Profilo Commerciale TIM Protezione Dispositivi

1. DESCRIZIONE DELL'OFFERTA

Il servizio TIM Protezione Dispositivi (di seguito, per brevità, definito come il "Servizio" o il "Prodotto"), erogato da TIM tramite Telsy S.p.A. (di seguito, per brevità, "Telsy") e descritto nel presente Profilo Commerciale (di seguito anche "Offerta"), ha l'obiettivo di offrire una soluzione di sicurezza per Postazione di Lavoro (PdL), Server e Dispositivi Mobili (collettivamente "End Point") sfruttando tecnologie di rilevamento, protezione e risposta. Il Servizio è rivolto a tutte le organizzazioni (di seguito, per brevità, definite come il "Cliente") alla ricerca di una soluzione estesa di monitoraggio e protezione che a differenza delle soluzioni "point solution" non collegate tra loro, riesce a circoscrivere la semplice generazione di alert (difficilmente gestibili da staff IT con risorse limitate) ed a fornire un contesto abbastanza ampio per una comprensione totale del livello di esposizione al rischio dell'azienda.

2. CONDIZIONI SPECIFICHE DEL SERVIZIO

Il Servizio per salvaguardare al meglio la sicurezza informatica delle organizzazioni attraverso servizi di sicurezza gestita per PdL, Server e Mobile ricorre a due differenti piattaforme tecnologiche per i differenti seguenti profili di servizio:

a) DefenX, piattaforma sviluppata e fornita da Trend Micro.
b) Mobile Threat Defense basato sulla soluzione Ermetix sviluppata e fornita da Ermetix SrL.

Il Servizio è regolato oltre che dal presente Profilo Commerciale e dalle Condizioni Generali dei Servizi di Security Solutions anche dalle End User Licensing Agreement (di seguito, per brevità anche "EULA") presenti sulle piattaforme Trend Micro e Ermetix, allegate al presente Profilo Commerciale e accettate dal Cliente al momento della sottoscrizione del presente Profilo Commerciale. Il Cliente prende atto e accetta che ogni Utente sarà tenuto ad accettare l'EULA al momento del primo accesso in Piattaforma per poter fruire del Servizio. Il Cliente prende atto e accetta, inoltre, che in caso di contrasto tra le previsioni delle EULA e quelle del medesimo tenore contenute nelle Condizioni Generali dei Servizi di Security Solutions come eventualmente integrate dal presente Profilo Commerciale, queste ultime avranno prevalenza.

2.a) DefenX

DefenX si propone di accelerare ed efficientare le attività di identificazione e investigazione delle minacce, nonché di offrire soluzioni di protezione automatica per Endpoint (PC Fisso o portatile e Server) con lo scopo di prevenire attacchi cyber di varia natura, tra i quali:

- malware (es. anti-Ransomware, anti-Spyware);
- accessi non autorizzati (es. Device Control);
- comportamenti malevoli (es. Intrusion Prevention, Web Reputation);
- data breach (es. DLP);
- vulnerabilità potenziali (es. Virtual Patching);

Il profilo di servizio DefenX fornisce al Cliente la possibilità di accedere alle capacità di detection, protection e response per endpoint (PC Fissi o portatili e/o Server), secondo due diverse tipologie di sottoscrizione:

- **Core:**
  - Software locale di protezione avanzata per endpoint (PC fissi o portatili, Server).
  - Console Web-Based per la gestione del Prodotto (es. gestione regole), scansioni manuali e/o programmate e reportistica automatica.
  - Assistenza dedicata al Cliente in fase di installazione e configurazione (es. policy setting).

- Protezione fino a 2 device mobili inclusa, per ogni endpoint protetto (PC o Server).

