Profilo Commerciale

Servizio TIM Guardian Mobile

1 Descrizione del servizio

Il Servizio TIM Guardian Mobile (di seguito “Servizio”), descritto nel presente Profilo commerciale (di seguito “Offerta”, anche “Opzione”) è una delle soluzioni appartenenti alle offerte di sicurezza, commercializzata da TIM S.p.A. (di seguito “TIM”), ”), ed è rivolta alle Aziende e/o persone fisiche intestatarie di partite IVA (di seguito “Cliente/i”) che sottoscrivono o sono già titolari di un Contratto MultiBusiness per linee mobili TIM, sia ricaricabili che in abbonamento.
Il Cliente potrà attivare l’Opzione su una o più linee mobili del Contratto Multibusiness di cui è titolare.

2 Caratteristiche del servizio

Il servizio offre al Cliente una protezione dalle più diffuse e dannose minacce informatiche legate alla navigazione web grazie alle funzionalità anti-phishing e di contenimento malware direttamente integrate nella rete TIM, senza necessità di alcuna installazione software sui dispositivi di rete mobile.
In particolare, con il termine anti-phishing si intendono soluzioni atte a mitigare le minacce provenienti da internet, mirate a sottrarre informazioni personali, quali password, dati delle carte di credito o codici di accesso ai conti correnti bancari. Gli attacchi di phishing si verificano prevalentemente attraverso l’apertura di link verso siti malevoli contenuti nelle e-mail.
Con il termine *contenimento* malware si intende la capacità di un sistema di protezione di impedire l’attivazione di un software dannoso inconsapevolmente installato dall’utente sul proprio dispositivo tenuto conto che nel corso di sessioni di navigazione Internet, anche

semplicemente cliccando su link apparentemente affidabili, è possibile avviare il download di software dannosi in grado di compromettere il dispositivo dell'utente, raccogliendo informazioni sensibili , criptando o distruggendone i dati .

Di seguito una breve descrizione delle funzionalità:

a) Navigazione protetta

Questa funzionalità consente ai Clienti che attivano il Servizio di configurare profili di sicurezza personalizzati per ciascuna SIM censita nel sistema dell'organizzazione aziendale. Grazie a questa configurazione avanzata, tutti i dispositivi connessi sono protetti dalla maggior parte delle minacce cyber. Questo livello di protezione assicura un ambiente digitale sicuro e affidabile per le attività aziendali.

b) Privacy & Ad Blocker

L'attivazione di questa funzionalità offre al Cliente la possibilità di impedire l'accesso a domini di web analytics che tracciano le attività online, nonché di bloccare i network pubblicitari e gli Ad server utilizzati per la distribuzione di contenuti pubblicitari invasivi. Ciò contribuisce a favorire un maggiore controllo sulla privacy dei Clienti e previene la fruizione di annunci indesiderati, migliorando l'esperienza di navigazione in rete.

c) Web Content Filter

La funzionalità di Web Content Filter consente ai Clienti di definire regole per la gestione dei contenuti web sui dispositivi mobili aziendali. Grazie al Web Content Filter, i Clienti hanno la possibilità di limitare l'accesso a tipologie di contenuti web potenzialmente pericolosi o non conformi alle politiche aziendali di navigazione.

I livelli di Web Content Filter impostati sono i seguenti:

- **livello Basso**: blocca l'accesso ai contenuti illegali e pericolosi, come quelli che potrebbero rivelare orientamenti, credenze ed opinioni;
- **livello Medio**: oltre a bloccare i contenuti precedentemente menzionati, il livello Medio impedisce l'accesso a contenuti ritenuti inappropriati per lo svolgimento delle attività lavorative aziendali. Ciò contribuisce a mantenere un ambiente di lavoro professionale e conforme alle politiche aziendali;
- **livello Alto**: questo livello, oltre a bloccare i contenuti precedentemente menzionati, inibisce l'accesso ai contenuti espliciti, illegali o che generino dipendenza (ad esempio gambling ..). Garantisce un ambiente di navigazione sicuro e legale;

Il Cliente accedendo ai portali dedicati ai professionisti/piccole aziende e alle grandi aziende, e seguendo le istruzioni riportate nel Manuale della Dashboard, potrà accedere ad una dashboard web personale per:

- impostare le policy di sicurezza e data control da applicare alle linee su cui è attivo il servizio,

- verificare le minacce bloccate
- consultare la reportistica prevista.

