



Condizioni Generali del servizio TeamSystem Digital Cyber Security powered by Axitea

Le presenti condizioni generali (di seguito definite le “**Condizioni Generali**”) disciplinano i termini e condizioni della fornitura al Cliente del Servizio di Cyber Security erogato da Axitea e distribuito da TeamSystem.

PREMESSA

Documenti contrattuali ed efficacia

La disciplina contrattuale complessiva della fornitura del Servizio di Cyber Security è contenuta nelle presenti Condizioni Generali, nonché nei moduli d'ordine tempo per tempo sottoscritti dal Cliente, che contengono le condizioni particolari di contratto (gli “**Ordini**”). Le Condizioni Generali e gli Ordini sono di seguito congiuntamente definiti il “**Contratto**”. In caso di discordanza tra le disposizioni delle Condizioni Generali e quelle contenute negli Ordini tempo per tempo sottoscritti dal Cliente e accettati da TeamSystem, prevalgono le disposizioni contenute negli Ordini.

Fermo restando quanto sopra previsto, le presenti Condizioni Generali modificano le condizioni generali eventualmente già applicate al Cliente con riferimento a quanto forma oggetto del Contratto.

Nessun Ordine potrà considerarsi vincolante per TeamSystem fino a che non sia accettato mediante conferma scritta o inizio di esecuzione da parte di quest'ultima.

Eventuali termini o condizioni diversi o aggiuntivi proposti dal Cliente, anche tramite moduli prestampati o in altra forma, o comunque richiamati dal Cliente nei propri documenti, non avranno efficacia alcuna nei confronti di TeamSystem, salvo che non siano dalla medesima espressamente accettati per iscritto.

Dichiarazioni del Cliente

Con l'accettazione delle presenti Condizioni Generali il **Cliente dichiara di:** (i) avere tutti i diritti e poteri necessari per concludere e dare esecuzione piena ed efficace al Contratto; e (ii) **voler utilizzare il Servizio di Cyber Security nell'ambito della propria attività imprenditoriale, artigianale, commerciale o professionale, e che, pertanto, non si applicano nei suoi confronti le disposizioni del D. Lgs. 206/2005 a protezione dei consumatori.**

1. Definizioni.

Nelle presenti Condizioni Generali, i termini e le espressioni di seguito elencati, quando riportati con iniziale maiuscola, devono intendersi con il significato ad essi attribuito nel presente paragrafo. I termini indicati al singolare si intendono anche al plurale e viceversa.

Axitea: indica Axitea S.p.A. con sede in Milano, via Gallarate 156, P.IVA 00818630188.

Cliente: indica il soggetto indicato nell'Ordine a cui sarà fornito il Servizio di Cyber Security.

GDPR: significa il Regolamento (UE) n. 2016/679 del 27 aprile 2016 relativo alla protezione 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

Legislazione in materia di Protezione dei Dati Personali: indica il GDPR, e ogni eventuale ulteriore norma e/o regolamento di attuazione emanati ai sensi del GDPR o comunque vigenti in Italia, incluso il Decreto Legislativo no. 196/2003, come modificato dal Decreto no. 101/2018, nonché ogni provvedimento vincolante che risulti emanato dalle autorità di controllo competenti in materia (es. Garante per la protezione dei dati personali) e conservi efficacia vincolante (ivi inclusi i requisiti delle Autorizzazioni generali al trattamento dei dati sensibili e giudiziari, se applicabili e ove mantengano la propria efficacia vincolante successivamente al 25 maggio 2018)

Parti: indica il Cliente e la Società.

Prodotti: indica i prodotti hardware, software e in generale qualsivoglia apparato eventualmente forniti da Axitea nell'ambito dell'erogazione del Servizio di Cyber Security.

Rete Commerciale TeamSystem: indica congiuntamente i soggetti indicati nella definizione di “Società” che segue.

SOC: indica il *security operation center* di Axitea ovvero i locali opportunamente attrezzati come da normative in vigore, per la ricezione e gestione di eventi ed immagini originati da sistemi remoti installati c/o il Cliente.

Servizio di Cyber Security: indica il servizio o l'insieme dei servizi indicati nell'Ordine erogati da Axitea.

Società: si intende, alternativamente, uno dei seguenti soggetti:

- (i) TeamSystem S.p.A., con sede legale in Pesaro (PU), via Sandro Pertini 88, codice fiscale e partita IVA n. 01035310414 (“**TeamSystem**”); oppure
- (ii) la società appartenente al gruppo facente capo a TeamSystem e indicata nell'Ordine; oppure
- (iii) il distributore ufficiale TeamSystem indicato nell'Ordine.

2. Servizio di Cyber Security

2.1 Il Servizio di Cyber Security consiste in una attività volta alla **protezione continuativa** rispetto all'evoluzione degli attacchi informatici condotti attraverso malware (quali virus, APT, ransomware e similari) e all'identificazione degli interventi necessari alle misure di protezione in essere. Volta alla **rilevazione** della diffusione su internet di **nuove tipologie di malware**, e alla valutazione del livello di efficacia del servizio di protezione attivo nei confronti di tali malware; in aggiunta, consiste in un'attività volta all'identificazione di eventuali misure aggiuntive per migliorare l'adeguatezza delle misure di protezione rispetto alle nuove minacce che sono state rilevate; **Supporto specialistico nel caso di infezioni da malware** (quali virus, APT, ransomware e similari) al fine di supportare il Cliente nell'identificazione delle azioni da effettuare sia per il massimo contenimento del danno, sia per il rapido ripristino delle precedenti condizioni di operatività. Nello specifico, il Servizio di Cyber Security può prevedere un'attività di protezione da malware sulla rete informatica del Cliente eseguita da Axitea, finalizzata ad esprimere una valutazione sul livello di sicurezza della stessa, nonché nelle attività di protezione da malware di postazione singola ovvero di server erogate da Axitea tramite l'installazione di appositi software presso le macchine del Cliente. Il Servizio di Cyber Security viene eseguito dal personale tecnico incaricato da Axitea con le modalità indicate nel Contratto e secondo le specifiche tecniche di cui alla documentazione tecnica. Il Servizio di Cyber Security potrà prevedere il blocco tempestivo delle attività malevoli e la rilevazione di tentativi di attacco e le potenziali compromissioni, così da contrastare l'appropriazione indebita dei dati critici del Cliente o le frodi informatiche in suo danno.

2.2 In relazione al Servizio di Cyber Security, potrà essere richiesta al Cliente una parola di identificazione che viene formalizzata in occasione



dell'attivazione del Servizio di Cyber Security (c.d. "Password"). La Password deve essere utilizzata dal Cliente in ogni comunicazione verbale con Axitea e/o la Società per permettere a quest'ultima di riconoscere, in maniera inequivocabile, il proprio interlocutore. Ogni comunicazione effettuata con l'utilizzo della Password definita si presumerà effettuata dal Cliente stesso o con il suo diretto consenso e lo stesso Cliente ne sarà responsabile, manlevando, ora per allora, Axitea e la Società da ogni conseguenza dannosa che possa derivare dall'uso non corretto e/o non autorizzato della/e Password.

2.3 Il Cliente prende atto che la Società e/o Axitea potranno effettuare, nel corso della durata del Contratto e senza nessun preavviso, verifiche sulla valida attivazione del Servizio di Cyber Security. Tali verifiche potranno essere effettuate anche con l'ausilio di programmi informatici. Il Cliente espressamente autorizza la Società e Axitea ad utilizzare, ai fini della convalida, le informazioni raccolte nell'ambito della predetta attività di verifica. Qualora il Servizio di Cyber Security non sia stato validamente attivato, non sia originale, sia contraffatto o il Cliente non disponga di un regolare Contratto, Axitea e/o la Società potranno, senza alcun preavviso, interrompere l'erogazione del Servizio di Cyber Security.

3. Assistenza

3.1 Il Cliente potrà fruire di un servizio di supporto tecnico da remoto volto a suggerirgli, su richiesta di quest'ultimo e laddove possibile, soluzioni tecniche per assicurare la corretta fruizione del Servizio di Cyber Security ("Assistenza"). L'Assistenza sarà erogata esclusivamente da Axitea dietro apertura da parte del Cliente di appositi ticket attraverso il sistema messo a disposizione della Società. Pertanto, il Cliente prende atto ed accetta che la Società non potrà essere ritenuta responsabile per qualsiasi ritardo o inefficienza relativo all'Assistenza, a meno che ciò non dipenda da malfunzionamenti della piattaforma di ticketing in tal caso esonerando e manlevando Axitea da eventuali pretese del Cliente.

3.2 Il Cliente può richiedere ad Axitea verifiche tecniche da remoto, a causa di problematiche tecnologiche riscontrate nella propria rete IT (esempio: navigazione web, funzionamento software, etc.). Axitea procederà alle opportune analisi e, se risconterà che la causa non è riconducibile ai Prodotti, i relativi costi saranno addebitati al Cliente. In tutti i casi in cui è necessario effettuare nuovamente l'attività di installazione dei Prodotti per cause non imputabili ad Axitea o alla Società (ad esempio: formattazione o sostituzione di un personal computer, sostituzione di dispositivo mobile, ecc.) l'intervento sarà a carico del Cliente.

4. Durata del Contratto recesso e risoluzione

4.1 Il Contratto, è valido ed efficace fino al 31 dicembre dell'anno di sottoscrizione del Contratto e si rinnoverà automaticamente alla scadenza per periodi successivi di un anno, salvo che una delle Parti comunichi all'altra Parte la propria disdetta con le modalità tecniche tempo per tempo indicate da TeamSystem oppure, in mancanza di diversa indicazione, a mezzo raccomandata A/R e/o PEC, almeno 6 (sei) mesi prima del termine via via in scadenza. Pertanto, in caso di mancata tempestiva disdetta, la fornitura del Servizio di Cyber Security si rinnoverà automaticamente per successivi periodi di un anno. Al contrario, in caso di disdetta, l'obbligo della Società e di Axitea di fornire il Servizio di Cyber Security cesserà definitivamente di essere efficace.

