM.

Le Risorse Cloud "*Reserved*" saranno a disposizione del Cliente a prescindere dal loro effettivo utilizzo fino alla cessazione della Risorsa o dell'intero Progetto ("Project") e verranno fatturate da TIM al Cliente a consuntivo a partire dal primo ciclo di fatturazione utile successivo alla loro attivazione. Il listino di riferimento è quello in vigore al momento dell'attivazione di tali Risorse, che rimane invariato per la durata del periodo in cui restano attive, al netto delle fluttuazioni valutarie. L'eventuale eccedenza verrà addebitata da TIM sulla base del consumo registrato dal Cloud Service Provider. Il Cliente può cessare tali Risorse in qualsiasi momento senza oneri a proprio carico.

Se il Cliente acquista Risorse Reserved in abbinamento all'impegno di consumo di un determinato volume in un determinato periodo di tempo, tali Risorse riservate rimarranno disponibili al Cliente per il periodo concordato.

Dettagli e condizioni sono pubblicati sul sito di Google al link https://cloud.google.com/compute/docs/instances/reserving-zonal-resources**.**

Il Cliente può monitorare i consumi delle Risorse Cloud e il relativo corrispettivo consultando la Console di Gestione Servizi.

TIM Managed Services

I TIM Managed Services verranno fatturati a consuntivo. I corrispettivi dovuti vengono valorizzati tramite una percentuale calcolata sul corrispettivo dovuto per i consumi delle Risorse Cloud.

I Servizi professionali verranno fatturati da TIM in unica soluzione (Una Tantum) nella prima fattura utile a partire dalla data di chiusura del relativo Ticket.

TIM avrà la facoltà di avvalersi dell'istituto della cessione del credito nel rispetto delle normative applicabili (Art. 106, comma 13, del D. Lgs. 50/2016 e s.m.i..)

La fatturazione dei corrispettivi dovuti per il Servizio avverrà in unica soluzione. In applicazione del DM 55 del 03.04.2013 ("Regolamento in materia di emissione, trasmissione e ricevimento della fattura elettronica da applicarsi alle amministrazioni pubbliche ai sensi dell'articolo 1, commi da 209 a 213, della legge 24/12/2007, n. 244"), il Cliente dovrà fornire a TIM il Codice Ufficio di destinazione delle fatture elettroniche ivi previsto nonché il Codice Identificativo di Gara (CIG) e, nei casi previsti, il CUP. Le

fattura e/o le comunicazioni inviate sia in via elettronica che cartacea si intenderanno come pervenute trascorsi 15 (quindici) giorni dalla data del relativo invio e la prova contraria fornita dal Cliente.

Telecom assume tutti gli obblighi di tracciabilità dei flussi finanziari di cui all'art. 3 della legge 13 agosto 2010, n. 136 e successive modifiche.

6. TRATTAMENTO DEI DATI PERSONALI AI SENSI DEL REGOLAMENTO 2016/679/EU (REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI)

Nomina a Responsabile del trattamento

Per l'esecuzione del presente Contratto, le Parti si conformano al Regolamento 2016/679/EU (Regolamento Generale sulla Protezione dei Dati - d'ora in avanti "GDPR") ed alle ulteriori disposizioni normative vigenti in materia di protezione dei dati personali (d'ora in avanti congiuntamente "Normativa sulla protezione dei dati personali applicabile").

In particolare, TIM Spa (d'ora in avanti anche il "Responsabile") viene nominata dal Cliente (d'ora in avanti anche il "Titolare"), ai sensi dell'art. 28 del GDPR, responsabile del trattamento dei dati personali relativi ai clienti e/o dipendenti e/o fornitori del Titolare trattati nell'ambito della fruizione del Servizio oggetto del presente Contratto, esclusivamente per la finalità relativa all'erogazione di tale Servizio.

Il Richiedente dichiara di non utilizzare il Servizio per il trattamento delle categorie particolari di dati di cui all'articolo 9 del GDPR.

Il Responsabile, nell'ambito delle condizioni/istruzioni fornite dal Titolare nella presente clausola:

- tratta solo dati personali comuni;
- relativamente al bundle di Managed Services selezionato dal Richiedente nell'Allegato 5 – Scheda Tecnica, effettua i seguenti trattamenti:

Bundle	**Trattamenti effettuati**
Base Managed	Gestione infrastrutturale (*)
Full Managed	Gestione Infrastrutturale (*), Gestione sistemistica, Gestione Middleware, Storage, Backup
Full Managed Plus	Gestione Infrastrutturale (*), Gestione sistemistica, Gestione Middleware, Gestione applicativa, Storage, Backup

(*) In relazione alle attività di Gestione Infrastrutturale, le attività relative al trattamento dei dati personali è affidata e saranno svolte dal Subfornitore indicato di seguito al paragrafo "**Trattamento di dati personali da parte di Sub-fornitori/Sub-appaltatori**"

- effettua i trattamenti mediante strumenti elettronici o comunque automatizzati e/o con strumenti cartacei.

TIM cesserà il trattamento dei dati personali effettuato ai sensi del Contratto entro un termine massimo di 30 (trenta) giorni dalla data di cessazione del Servizio o dalla scadenza dell'ulteriore termine previsto nel Contratto successivamente alla cessazione, per il salvataggio dei dati.

Limitatamente ai servizi offerti su Risorse in Cloud fornite da Google, la cancellazione di tutti i dati presenti sulle Risorse in Cloud sarà effettuata da Google non appena ragionevolmente possibile e comunque entro un periodo massimo di 180 giorni, salvo il caso in cui Google sia tenuto a conservare i dati in osservanza della normativa applicabile.

TIM dichiara di fornire garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del GDPR e garantisca la tutela dei diritti degli Interessati.

A tal fine, il Responsabile, per mezzo del procuratore che sottoscrive il Contratto, dichiara di accettare sin d'ora tale nomina e di impegnarsi ad osservare le condizioni/istruzioni riportate nella presente clausola, negli Allegati qui richiamati e nella Proposta di Attivazione Servizi Infrastrutturali e Multicloud.