- **Advanced:**
  - Software locale di protezione avanzata per endpoint (PC fissi o portatili, Server).
  - Integrazione con tecnologia di detection e response (EDR) e di Cloud Sandbox per l'investigazione e blocco automatico di minacce reali e/o potenziali, anche zero-day.
  - Assistenza dedicata al Cliente in fase di installazione e configurazione (es. policy setting).
  - Monitoraggio 24/7 e gestione degli alert dell'intero comparto endpoint e mobile protetto, ad opera del SOC di Telsy.
  - Reportistica periodica di sicurezza dedicata.
  - Notifica su incidenti potenziali o in corso.
  - Report di dettaglio in caso di incidenti potenziali o in corso (incl. azioni suggerite di remediation).
  - Protezione fino a 2 device mobili inclusa, per ogni endpoint protetto (PC o Server).

Come indicato sopra, ogni tipologia (Core o Advanced) di sottoscrizione include anche la protezione fino a 2 device mobili (telefoni cellulari aziendali) per ogni licenza DefenX acquistata.

Si specifica inoltre che nel profilo di servizio "DefenX Advanced", il SOC di Telsy non svolgerà azioni dirette di risposta e rimedio agli attacchi (es: incident response) ma solamente le azioni permesse dalla tecnologia di protezione prevista all'interno dell'offerta (es: isolamento endpoint). In tutti i casi di incidente come descritto sopra, il SOC di Telsy svolgerà le attività di notifica istantanea e produzione report di dettaglio sugli incidenti in corso, includendo anche le informazioni utili in merito alle azioni suggerite di rimedio che il Cliente può porre in atto.

Le funzionalità di protezione di device mobili, che è esclusiva per dispositivi con sistema operativo iOS, Android e Chromebook, includono, tra le altre:

- Password Hardening, per il mantenimento di password sicure (solo device con sistema operativo Android e iOS);
- Blocco del dispositivo da remoto, per i casi di furto o smarrimento (solo device con sistema operativo Android e iOS);
- Cancellazione centralizzata dei dati sensibili, per i casi di furto e smarrimento (solo device con sistema operativo Android e iOS);
- Scan Anti-Malware (solo device con sistema operativo Android);
- App Scanning (solo device con sistema operativo Android);
- Web Reputation & Filtering (solo device con sistema operativo Android, Chromebook);
- Localizzazione del dispositivo (solo device con sistema operativo Android).

2.b) Mobile Threat Defense

Il profilo di servizio Mobile Threat Defense, specifico per dispositivi mobili, è erogato tramite una piattaforma cloud ubicata in data center su territorio italiano (integrata con il Security Information Event Management e il SOC di Telsy), la quale attraverso un agent installato sui device del Cliente ne consente il monitoraggio, la gestione e la sicurezza.

Il Servizio consente al Cliente di avere piena autonomia nella gestione della propria flotta di device mobili, in particolare consente:

- Gestione device da remoto attraverso una web dashboard in cui è possibile attivare circa 100 restrizioni (a titolo di esempio blocco download APPs, creazione policies password, livelli di sicurezza connessioni wifi) in modo da impedirne qualsiasi utilizzo inappropriato;
- Distribuzione uniforme sui device di App, APK, file e risorse, restrizioni, impostazioni ed aggiornamenti, in modo da garantire che tutti i dispositivi siano configurati in modo congruente al loro utilizzo;
- Protezione device centralizzata e da remoto tramite impostazione di nuove policies di sicurezza e/o modifica di quelle preconfigurate, controllo dei servizi di Endpoint Security quali antivirus / anti malware, smart firewall, navigazione sicura, anti phishing;

- Monitoraggio tramite dashboard di eventuali anomalie segnalate dal sistema in relazione ai device gestiti (a titolo di esempio incremento anomalo del traffico di rete, accessi geograficamente incongrui, stato batteria, versioning OS e APPs,), con possibilità di intervento da remoto in caso di smarrimento o furto.