La sezione «Report» della dashboard consentirà di avere accesso agli **eventi di sicurezza** occorsi sulle linee mobili. In particolare, ,le informazioni saranno disponibili in forma aggregata con le quali sarà possibile visualizzare gli eventi occorsi nell'ultime 24h, nell'ultima settimana e nell'ultimo mese. Il Cliente potrà visualizzare quanto di seguito riportato:

a) l'andamento degli eventi di sicurezza nell'intervallo di tempo impostato;
b) i blocchi di web content filtering occorsi nell'intervallo di tempo impostato, suddivisi per categoria di servizio o contenuto web;
c) gli eventi di sicurezza rilevati e bloccati nell'intervallo di tempo impostato, suddivisi per tipologia di minacce cyber e il dettaglio della data/orario.
d) Le funzionalità opzionali di controllo del traffico dati light

Il controllo del traffico dati, sempre attraverso una sezione della Dashboard, consente:

- Piena visibilità sul consumo del traffico dati per SIM o aggregati: la soluzione offre una visibilità completa sul consumo del traffico dati, categorizzandolo in base alle diverse famiglie di applicazioni. Questo consente ai clienti di monitorare in modo accurato come vengono utilizzate le risorse aziendali e di adottare strategie di ottimizzazione in base alle esigenze.
- Piena visibilità del consumo dei dati per singola SIM in base alle zone di roaming, questo mediante la gestione delle policy di blocco per SIM o aggregati. Grazie a TIM Guardian, i clienti possono stabilire politiche di blocco selettivo per categorie specifiche di applicazioni in relazione alla zona di Roaming. Questo permette un controllo preciso sulle applicazioni che possono essere utilizzate in contesti di roaming, ottimizzando l'utilizzo della connettività e i costi associati.

Il Servizio, quindi, non consente la navigazione su siti contraffatti che hanno l'obiettivo di sottrarre informazioni personali riservate, dati finanziari o codici privati e impedisce l'accesso a siti malevoli progettati per compromettere i dispositivi connessi con software dannosi, mitigando anche la diffusione dei malware di ultima generazione (ransomware).

Tim Guardian Mobile grazie all'integrazione di una nuova piattaforma tecnologica centralizzata di sicurezza analizza e verifica gli indirizzi Internet cliccati o digitati dagli utenti finali dei nostri Clienti prima di stabilire la connessione al sito internet. Ciò consente di prevenire la

minaccia in tutti i casi in cui il dominio sia valutato potenzialmente malevolo. Tim Guardian Mobile non consentirà l'accesso al sito malevolo. E' importante evidenziare come l'efficacia di un servizio di questo tipo dipenda fortemente dalla qualità della base dati utilizzata per tenere traccia dei siti contraffatti e malevoli, in termini di affidabilità, numero delle fonti, dimensione, frequenza e tempestività degli aggiornamenti. TIM Guardian Mobile utilizza una delle tecnologie più efficaci e performanti al mondo come verificato anche sperimentalmente dai laboratori di ricerca TIM.

Come ogni soluzione di sicurezza, anche TIM Guardian Mobile non può garantire una copertura del 100% da attacchi malware e phishing, sebbene contribuiscano a ridurre significativamente il grado di esposizione a queste minacce grazie alla qualità della tecnologia impiegata.

La protezione di TIM Guardian Mobile è disponibile anche su tutti i dispositivi collegati, anche in modalità HotSpot o Tethering, che accedono ad internet utilizzando la linea mobile su cui è attivo il Servizio.

La protezione di TIM Guardian Mobile non è disponibile invece su tutti i dispositivi collegati ad internet che accedono ad Internet utilizzando una connettività su cui non è attivo il Servizio.

Per i clienti che hanno attivo il servizio One Number, i servizi Tim Guardian sono disponibili solo sulla linea principale

Il Servizio è basato su APN Commerciale ovvero wap.tim.it o ibox.tim.it, tutto e solo il traffico proveniente da questi APN e per le linee su cui è attivo il servizio verrà analizzato e filtrato da una piattaforma centralizzata.