La presente nomina decorre dalla data in cui viene sottoscritto il Contratto dalle Parti ed è valida fino alla cessazione delle attività sopra citate e comunque non oltre la scadenza del Contratto, ovvero fino alla revoca anticipata per qualsiasi motivo da parte del Titolare, fermo restando l'eventuale periodo ulteriore di conservazione dei dati indicata nella tabella qui sopra per il salvataggio dei dati e la cancellazione dei backup. Fermo restando il diritto del Richiedente di ottenere il salvataggio dei dati secondo quanto previsto dalle condizioni contrattuali, la cessazione delle attività o la revoca anticipata comportano automaticamente cessazione dei trattamenti e la distruzione o cancellazione dei relativi dati personali, come indicato al successivo punto 11 delle **Istruzioni e misure di sicurezza**.

Trattamento di dati personali da parte di Sub-fornitori/Sub-appaltatori

Il Titolare, ai sensi del paragrafo 2 dell'art. 28 del GDPR autorizza il Responsabile ad avvalersi di Google LLC, Google Ireland Limited, Google Asia Pacific Pte. Ltd., o qualsiasi altra entità che direttamente o indirettamente controlla, è controllata da, o è sotto controllo comune con Google LLC (cumulativamente, "Google") per svolgere le attività di cui alla presente nomina in qualità di responsabile ulteriore del trattamento (sub-responsabile).

Inoltre, il Titolare autorizza il Responsabile ad avvalersi di eventuali ulteriori soggetti terzi (subappaltatori/subfornitori) (collettivamente, "Sub-responsabili") per svolgere le attività di cui alla presente nomina il cui elenco aggiornato è reperibile al seguente indirizzo: https://assistenza.timbusiness.it/guida/wp-content/uploads/2018/05/Elenco-partner-di-TIM-GDPR-v1.pdf.

Conseguentemente il Responsabile si impegna, prima dell'inizio del trattamento, a nominare i propri Sub-responsabili utilizzando le medesime istruzioni con le quali è stato nominato a sua volta Responsabile del trattamento dal Titolare, o comunque, prevedendo obblighi analoghi in materia di protezione dei dati contenuti nel presente Contratto, in modo tale che il trattamento soddisfi i requisiti previsti dai paragrafi 2 e 4 dell'art. 28 del GDPR. Inoltre, con riferimento ai trattamenti effettuati da Google e dai suoi ulteriori Sub-responsabili si applicano le ulteriori **Istruzioni specifiche del trattamento dai dati personali effettuato da Google** di seguito indicate.

Il Responsabile informerà il Titolare rendendo disponibili l'elenco dei nuovi Sub-responsabili. In caso di modifiche riguardanti l'aggiunta o la sostituzione di Sub-responsabili, il Responsabile provvederà a informare tempestivamente il Titolare attraverso PEC o e-mail (all'indirizzo comunicato dal Titolare).

Il Titolare del trattamento potrà opporsi alle modifiche proposte dal Responsabile mediante comunicazione scritta da inviarsi al Responsabile entro 10 (dieci) giorni dalla proposta di modifica. Qualora il Titolare del trattamento si opponga alla modifica , ove possibile e fatta eccezione per i servizi offerti da Google (se applicabili ai Servizi) per cui valgono le **Istruzioni specifiche del trattamento dai dati personali effettuato da Google** di seguito indicate, il Responsabile si riserva il diritto di scegliere un altro Sub-responsabile; nel caso in cui il Titolare del trattamento si opponga, nei termini sopra previsti, anche a tale ultima modifica, il Titolare prende atto e accetta che il Contratto si intenderà cessato per mutuo consenso del Titolare e del Responsabile e il Titolare dovrà rimborsare i costi sostenuti dal Responsabile per l'implementazione del servizio oggetto del Contratto e non ancora ammortizzati.

In caso di trasferimento dei dati personali verso Paesi extra UE senza un adeguato livello di protezione dei dati personali ad un'eventuale Sub-responsabile, TIM è autorizzata dal Titolare a sottoscrivere, per conto del Titolare ai sensi dell'art. 1704 c.c., con il Sub-responsabile anche le "clausole tipo di protezione dei dati" previste dalla Commissione Europea ed adottate dal Garante privacy con l'autorizzazione n. 35/2010, ai sensi della Direttiva 95/46/CE.

Istruzioni e misure di sicurezza

Il Responsabile si impegna ad osservare ed a fare osservare, ai propri dipendenti e a chiunque altro sia deputato a trattare i dati personali forniti dal Titolare, le disposizioni di cui alla Normativa sulla protezione dei dati personali applicabile, nonché le istruzioni previste nella presente clausola.

In relazione al provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 in materia di misure e accorgimenti relativi all'attribuzione delle funzioni di amministratore di sistema e successive modifiche ed integrazioni, il Responsabile si impegna ad osservare quanto previsto dal citato provvedimento.

Il Titolare si riserva di verificare l'efficacia delle misure di sicurezza adottate dal Responsabile, anche attraverso controlli presso le sedi del Responsabile stesso ove sono effettuati i trattamenti di dati personali; a tal fine il Responsabile permetterà l'accesso al personale autorizzato dal Titolare ad effettuare tali controlli, avendo ricevuto un preavviso di almeno 20 giorni lavorativi. Le verifiche saranno condotte nei normali orari di ufficio e senza ostacolare il normale svolgimento delle attività del Responsabile, previo accordo che stabilisca le modalità ed i corrispettivi.