Il profilo di servizio Mobile Threat Defense:

1. Garantisce al Cliente altissimi standard tecnologici grazie alle certificazioni Android EMM Enterprise certified, Samsung Knox certified e validazioni Apple;
2. Consente la protezione dei dispositivi sia da minacce note (Trojan e Ransomware) sia da minacce sconosciute (Zero Day Malware);
3. Presenta una interfaccia UX web based chiara ed intuitiva che consente al Cliente di avere la piena autonomia di gestione.

Il Servizio TIM Protezione Dispositivi è da intendersi a titolo ed uso esclusivo per il Cliente, fermo restando che non potrà essere utilizzato per finalità commerciali e/o a scopo di lucro. Il Cliente adotterà altresì ogni cautela idonea a garantire l'accesso al Servizio solo al proprio personale interno. Il Servizio non potrà in nessun caso essere ceduto a terzi, neanche a titolo gratuito, parzialmente o totalmente.

3. INTERVENTI E MANUTENZIONE E ASSISTENZA TECNICA

Il servizio di assistenza è erogato attraverso un Help Desk dedicato mediante la casella di posta elettronica (support-timprotezionedispositivi@telsy.com).
Il servizio di assistenza ha la finalità di offrire al Cliente assistenza reattiva per le casistiche di supporto all'installazione, configurazione iniziale del Prodotto e durante il ciclo di vita del servizio ed è attivo nei giorni infra-settimanali durante il normale orario di lavoro (9,00-18,00).

4. CONDIZIONI ECONOMICHE

Il Servizio TIM Protezione Dispositivi prevede il pagamento di un canone mensile per ciascuna licenza installata da corrispondersi nel corso della durata dell'Offerta a partire dall'attivazione del Servizio e per la sua durata.
In base al profilo di servizio da erogare il costo è il seguente:

TIM Protezione Dispositivi	Profili	Prezzo mensile
Per PC Fissi o Portatili, Server		
	DefenX Core	3,5€ / mese / dispositivo
	DefenX Advanced	8,9€ / mese / dispositivo
Per Dispositivi Mobili		
	Mobile Threat Defense	5€ / mese / dispositivo

L'acquisto di una licenza **DefenX** per la protezione di Endpoint (PC o Server), sia Core che Advanced, offre al Cliente, incluso nel prezzo, la possibilità di proteggere fino a n.2 (DUE) device mobili per ciascun PC e/o Server protetto.

Le licenze **Mobile Threat Defense** possono essere acquistate ed utilizzate dal Cliente sia indipendentemente da quelle DefenX sia per poter aggiungere le funzionalità di protezione specifiche per i device Mobile incluse in Mobile Threat Defense a quelle dei profili DefenX, sia Core che Advanced.
In questo secondo caso sui terminali mobili NON va installato l'agent mobile di DefenX ma solo quello di Mobile Threat Defense.

Nel caso in cui un Cliente abbia necessità di aumentare o diminuire il numero di End Point da proteggere rispetto a quelli indicati alla sottoscrizione della presente Offerta e, quindi, richiedere nuove licenze o cessarne alcune, dovrà disattivare la presente Offerta e sottoscrivere una nuova offerta per la quantità di licenze aggiuntive da attivare o residue da mantenere secondo il prezzo applicabile al momento della sottoscrizione.

5. MODALITA' DI ATTIVAZIONE

A valle dell'acquisto tramite i canali Digital Store, il Cliente riceverà un'email ("Welcome Letter") di notifica dell'acquisto effettuato. In una fase immediatamente successiva, dopo la creazione del profilo da parte di Telsy, il Cliente riceverà, una seconda comunicazione e-mail contenente le credenziali e le istruzioni per l'accesso in dipendenza del profilo di servizio sottoscritto e come di seguito indicato:

5.a) DefenX

- **Modalità di erogazione DefenX Core:** il Cliente riceverà un link e le credenziali necessarie (username e password) ad accedere, per il tramite di un'area a lui riservata, alla Web Console centrale. Da qui dovrà procedere in autonomia ad effettuare il deployment degli agent sugli End Point che ha scelto di proteggere. La console permette l'invio degli agent in modalità massiva e centralizzata tramite link URL o invio del file eseguibile.