4.2 La Società potrà recedere anzitempo dal Contratto nelle seguenti ipotesi: (i) in qualsiasi momento, con un preavviso scritto al Cliente di 6 mesi; (ii) mediante semplice comunicazione scritta con effetto immediato, qualora il Cliente divenga insolvente, sia posto in liquidazione, sia assoggettato ad una qualsiasi procedura concorsuale; (iii) mediante semplice comunicazione scritta con effetto immediato qualora il Cliente abbia ricevuto dalla Società (o da una qualsiasi società del gruppo TeamSystem) una diffida ad adempiere ai sensi di un qualsiasi contratto in essere tra il Cliente e la Società (o una qualsiasi società del gruppo TeamSystem) e sia rimasto inadempiente per oltre 30 giorni dal ricevimento di detta diffida. È fatto comunque salvo il diritto della Società e di Axitea di ottenere il risarcimento di tutti i danni subiti.

4.3 Ferme restando le ulteriori ipotesi di risoluzione previste dal Contratto la Società potrà risolvere il Contratto, con effetto immediato, mediante l'invio di una semplice comunicazione scritta in tal senso al Cliente, in caso di inadempimento da parte del Cliente anche ad un solo degli obblighi previsti a suo carico contenuti nelle seguenti clausole: 5 (Corrispettivo); 6 (Obblighi del Cliente); 7 (Esecuzione del Contratto, limitazione ed esonero della responsabilità della Società); 8 (Comodato Prodotti).

È fatto comunque salvo il diritto della Società di ottenere il risarcimento di tutti i danni subiti.

4.4 Alla scadenza del Contratto o in caso di sua cessazione per qualsiasi ragione intervenuta, la Società cesserà di fornire il Servizio di Cyber Security.

5. Corrispettivo

5.1 Il corrispettivo dovuto dal Cliente alla Società per il Servizio di Cyber Security, è quello indicato, complessivamente, nell'Ordine (il "Corrispettivo").

5.2 Il Cliente prende atto e accetta espressamente che il Corrispettivo è soggetto ad aggiornamento annuale nella misura del 100% della variazione in aumento dell'indice ISTAT dei prezzi della produzione dei servizi, calcolato come media degli ultimi dodici mesi.

5.3 Il Cliente prende atto che le attività prestate dalla Società ai sensi del Contratto sono soggette, per loro natura, ad una costante evoluzione tecnologica e normativa che richiede continue e onerose attività di aggiornamento e sviluppo necessarie al fine di garantire la corretta e completa erogazione del Servizio di Cyber Security. In ragione di quanto precede, la Società avrà il diritto di modificare il Corrispettivo anche in misura superiore all'indice ISTAT con le modalità previste dall'art. 11.4 che segue.

5.4 Fermo restando quanto previsto al precedente paragrafo, qualora, nel corso della durata del Contratto, dovessero verificarsi circostanze imprevedibili tali da rendere maggiormente onerosa l'esecuzione delle prestazioni da parte della Società e di Axitea, la Società avrà il diritto di richiedere al Cliente un equo compenso *una tantum* ovvero una modifica del Corrispettivo.

5.5 Fatto salvo quanto previsto dall'Ordine, tutti i corrispettivi previsti dal presente Contratto si intendono al netto di IVA e di ogni ulteriore imposta eventualmente applicabile.

5.6 I pagamenti dovranno essere effettuati dal Cliente nel termine espressamente indicato nell'Ordine o, in mancanza di espressa previsione nell'Ordine, nel termine di 30 giorni dal ricevimento di fattura emessa dalla Società. Il Corrispettivo annuo dovuto in relazione al Servizio di Cyber Security sarà calcolato pro quota nel caso di fruizione del servizio solamente per frazioni dell'anno.

5.7 In caso di mancato o ritardato pagamento di una qualsiasi somma dovuta ai sensi del Contratto, il Cliente decadrà automaticamente dal beneficio del termine e la Società avrà il diritto di applicare sulle somme ad essa dovute interessi di mora nella misura prevista dal D.Lgs. 231/2002. In tal caso, la Società si riserva di inviare al Cliente una diffida ad adempiere entro il termine di quindici giorni dalla data della diffida. Decorso inutilmente il termine, la Società avrà diritto di sospendere immediatamente e senza ulteriore avviso ogni prestazione dovuta ai sensi del Contratto. Inoltre, decorso inutilmente il



termine di trenta giorni dal ricevimento della diffida di cui sopra, la Società avrà diritto di (i) di risolvere anticipatamente il Contratto mediante semplice comunicazione scritta e/o (ii) di recedere da eventuali altri contratti in essere con il Cliente. In deroga a quanto previsto dall'art. 1460 c.c., il Cliente rinuncia a proporre eventuali contestazioni o eccezioni senza aver preventivamente adempiuto alle proprie obbligazioni di pagamento ai sensi del presente articolo.

6. Obblighi del Cliente

6.1 Il Cliente non può utilizzare il Servizio di Cyber Security: i) in violazione delle leggi vigenti; ii) in modo da creare turbativa a terzi; iii) in modo da abusare dell'offerta commerciale relativa al Servizio di Cyber Security tramite un suo utilizzo non conforme al presente Contratto e alle eventuali licenze concesse.

6.2 Il Cliente prende atto e riconosce che ogni diritto di proprietà industriale e/o intellettuale sul Servizio di Cyber Security e sulla relativa documentazione, ivi inclusi i diritti di sfruttamento economico, in tutto e in parte, ovunque nel mondo, è e rimane di esclusiva titolarità di TeamSystem, Axitea e/o dei relativi danti causa (fatte salve eventuali diverse indicazioni contenute nella documentazione tecnica relativa al Servizio di Cyber Security) e, con il Contratto, non viene in alcun modo ceduto al Cliente. Il Cliente potrà utilizzare il Servizio di Cyber Security esclusivamente nei modi espressamente consentiti dal Contratto e dovrà attenersi a qualsiasi limitazione tecnica dello stesso. A titolo esemplificativo e non esaustivo, il Cliente non potrà:

- (i) aggirare le limitazioni tecniche e le misure tecnologiche presenti nel Servizio di Cyber Security;
- (ii) cedere ad alcun titolo né a far utilizzare ad alcun titolo a terzi il Servizio di Cyber Security.

6.3 Nel caso di fine supporto del sistema informativo (ogni sistema operativo ha un ciclo di vita e quando termina il produttore — es. Microsoft — non fornisce più correzioni automatiche, aggiornamenti o assistenza tecnica) il Servizio di Cyber Security non sarà più efficace per la protezione della postazione stessa (anche se sarà attiva sempre la protezione di rete). In questo caso, per una protezione più completa, sarà necessario che il Cliente provveda ad aggiornare il sistema operativo con una versione supportata dal produttore e avvisare prontamente Axitea e la Società.

6.4 L'alta affidabilità verrà collegata solo se il Cliente dispone di uno switch management layer3. In questo caso gli elementi da installare saranno 2. Il Cliente è consapevole che non attivando il Firewall in HA, in caso di guasto al firewall, potrebbe interrompersi il traffico Internet. Axitea farà il possibile per ripristinare la rete in tempi brevi, fermo restando che Axitea non è responsabile per inconvenienti tecnici legati all'infrastruttura del Cliente.

6.5 Il Cliente prende atto ed accetta che dovrà dotarsi delle apparecchiature, dei software, dei servizi telefonici e/o di rete e di quant'altro necessario al fine di utilizzare il Software e di fruire del Servizio di Cyber Security nonché adeguare autonomamente le caratteristiche dei propri sistemi e della propria connessione alle modifiche, alle sostituzioni e ai correttivi eventualmente apportati al Servizio di Cyber Security successivamente alla sottoscrizione del Contratto, il Cliente sarà tenuto a verificare l'idoneità dei propri sistemi hardware, software e di rete ai fini della fruizione del Servizio di Cyber Security e rinuncia sin d'ora a qualsiasi pretesa nei confronti della Società, degli altri soggetti appartenenti alla Rete Commerciale TeamSystem e di Axitea collegata alla mancata o non corretta erogazione del Servizio di Cyber Security conseguenti alla inidoneità dei propri sistemi hardware, software e/o di rete.

7. Esecuzione del Contratto, limitazione ed esonero della responsabilità della Società

7.1 Il Cliente prende atto ed accetta che la Società è mera rivenditrice del Servizio di Cyber Security. Axitea ha l'esclusiva responsabilità della fornitura del Servizio di Cyber Security, dei Prodotti, nonché dell'erogazione delle relative attività di Assistenza e manutenzione. Conseguentemente, il Cliente prende atto ed accetta che, salvo dolo o colpa grave direttamente ascrivibili alla Società, la Società non potrà essere ritenuta responsabile per qualsiasi danno, diretto, indiretto o spesa sofferti dal Cliente con riferimento alla fruizione o alla mancata fruizione del Servizio Cyber Security, fatto salvo quanto strettamente inerente alle attività di fatturazione a carico della Società.

7.2 Il Cliente prende atto e accetta che il Servizio di Cyber Security è fornito "così come è" e che la Società, Axitea e gli altri soggetti appartenenti alla Rete Commerciale TeamSystem non rilasciano dichiarazioni e garanzie espresse o implicite sul fatto che il Servizio di Cyber Security sia adatto a soddisfare le esigenze del Cliente, che lo stesso sia esente da errori o che abbia funzionalità non previste nelle specifiche tecniche e nella documentazione relativa.

7.3 Il Cliente riconosce ed accetta che il Servizio di Cyber Security costituisce obbligazione di mezzi e non di risultato.

7.4 Il Cliente prende atto ed accetta che, salvi i casi di dolo o colpa grave, Axitea sarà unicamente responsabile per i danni diretti conseguenti all'inadempimento delle obbligazioni assunte e che la responsabilità di Axitea è in ogni caso limitata ad un importo complessivo pari ai Corrispettivi annuali effettivamente pagati dal Cliente.

7.5 La Società e Axitea non potranno, in alcun modo, essere ritenute responsabili nel caso in cui per cause di forza maggiore non siano in grado di prestare il Servizio di Cyber Security ovvero ritardino nell'adempimento delle obbligazioni assunte.

7.6 Fermi restando i limiti inderogabili di legge con riguardo al dolo e alla colpa grave, né la Società, né gli altri soggetti appartenenti alla Rete Commerciale TeamSystem né Axitea potranno essere ritenute responsabili di eventuali danni diretti e/o indiretti che dovessero occorrere al sistema informatico del Cliente in conseguenza dell'esecuzione del Servizio di Cyber Security e che la responsabilità della Società, gli altri soggetti appartenenti alla Rete Commerciale TeamSystem e di Axitea è in ogni caso limitata ai danni diretti e per un importo complessivo pari ai Corrispettivi annuali effettivamente pagati dal Cliente.