Il Responsabile del trattamento si conforma inoltre alle seguenti istruzioni:

1. Garantisce che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza.
2. In conformità a quanto previsto dall'art. 32 del GDPR, realizza le misure di sicurezza previste nel presente Contratto e quelle prescritte da eventuali provvedimenti del Garante Privacy in relazione alle attività oggetto della presente nomina. L'elenco aggiornato è reperibile al seguente indirizzo: https://assistenza.timbusiness.it/professionisti/risorse-utili/trattamento-dati-personali/ .
3. In conformità a quanto previsto dall'art. 32 del GDPR, fornisce alle persone autorizzate al trattamento precise istruzioni operative per il trattamento dei dati personali, tenuto anche conto della natura dei dati trattati (categorie particolari di dati personali) e di eventuali situazioni organizzative/ambientali particolari.
4. Assicura la riservatezza, l'integrità e la disponibilità dei dati, nonché il loro utilizzo esclusivo per le finalità in base alle quali il trattamento è stato autorizzato, comunicando immediatamente al Titolare qualunque evento, di cui il Responsabile sia venuto a conoscenza in esecuzione del Contratto, che abbia violato o posto in pericolo la riservatezza, l'integrità o la disponibilità dei dati medesimi per i possibili eventi di "violazione di dati personali" in conformità a quanto previsto dalla normativa sul trattamento dei dati personali applicabile.
5. Assicura che i dati personali siano conservati per il periodo di tempo strettamente necessario all'esecuzione delle attività/servizi richiesti dal Titolare, e comunque non oltre i termini di volta in volta indicati dal Titolare medesimo.
6. Tenendo conto della natura del trattamento, assiste il Titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del Titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al Capo III del GDPR.
7. Comunica al Titolare, al momento della ricezione, eventuali richieste di informazioni o comunicazioni degli interessati o del Garante per la protezione dei dati personali, in modo da consentire al Titolare di provvedere al relativo riscontro. Ove richiesto, il Responsabile fornirà al Titolare le necessarie informazioni e/o collaborazione, per quanto di competenza.
8. Assiste il Titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 del GDPR, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento.
9. Assicura che i dati personali oggetto di trattamento non siano comunicati o diffusi in Italia o che non siano trasferiti, comunicati, diffusi o altrimenti trattati all'estero (Paesi Ue ed extra Ue), neanche presso propri uffici o collaboratori, senza la preventiva autorizzazione del Titolare.
10. Effettua, ai fini della corretta applicazione della Normativa sulla protezione dei dati personali applicabile e delle istruzioni/procedure fornite dal Titolare, controlli periodici sugli adempimenti e sulle attività delle persone autorizzate al trattamento dei dati personali, realizzando le azioni correttive eventualmente necessarie.

11. Assicura che alla cessazione del contratto per qualsiasi causa i dati, secondo le istruzioni ricevute Titolare e sulla base delle previsioni del Contratto, vengano cancellati o restituiti (mediante salvataggio dei dati stessi, nei casi previsti dal Contratto) al Titolare o al terzo autorizzato dallo stesso Titolare, provvedendo in ogni caso a dichiarare per iscritto al Titolare o al terzo autorizzato che i dati sono stati restituiti o distrutti e che presso il Responsabile non ne esiste alcuna copia.
12. Informa immediatamente il Titolare del trattamento qualora, a suo parere, un'istruzione violi la Normativa sulla protezione dei dati personali applicabile.
13. Esegue ogni altro adempimento e/o operazione necessari per garantire il pieno rispetto delle disposizioni del GDPR e dei provvedimenti emessi dal Garante per la protezione dei dati personali.
14. Il Responsabile deve tenere un registro di tutte le categorie di attività relative al trattamento svolte per conto del Titolare, in conformità a quanto previsto dal paragrafo 2 dall'articolo 30 del GDPR.

Le Parti si impegnano, ognuna per quanto di competenza nell'ambito del presente Contratto, a mantenersi reciprocamente indenni da ogni contestazione, azione o pretesa avanzate da parte degli interessati e/o di qualsiasi altro soggetto e/o Autorità a seguito di eventuali inosservanze alla Normativa sulla protezione dei dati personali applicabile nei limiti di quanto indicato nel punto 5) dell'Articolo 2.1.11 delle Condizioni Particolari.

Il Responsabile si impegna a prevedere le garanzie indicate nella presente clausola e negli Allegati ivi richiamati a favore del Titolare nell'eventuale contratto di subappalto o di subfornitura.

Il Responsabile, ai sensi dell'art. 28 paragrafo 4 del GDPR, riconosce che, qualora il proprio subappaltatore o subfornitore ometta di adempiere ai propri obblighi relativi alla nomina a Responsabile ricevuta, conserva nei confronti del Titolare l'intera responsabilità dell'adempimento degli obblighi del proprio subappaltatore o subfornitore, nei limiti previsti dal Contratto e nella presente nomina.

Istruzioni specifiche del trattamento dai dati personali effettuato da Google

In relazione alle Risorse Cloud fornite da Google, il Richiedente prende atto delle seguenti istruzioni specifiche relative ai trattamenti effettuati da Google, quale Sub-responsabile del trattamento, ai fini del Contratto e dichiara e riconosce che dette istruzioni specifiche sono rilevanti a tutti gli effetti quali istruzioni impartite per il trattamento dei Dati del Richiedente ("Istruzioni Specifiche").

Per quanto non diversamente precisato nel presente Allegato, gli obblighi previsti nell'art. 7 Trattamento dei dati personali – Nomina a responsabile del trattamento del Profilo/Offerta Commerciale trovano applicazione anche in relazione al trattamento svolto da Google.

1. Definizioni

1.1 Ad integrazione delle definizioni contenute nel testo del Contratto, ai fini del presente Allegato i seguenti termini avranno il significato di seguito descritto:

- Clausole Contrattuali Tipo o SSC si intendono le clausole standard di protezione dei dati per il trasferimento di dati personali a responsabili del trattamento stabiliti in paesi terzi che non garantiscono un livello adeguato di protezione dei dati, come descritto nell'Articolo 46 del GDPR UE, resi disponibili al seguente link https://cloud.google.com/terms/eu-model-contract-clause (/terms/eu-model-contract-clause).
- Controlli di Sicurezza Aggiuntivi si intendono le risorse di sicurezza, le caratteristiche, le funzionalità e/o i controlli che TIM può utilizzare a sua discrezione e/o secondo le sue decisioni, tra cui la Console di Amministrazione, la crittografia, la registrazione e il monitoraggio, la gestione dell'identità e degli accessi, la scansione della sicurezza e i firewall.
- Documentazione di Sicurezza si intendono tutti i documenti e le informazioni messi a disposizione di TIM da Google, quali le certificazioni di conformità e i rapporti SOC al fine di dimostrare la conformità di Google agli obblighi contrattuali con TIM.