- **Modalità di erogazione DefenX Advanced:** in questa modalità, che prevede la gestione in carico al SOC di Telsy della Web Console centrale, sarà onere di Telsy inviare al Cliente le informazioni necessarie per il download sui propri End Point degli agent di protezione. Il processo standard di erogazione, in questo caso, prevede l'invio da parte di Telsy del link e QR Code al referente incaricato del Cliente che consentirà a quest'ultimo il download del file eseguibile necessario all'installazione dell'agent su ogni endpoint di interesse.

  Per entrambe le tipologie di profilo sottoscritto, "Core" o "Advanced", sarà responsabilità ed onere del Cliente installare i software locali di protezione sui propri End Point. Le modalità di installazione sono due:
  - Individuale su ogni End Point: Nei casi di Clienti non dotati di strumenti di gestione multipla e centralizzata dei propri End Point. In questo caso l'installazione sarà a carico dell'utente finale che dovrà, a valle della ricezione del link per il download o del file eseguibile, procedere ad effettuare la procedura di installazione sul proprio endpoint.
  - Massiva e centralizzata da un'unica postazione: Nei casi di Clienti dotati di strumenti di gestione multipla e centralizzata dei propri End Point (es. active directory) il Cliente, per il tramite del suo referente IT incaricato, potrà effettuare l'installazione in modalità centralizzata e massiva, tramite il download del file eseguibile apposito, senza alcun impegno da parte dell'utente finale.

  Il Cliente, per il tramite di un proprio referente incaricato ed indicato in fase di sottoscrizione dell'Offerta, potrà mettersi in contatto con l'Help Desk di Telsy in ogni momento, durante il ciclo di vita contrattuale, attraverso il canale e-mail dedicato (riferimento in INTERVENTI E MANUTENZIONE E ASSISTENZA TECNICA). In particolare, potrà richiedere assistenza nei casi di:
  - supporto all'installazione e configurazione della Soluzione (on-boarding e start-up);
  - malfunzionamenti della Soluzione.

5.b) Mobile Threat Defense

- **Modalità di erogazione Mobile Threat Defense:** il Cliente riceve per il tramite di una comunicazione e-mail, il link e le credenziali (username e password) per accedere alla Web Console centrale necessaria alla gestione del Servizio. Da qui potrà procedere in autonomia, ad effettuare il deployment degli agent sui dispositivi mobili che ha scelto di proteggere.

L'installazione e configurazione può essere eseguita in due modalità distinte:

- **Controllo Completo**, consigliabile nel caso di dispositivi di proprietà dell'azienda la quale voglia averne il controllo totale e attivare il massimo delle restrizioni consentite dalla piattaforma. Questa modalità, tuttavia, richiede che i dispositivi siano nuovi o ripristinati ai dati di fabbrica; in caso di dispositivi già in uso si potrà procedere con il backup (per Android) o sincronizzazioni iCloud/Google/Dropbox (per iOS) in modo che gli utenti salvino eventuali dati personali prima di procedere.

- **Controllo Parziale**, procedura consigliata in caso di dispositivi in policy BYOD (Bring Your On Device) quindi di proprietà del dipendente. Questa modalità NON richiede l'inizializzazione del dispositivo e consente di creare sul dispositivo stesso un ambiente di 'Lavoro' separato da quello 'Personale'. È sempre garantita la sicurezza del dispositivo, dei dati aziendali e dei relativi flussi in quanto resta sempre valida la scansione

antimalware su file system. La differenza con la modalità Controllo Completo è legata in generale al controllo del dispositivo stesso, che, senza inizializzazione, consente di applicare le restrizioni e configurazioni quasi solamente al profilo di lavoro.