7.7 Il Cliente, con l'accettazione del presente documento, dichiara di essere consapevole che il Servizio di Cyber Security, pur potendo ridurre sensibilmente l'esposizione al rischio informatico della propria infrastruttura tecnologica, non può tuttavia annullare completamente il rischio medesimo. Pertanto, la Società e Axitea non potranno in ogni caso essere ritenute responsabili dei danni subiti dal Cliente e/o da terzi a seguito di eventuali incidenti informatici, fatti salvi i casi di dolo o colpa grave delle stesse.

8. Comodato Prodotti

8.1 I Prodotti di cui ai Servizi di Cyber Security vengono concessi in comodato d'uso al Cliente da parte di Axitea, rimarranno di esclusiva proprietà di Axitea. Axitea resta titolare di ogni diritto di proprietà intellettuale relativo ai Prodotti, nonché alle metodologie e al know-how ad essi relativi, su cui il Cliente non acquisisce alcun diritto o titolo di qualsivoglia natura, tranne la facoltà di uso necessaria per l'esecuzione del Contratto

8.2 I Prodotti sono forniti esclusivamente da Axitea, in base alle informazioni date dal Cliente che resta l'unico responsabile della loro correttezza e quindi della scelta operata circa l'adeguatezza dei sistemi; conseguentemente Axitea declina ogni responsabilità in caso di difformità di quanto ordinato dal Cliente rispetto a quanto emerso nelle analisi (sin d'ora intese come semplici pareri non vincolanti per Axitea) precedenti l'Ordine.

I termini per la consegna sono indicativi e non vincolanti e in ogni caso Axitea non risponderà di eventuali danni derivanti da ritardi non dipendenti dalla propria volontà ivi compresi scioperi di personale, autotrasportatori, FFSS, dogane, ecc. In ogni caso l'eventuale ritardo nella consegna non potrà dar luogo



ad annullamento dei relativi Ordini od a pretesa e/o richiesta di indennizzo.

8.3 I Prodotti saranno installati a cura di Axitea nei siti predisposti dal Cliente e saranno messi in condizione di corretto funzionamento; contestualmente al termine dell'installazione, verrà redatto un verbale di collaudo che sarà firmato dal Cliente e dal tecnico di Axitea. Ai sensi e per gli effetti di cui all'art. 1655 C.C., se il Cliente riceve senza riserve l'installazione del Prodotto, questa si intende accettata ancorché non si sia proceduto alla verifica.

8.4 Il Cliente dovrà sostenere i costi relativi al materiale di consumo (ad es. le batterie), inclusi i costi per gli interventi, in qualsiasi modo effettuati, per la sostituzione dello stesso, dei Prodotti e dei relativi eventuali elementi. Qualsiasi tipo di intervento sui Prodotti (ivi compreso il cambio di batterie) e dei relativi eventuali elementi deve essere effettuato unicamente da personale incaricato di Axitea; il mancato rispetto da parte del Cliente di tale obbligo che comporta un intervento di Axitea al fine di ripristinare i Prodotti e/o gli altri elementi connessi alle stesse è a totale carico del Cliente. Il Cliente dovrà consentire al personale di Axitea di avere accesso ai Prodotti ed ai predetti elementi connessi.

8.5 Nel caso di software prodotto da Axitea, quest'ultima si impegna a concederlo in uso al Cliente che s'impegna a non duplicarlo e/o cederlo a terzi. Nessun diritto di proprietà intellettuale inclusi marchi, brevetti, know-how è da considerarsi trasferito o dato in licenza al Cliente per effetto del presente Contratto.

8.6 Axitea non potrà altresì essere in alcun modo ritenuta responsabile del mancato funzionamento delle reti pubbliche di comunicazione utilizzate per la trasmissione degli eventi (reti telefoniche fisse, reti mobili, reti di comunicazione a larga banda, reti wireless, ecc.).

8.7 Nel caso in cui le apparecchiature siano di proprietà del Cliente o di terzi, Axitea non si assumerà alcuna responsabilità in merito alle stesse e, in particolare – a mero titolo esemplificativo e non esaustivo – non si assumerà alcuna responsabilità circa la loro adeguatezza, idoneità, ad eventuali difetti di funzionamento, difetti di installazione od omessa manutenzione sia ordinaria che straordinaria. Restano a carico del Cliente gli oneri relativi a prove e verifiche di compatibilità dei protocolli di comunicazione di dette apparecchiature con i Prodotti in dotazione ai SOC.

8.8 Il Cliente riconosce ed accetta, altresì, che Axitea non può essere considerata, in alcun modo, responsabile del risarcimento di eventuali furti di informazioni subiti dal Cliente. In caso di inadempimento alle obbligazioni assunte, Axitea sarà unicamente responsabile per i danni materiali diretti, con espressa esclusione di qualsivoglia danno indiretto e/o immateriale.

8.9 Il Cliente si impegna a conservare con la massima diligenza i Prodotti e/o gli altri elementi connessi alle stesse concessi in comodato d'uso da Axitea e sarà responsabile nei confronti di Axitea per eventuali danneggiamenti o manomissioni o malfunzionamenti delle stesse, anche se imputabili ad attività di terzi. Qualora il Cliente dovesse richiedere ad Axitea un intervento per malfunzionamento ed il tecnico non riscontrasse alcuna anomalia o la stessa risultasse riconducibile al Cliente (ad es. malfunzionamento dell'infrastruttura del Cliente o intervento non autorizzato del Cliente), quest'ultimo dovrà sostenere i costi per tale intervento. Qualora i Prodotti e/o gli altri elementi connessi dovessero subire un danneggiamento o risultare malfunzionanti o non funzionanti a causa di un evento di forza maggiore (ad es. un agente atmosferico), le spese per l'intervento del tecnico e la riparazione o sostituzione sono a totale carico del Cliente.

8.10 Axitea ha il diritto di ottenere entro e non oltre 30 gg dalla cessazione del Contratto, per qualsivoglia titolo o ragione, l'immediata restituzione dei Prodotti e/o altri elementi connessi che siano stati concessi in comodato d'uso al Cliente. A tal riguardo, il Cliente garantisce, sin d'ora, che si adopererà al meglio per consentire il tempestivo e libero accesso al personale di Axitea nei luoghi in cui si trovano i Prodotti e/o gli altri elementi tecnici da disinstallare. Salvo ove diversamente previsto, i costi di disinstallazione sono a carico del Cliente.

8.11 In caso di guasto dei Prodotti di proprietà di Axitea, Axitea si impegna a fare quanto possibile per riparare e/o far riparare tempestivamente il guasto. I costi relativi a tali interventi di riparazione saranno a carico di Axitea, a meno che tale guasto non dipenda da cause imputabili ad azioni od omissioni del Cliente ovvero a cause di forza maggiore. In caso, invece, di guasto dei Prodotti di proprietà del Cliente, quest'ultimo dovrà provvedere, a proprie cure e spese, a riparare tempestivamente il guasto.

8.12 Il Cliente sarà soggetto agli obblighi di cui art. 1803 cod. civ. e ss. I Prodotti potranno essere muniti di contrassegno di legittimazione che abilitano Axitea al ritiro delle stesse alla scadenza del Contratto. La mancanza del contrassegno di legittimazione non preclude il diritto di Axitea di ritirare i Prodotti. Il comodato d'uso avrà la durata pari alla durata del Contratto.

9. Spese ed oneri

9.1 Tutte le spese, gli oneri, tasse, imposte o tributi, relativi al Contratto, anche se non espressamente previsti nei presenti articoli, si intendono ad esclusivo carico del Cliente.

10. Cessione dei diritti di credito e del Contratto

10.1 Il Cliente autorizza fin da ora la Società a cedere a terzi i diritti di credito derivanti dal presente Contratto, ai sensi degli artt. 1260 c.c. e ss, nonché a cedere a terzi il presente Contratto, ai sensi degli art. 1406 c.c. e ss. Il Cliente acconsente sin da ora, ai sensi e per gli effetti dell'art. 1407 c.c., alla cessione da parte di un componente della Rete Commerciale TeamSystem a TeamSystem (o ad altro componente della Rete Commerciale TeamSystem indicato da TeamSystem) del contratto avente ad oggetto il Servizio di Cyber Security eventualmente intercorrente tra il Cliente e il componente della Rete Commerciale TeamSystem che abbia cessato, per qualsivoglia motivo, di essere un distributore autorizzato TeamSystem. Salva preventiva autorizzazione scritta di TeamSystem, è fatto divieto al Cliente di cedere, in tutto o in parte, il Contratto.

11. Trattamento dei dati personali

11.1 Le Parti riconoscono e si danno reciprocamente atto che la sottoscrizione del presente Contratto e l'esecuzione del relativo rapporto contrattuale comporta il trattamento di dati personali del Cliente (nonché di parti ad esso correlate, quali procuratori, legali rappresentanti, etc.) da parte della Società per le finalità necessarie all'esecuzione del predetto Contratto e in conformità alle previsioni di legge applicabili. La Società tratterà tali dati in qualità di titolare del trattamento, secondo quanto riportato nell'informativa disponibile al link <https://tc.teamssystem.com/InformativaPrivacy.pdf> o al diverso link che sarà messo a disposizione dalla Società.

11.2 Con riguardo ai dati personali di soggetti terzi di cui il Cliente è titolare ai sensi della Legislazione dei dati personali (i "Dati Personali di Terzi") e che potranno essere trattati da Axitea in occasione della fornitura del Servizio di Cyber Security, le Parti riconoscono e si danno atto che:

i) Axitea agirà quale responsabile ai sensi dell'art. 28 del GDPR (il "Responsabile") in relazione al trattamento dei Dati Personali di Terzi. Al riguardo, Axitea ed il Cliente accettano di conformarsi a quanto previsto nell'Accordo per la Protezione dei dati personali ("DPA") allegato al presente Contratto (Allegato 1);

ii) la Società non effettua alcuna operazione di trattamento dei Dati Personali di Terzi, essendo una mera rivenditrice del Servizio di Cyber Security e rimarrà, pertanto, estranea alle attività di trattamento che saranno svolte per conto del Cliente esclusivamente da Axitea in qualità di Responsabile ai sensi del DPA.

11.3 Il Cliente dovrà manlevare e tenere indenne la Società ed Axitea da qualunque pregiudizio, onere, sanzione o pretesa che dovessero subire o ricevere in ragione della violazione da parte del Cliente degli obblighi su di esso gravanti in qualità di titolare del trattamento in base al GDPR e alla Legislazione in



materia di protezione dei Dati Personali ad esso applicabile.