- GDPR significa, a seconda dei casi: a) il GDPR UE; e/o b) il GDPR UK.
- GDPR UE significa Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE.
- GDPR UK si intende il GDPR UE come modificato e incorporato nella legislazione del Regno Unito ai sensi del UK European Union (Withdrawal) Act 2018, se in vigore.
- Normativa Europea o Nazionale si intende, a seconda dei casi: (a) la legislazione dell'UE o di uno Stato membro dell'UE (se il GDPR dell'UE si applica al trattamento dei dati personali del Partner); e/o (b) la legislazione del Regno Unito o di una parte del Regno Unito (se il GDPR del Regno Unito si applica al trattamento dei Dati del Richiedente).
- Normativa Europea sulla Protezione dei Dati si intende, a seconda dei casi: a) il GDPR; e/o b) la Legge Federale sulla Protezione dei Dati del 19 giugno 1992 (Svizzera).
- Normativa sulla Protezione dei Dati Non Europea si intendono le leggi sulla protezione dei dati o sulla privacy in vigore al di fuori dello Spazio Economico Europeo, della Svizzera e del Regno Unito.
- Revisore Terzo di Google si intende un revisore di terza parte nominato da Google, qualificato e indipendente, la cui identità sarà comunicata da Google a TIM.
- SEE significa Spazio Economico Europeo.
- Servizi Affidati significano i servizi Google Cloud Platform offerti da TIM al Richiedente.
- Servizi Revisionati si intendono i Servizi elencati nell'ambito di applicazione della relativa certificazione o revisione come individuati, nel tempo, su https://cloud.google.com/security/compliance/services-in-scope. Google potrà rimuovere dall'elenco presente in tale indirizzo URL un Servizio inizialmente inserito solo se tale Servizio è stato dismesso da Google nel rispetto di quanto previsto dal Contratto.
- Soluzione Alternativa di Trasferimento si intende una soluzione, diversa dalle Clausole Contrattuali Tipo, che consente il legittimo trasferimento di dati personali verso un paese terzo in conformità con la Normativa Europea sulla Protezione dei Dati.
- Sub-responsabile si intende una terza parte autorizzata come ulteriore responsabile, ai sensi del presente Allegato, ad avere accesso logico e a trattare i Dati del Richiedente al fine di fornire parte dei Servizi e dei TSS.

2. Trattamento dei Dati

2.1 Il trattamento dei Dati del Richiedente effettuato da Google è il seguente:

Oggetto: Fornitura del servizio Google Cloud Platform e del supporto tecnico (TSS) a TIM.

Durata del Trattamento: Per tutto il periodo di validità del Contratto e il periodo transitorio dalla cessazione del Contratto fino alla cancellazione di tutti i Dati del Richiedente secondo i tempi descritti al punto 3.

Natura e Finalità del Trattamento: Google tratterà i Dati del Richiedente ai fini della fornitura dei Servizi Affidati correlati alle Risorse Cloud come individuate nel Profilo/Offerta Commerciale e dei servizi di TSS a TIM.

Categorie di Dati: Dati relativi agli Interessati del trattamento e che sono forniti a Google tramite i Servizi Affidati, da (o su indicazione di) TIM o dei Richiedente.

Interessati del Trattamento: I soggetti interessati comprendono i soggetti a cui si riferiscono i dati forniti a Google tramite i Servizi Affidati da (o su indicazione di) TIM o del Richiedente.

3. Cancellazione dei Dati

3.1 Fermo restando quanto previsto nella Nomina a responsabile del trattamento riportata nel Profilo/Offerta Commerciale in termini di durata del trattamento e delle conseguenze in caso di cessazione del Contratto in relazione ai Servizi Affidati, resta inteso che qualora TIM provveda, in pendenza del periodo di validità del Contratto, alla cancellazione dei Dati del Richiedente (o di parte di essi) secondo le istruzioni impartite dal Richiedente utilizzando le funzionalità dei Servizi Affidati, i Dati del Richiedente saranno cancellati dai sistemi di Google, nel rispetto della normativa applicabile non appena ragionevolmente possibile, e comunque entro un termine massimo di 180 giorni, a meno che la Normativa Europea e Nazionale non ne richieda la conservazione.

4. Sicurezza dei Dati

4.1 Misure di Sicurezza di Google. Google applicherà e manterrà in vigore misure tecniche e organizzative per proteggere i Dati del Richiedente da distruzione accidentale o illegale, perdita, alterazione, divulgazione o accesso non autorizzati, come descritto nel paragrafo **Misure di Sicurezza Google** di seguito riportato (le "Misure di Sicurezza"). Le Misure di Sicurezza includono misure per la crittografia dei dati personali; per contribuire a garantire la costante riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi di Google; per contribuire a ripristinare tempestivamente l'accesso ai dati personali in seguito ad un incidente; e per effettuare regolari test di efficacia. Google può aggiornare le Misure di Sicurezza di volta in volta, a condizione che tali aggiornamenti non comportino il degrado della sicurezza complessiva dei Servizi Affidati.

4.2 Controlli di Sicurezza Aggiuntivi. Google metterà a disposizione Controlli di Sicurezza Aggiuntivi volti a (a) adottare misure per proteggere i Dati del Richiedente; e (b) fornire a TIM informazioni sulla sicurezza, sull'accesso e sull'utilizzo dei Dati del Richiedente.

4.3 Supporto in relazione alla Sicurezza. Google (tenendo conto della natura del trattamento dei Dati del Richiedente e delle informazioni a disposizione di Google) supporterà TIM nell'adempimento degli obblighi ai sensi degli Artt. 32-34 del GDPR:

a. applicando e mantenendo le Misure di Sicurezza
b. mettendo a disposizione di TIM i Controlli di Sicurezza Aggiuntivi;
c. provvedendo prontamente a informare TIM in caso di *data breach* nel rispetto di quanto previsto dal GDPR;
d. fornendo a TIM la Documentazione di Sicurezza e
e. fornendo, su richiesta di TIM, ulteriore ragionevole assistenza.