Entrambe le modalità di installazione e configurazione variano a seconda del sistema operativo presente sul dispositivo (Android o iOS). Per il dettaglio delle procedure da seguire si rimanda alla documentazione tecnica che sarà fornita nella Welcome Letter dall'Help Desk Telsy in fase di attivazione del servizio.

Si esplicita che le attività di on-boarding degli utenti e la configurazione iniziale della piattaforma e dei dispositivi sono di esclusiva competenza del Cliente. Tuttavia, per garantire la migliore fruibilità del Servizio, è reso disponibile al Cliente un canale di assistenza, tramite Help Desk di Telsy (riferimento in INTERVENTI E MANUTENZIONE E ASSISTENZA TECNICA) per fornire supporto durante le fasi iniziali di configurazione e, nel corso di validità dell'intero contratto, per tutte le attività di assistenza in caso di malfunzionamenti.

6. DURATA DELL'OFFERTA

L'Offerta ha una durata di 12 (dodici) mesi con decorrenza dalla data della sua attivazione.
Alla scadenza l'Offerta si rinnoverà tacitamente per successivi periodi di 12 (dodici) mesi, nei limiti consentiti dalla legge, salvo disdetta di una delle Parti da comunicarsi, con un preavviso di 30 (trenta) giorni rispetto a ciascuna scadenza annuale, per quanto riguarda TIM con lettera raccomandata A/R o PEC e per quanto riguarda il Cliente disabilitando il rinnovo automatico mediante la funzionalità "disabilità rinnovo automatico" presente sul Portale di Controllo dei Servizi Digitali https://digitalstore.tim.it/area-privata. In alternativa, il Cliente potrà comunicare la disdetta, nel rispetto del termine di preavviso indicato, chiamando il Servizio Clienti 191 o il Numero Verde 800.405.800 oppure con Posta Elettronica Certificata (PEC), e per le Grandi Aziende il Numero Verde 800.191.101. In caso di disdetta la cessazione del Servizio sarà efficace alla data di scadenza dell'annualità in corso.

Il Cliente potrà recedere dall'Offerta utilizzando la funzionalità "annulla abbonamento" presente sul Portale di Controllo dei Servizi Digitali https://digitalstore.tim.it/area-privata. In alternativa, il Cliente potrà comunicare il recesso, nel rispetto del termine di preavviso di 30 (trenta) giorni, chiamando il Servizio Clienti 191 o il Numero Verde 800.405.800, e per le Grandi Aziende il Numero Verde 800.191.101 oppure con Posta Elettronica Certificata (PEC). La cessazione del Servizio avverrà nei tempi strettamente necessari per la disattivazione. Il recesso dall'Offerta effettuato prima della scadenza dell'annualità in corso, comporterà l'addebito dei canoni a scadere.

Prima della cessazione del Servizio, il Cliente dovrà procedere a propria cura e spese al salvataggio dei dati e dei contenuti associati al Servizio.

7. TRATTAMENTO DEI DATI PERSONALI

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 sul trattamento dei dati personali applicabile").
TIM dichiara che per l'erogazione del Servizio di Cyber Security, relativamente ai profili descritti nel presente documento, non tratta dati personali di cui il Richiedente è Titolare (d'ora in avanti il "Titolare").
TIM dichiara, inoltre, che per l'erogazione del Servizio, si avvale della società Telsy che tratterà i dati personali del Titolare.
Pertanto, Il Titolare, autorizza TIM ad avvalersi di Telsy per svolgere le attività connesse al citato Servizio; conseguentemente il Titolare conferisce a TIM, ai sensi dell''articolo 1704 del Codice Civile Italiano, un mandato al fine di nominare, Telsy responsabile del trattamento dei dati.
A tal fine, TIM si impegna, prima dell'inizio del trattamento, a nominare Telsy (d'ora in avanti il "Responsabile") responsabile del trattamento in nome e per conto del Titolare, esclusivamente per la finalità relativa all'erogazione del Servizio oggetto del presente contratto, utilizzando le istruzioni di cui alla presente clausola o comunque, prevedendo gli stessi obblighi in materia di protezione dei dati contenuti nel presente contratto, in modo tale che il trattamento soddisfi i requisiti previsti dall'art. 28 del GDPR.