12. Clausole finali

12.1 Il fatto che la Società non faccia valere nei confronti del Cliente dei diritti stabiliti nel Contratto o dalla legge, non comporta rinuncia a tali diritti, nei limiti dei termini di prescrizione.

12.2 Ogni comunicazione collegata e/o connessa al Contratto sarà valida ed efficace, nei confronti della Società, solo se effettuata per iscritto – a mezzo lettera raccomandata A.R. o PEC – presso la sede legale della Società. Il Cliente si impegna a fornire gli indirizzi ed i numeri di telefono e/o fax e/o e-mail / PEC delle persone a cui (verificandosene la necessità) la Società dovrà effettuare eventuali comunicazioni. Tali persone saranno a tutti gli effetti considerate rappresentanti del Cliente, abilitate a ricevere ogni comunicazione e ad impartire le necessarie conseguenti disposizioni. Il Cliente si impegna a comunicare eventuali variazioni al riguardo per iscritto, a mezzo raccomandata A/R o PEC.

12.3 Il presente Contratto supera e sostituisce ogni accordo precedentemente intercorso tra il Cliente e la Società, avente ad oggetto il Servizio di Cyber Security. Ogni modifica al presente Contratto sarà valida ed efficace solo ove risultante da accettazione per iscritto da parte della Società.

12.4 Il Contratto potrà essere modificato dalla Società in qualsiasi momento, dandone semplice comunicazione scritta (anche via e-mail o con l'ausilio di programmi informatici) al Cliente. In tal caso, il Cliente avrà il diritto di recedere dal Contratto con comunicazione scritta inviata alla Società a mezzo raccomandata con ricevuta di ricevimento nel termine di 15 giorni dal ricevimento della comunicazione della Società. In mancanza di esercizio del diritto di recesso da parte del Cliente, nei termini e nei modi sopra indicati, le modifiche al Contratto si intenderanno da questi definitivamente conosciute e accettate e diverranno definitivamente efficaci e vincolanti.

12.5 L'eventuale nullità e/o inefficacia di alcuna delle previsioni delle presenti Condizioni Generali non inficia le altre clausole e/o previsioni delle Condizioni Generali che rimangono valide ed efficaci.

12.6 Il Cliente riconosce che tutte le informazioni di cui verrà a conoscenza nell'esecuzione del Contratto hanno natura confidenziale e riservata e, pertanto, si impegna a non utilizzarle o divulgarle a terzi, in qualunque modo e con qualunque mezzo, per finalità diverse da quelle di cui al Contratto. L'obbligo di riservatezza che precede non riguarda le informazioni che sono di dominio pubblico.

13. Codice Etico, Codice di Condotta Anti-corrruzione e Modello Organizzativo di TeamSystem S.p.A.

13.1 Il Cliente dichiara di essere a conoscenza delle disposizioni di cui al Decreto Legislativo 8 giugno 2001 n. 231, e successive integrazioni in materia di responsabilità amministrativa degli enti, nonché delle norme del Codice Etico, del Codice di Condotta Anti-corrruzione e del Modello Organizzativo adottati da TeamSystem S.p.A., disponibili sul sito www.teamsystem.com e si impegna a rispettarne i contenuti, per quanto applicabili alla propria attività, e ad astenersi da comportamenti ad essi contrari. L'inosservanza da parte del Cliente dell'obbligo assunto ai sensi del presente articolo, ovvero la non correttezza o veridicità delle dichiarazioni ivi contenute, determinano un inadempimento grave, in presenza del quale TeamSystem avrà il diritto di risolvere il presente Contratto ai sensi dell'art. 1456 c.c.

14. Legge applicabile e Foro competente

14.1 Il Contratto è regolato dalla legge italiana.

14.2 Per ogni controversia che dovesse insorgere tra le Parti, comunque connessa o derivante dall'interpretazione, conclusione, esecuzione e/o efficacia del Contratto, sarà esclusivamente competente il Foro di Milano.



Allegato 1

ACCORDO SUL TRATTAMENTO DEI DATI - DATA PROCESSING AGREEMENT (ex art. 28 del Regolamento UE 2016/679) ("Accordo o DPA")

Il presente accordo per la protezione di dati personali è concluso tra:

1. Axitea S.p.A., con sede legale in via Gallarate 156, Milano 20151 n. d'iscrizione al Registro Imprese di Milano, P.IVA 00818630188 (il "Fornitore")

E

2. il soggetto indicato nel Contratto quale cliente (di seguito il "Cliente"), di seguito, congiuntamente, le "Parti" o disgiuntamente la "Parte"

PREMESSO CHE:

- A. Il Cliente ha sottoscritto uno o più contratti con il Fornitore (di seguito il "Contratto");
- B. le Parti intendono disciplinare nel presente Accordo le condizioni e le modalità del trattamento dei dati personali eseguito dal Fornitore nell'ambito del Contratto e della prestazione dei Servizi (come di seguito definiti) e le responsabilità connesse al trattamento medesimo, ivi incluso l'impegno assunto dal Fornitore quale Responsabile del trattamento dei dati personali ai sensi dell'art. 28 del Regolamento generale europeo sulla protezione dei dati del 27 aprile 2016 n. 679 (nel seguito "GDPR").

TUTTO CIÒ PREMESSO, le Parti convengono quanto segue.

1. DEFINIZIONI E INTERPRETAZIONE

- 1.1 Le premesse costituiscono parte integrante del presente Accordo. Nell'Accordo i seguenti termini ed espressioni avranno il significato associato ad essi qui di seguito:

"Clausole Contrattuali Tipo" indica le clausole contrattuali tipo previste nella Decisione della Commissione europea 2010/87/UE, del 5 febbraio 2010, per il trasferimento di dati personali a incaricati del trattamento stabiliti in paesi terzi;

"Data di Decorrenza dell'Accordo" indica la data in cui il Cliente sottoscrive o accetta il presente Accordo; "Dati Personali" ha il significato di cui alla Legislazione in materia di Protezione dei Dati Personali e includerà, a titolo puramente esemplificativo, tutti i dati forniti, archiviati, inviati, ricevuti o altrimenti elaborati, o creati dal Cliente, nella misura in cui siano oggetto di trattamento da parte del Fornitore, sulla base del Contratto.

"Decisione di Adeguatezza" indica una decisione della Commissione Europea sulla base dell'Articolo 45(3) del GDPR in merito al fatto che le leggi di un certo paese garantiscano un accordo sul trattamento dei dati personali – Data Processing Agreement adeguato livello di protezione, come previsto dalla Legislazione in materia di Protezione dei Dati Personali;

"Giorni Lavorativi" indica ciascun giorno di calendario, a eccezione del sabato, della domenica e dei giorni nei quali le banche di credito ordinarie non sono di regola aperte sulla piazza di Milano, per l'esercizio della loro attività;

"Email di notifica" si intende l'indirizzo (o gli indirizzi) email fornito/i dal Cliente, all'atto della sottoscrizione del servizio o fornito tramite altro canale ufficiale al Fornitore, a cui il Cliente intende ricevere le notifiche da parte del Fornitore;

"SOC" si intende il Security Operation Center da cui vengono forniti servizi finalizzati alla sicurezza dei sistemi informativi;

"Istruzioni" indica le istruzioni scritte impartite dal Titolare nel presente Accordo e, eventualmente, nel Contratto;

"Legislazione in materia di Protezione dei Dati Personali" indica il GDPR, e ogni eventuale ulteriore norma e/o regolamento di attuazione emanati ai sensi del GDPR o comunque vigenti in Italia in materia di protezione dei Dati Personali, nonché ogni provvedimento vincolante che risulti emanato dalle autorità di controllo competenti in materia di protezione dei Dati Personali (es. Garante per la protezione dei dati personali) e conservi efficacia vincolante (ivi inclusi i requisiti delle Autorizzazioni generali al trattamento dei dati sensibili e giudiziari, se applicabili e ove mantengano la propria efficacia vincolante successivamente al 25 maggio 2018);

"Personale del Fornitore" indica i dirigenti, dipendenti consulenti, e altro personale del Fornitore, con esclusione del personale dei Responsabili Ulteriori del Trattamento;

"Report" indica specifici report redatti da professionisti indipendenti selezionati dal Fornitore per lo svolgimento di audit secondo standard internazionali e/o best practice;



“Richiesta” indica una richiesta di accesso di un Interessato, una richiesta di cancellazione o correzione dei Dati Personali, o una richiesta di esercizio di uno degli altri diritti previsti dal GDPR;

“Responsabile Ulteriore del Trattamento” indica qualunque subappaltatore cui il Fornitore abbia subappaltato uno qualsiasi degli obblighi assunti contrattualmente e che, nell’adempiere tali obblighi, potrebbe dover raccogliere, accedere, ricevere, conservare o altrimenti trattare Dati Personali; “Servizio/i” indica il servizio o i servizi oggetto dei Contratti sottoscritti tempo per tempo tra il Cliente e il Fornitore;

“Violazione della Sicurezza dei Dati Personali” indica la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l’accesso ai Dati Personali occorsa su sistemi gestiti dal Fornitore o comunque sui quali il Fornitore abbia un controllo.

- 1.2 I termini “ivi compreso/a/i/e” e “incluso/a/i/e” saranno interpretati come se fossero seguiti dall’espressione “a titolo puramente esemplificativo”, così da fornire un elenco non esaustivo di esempi.
- 1.3 Per le finalità del presente Accordo, i termini “Interessato”, “Trattamento”, “Titolare del trattamento”, “Responsabile del trattamento”, “Trasferimento” e “Misure tecnico-organizzative adeguate” saranno interpretati in conformità alla Legislazione in materia di Protezione dei Dati Personali applicabile.

2. RUOLO DELLE PARTI

- 2.1 Le Parti riconoscono e convengono che il Fornitore agisce quale Responsabile del trattamento in relazione ai Dati Personali e il Cliente agisce di regola quale Titolare del trattamento dei Dati Personali.
- 2.2 Qualora il Cliente svolga operazioni di trattamento per conto di altro Titolare, il Cliente potrà agire come Responsabile del trattamento. In tal caso, il Cliente garantisce che le istruzioni impartite e le attività intraprese in relazione al trattamento dei Dati Personali, inclusa la nomina, da parte del Cliente, del Fornitore quale ulteriore Responsabile del trattamento derivante dalla stipulazione del presente Accordo è stata autorizzata dal relativo Titolare del trattamento e si impegna ad esibire al Fornitore, dietro sua semplice richiesta scritta, la documentazione attestante quanto sopra.
- 2.3 Ciascuna delle Parti si impegna a conformarsi, nel trattamento dei Dati Personali, ai rispettivi obblighi derivanti dalla Legislazione in materia di Protezione dei Dati Personali applicabile.
- 2.4 Il Fornitore ha nominato un Responsabile della protezione dei dati (DPO), domiciliato presso la sede di via Gallarate 156, Milano 20151, che può essere contattato al seguente indirizzo: dpo@axitea.it.