4.4 Certificazioni di Conformità e Rapporti SOC. Con riguardo ai Servizi Revisionati, al fine di valutare la continua efficacia delle Misure di Sicurezza, Google si impegna a mantenere quantomeno (a) i certificati rilasciato a fini ISO 27001 , ISO 27017 e ISO 27018 e la relativa Attestazione di Conformità PCI DSS (le "Certificazioni di Conformità") e (b) i rapporti SOC 2 e SOC 3 prodotti dal Revisore Terzo di Google e aggiornati annualmente sulla base di un audit effettuato almeno una volta ogni 12 mesi (i "Rapporti SOC"). Google può aggiungere altri standard in qualsiasi momento e sostituire una Certificazione di Conformità o un Rapporto SOC con alternative equivalenti o superiori.

4.5 Diritti di verifica.

a. Qualora si applichi la Normativa Europea sulla Protezione dei Dati al trattamento dei Dati del Richiedente, Google consentirà a TIM o a un revisore indipendente nominato da TIM o dal Richiedente di condurre verifiche (comprese le ispezioni) per accertare il rispetto da parte di Google degli obblighi previsti contrattualmente in merito al trattamento dei Dati del Richiedente.
b. TIM può condurre verifiche per accertare il rispetto da parte di Google degli obblighi previsti contrattualmente, esaminando la Documentazione di Sicurezza (che riflette l'esito delle verifiche condotte dal Revisore Terzo di Google).

5. Collaborazione nelle Valutazioni d'Impatto e Consultazioni; Accesso ecc.; Diritti dell'interessato; Esportazione dei Dati

5.1 Valutazioni di impatto. Google (tenendo conto della natura del trattamento e delle informazioni a disposizione di Google) fornirà assistenza a TIM al fine di garantire l'adempimento degli obblighi di collaborazione, quale responsabile del trattamento, nei confronti del Richiedente in caso di supporto ai fini della conduzione di valutazioni di impatto, o consultazioni ai sensi dell'art. 36 del GDPR, rendendo disponibile i Controlli di Sicurezza Aggiuntivi, la Documentazione di Sicurezza e i Controlli della Documentazione di Sicurezza e, se necessario, fornendo ulteriore ragionevole assistenza.

5.2 Accesso; Rettifica; Limitazione del Trattamento; Portabilità. Nel corso del periodo di validità del Contratto:

a. Google consentirà a TIM, in modo coerente con la funzionalità dei Servizi, di accedere, rettificare e limitare il trattamento dei Dati del Richiedente e di esportare i Dati del Richiedente;
b. qualora Google riceva una richiesta da un soggetto interessato in relazione ai Dati del Richiedente e la richiesta identifica il Richiedente, Google consiglierà al soggetto interessato di presentare la sua richiesta a TIM, il quale potrà dar seguito a tale richiesta, ove ciò sia autorizzato dal Richiedente, utilizzando le funzionalità dei Servizi Affidati.

6. Trasferimenti di Dati

6.1 Obblighi Relativi al Trasferimento dei Dati. Se la conservazione e/o il trattamento dei Dati del Richiedente comportano, nel rispetto delle istruzioni impartite dal Richiedente, il trasferimento di Dati del Richiedente al di fuori dallo SEE, Svizzera o Regno Unito, Google si impegna a:

a. stipulare le Clausole Contrattuali Tipo con TIM, che agirà per conto del Richiedente, e assicurare che i trasferimenti siano effettuati in conformità a tali Clausole Contrattuali Tipo; e/o

b. offrire una Soluzione Alternativa di Trasferimento di tali dati prevista dalla Normativa sulla protezione dei dati personali applicabile, garantire che i trasferimenti siano effettuati in conformità a tale Soluzione Alternativa di Trasferimento e mettere a disposizione di TIM informazioni su tale Soluzione Alternativa di Trasferimento che TIM accetterà per conto del Richiedente.

Nel caso in cui il Richiedente non ritenesse le Clausole Contrattuali Tipo più idonee per il trasferimento dei dati al di fuori dallo SEE, Svizzera o Regno Unito e non fosse possibile individuare una Soluzione Alternativa di Trasferimento dei dati, il Richiedente potrà recedere dall'Offerta senza oneri a proprio carico con un preavviso di 30 (trenta) giorni secondo le modalità indicate nell'articolo 16.4 delle Condizioni Generali ICT Infrastrutturali e Multicloud relativamente all'invio delle comunicazioni.

6. Informazioni sui Data Center. Le informazioni relative all'ubicazione delle strutture di Google sono disponibili all'indirizzo: https://cloud.google.com/about/locations/ (soggetto ad aggiornamento nel tempo da parte di Google).

6.3 Comunicazione di Informazioni Riservate Contenenti Dati Personali. In caso di trasferimento dei Dati del Richiedente sulla base delle Clausole di Contratto Tipo, Google garantirà che qualunque comunicazione delle Informazioni Riservate contenenti Dati del Richiedente, e qualsiasi notifica relativa a tali comunicazioni, sarà effettuata in conformità a tali Clausole di Contratto Tipo.

7. Sub-responsabili

7.1 Consenso ad Avvalersi di Sub-responsabili. Il Richiedente, tramite TIM, autorizza specificamente Google affinché si avvalga dei seguenti soggetti quali Sub-responsabili: (a) i soggetti elencati all'URL indicata nel punto 7.2 che segue e (b) tutte le altre Affiliate Google che sono di volta in volta incaricate di specifici compiti, nonché Google LLC. Inoltre, fatto salvo quanto previsto al punto 7.4, TIM, su incarico del Richiedente, autorizza Google, in via generale, ad avvalersi di terze parti quali Sub-responsabili ("Nuovi Sub-responsabili Terzi"). Qualora TIM abbia stipulato, su incarico del Richiedente, Clausole Contrattuali Tipo, le suddette autorizzazioni sono valide ai fini del previo consenso scritto al subappalto a Google LLC del trattamento dei Dati del Richiedente.

7.3 Informazioni sui Sub-responsabili. Le informazioni sui Sub-responsabili di cui Google potrà avvalersi, ove autorizzata per il tramite di TIM, incluse le loro funzioni e la loro ubicazione, sono disponibili all'indirizzo: https://cloud.google.com/terms/subprocessors (che potrà essere aggiornato nel tempo).