Al fine di erogare il Servizio Telsy si avvale di tre fornitori che vengono nominati rispettivamente sub-responsabili del trattamento dei dati:

1. Per la componente applicativa dei profili DefenX, Telsy si avvale del partner TrendMicro Inc. (informativa Privacy disponibile qui https://www.trendmicro.com/it_it/about/trust-center/privacy/notice.html)
2. Per la componente applicativa dei profili Mobile Threat Defense, Telsy si avvale del partner e Ermetix SrL
3. Per la componente infrastrutturale su cui è installata la soluzione software Ermetix di cui sopra) Telsy si avvale della società del gruppo TIM: Noovle S.p.A.

Il Responsabile, nell'ambito delle condizioni/istruzioni fornite da TIM per conto del Titolare nella presente clausola:

- tratta dati personali comuni, (nome e cognome, email, n. telefonico) dell'utente del Cliente che assume il ruolo di amministratore del servizio, e degli eventuali ulteriori utenti che possono essere configurati in piattaforma come amministratori;
- effettua i trattamenti relativi alla mitigazione di attacchi informatici, migliorando il livello di sicurezza e affidabilità delle infrastrutture ICT a supporto delle applicazioni business-critical del Titolare senza la possibilità di collegarli all'identità dell'utilizzatore finale;
- effettua i trattamenti mediante strumenti elettronici e/o con strumenti cartacei.

Il Responsabile fornisce 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 clienti, dipendenti e fornitori del Titolare.

La nomina del Responsabile 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 9.
Inoltre, il Titolare autorizza TIM Spa ad avvalersi di eventuali ulteriori soggetti terzi (subappaltatori/subfornitori) per svolgere le attività connesse al citato Servizio, e a tal fine conferisce a TIM Spa, ai sensi dell''articolo 1704 del Codice Civile Italiano, un ulteriore mandato per nominare ulteriori soggetti terzi responsabili del trattamento, con le medesime istruzioni previste nella presente clausola.

A tal proposito TIM 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 attraverso PEC al Titolare.

Il Titolare del trattamento potrà opporsi alle modifiche proposte da TIM mediante comunicazione scritta da inviarsi al TIM entro 10 (dieci) giorni dalla proposta di modifica. Qualora il Titolare del trattamento si opponga alla modifica del subappaltatore/subfornitore scelto da TIM, 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 di TIM e il Titolare dovrà rimborsare i costi sostenuti da TIM per l'implementazione del Servizio oggetto del Contratto e non ancora ammortizzati.

Istruzioni e misure di sicurezza ai sensi dell'articolo 28 del GDPR:

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 sul trattamento 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, nell'Allegato Tecnico "Requisiti di sicurezza dei dati ", 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, tramite TIM, 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.
6. Comunica al Titolare, tramite TIM, 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.
7. 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.
8. Effettua, ai fini della corretta applicazione della normativa sul trattamento 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.
9. 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.
10. Informa immediatamente il Titolare, tramite TIM del trattamento qualora, a suo parere, un'istruzione violi la normativa sul trattamento dei dati personali applicabile.
11. 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.
12. 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 comma 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 sul trattamento dei dati personali applicabile

8. CONDIZIONI GENERALI

L'Offerta è regolata dalle Condizioni Generali dei Servizi di Security Solutions pubblicate sul sito timbusiness.it nella sezione Informazioni utili per il Cliente (Condizioni Generali Offerta) che congiuntamente al presente Profilo Commerciale e alle EULA di TrendMicro e Ermetix, costituiscono, per quanto dagli stessi non espressamente derogato, la disciplina contrattuale applicabile all'Offerta.