Il Servizio non è compatibile con le linee che hanno attivo il servizio di DENAT/DENAT DATI IBOX, con il servizio TIM SAFE WEB Mobile.

TIM per effettuare la diagnostica e per la produzione del report conserverà le URL su cui sono state applicate policy di blocco per 6 mesi.

3 Modalità di attivazione

Per poter usufruire di TIM Guardian Mobile al primo utilizzo dopo l'attivazione da parte di TIM, è necessario spegnere e riaccendere l'apparato mobile. Si consiglia in ogni caso di verificare l'avvenuta attivazione di TIM Guardian Mobile nell'Area Privata Cliente.

4 Componenti del servizio

4.1 Componente Base del Servizio (Mobile Security)

Il Servizio nella sua configurazione base prevede le seguenti impostazioni di sicurezza configurate come di seguito :

Filtro Privacy On
Navigazione Sicura On
Web Content Filtering su 3 livelli (impostato a Basso)

4.2 Componente Opzionale (Mobile Data Control Light)

In aggiunta alle componenti di base configurate come sopra elencato, il Cliente può richiedere l'erogazione della componente opzionale **Mobile Data Control Light** che prevede le seguenti configurazioni:

Blocco selettivo di categorie applicative per zona di roaming

4.3 Tim Guardian Mobile Dashboard

Il Cliente per poter accedere al Servizio dovrà indicare nella Proposta di attivazione allegata al presente documento l'indirizzo del Referente Tecnico che sarà abilitato all'accesso della dashboard di TIM Guardian Mobile al fine di eseguire le seguenti attività:

a) Consultare Report degli eventi di sicurezza generati in near real-time in forma aggregata

ed in caso di sottoscrizione della componente opzionale Mobile Data Control Light:

b) Report near real-time del traffico per categoria di applicazione
c) Report del traffico per Zona di Roaming

4.4 AI Virtual Assistant

La Dashboard del servizio si integra con un modello di Intelligenza Artificiale avanzato per la creazione di un sistema in grado di fornire risposte accurate e tempestive alle principali domande in ambito cyber security del Cliente.

5 Condizioni Economiche

Il Servizio al Cliente verrà erogato alle seguenti condizioni economiche:

a) Componente Base (Mobile Security): **5€/mese/linea** il servizio in fattura sarà indicato con "**TIM Guardian Mobile_sec"**
b) Componente Opzionale (Mobile Data Control Light): **2,90€/mese/linea** il servizio in fattura sarà indicato con "**TIM Guardian Mobile_mdc**"
L'importo del canone mensile, in base alle componenti sottoscritte, sarà addebitato nella Fattura TIM della linea mobile ricaricabile e/o in abbonamento nella sezione "Riepilogo costi" e con le voci specificate sopra.

6 Canali di Assistenza

In caso di malfunzionamenti, l'assistenza tecnica potrà essere richiesta al numero: **191.** Per le grandi aziende private sono a disposizione il contatto abituale di TIM o il numero 800.191.101.

L'assistenza è fornita nella seguente copertura di orario: **lunedì - venerdì 8.00 - 20.00 e sabato 8.00 - 18.30, festivi esclusi,** ed è disponibile sia per problemi commerciali sia legati all'accesso dati sia per problematiche legate alla sicurezza.

7 Durata del contratto e condizioni di recesso

TIM Guardian Mobile è un servizio a tempo indeterminato e decorre dalla data di attivazione da parte di TIM. Il Cliente potrà verificare l'avvenuta attivazione del Servizio anche attraverso l'accesso all'area privata Cliente.

Il Cliente può recedere dall'Offerta in qualsiasi momento, senza nessun costo aggiuntivo, dandone comunicazione scritta a TIM, mediante lettera raccomandata con avviso di ricevimento all'indirizzo indicato in Fattura oppure con posta elettronica certificata (PEC) all'indirizzo indicato in fattura . In alternativa, nel rispetto del termine indicato, il recesso può essere comunicato con modalità telematica tramite il sito web, chiamando il Servizio Clienti 191 dedicato ai Liberi Professionisti e Partite Iva oppure al Numero Verde 800.191.101, dedicato alle Medie e Grandi Aziende, senza alcun onere aggiuntivo o comunque anche con le altre modalità riportate in dettaglio all'articolo 13.1 delle Condizioni Generali di Contratto Multibusiness. Il recesso avrà effetto decorsi 30 (trenta) giorni dalla data di ricezione della comunicazione di recesso da parte di TIM. Alla comunicazione di recesso in forma scritta è necessario allegare copia del documento di identità del Rappresentante Legale o del Titolare del contratto.
Il recesso dall'Offerta non comporta il recesso dal Contratto MultiBusiness sottoscritto dal Cliente che pertanto, rimarrà valido ed efficace finché con riferimento allo stesso Contratto resterà attiva almeno una utenza. Il recesso del Cliente dal Contratto MultiBusiness comporta l'automatica cessazione dell'Offerta.