7.4 Condizioni per Avvalersi di Sub-responsabili. In caso di affidamento di attività di trattamento da parte di Google ad un ulteriore Sub-responsabile, Google:

a. garantirà attraverso un contratto scritto che:

   i. il Sub-responsabile acceda e utilizzi i Dati del Richiedente solo nella misura necessaria ad adempiere agli obblighi ad esso subappaltati, e che agisca in conformità al Contratto e alle eventuali Clausole Contrattuali Tipo stipulate da Google o all'eventuale Soluzione Alternativa di Trasferimento adottata da Google come descritto al punto 6, e

   ii. gli obblighi di protezione dei dati di cui all'Articolo 28, paragrafo 3, del Regolamento europeo Regolamento 2016/679/EU (Regolamento generale sulla protezione dei dati) siano imposti al Sub-responsabile.

7.5 Possibilità di Opporsi a Modifiche dei Sub-responsabili.

a. In caso di affidamento di un incarico ad un ulteriore Sub-responsabile da parte di Google, TIM notificherà al Richiedente (e, in particolare, all'indirizzo e-mail del Referente Tecnico indicato dal Richiedente nel Contratto) l'affidamento dell'incarico relativo al nuovo Sub-responsabile (comunicando altresì il nome e la sede del relativo Sub-responsabile e le attività che svolgerà) con un preavviso di almeno 20 giorni rispetto all'inizio dei trattamenti dei Dati del Richiedente.

b. Entro 15 giorni dalla notifica da parte di TIM dell'affidamento dell'incarico ad un nuovo Sub-responsabile di Google, il Richiedente potrà opporsi a tale affidamento solo ed esclusivamente mediante recesso dal Contratto previa comunicazione scritta a TIM tramite raccomandata a/r oppure con Posta Elettronica Certificata (PEC), restando intesto che il recesso diverrà efficace al quinto giorno successivo la ricezione della comunicazione da parte di TIM. Tale diritto di recesso è l'unico ed esclusivo rimedio del Richiedente nel caso in cui si opponga a un nuovo Sub-responsabile di Google.

Misure di Sicurezza Google

Nell'erogazione dei Servizi in subappalto (Google Cloud Platform) Google garantisce il mantenimento delle seguenti misure di sicurezza.

1. Sicurezza del data center e della rete

a) Data Center.

Infrastruttura. Google gestisce data center geograficamente distribuiti. Google conserva tutti i dati di produzione in data center sicuri in termini di misure di sicurezza fisiche.

Ridondanza. I sistemi infrastrutturali sono stati progettati per eliminare i singoli punti di guasto e ridurre al minimo l'impatto dei rischi ambientali previsti. I circuiti doppi, gli interruttori, le reti o altri dispositivi necessari contribuiscono a fornire questa ridondanza. I Servizi sono progettati in modo da consentire a Google di eseguire alcuni tipi di manutenzione preventiva e correttiva senza interruzioni. Tutte le apparecchiature e le strutture ambientali sono dotate di procedure di manutenzione preventiva documentate che descrivono in dettaglio il processo e la frequenza delle prestazioni in conformità alle specifiche del produttore o alle specifiche interne. La manutenzione preventiva e correttiva delle apparecchiature del data center è pianificata attraverso un processo di modifica standard secondo procedure documentate.

Alimentazione. I sistemi di alimentazione elettrica dei data center sono progettati per essere ridondanti e soggetti a manutenzione senza impatto per le operazioni continue, 24 ore al giorno, 7 giorni alla settimana. Nella maggior parte dei casi, una fonte di alimentazione primaria così come una fonte di alimentazione alternativa, ciascuna con uguale capacità, è fornita per i componenti critici dell'infrastruttura del data center. L'alimentazione di backup è fornita con varie modalità come le batterie dei gruppi di continuità (UPS), che forniscono una protezione di alimentazione costantemente affidabile durante i blackout, i blackout, le sovratensioni, le sottotensioni e le condizioni di frequenza fuori tolleranza. In caso di interruzione dell'alimentazione di rete, l'alimentazione di riserva è progettata per fornire energia transitoria al data center a piena capacità per un massimo di 10 minuti fino a quando i generatori diesel subentrano. I generatori diesel sono in grado di avviarsi automaticamente in pochi secondi per fornire energia elettrica di emergenza sufficiente a far funzionare il data center a piena capacità, tipicamente per un periodo di giorni.

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

Business Continuity. Google ha progettato e pianifica e verifica regolarmente i suoi programmi di pianificazione di business continuity e di ripristino di emergenza.

b) Reti e trasmissione.

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

Protezione da attacchi esterni. Google utilizza più strati di dispositivi di rete e di rilevamento delle intrusioni per proteggere la sua superficie di attacco esterno. Google analizza i potenziali vettori di attacco e incorpora tecnologie appropriate nei sistemi a tutela da attacchi esterni.

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

- rigorosi controlli sulle dimensioni e sulla composizione della superficie d'attacco di Google attraverso misure preventive;
- utilizzo di controlli di rilevamento intelligenti nei punti di ingresso dati; e
- utilizzo di tecnologie che pongono automaticamente rimedio ad alcune situazioni di pericolo.

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

Tecnologie di crittografia. Google mette a disposizione la crittografia HTTPS (chiamata anche connessione SSL o TLS). I server di Google supportano lo scambio di chiavi crittografiche effimere a curva ellittica Diffie-Hellman firmato con RSA ed ECDSA. Questi metodi di perfetta segretezza in avanti (PFS) aiutano a proteggere il traffico e a minimizzare l'impatto di una chiave compromessa, o di una svolta crittografica.

2. Controlli di accesso e del sito

(a) Controlli del Sito.

Operazione di Sicurezza del Data Center In Loco. I data center di Google mantengono un servizio di sicurezza in loco responsabile di tutte le funzioni di sicurezza dei data center fisici 24 ore al giorno, 7 giorni alla settimana. Il personale addetto alle operazioni di sicurezza in loco controlla le telecamere a circuito chiuso (CCTV) e tutti i sistemi di allarme. Il personale addetto alle operazioni di sicurezza in loco effettua regolarmente pattugliamenti interni ed esterni del centro dati.