3. TRATTAMENTO DEI DATI PERSONALI

- 3.1 Con la stipulazione del presente Accordo, il Cliente affida al Fornitore l’incarico di trattare i Dati Personali ai fini della prestazione dei Servizi, così come meglio dettagliato nel Contratto.
- 3.2 Il Fornitore si impegna a conformarsi alle Istruzioni, fermo restando che, qualora il Cliente richieda variazioni rispetto alle Istruzioni iniziali, il Fornitore valuterà gli aspetti di fattibilità e concorderà con il Cliente le predette variazioni ed i costi connessi.
- 3.3 Nei casi di cui all’art. 3.2 e in caso di richieste del Cliente che comportino il trattamento di Dati Personali che siano, ad avviso del Fornitore, in violazione della Legislazione in materia di Protezione dei Dati Personali, il Fornitore è autorizzato ad astenersi dall’eseguire tali Istruzioni e ne informerà prontamente il Cliente. In tali casi il Cliente potrà valutare eventuali variazioni alle Istruzioni impartite o contattare l’Autorità di controllo per verificare la liceità delle richieste avanzate.

4. LIMITAZIONI ALL'UTILIZZO DEI DATI PERSONALI

- 4.1 Nell’eseguire il trattamento dei Dati Personali ai fini della prestazione dei Servizi il Fornitore si impegna a eseguire il trattamento dei Dati Personali:
 - (i) soltanto nella misura, e con le modalità necessarie, per erogare i Servizi o per adempiere opportunamente i propri obblighi previsti dal Contratto e dal presente Accordo ovvero imposti dalla legge o da un organo di vigilanza o controllo competente. In tale ultima circostanza il Fornitore ne informerà il Cliente (salvo il caso in cui ciò sia vietato dalla legge per ragioni di pubblico interesse) mediante comunicazione trasmessa all’Email di notifica;
 - (ii) in conformità alle Istruzioni del Cliente.
- 4.2 Il Personale del Fornitore che accede, o comunque tratta i Dati Personali, è preposto al trattamento di tali dati sulla base di idonee autorizzazioni e ha ricevuto la necessaria formazione anche in merito al trattamento dei dati personali. Tale personale è altresì vincolato da obblighi di riservatezza, e deve attenersi alle policy di riservatezza e di protezione



dei dati personali adottate dal Fornitore.

5. AFFIDAMENTO A TERZI

5.1 In relazione all'affidamento a Responsabili Ulteriori del Trattamento di operazioni di trattamento di Dati Personali le Parti convengono quanto segue:

- (iii) Il Cliente acconsente espressamente che alcune operazioni di trattamento di Dati Personali siano affidate dal Fornitore a soggetti terzi;
- (iv) Il Cliente acconsente altresì all'affidamento di operazioni di Trattamento dei Dati Personali a ulteriori soggetti;
- (v) Nei casi in cui il Fornitore ricorra a Responsabili Ulteriori del Trattamento per l'esecuzione di specifiche attività di trattamento dei Dati Personali, il Fornitore si impegna ad avvalersi di Responsabili Ulteriori del Trattamento che garantiscono misure tecniche e organizzative adeguate e garantisce che l'accesso ai Dati Personali, e il relativo trattamento, sarà effettuato esclusivamente nei limiti di quanto necessario per l'erogazione dei servizi subappaltati.

6. DISPOSIZIONI IN MATERIA DI SICUREZZA

6.1 Il Fornitore ha definito e formalizzato un Sistema di Gestione per la Sicurezza delle Informazioni (in seguito "SGSI") conforme allo Standard ISO / IEC 27001:2013.

Il SGSI viene regolarmente applicato e aggiornato ogni qualvolta se ne ravvisi l'utilità, perseguendo il suo continuo miglioramento in conformità ai principi e ai requisiti indicati dalle norme di riferimento.

6.2 Il Fornitore, nell'eseguire il trattamento dei Dati personali si impegna ad adottare misure tecnico- organizzative adeguate (vedi "Allegato A") per evitare il trattamento illecito o non autorizzato, la distruzione accidentale o illecita, il danneggiamento, la perdita accidentale, l'alterazione e la divulgazione non autorizzata, o l'accesso ai Dati Personali.

6.3 Coerentemente, l'organizzazione aziendale ha suddiviso tutta l'attività operativa in una sequenza di processi determinati, individuando i rispettivi responsabili. L'azienda ha così stabilito i criteri e metodi per assicurare l'efficace funzionamento e il controllo delle prassi formalizzate in apposite procedure e dei moduli di registrazione delle attività svolte.

6.4 Sulla base dei processi così determinati, sono state definite e dimensionate le risorse tecniche e professionali necessarie al conseguimento dei risultati perseguiti e alla loro ottimizzazione, nonché finalizzate ad assicurare il funzionamento, il monitoraggio e la misura, ove applicabile, delle prestazioni.

6.5 Il Fornitore presterà assistenza al Cliente nel garantire il rispetto degli obblighi di sicurezza di cui agli artt. 32-34 del GDPR.

6.6 Il Cliente si impegna ad adottare tutte le misure di sicurezza idonee in relazione alla fruizione dei servizi da parte del proprio personale e di coloro che sono autorizzati ad accedervi.

7. LIMITAZIONI AL TRASFERIMENTO DEI DATI PERSONALI AL DI FUORI DELLO SPAZIO ECONOMICO EUROPEO (SEE)

7.1 Fornitore non trasferirà i Dati Personali al di fuori dello SEE se non in accordo con il Cliente.

7.2 Se, ai fini della conservazione o del trattamento dei Dati Personali da parte di un Responsabile Ulteriore del trattamento, è necessario effettuare il trasferimento dei Dati Personali fuori dallo SEE in un paese che non gode di una decisione di adeguatezza da parte della Commissione Europea ai sensi dell'art. 45 del GDPR, il Fornitore:

(vi) farà in modo che il Responsabile Ulteriore del trattamento stipuli le Clausole Contrattuali Tipo, o loro equivalente, se modificate nel tempo. Copia delle Clausole Contrattuali Tipo sottoscritte dal Fornitore per conto del Cliente saranno rese disponibili al Cliente; e/o

(vii) potrà proporre al Cliente altre modalità di trasferimento dei Dati Personali conformi a quanto previsto dalla Legislazione in materia di Protezione dei Dati Personali.

7.3 Nei casi di cui al precedente punto (i) con il presente Accordo il Cliente conferisce espressamente mandato al Fornitore a sottoscrivere le Clausole Contrattuali Tipo con i Responsabili Ulteriori del Trattamento. Qualora Titolare del trattamento sia l'Utente Finale, il Cliente si impegna a informare l'Utente Finale di tale trasferimento e dichiara che l'autorizzazione ad avvalersi del Responsabile Ulteriore del Trattamento situato fuori dallo SEE equivale al mandato di cui sopra.

8. VERIFICHE E CONTROLLI

8.1 Il Fornitore sottopone ad audit periodici la sicurezza dei sistemi e degli ambienti di elaborazione dei Dati Personali dallo stesso utilizzati per l'erogazione dei Servizi e le sedi in cui avviene tale trattamento. Il Fornitore avrà la facoltà di



incaricare dei professionisti indipendenti selezionati dal Fornitore per lo svolgimento di audit secondo standard internazionali e/o best practice, i cui esiti saranno riportati nei Report. Tali Report, che costituiscono informazioni confidenziali del Fornitore, potranno essere resi disponibili al Cliente per consentirgli di verificare la conformità del Fornitore agli obblighi di sicurezza di cui al presente Accordo.

- 8.2 Nei casi previsti dall'art. 8.1, il Cliente concorda che il proprio diritto di verifica sarà esercitato attraverso la verifica dei Report messi a disposizione dal Fornitore.
- 8.3 Il Fornitore riconosce il diritto del Cliente, con le modalità e nei limiti di seguito indicati, ad effettuare audit indipendenti per verificare la conformità del Fornitore agli obblighi previsti nel presente Accordo e di quanto previsto dalla normativa. Il Cliente potrà avvalersi per tali attività di proprio personale specializzato o di revisori esterni, purché tali soggetti siano previamente vincolati da idonei impegni alla riservatezza.
- 8.4 Nel caso di cui al precedente punto 8.2, il Cliente dovrà previamente inviare richiesta scritta al Responsabile della Protezione dei Dati (DPO) del Fornitore. Successivamente alla richiesta di audit o ispezione il Fornitore e il Cliente concorderanno, prima dell'avvio delle attività, i dettagli di tali verifiche (data di inizio e durata), le tipologie di controllo e l'oggetto delle verifiche, i vincoli di riservatezza a cui devono essere vincolati il Cliente e coloro che effettuano le verifiche e i costi che il Fornitore potrà addebitare per tali verifiche e che saranno determinati in relazione all'estensione e alla durata delle attività di verifica.
- 8.5 Il Fornitore potrà opporsi per iscritto alla nomina da parte del Cliente di eventuali revisori esterni che siano, ad insindacabile giudizio del Fornitore, non adeguatamente qualificati o indipendenti, siano concorrenti del Fornitore o che siano evidentemente inadeguati. In tali circostanze il Cliente sarà tenuto a nominare altri revisori o a condurre le verifiche in proprio.
- 8.6 Il Cliente si impegna a corrispondere al Fornitore gli eventuali costi calcolati dal Fornitore e comunicati al Cliente nella fase di cui al precedente punto 8.4, con le modalità e nei tempi ivi concordati. Restano a carico esclusivo del Cliente i costi delle attività di verifica dallo stesso commissionate a terzi.
- 8.7 Resta fermo quanto previsto in relazione ai diritti di ispezione del Titolare del trattamento e delle autorità nelle Clausole Contrattuali Tipo eventualmente sottoscritte ai sensi del precedente punto 7, che non potranno considerarsi modificate da alcuna delle previsioni contenute nel presente Accordo.
- 8.8 Le attività di verifica che interessino eventuali Responsabili Ulteriori dovranno essere svolte nel rispetto delle regole di accesso e delle politiche di sicurezza dei Responsabili Ulteriori.