8 Trattamento dei dati personali

8.1 Nomina a responsabile del trattamento

Per **l'esecuzione del presente Profilo Commerciale**, 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 sul trattamento dei dati personali applicabile").

TIM S.p.A. (di seguito, per brevità, "TIM") dichiara che per l'erogazione del Servizio TIM Guardian Mobile, relativamente ai profili descritti nel presente documento, tratta dati personali di cui il richiedente è Titolare (d'ora in avanti il "Titolare"); I dati personali potranno essere trattati da TIM in misura strettamente necessaria e proporzionata per l'elaborazione delle reportistiche disponibili nella Dashboard su portale web

Per quanto sopra, TIM (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 dipendenti del Cliente, esclusivamente per la finalità relativa all'erogazione del servizio oggetto del presente Profilo Commerciale.

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

- tratta i seguenti tipi di dati: Dati Comuni di cui all'art. 4, punto 1, GDPR: dati anagrafici (nome, cognome, sesso, data e luogo di nascita, codice fiscale/P.IVA ragione sociale/denominazione); dati di contatto (numero di telefono fisso e/o mobile, indirizzo postale e di posta elettronica); dati di accesso e di identificazione (es. username, password); dati relativi ai prodotti venduti ed ai servizi attivati; dati relativi alla connessione (es. indirizzo IP) ed alla navigazione internet;
- effettua i trattamenti relativi a: ... Selezione e presentazione dei dati di pertinenza del cliente , conservazione , backup di dati , gestione sistemistica
- effettua i trattamenti mediante strumenti elettronici o comunque automatizzati.

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 dei dipendenti del Cliente

Pertanto, il Responsabile, per effetto della formalizzazione del Contratto relativo al Servizio, dichiara di accettare la nomina a Responsabile del trattamento e di impegnarsi ad osservare le condizioni/istruzioni riportate nella presente.

La presente nomina decorre dalla data di accettazione da parte di TIM della proposta di attivazione del Servizio, intendendosi per tale la data di attivazione del servizio stesso comunicata da TIM, 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. La cessazione delle attività o la revoca anticipata comportano automaticamente l'immediata cessazione dei trattamenti e la restituzione e/o la distruzione dei relativi dati personali, come indicato al successivo punto **11**. Inoltre, il Titolare può chiedere al Responsabile di sospendere il trattamento dei dati personali fino a quando quest'ultimo non rispetti le istruzioni contenute nella presente clausola.

Trattamento di dati personali da parte di Subfornitori/Subappaltatori

Il Titolare, ai sensi del paragrafo 2 dell'art. 28 del GDPR autorizza il Responsabile ad avvalersi di Telsy S.p.A., in qualità di sub responsabile del trattamento, Iper svolgere le attività di cui alla presente nomina.

Inoltre, il Titolare autorizza il Responsabile ad avvalersi di eventuali ulteriori soggetti terzi (subappaltatori/ subfornitori) per svolgere le attività di cui alla presente nomina.

Conseguentemente il Responsabile si impegna, prima dell'inizio del trattamento, a nominare Responsabili i propri subappaltatori/subfornitori utilizzando le medesime istruzioni con le quali è stato nominato a sua volta Responsabile del trattamento dal Titolare e, comunque, prevedendo nel contratto con i propri subappaltatori/subfornitori gli stessi obblighi in materia di protezione dei dati contenuti nel presente Profilo Commerciale, in modo tale che il trattamento soddisfi i requisiti previsti dai paragrafi 2 e 4 dell'art. 28 del GDPR. Su richiesta, il Responsabile fornisce al Titolare copia del contratto stipulato con i propri subappaltatori/subfornitori e di ogni successiva modifica.