Procedure di Accesso al Data Center. Google mantiene procedure di accesso formali per consentire l'accesso fisico ai data center. I data center sono ospitati in strutture che richiedono l'accesso con chiave elettronica, con allarmi collegati al servizio di sicurezza in loco. Tutti coloro che accedono al data center sono tenuti a identificarsi e a mostrare un documento di identità al servizio di sicurezza in loco. Solo i dipendenti autorizzati, gli appaltatori e i visitatori sono autorizzati ad entrare nei data center. Solo i dipendenti e gli appaltatori autorizzati sono autorizzati a richiedere l'accesso con chiave elettronica a queste strutture. Le richieste di accesso con chiave elettronica al data center devono essere effettuate tramite e-mail e richiedono l'approvazione del responsabile del richiedente e del direttore del data center. Tutti gli altri partecipanti che richiedono l'accesso temporaneo al data center devono: (i) ottenere l'approvazione in anticipo dai responsabili del data center per il data center specifico e le rispettive aree interne che desiderano visitare; (ii) registrarsi presso il servizio di sicurezza in loco; e (iii) registrarsi in un registro di accesso dei soggetti autorizzati al data center che identifichi l'individuo come approvato.

Dispositivi di Sicurezza del Data Center In Loco. I data center di Google utilizzano una chiave elettronica e un sistema di controllo accessi biometrico collegato ad un sistema di allarme. Il sistema di controllo degli accessi monitora e registra la chiave elettronica di ogni individuo e quando accede alle porte perimetrali, all'area spedizione e ricevimento e ad altre aree critiche. Le attività non autorizzate e i tentativi di accesso non riusciti vengono registrati dal sistema di controllo d'accesso e investigati, a seconda dei casi. L'accesso autorizzato in tutte le aree aziendali e nei data center è limitato in base alle zone e alle responsabilità lavorative dell'individuo. Le porte antincendio dei data center sono allarmate. Le telecamere a circuito chiuso sono in funzione sia all'interno che all'esterno dei data center. Il posizionamento delle telecamere è stato progettato per coprire aree strategiche che comprendono, tra l'altro, il perimetro, le porte dell'edificio del data center e l'area spedizione/ricevimento. Il personale addetto al servizio di sicurezza in loco gestisce le apparecchiature di monitoraggio, registrazione e controllo delle telecamere a circuito chiuso. In tutti i data center le apparecchiature CCTV sono collegate da cavi cablati. Le telecamere registrano sul posto tramite videoregistratori digitali 24 ore al giorno, 7 giorni alla settimana. Le registrazioni di sorveglianza vengono conservate per un massimo di 30 giorni in base all'attività.

b) Controllo degli Accessi.

Personale di Sicurezza delle Infrastrutture. Google ha e mantiene una politica di sicurezza per il suo personale e ritiene necessaria una formazione sulla sicurezza come parte del pacchetto di formazione per il suo personale. Il personale addetto alla sicurezza delle infrastrutture di Google è responsabile del monitoraggio continuo dell'infrastruttura di sicurezza di Google, della revisione dei Servizi e della risposta agli incidenti di sicurezza.

Controllo degli Accessi e Gestione dei Privilegi. Per amministrare i Servizi gli amministratori del Partner devono autenticarsi tramite un sistema di autenticazione centrale o tramite sistema ad autenticazione singola.

Processi e Politiche Interne di Accesso ai Dati - Politica di Accesso. I processi e le politiche interne di accesso ai dati di Google sono definiti in modo da impedire a persone e/o sistemi non autorizzati di accedere ai sistemi utilizzati per il trattamento dei dati personali. Google progetta i propri sistemi in modo da (i) consentire solo alle persone autorizzate di accedere ai dati a cui sono autorizzate ad accedere; e (ii) garantire che i dati personali non possano essere letti, copiati, alterati o rimossi senza autorizzazione durante il trattamento, l'uso e dopo la registrazione. I sistemi sono progettati per rilevare qualsiasi accesso inappropriato. Google utilizza un sistema di gestione degli accessi centralizzato per controllare l'accesso del personale ai server di produzione e fornisce l'accesso solo a un numero limitato di persone autorizzate. I sistemi di autenticazione e autorizzazione di Google utilizzano certificati SSH e chiavi di sicurezza e sono progettati per fornire a Google meccanismi di accesso sicuri e flessibili. Questi meccanismi sono progettati per concedere solo diritti di accesso approvati agli host del sito, ai log, ai dati e alle informazioni di configurazione. Google richiede l'uso di ID utente univoci, password forti, autenticazione a due fattori e liste di accesso attentamente monitorate per ridurre al minimo il potenziale di utilizzo non autorizzato dell'account. La concessione o la modifica dei diritti di accesso si basa su: le responsabilità lavorative del personale autorizzato, i requisiti di lavoro necessari per svolgere le attività autorizzate e la necessità di conoscere le basi. La concessione o la modifica dei diritti di accesso deve anche essere conforme alle politiche interne di accesso ai dati e alla formazione di Google. Le approvazioni sono gestite da strumenti di workflow che conservano registrazioni di audit di tutte le modifiche. L'accesso ai sistemi viene registrato per creare una traccia di audit per la responsabilità. Laddove le password vengono utilizzate per l'autenticazione (ad esempio, il login alle workstation), vengono implementate politiche di password che seguono almeno le pratiche standard del settore. Questi standard includono restrizioni sul riutilizzo delle password e una sufficiente robustezza delle password. Per l'accesso a informazioni estremamente sensibili (ad es. dati della carta di credito), Google utilizza token hardware.