9. ASSISTENZA A FINI DI CONFORMITÀ

- 9.1 Il Fornitore presterà assistenza al Cliente e coopererà nei modi di seguito indicati al fine di consentire al Cliente il rispetto degli obblighi previsti dalla Legislazione in materia di Protezione dei Dati Personali.
- 9.2 Qualora il Fornitore riceva Richieste o reclami da un Interessato in relazione ai Dati Personali, il Fornitore raccomanderà all'Interessato di rivolgersi al Cliente o all'Utente Finale, nel caso in cui quest'ultimo sia il Titolare del Trattamento. In tali casi il Fornitore informerà tempestivamente il Cliente del ricevimento della Richiesta mediante invio di E-mail di notifica e fornirà al Cliente le informazioni ad esso disponibili unitamente a copia della Richiesta o del reclamo. Resta inteso che tale attività di cooperazione sarà svolta in via eccezionale, in quanto la gestione dei rapporti con gli Interessati resta esclusa dai Servizi ed è responsabilità del Cliente gestire eventuali reclami in via diretta e provvedere a dar seguito a tali Richieste o reclami.
- 9.3 Il Fornitore provvederà a informare tempestivamente il Cliente, salvo il caso in cui ciò sia vietato dalla legge, con avviso all'Email di notifica di eventuali ispezioni o richieste di informazioni presentate da autorità di controllo e forze di polizia rispetto a profili che riguardano il trattamento dei Dati Personali.
- 9.4 Qualora, ai fini dell'evasione delle Richieste di cui ai precedenti punti, il Cliente abbia necessità di ricevere informazioni dal Fornitore circa il trattamento dei Dati Personali, il Fornitore presterà la necessaria assistenza nei limiti di quanto ragionevolmente possibile, a condizione che tali richieste siano presentate con congruo preavviso.
- 9.5 Il Fornitore, tenuto conto della natura dei Dati Personali e delle informazioni ad esso disponibili, fornirà ragionevole assistenza al Cliente nel rendere disponibili informazioni utili per consentire al Cliente l'effettuazione di valutazioni di impatto sulla protezione dei Dati Personali nei casi previsti dalla legge. In tal caso il Fornitore renderà disponibili informazioni di carattere generale in base al Servizio, quali le informazioni contenute nel Contratto e nel presente Accordo. Eventuali richieste di assistenza personalizzate potranno essere soggette al pagamento di un corrispettivo da parte del Cliente. Resta inteso che è responsabilità e onere esclusivo del Cliente procedere alla valutazione di impatto in base alle caratteristiche del trattamento dei Dati Personali dallo stesso posto in essere nel contesto dei Servizi.
- 9.6 Il Fornitore si impegna a rendere Servizi improntati ai principi di minimizzazione del trattamento (privacy by design & by



default).

- 9.7 Il Cliente prende atto che, in caso di Richieste di portabilità dei Dati Personali avanzate dai rispettivi Interessati, e solo in relazione ai Servizi che generano Dati Personali rilevanti a tal fine, il Fornitore presterà assistenza al Cliente mettendo a disposizione le informazioni necessarie per estrarre i dati richiesti in formato conforme a quanto previsto dalla Legislazione in materia di Protezione dei Dati Personali.

10. OBBLIGHI DEL CLIENTE E LIMITAZIONI

- 10.1 Il Cliente si impegna a impartire Istruzioni conformi alla normativa e a utilizzare i Servizi in modo conforme alla Legislazione in materia di Protezione dei Dati Personali e solo per trattare Dati Personali che siano stati raccolti in conformità alla Legislazione in materia di Protezione dei Dati Personali.
- 10.2 Il Cliente si impegna ad assolvere a tutti gli obblighi posti in capo al Titolare del Trattamento dalla Legislazione in materia di Protezione dei Dati Personali, ivi inclusi gli obblighi di informativa nei confronti degli Interessati. Il Cliente si impegna inoltre a garantire che il trattamento dei Dati Personali effettuato mediante l'utilizzo dei Servizi avvenga solo in presenza di idonea base giuridica.
- 10.3 Qualora il rilascio dell'informativa e l'ottenimento del consenso debbano avvenire per il tramite del prodotto oggetto del Contratto, il Cliente dichiara di aver valutato il prodotto e che esso risponde alle esigenze del Cliente.
- 10.4 È altresì onere esclusivo del Cliente provvedere alla gestione dei Dati Personali in conformità alle Richieste avanzate dagli Interessati, e pertanto provvedere ad esempio agli eventuali aggiornamenti, integrazioni, rettifiche e cancellazioni dei Dati Personali.
- 10.5 È onere del Cliente mantenere l'account collegato all'Email di notifica, attivo ed aggiornato.
- 10.6 Il Cliente prende atto che, ai sensi dell'art. 30 del GDPR, il Fornitore è tenuto a mantenere un registro delle attività di trattamento eseguite per conto dei Titolari (o Responsabili) del Trattamento e a raccogliere a tal fine i dati identificativi e di contatto di ciascun Titolare (e/o Responsabile) del Trattamento per conto del quale il Fornitore agisce e che tali informazioni devono essere rese disponibili all'autorità competente, su richiesta. Pertanto, quando richiesto, il Cliente si impegna a dare al Fornitore i dati identificativi e di contatto sopra indicati con le modalità individuate dal Fornitore nel tempo e a mantenere aggiornate tali informazioni tramite i medesimi canali.
- 10.7 Il Cliente dichiara pertanto che le attività di trattamento dei Dati Personali, come descritte nei Contratti, e nel presente Accordo, sono lecite.

11. DURATA

Il presente Accordo avrà efficacia a decorrere dalla Data di Decorrenza dell'Accordo e cesserà automaticamente, alla data di cancellazione di tutti i Dati Personali da parte del Fornitore, come previsto nel presente Accordo.

12. DISPOSIZIONI PER LA RESTITUZIONE O LA CANCELLAZIONE DEI DATI PERSONALI

- 12.1 Alla cessazione del Servizio, per qualunque causa intervenuta, il Fornitore cesserà ogni trattamento dei Dati Personali e
- (i) provvederà alla cancellazione dei Dati Personali (ivi incluse eventuali copie) dai sistemi del Fornitore o da quelli su cui lo stesso abbia controllo entro il termine previsto nel Contratto, tranne il caso in cui la conservazione dei dati da parte del Fornitore sia necessaria al fine di assolvere ad una disposizione di legge italiana o europea;
 - (ii) distruggerà eventuali Dati Personali conservati in formato cartaceo in suo possesso, tranne il caso in cui la conservazione dei dati da parte del Fornitore sia necessaria ai fini del rispetto di norme di legge italiane o europee; e
 - (iii) manterrà a disposizione del Cliente i Dati Personali per l'estrazione per il periodo di 12 (dodici) mesi successivi alla cessazione del Contratto. Durante tale periodo, il trattamento sarà limitato alla sola conservazione finalizzata a mantenere i Dati Personali a disposizione del Cliente per l'estrazione di cui al punto 12.2.
- 12.2 Fermo restando quanto altrimenti previsto nel presente Accordo, il Cliente riconosce di poter estrarre i Dati Personali, alla cessazione del Servizio, nei modi convenuti nel Contratto e conviene che è sua responsabilità provvedere all'estrazione totale o parziale dei soli Dati Personali che ritenga utile conservare e che tale estrazione dovrà essere effettuata prima della scadenza del termine di cui al punto (iii).
- 12.3 Resta altresì responsabilità del Cliente provvedere alla cancellazione dei Dati Personali nel rispetto delle norme di legge.

13. RESPONSABILITÀ

- 13.1 Ciascuna Parte è responsabile per l'adempimento dei propri obblighi previsti dal presente Accordo e dalla Legislazione in materia di protezione dei Dati Personali.
-



14. DISPOSIZIONI VARIE

- 14.1 Il presente Accordo sostituisce qualsiasi altro accordo, contratto o intesa tra le Parti con riferimento al suo oggetto nonché qualsivoglia istruzione fornita in qualsiasi forma dal Cliente al Fornitore precedentemente alla data del presente Accordo in merito ai Dati Personali trattati nell'ambito dell'esecuzione del Contratto.
 - 14.2 Il presente Accordo potrà essere modificato per iscritto previo accordo tra le Parti.
 - 14.3 Il presente Accordo è regolato dalla Legge italiana. Eventuali controversie derivanti da o connesse con il presente Accordo saranno soggette a giurisdizione esclusiva del Foro di Milano.
-



ALLEGATO A

Misure Tecnico-organizzative

Misure organizzative:

- **Policy e Disciplinari utenti – Il Fornitore applica dettagliate policy e disciplinari, ai quali tutta l'utenza con accesso ai sistemi informativi ha l'obbligo di conformarsi e che sono finalizzate a garantire comportamenti idonei ad assicurare il rispetto dei principi di riservatezza, disponibilità ed integrità dei dati nell'utilizzo delle risorse informatiche.**
- Autorizzazione accessi logici – Il Fornitore definisce i profili di accesso nel rispetto del least privilege necessari all'esecuzione delle mansioni assegnate. I profili di autorizzazione sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento. Tali profili sono oggetto di controlli periodici finalizzati alla verifica della sussistenza delle condizioni per la conservazione dei profili attribuiti.
- Gestione interventi di assistenza – Gli interventi di assistenza sono regolamentati allo scopo di garantire l'esecuzione delle sole attività previste contrattualmente e impedire il trattamento eccessivo di dati personali la cui titolarità è in capo al Cliente o all'Utente Finale.
- Formazione – Il Fornitore eroga periodicamente ai propri dipendenti coinvolti nelle attività di trattamento corsi di formazione sulla corretta gestione dei dati personali.
- Data Breach – Il Fornitore ha implementato un'apposita procedura finalizzata alla gestione degli eventi e degli incidenti con un potenziale impatto sui dati personali che definisce ruoli e responsabilità, il processo di rilevazione (presunto o accertato), l'applicazione delle azioni di contrasto, la risposta e il contenimento dell'incidente / violazione nonché le modalità attraverso le quali effettuare le comunicazioni delle violazioni di dati personali al Cliente.
- Incident Management – Il Fornitore ha realizzato una specifica procedura di Incident Management allo scopo di garantire il ripristino delle normali operazioni di servizio nel più breve tempo possibile, garantendo il mantenimento dei livelli migliori di servizio.
- Log Management – L'organizzazione definisce le opportune misure di tracciamento delle attività sui sistemi da parte degli Amministratori di Sistema, al fine di ottemperare alle prescrizioni normative in materia, e a tutela della privacy dei dipendenti e dei clienti del Fornitore. Inoltre, per i sistemi relativi ai servizi del SOC vengono implementate specifiche attività di tracciatura anche a fini di auditing, con la memorizzazione dei Log in sistemi ove la modifica e cancellazione degli stessi non è consentita agli amministratori di sistema.
- Change Management – I cambiamenti che hanno impatto sulla sicurezza delle informazioni vengono preventivamente valutati. Il principio che viene applicato è quello della sicurezza by default e by design. A tal fine è predisposta una procedura di Change Management da applicare ogni qualvolta si renda necessario una modifica ai sistemi di produzione ICT del Fornitore che possa compromettere la sicurezza dei dati e delle informazioni elaborate, ivi inclusi i sistemi dei servizi del SOC.
- Gestione della continuità e disponibilità del servizio – La continuità dei servizi erogati dai SOC del Fornitore è garantita progettando l'architettura di servizio su distinte direttrici non mutualmente esclusive:
 - a) La presenza di strutture tecnologiche ridondate o in alta affidabilità, che permettono di contenere eventuali guasti sui sistemi, mantenendo inalterato il servizio,
 - b) La presenza di infrastrutture di servizio atte a garantire la continuità del servizio in assenza di erogazione dell'elettricità, quali ad esempio gli UPS ed i generatori ausiliari,
 - c) La distribuzione geografica dei SOC, che permette di contenere gli effetti di eventuali calamità naturali o di incidenti aventi ripercussioni sulla agibilità delle Centrali Operative,
 - d) La predisposizione e configurazione dei SOC ad operare uno in back-up dell'altro, attivando la gestione del servizio presso l'altro SOC qualora non sia possibile garantirne localmente l'erogazione, a seguito di malfunzionamenti tecnici presso il SOC o dei servizi esterni essenziali.

In merito al personale l'erogazione dei servizi, anche in casi di eventi estremi (es. calamità naturali), è garantita dalla distribuzione del personale su più turni e su SOC diversi, che ne permettono di sanare eventuali carenze in situazioni di emergenza.

A prescindere dalla tipologia di evento accaduto, dal suo impatto e dagli effetti da esso derivanti, il processo di gestione della continuità operativa può essere sinteticamente descritto attraverso le seguenti fasi: Risposta all'evento; Operatività in Continuity; Rientro alla normale operatività.



Misure tecniche:

- Il Fornitore ha installato una «scatola nera» (incident recorder) nel sistema che in automatico memorizza le attività permettendo così di ricostruire eventi critici in modo da:
 - fornire le informazioni all'Autorità Garante relative a un data breach per dimostrare che la responsabilità dell'evento è riconducibile ad un attacco hacker effettuato da ignoti e non ad una condotta negligente del Fornitore;
 - identificare le cause di un malfunzionamento interno del sistema;
 - fornire a terzi (es. Polizia postale) lo storico di un avvenimento specifico.
 - Il Fornitore effettua il monitoraggio degli eventi e l'Incident Handling centralizzando gli eventi di sicurezza mediante le seguenti attività:
 - controllo continuo delle anomalie registrate dai log;
 - segnalazione immediata di eventi critici e di attività potenzialmente dannose sui sistemi monitorati;
 - un processo di gestione degli incidenti di sicurezza che lo aiuta ad arginare gli attacchi e ad effettuare tempestive azioni correttive;
 - report per documentare gli eventi di sicurezza fondamentali per le attività di audit.
 - Il Fornitore ha adottato un sistema di sicurezza informatico con le seguenti funzionalità:
 - la protezione continuativa rispetto all'evoluzione degli attacchi informatici condotti attraverso malware (quali virus, APT, ransomware e similari) e l'identificazione degli interventi necessari alle misure di protezione in essere;
 - la rilevazione tempestiva della diffusione su internet di nuove tipologie di malware e la relativa valutazione del livello di efficacia del servizio di protezione, in aggiunta, l'identificazione di eventuali misure migliorative dalle nuove minacce rilevate.
-

INFORMATIVA SUL TRATTAMENTO DEI DATI PERSONALI

ai sensi degli artt. 13 e 14 del Regolamento (UE) 2016/679

relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali

La presente informativa contiene le informazioni rese ai sensi degli artt. 13 e 14 del Regolamento Europeo 679/2016 relativo alla protezione dei dati personali (“**GDPR**”) dalla Società (come di seguito definita), in qualità di titolare del trattamento, ai soggetti che hanno acquistato, richiesto o fruito di servizi e/o prodotti dalla stessa commercializzati (nel seguito, il “**Cliente**”).

Per “**Società**”, titolare del trattamento, deve intendersi TeamSystem S.p.A., società con socio unico soggetta all’attività di direzione e coordinamento di TeamSystem Holding S.p.A. - Cap. Soc. € 24.000.000 I.v. - C.C.I.A.A. di Pesaro e Urbino - P.I. 01035310414 - Sede Legale: Via Sandro Pertini, 88 - 61122 Pesaro (PU), ovvero la società appartenente al gruppo facente capo a TeamSystem S.p.A. che ha stipulato con il Cliente il contratto per l’utilizzo dei servizi o delle soluzioni software TeamSystem (nel seguito, il “**Contratto**”). La Società titolare del trattamento può essere contattata secondo le modalità previste nella presente informativa (e in particolare all’articolo 8, “**Quali sono i diritti dell’interessato**”).

1 TIPOLOGIA DI DATI TRATTATI

La Società è titolare del trattamento dei dati personali del Cliente trattati in collegamento con il Contratto. I dati personali del Cliente che la Società raccoglie in relazione alla gestione del rapporto contrattuale e nelle eventuali fasi precontrattuali possono essere forniti direttamente dal Cliente o acquisiti da fonti pubbliche. In particolare, i dati personali trattati dalla Società comprendono, in via esemplificativa e non esaustiva, i nominativi, le qualifiche, i numeri di telefono, codice fiscale, dati di pagamento e bancari, eventualmente la ragione sociale e gli indirizzi di posta elettronica di persone fisiche e di rappresentanti legali del Cliente. Le informazioni del Cliente acquisite da fonti pubbliche comprendono ad esempio i dati dei rappresentanti e procuratori o ai bilanci o all’affidamento della clientela che vengono raccolte tramite ad esempio le Camere di Commercio o i servizi di informazione commerciale. Le categorie di dati personali del Cliente sopra indicate sono congiuntamente definite i “**Dati**”.

2 FINALITÀ DEL TRATTAMENTO

I Dati del Cliente sono trattati dalla Società con strumenti manuali e mediante strumenti informatici, per le seguenti finalità:

- a) l’esecuzione di obblighi strettamente connessi all’instaurazione, gestione ed esecuzione del Contratto, ivi compresa la gestione del rapporto pre-contrattuale, la gestione amministrativa e contabile del Contratto, la gestione dei relativi pagamenti e delle fatture, la fornitura dei servizi oggetto del Contratto e la gestione dei servizi di supporto connessi allo stesso; e
- b) l’adempimento di obblighi derivanti dalla legge, regolamenti o normativa comunitaria (es. obblighi fiscali e contabili);

(le finalità sopra elencate sono congiuntamente definite le “**Finalità Contrattuali**”)

- c) per l’analisi e il miglioramento dei servizi offerti attraverso il Contratto;
- d) per far valere e difendere i propri diritti, anche nell’ambito di procedure di recupero crediti, anche attraverso terze parti;
- e) per portare a termine una potenziale fusione, cessione di beni, cessione d’azienda o di ramo d’azienda divulgando e trasferendo i Dati alla/e terza/e parte/i coinvolta/e;

(le finalità di cui alle lettere da c) ad e) sono congiuntamente definite le “**Finalità di Legittimo Interesse di Business**”)

- f) per inviare, ai sensi dell’articolo 130 del Decreto Legislativo 196/2003 (il “**Codice Privacy**”), comunicazioni di marketing su servizi o prodotti analoghi a quelli oggetto del Contratto, tramite e-mail, fermo restando che, in qualsiasi momento, l’Interessato avrà la possibilità di opporsi all’invio di tali comunicazioni;
 - g) fermo restando quanto indicato alla precedente lettera f), per inviare - previo consenso dell’Interessato - comunicazioni di marketing relative ai prodotti e servizi offerti dalla Società, condurre ricerche di mercato o altre iniziative di customer satisfaction sia tramite canali di comunicazione tradizionali quali la posta cartacea o la telefonata da parte di un operatore che tramite strumenti di comunicazione automatizzati quali email, chat, SMS, MMS, videochiamata, chiamata automatica, instant message, chatbot e altri strumenti di comunicazione a distanza;
-

- h) per inviare, con il previo consenso del Cliente, comunicazioni di marketing secondo le modalità di cui alle precedenti lettere f) e g) relative ai prodotti e servizi delle altre società del gruppo di cui la Società è parte e/o di partner commerciali appartenenti alle rete commerciale TeamSystem, a cui i Dati potranno essere comunicati e il cui elenco è disponibile contattando la Società tramite le modalità indicate in questa informativa;
- i) fermo restando quanto indicato alla successiva lettera j), per eseguire, con il previo consenso del Cliente, un'analisi delle preferenze, attività e abitudini di spesa del Cliente, al fine di inviare le comunicazioni di marketing sopra indicate.

(le finalità di cui alle lettere da f) ad i) sono congiuntamente definite le "**Finalità di Marketing**");

- j) per eseguire attività di segmentazione dei Clienti, a cui è possibile inviare comunicazioni per Finalità di Marketing sulla base di quanto indicato nella presente informativa, basate su categorie non invasive di appartenenza, quali tra gli altri, la categoria professionale di appartenenza, la città/provincia/regione in cui ha sede, la tipologia di prodotto o di servizio acquistato.

(la finalità di cui alla lettera j) è definita "**Finalità di Legittimo Interesse di Marketing**").

3 **BASE GIURIDICA DEL TRATTAMENTO**

Il trattamento dei Dati è necessario con riferimento alle Finalità Contrattuali data la sua essenzialità al fine di:

- dare esecuzione al Contratto con riferimento alla fornitura dei servizi richiesti relativamente ai casi di cui alla Sezione 2, lettera a); e
- adeguarsi alle disposizioni di cui alla normativa applicabile come previsto dalla Sezione 2, lettera b).