A tal proposito il Responsabile informerà il Titolare rendendo disponibile l'elenco dei subappaltatori/subfornitori nominati responsabili in caso di modifiche riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento con le seguenti modalità: Pubblicazione allegato privacy su Canali Digitali (Portali Mybusiness , TimBuiness , etc) , comunicazione ai classici canali di contatto del cliente (ovvero il referente mandatario)

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 del subappaltatore/subfornitore scelto dal Responsabile, quest'ultimo si riserva il diritto di scegliere un altro subappaltatore/subfornitore; 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.

Trasferimento di dati all'estero

Le Parti concordano che il trasferimento dei dati personali da parte di TIM ad un'eventuale subappaltatore/subfornitore, stabilito in un Paese Ue/See o extra Ue/See, deve essere preventivamente autorizzato per iscritto dal Titolare. In caso di trasferimento dei dati personali verso Paesi extra Ue/See senza un adeguato livello di protezione dei dati personali TIM (in qualità di esportatore) dovrà preventivamente sottoscrivere con l'appaltatore/fornitore (in qualità di importatore) le "clausole contrattuali tipo" (modulo 3) adottate dalla Commissione Europea con Decisione n. 2021/914 del 4 giugno 2021, ai sensi dell'art. 46.2 del GDPR, purché le condizioni per l'uso di tali clausole contrattuali tipo siano soddisfatte.

Istruzioni e misure di sicurezza

Il Responsabile garantisce l'esperienza, la capacità e l'affidabilità dei propri dipendenti e di chiunque altro sia deputato a trattare i dati personali forniti dal Titolare e si impegna a far osservare loro le disposizioni di cui alla normativa sul trattamento dei dati personali applicabile, nonché le istruzioni previste nella presente clausola.

Il Responsabile assicura, inoltre, che i propri dipendenti e chiunque altro sia deputato a trattare i dati personali forniti dal Titolare abbiano ricevuto adeguata formazione con riferimento alla normativa sul trattamento dei dati personali applicabile

Il Responsabile si impegna ad osservare quanto previsto dal 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 Titolare si riserva di verificare il rispetto delle istruzioni impartite e 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, inoltre, sarà direttamente ritenuto responsabile per qualsiasi divulgazione dei dati personali dovesse realizzarsi ad opera di tali soggetti.
2. In conformità a quanto previsto dall'art. 32 del GDPR, realizza le misure di sicurezza previste nel presente Contratto, nell'Allegato Tecnico "Requisiti di sicurezza dei dati", e di compliance ICT per i Fornitori") e quelle prescritte da eventuali provvedimenti del Garante Privacy in relazione alle attività oggetto della presente nomina.
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 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; inoltre, informa senza indugio il Titolare qualora venga a conoscenza del fatto che i dati personali che sta trattando siano inesatti o obsoleti.
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 privacy, 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, su scelta del Titolare, vengano cancellati o restituiti 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, salvo che la legge preveda la conservazione di tali dati, in tal caso il Titolare fornirà le opportune indicazioni al Responsabile. Finché i dati non sono cancellatio restituiti, il Responsabile continua ad assicurare il rispetto delle presenti istruzioni e della Normativa sul trattamento dei dati personali applicabile.
12. Informa immediatamente il Titolare del trattamento qualora, a suo parere, un'istruzione violi la Normativa sulla protezione dei dati personali applicabile; in tali circostanze, il Responsabile ha diritto di risolvere il contratto con il Titolare qualora quest'ultimo insista sul rispetto delle istruzioni.
13. Tiene 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.
14. 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.

Le Parti si impegnano, ognuna per quanto di competenza nell'ambito del presente Profilo Commerciale, 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.

9 Disciplina applicabile

Per quanto non espressamente previsto dal presente Profilo Commerciale, troveranno applicazione i termini della Proposta di Attivazione, delle Condizioni Generali dei Servizi di Security Solution, delle Condizioni Generali Multibusiness, di cui il presente documento costituisce parte integrante e sostanziale.

Per ogni altra informazione tecnico/commerciale è disponibile il Servizio Clienti Business 191, per le grandi aziende pubbliche e private sono a disposizione il contatto abituale di TIM o il numero 800.191.101.