3. Dati

a) Conservazione, Isolamento e Registrazione dei dati. Google memorizza i dati in un ambiente multi-tenant su server di proprietà di Google. Con riserva di eventuali istruzioni contrarie di TIM, in conformità alle istruzioni ricevute dal Richiedete (ad esempio, sotto forma di decisione specifica sul luogo di conservazione dei dati), Google replica i Dati del Richiedente tra più data center geograficamente distribuiti. Google isola logicamente anche i Dati del Richiedente. TIM avrà il controllo su specifiche policy di condivisione dei dati che gestirà nel rispetto delle istruzioni ricevute dal Richiedente. Tali policy, in conformità con le funzionalità dei Servizi, consentiranno a TIM di determinare le impostazioni di condivisione dei prodotti applicabili al Richiedente per scopi specifici. TIM può scegliere di utilizzare le funzionalità di registrazione che Google mette a disposizione tramite i Servizi, se così istruito dal Richiedente.

b) Dischi Dismessi e Politica di Cancellazione dei Dischi. I dischi contenenti dati possono presentare problemi di prestazioni, errori o guasti hardware che li portano alla disattivazione ("Disco Dismesso"). Ogni Disco Dismesso è soggetto a una serie di processi di distruzione dei dati (la "Disk Erase Policy") prima di lasciare la sede di Google per il riutilizzo o la distruzione. I Dischi Dismessi vengono cancellati in un processo in più fasi e verificati da almeno due validatori indipendenti. I risultati della cancellazione vengono registrati dal numero di serie del disco dismesso per il tracciamento. Infine, il Disco Dismesso cancellato viene rilasciato nell'inventario per il riutilizzo e il riposizionamento. Se, a causa di un guasto dell'hardware, il Disco Dismesso non potesse essere cancellato, viene conservato in modo sicuro fino a quando non può essere distrutto. Ogni struttura viene controllata regolarmente per monitorare la conformità con la Disk Erase Policy.

4. Sicurezza del Personale

Il personale di Google è tenuto a comportarsi in modo coerente con le linee guida dell'azienda in materia di riservatezza, etica commerciale, uso appropriato e standard professionali. Google effettua controlli di background ragionevolmente appropriati nella misura consentita dalla legge e in conformità con la normativa locale sul lavoro e le normative di legge vigenti.

Il personale è tenuto a sottoscrivere un accordo di riservatezza e deve confermare la ricezione e il rispetto delle politiche di riservatezza e privacy di Google. Al personale viene fornita una formazione sulla sicurezza. Il personale che tratta i Dati del Partner è tenuto a completare ulteriori requisiti appropriati al proprio ruolo (ad es., certificazioni). Il personale di Google non tratterà i Dati del Richiedente senza autorizzazione.

5. Sicurezza del Sub-responsabile

Prima di autorizzare nuovi Sub-responsabili, Google conduce un audit delle pratiche di sicurezza e privacy dei Sub-responsabili per verificare che i Sub-responsabili forniscano un livello di sicurezza e privacy adeguato al loro accesso ai dati e all'ambito dei servizi da fornire. Una volta che Google ha valutato i rischi presentati dal Sub-responsabile, in base ai requisiti descritti nel punto 7 del presente allegato, il Sub-responsabile è tenuto a stipulare le opportune condizioni contrattuali in materia di sicurezza, riservatezza e privacy.

7. VARIAZIONI

Il Richiedente può richiedere in qualsiasi momento variazioni al Profilo di Servizio contrattualizzato contattando il referente Vendite.

Le variazioni delle Risorse Cloud a consumo non comportano modifiche contrattuali.

8. DURATA DEL CONTRATTO E CONDIZIONI DI RECESSO

L'Offerta avrà la durata di un (1) anno a decorrere dalla data di attivazione del Servizio senza automatico rinnovo alla scadenza.

Il Cliente può recedere dall'Offerta in qualsiasi momento con un preavviso di 30 (trenta) giorni secondo le modalità indicate nell'articolo 16.4 delle Condizioni Generali ICT Infrastrutturali e Multicloud relativamente all'invio delle comunicazioni. In tal caso, qualora il Cliente abbia acquistato Risorse Cloud a consumo, saranno dovuti a TIM i corrispettivi relativi all'utilizzo di tali Risorse fino al completamento della migrazione del proprio Tenant su altro Cloud Service Provider o alla rimozione delle Risorse Cloud dal proprio Tenant unitamente al decimo dell'importo dei servizi o forniture non eseguite ai sensi dell'art. 109 del D.lgs. n. 50/2016 e s.m.i.. Qualora il Cliente abbia acquistato Risorse Reserved in abbinamento all'impegno di consumo di un determinato volume in un determinato periodo di tempo, il Cliente dovrà corrispondere a TIM il corrispettivo economico corrispondente al volume di consumi delle Risorse Reserved che si era impegnato ad utilizzare unitamente al decimo dell'importo dei servizi o forniture non eseguite ai sensi dell'art. 109 del D.lgs. n. 50/2016 e s.m.i...

9. DISCIPLINA APPLICABILE

L'Offerta è disciplinata dalle Condizioni Generali per i Servizi TIM Infrastrutturali e Multicloud, dalle Condizioni Particolari dei Servizi Google (ivi inclusa la documentazione resa disponibile nelle pagine web di Google) che, unitamente al presente Profilo Commerciale e ai documenti nello stesso richiamati e/o allegati e/o resi disponibili nelle pagine web di Google, alla Scheda Tecnica e/o all'Allegato tecnico, costituiscono, per tutto quanto dagli stessi non espressamente derogato e/o integrato, la disciplina contrattuale applicabile al Servizio.

La fornitura oggetto del presente Profilo Commerciale consiste nella messa a disposizione del Cliente, tramite accesso autenticato via web ad una piattaforma informatica, di un prodotto informatico con caratteristiche standard e comprensivo della manutenzione ufficiale e servizi accessori del produttore Google e dei servizi infrastrutturali di Noovle S.p.A., società soggetta a direzione e coordinamento di TIM, avente sede in Milano, Via Gaetano Negri, 1, CF/PIVA11432040969. La fornitura come sopra descritta rientra nella definizione di "prodotto informatico a catalogo".
La subfornitura a soggetti terzi come sopra descritta non è qualificabile come subappalto in considerazione di quanto disposto dall'art. 105, comma 3, lett. b) del Decreto Legislativo n. 50/2016 e s.m.i.
Con l'accettazione del presente documento di Profilo Commerciale, il Cliente conferma la suddetta interpretazione.

Data

_____

Timbro e Firma del Richiedente

_____