Qualora il Cliente non fornisca i Dati necessari per le Finalità Contrattuali, non sarà possibile procedere alla stipula del Contratto da parte della Società.

Il trattamento dei Dati per le Finalità di Legittimo Interesse di Business è effettuato ai sensi dell'articolo 6, lettera f) del GDPR per il perseguimento del legittimo interesse della Società che è equamente bilanciato con l'interesse legittimo dell'Interessato, in quanto l'attività di trattamento dei Dati è limitata a quanto strettamente necessario per l'esecuzione delle attività sopra indicate e unicamente nei casi in cui la medesima finalità non possa essere perseguita tramite il trattamento di dati aggregati o anonimizzati. Il trattamento per le Finalità di Legittimo Interesse di Business non è obbligatorio e l'Interessato potrà opporsi a detto trattamento con le modalità di cui alla presente informativa, ma qualora si opponesse a detto trattamento i Dati dell'Interessato non potranno essere utilizzati per Finalità di Legittimo Interesse di Business, fatto salvo il caso in cui la Società dimostri la presenza di motivi legittimi cogenti prevalenti o di esercizio o difesa di un diritto ai sensi dell'articolo 21 del GDPR.

Il trattamento dei Dati per Finalità di Marketing è basato:

- per quanto riguarda il trattamento di cui alla Sezione 2 lettera f), sull'articolo 130 del Codice Privacy a cui l'Interessato potrà opporsi al momento della raccolta dei dati e in ogni successiva comunicazione;
- per quanto riguarda il trattamento di cui alla Sezione 2, lettere da g) a i), sul consenso del Cliente.

Il trattamento dei dati per Finalità di Marketing non è obbligatorio. Pertanto in caso di opposizione all'invio di comunicazioni di marketing o di rifiuto a fornire il relativo consenso, quando richiesto, o di revoca dello stesso secondo le modalità previste dalla presente informativa privacy il Cliente non riceverà le comunicazioni di marketing.

Infine, il trattamento dei Dati per Finalità di Legittimo Interesse di Marketing è funzionale al perseguimento di un legittimo interesse della Società adeguatamente temperato con gli interessi dell'Interessato alla luce dei limiti indicati nella Sezione 2 lettera j). Anche in tal caso il trattamento per le Finalità di Legittimo Interesse di Marketing non è obbligatorio e l'Interessato potrà opporsi con le modalità di cui alla presente informativa. Tuttavia, qualora l'Interessato si opponesse a detto trattamento i Dati dell'Interessato non potranno essere utilizzati per Finalità di Legittimo Interesse di Marketing, fatto salvo il caso in cui la Società dimostri la presenza di motivi legittimi cogenti prevalenti. Nel caso in cui l'Interessato desiderasse ottenere maggiori informazioni circa le attività di bilanciamento degli interessi, diritti e libertà, può contattare in ogni momento la Società secondo le modalità indicate in questa informativa.

4 **MODALITÀ DEL TRATTAMENTO**

I Dati sono trattati dalla Società con sistemi elettronici e manuali secondo i principi di correttezza, lealtà e trasparenza previsti dalla normativa applicabile in materia di protezione dei dati personali e tutelando la riservatezza dell'Interessato tramite misure di sicurezza tecniche e organizzative per garantire un livello di sicurezza adeguato.

5 **CONSERVAZIONE DEI DATI**

I Dati sono conservati per il periodo di tempo necessario per il perseguimento delle finalità per cui tali dati sono stati raccolti. In ogni caso, i seguenti termini di conservazione si applicheranno con riferimento ai trattamenti dei Dati per le finalità riportate di seguito:

- a) per le Finalità Contrattuali e di Legittimo Interesse di Business, i Dati vengono conservati per un periodo pari alla durata del Contratto (ivi inclusi eventuali rinnovi) e per i 10 anni successivi al termine, risoluzione o recesso dello stesso, fatti salvi i casi in cui la conservazione per un periodo successivo sia richiesta per eventuali contenziosi, richieste delle autorità competenti o ai sensi della normativa applicabile;
- b) per le Finalità di Marketing di cui alla Sezione 2, lettere f) e g) e per la Finalità di Legittimo Interesse di Marketing, i Dati vengono conservati per la durata del Contratto e un periodo di 24 mesi successivi all'ultimo contatto con il Cliente da intendersi, tra gli altri, la partecipazione ad un evento della Società, la fruizione di un prodotto o servizio fornito dalla Società o l'apertura di una newsletter (congiuntamente definiti l'"**Ultimo Contatto**");
- c) per la Finalità di Marketing di cui alla Sezione 2, lettera h), i Dati vengono conservati per un periodo di 12 mesi dalla registrazione;
- d) per la Finalità di Marketing di cui alla Sezione 2, lettera i), i Dati vengono conservati dalla Società per la durata del Contratto e un periodo di 12 mesi successivi all' Ultimo Contatto con il Cliente, mentre sono conservati dai terzi per un periodo di 12 mesi dalla relativa registrazione.

6 COMUNICAZIONE E DIFFUSIONE DEI DATI

Per le Finalità Contrattuali, i Dati possono essere comunicati ai seguenti soggetti terzi che svolgono attività funzionali a quelli di cui al Contratto situati all'interno e all'esterno dell'Unione Europea: (a) terzi fornitori di servizi di assistenza e consulenza per la Società con riferimento alle attività dei settori (a titolo meramente esemplificativo) tecnologico, contabile, amministrativo, legale, assicurativo, (b) società del gruppo di cui la Società è parte, (c) nei casi in cui il rapporto contrattuale preveda l'intervento di partner commerciali, la Società potrà condividere alcuni Dati con i propri distributori, *reseller* e i partner facenti parte della catena di distribuzione dei prodotti e servizi del gruppo di cui la Società è parte; (d) soggetti ed autorità il cui diritto di accesso ai Dati Personali è espressamente riconosciuto dalla legge, da regolamenti o da provvedimenti emanati dalle autorità competenti.

Per le Finalità di Legittimo Interesse di Business, i Dati possono essere comunicati alle seguenti categorie di destinatari, situati all'interno e all'esterno dell'Unione Europea: (a) terzi fornitori di servizi di assistenza e di consulenza per la Società con riferimento alle attività dei settori (a titolo meramente esemplificativo) tecnologico, contabile, amministrativo, legale, assicurativo, (b) società del gruppo di cui la Società è parte, (c) potenziali acquirenti della Società ed entità risultanti dalla fusione o ogni altra forma di trasformazione riguardante la Società, (d) autorità competenti.

Per le Finalità di Marketing e per le Finalità di Legittimo Interesse di Marketing, i Dati possono essere comunicati alle seguenti categorie di destinatari, situati all'interno e all'esterno dell'Unione Europea: (a) terzi incaricati del trattamento dei dati personali fornitori di servizi di assistenza e consulenza per la Società con riferimento alle attività di invio delle comunicazioni marketing; (b) società del gruppo di cui la Società è parte.

Tali destinatari trattano i dati dei Clienti in qualità di titolari, responsabili o incaricati del trattamento a seconda delle circostanze.

La lista completa e aggiornata dei soggetti che trattano i Dati in qualità di responsabili del trattamento è disponibile su richiesta al Responsabile per la Protezione dei Dati.

7 TRASFERIMENTO DEI DATI ALL'ESTERO

I Dati potranno essere liberamente trasferiti fuori dal territorio nazionale a Paesi situati nell'Unione europea, ma potrebbero essere trasferiti anche al di fuori dell'Unione europea e in particolare negli Stati Uniti. Con riferimento ai trasferimenti al di fuori del territorio dell'Unione europea verso Paesi non considerati adeguati dalla Commissione europea, la Società adotta le misure di sicurezza adatte ed appropriate per proteggere i Dati degli Interessati. Conseguentemente l'eventuale trasferimento dei Dati in Paesi situati al di fuori dell'Unione europea avverrà, in ogni caso, nel rispetto delle garanzie appropriate e opportune ai fini del trasferimento stesso, come le clausole contrattuali tipo di protezione dei dati, ai sensi della normativa applicabile e in particolare degli articoli 45 e 46 del GDPR.

Nel caso in cui l'Interessato desideri ricevere ulteriori informazioni in merito alle garanzie in essere e richiedere una copia delle stesse, può contattare il Responsabile della Protezione dei dati secondo le modalità indicate nella presente informativa.

8 QUALI SONO I DIRITTI DELL'INTERESSATO

In relazione al trattamento dei Dati descritto in questa informativa, l'Interessato può esercitare in ogni momento, i diritti previsti dal GDPR (artt. 15-21), ivi inclusi:

- ricevere conferma dell'esistenza dei Dati e accedere al loro contenuto (diritto di accesso);
- aggiornare, modificare e/o correggere i Dati (diritto di rettifica);
- chiederne la cancellazione o la limitazione del trattamento dei Dati trattati in violazione di legge compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i Dati sono stati raccolti o altrimenti trattati (diritto all'oblio e diritto alla limitazione);
- opporsi al trattamento (diritto di opposizione);
- revocare il consenso, ove prestato, senza pregiudizio per la liceità del trattamento basata sul consenso prestato prima della revoca;
- proporre reclamo all'Autorità di controllo (Garante per la protezione dei dati personali www.garanteprivacy.it) in caso di violazione della disciplina in materia di protezione dei dati personali;
- ricevere copia in formato elettronico dei Dati che lo riguardano come Interessato, quando tali Dati siano stati resi nel contesto del contratto e chiedere che tali Dati siano trasmessi a sè stesso o ad un altro titolare del trattamento (diritto alla portabilità dei dati).

Per esercitare tali diritti l'Interessato può rivolgersi al Responsabile per della Protezione dei Dati inviando la sua richiesta all'indirizzo privacy@teamsystem.com, oppure indirizzando la comunicazione via posta a:

TeamSystem S.p.A.

Via Sandro Pertini 88

Pesaro

c.a.: Responsabile della Protezione dei Dati

Nel contattare la Società, l'Interessato dovrà accertarsi di includere il proprio nome, email/indirizzo postale e/o numero/i di telefono per essere sicuro che la sua richiesta possa essere gestita correttamente.

9 **MODIFICHE E AGGIORNAMENTI**

La presente informativa può essere soggetta a modifiche ed integrazioni, che saranno notificate in anticipo ai Clienti.
