Versione 16.04.2026

CONDIZIONI GENERALI DI UTILIZZO PRODOTTI SOFTWARE E SERVIZI DI AGGIORNAMENTO, ASSISTENZA E MANUTENZIONE

Le presenti condizioni generali (di seguito definite le "**Condizioni Generali**") disciplinano i termini e condizioni della licenza d 'uso di software concessa al cliente (il "**Cliente**") dalla Licenziante, come di seguito definita, nonché la fornitura al Cliente dei servizi di aggiornamento, assistenza e manutenzione descritti nell'Allegato A (i "**Servizi**"). Per "**Licenziante**" 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.

TeamSystem, le società appartenenti al gruppo facente capo a TeamSystem e i distributori ufficiali TeamSystem sono di seguito congiuntamente definiti la "**Rete Commerciale TeamSystem**".

PREMESSA

Documenti contrattuali ed efficacia

La disciplina contrattuale complessiva della licenza d'uso di software concessa al Cliente e della fornitura dei Servizi è contenuta nelle presenti Condizioni Generali, nonché nei moduli d'ordine tempo per tempo sottoscritti o accettati on-line dal Cliente, che contengono le condizioni particolari di contratto (gli "**Ordini**"). Le Condizioni Generali, gli Ordini e le eventuali Condizioni Integrative, come di seguito definite, 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 dalla Licenziante (anche se precedentemente alla data di accettazione delle presenti Condizioni Generali), 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 la Licenziante 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 della Licenziante, salvo che non siano dalla medesima espressamente accettati per iscritto.

Ambito di applicazione e dichiarazioni del Cliente

Le presenti Condizioni Generali si applicano all'utilizzo di ciascuno dei software indicati nell'Ordine (i "**Software**"), inclusi gli eventuali supporti di memorizzazione sui quali questi ultimi sono stati ricevuti. Le presenti Condizioni Generali si applicano, inoltre, a (i) tutti gli aggiornamenti, supplementi, adattamenti, sviluppi, migliorie, personalizzazioni e modifiche in genere apportate ai Software, anche nell'ambito della fornitura dei Servizi, da parte della Licenziante (di seguito complessivamente definiti come "**Aggiornamenti e Sviluppi**") e (ii) agli eventuali "**Sistemi di Intelligenza Artificiale"** (o i "**Sistemi di AI"**), da intendersi come i software e le tecnologie sviluppate, fornite e/o integrate da, e di titolarità di, TeamSystem e/o società del gruppo TeamSystem e/o terze parti che, attraverso l'impiego di tecniche avanzate sono in grado di generare output quali indicatori, alert, suggerimenti, raccomandazioni, decisioni, contenuti e/o previsioni (gli "**Output**"), basati, ove previsto, su attività di analisi, interconnessione e aggregazione dei dati (anche storici) immessi dal Cliente nei Software e/o in software e/o piattaforme di titolarità di TeamSystem o di altra società facente parte del gruppo TeamSystem e concessi in licenza al Cliente in virtù di separato e specifico accordo (le "**Soluzioni dell'Ecosistema TS**"). Ciò a meno che i Software, gli Aggiornamenti e Sviluppi e/o i Sistemi di AI siano accompagnati da autonome condizioni contrattuali (le "**Condizioni Integrative**") (nel qual caso, e salvo quanto diversamente concordato per iscritto tra la Licenziante e il Cliente, le disposizioni delle Condizioni Integrative prevarranno su quelle di cui alle presenti Condizioni Generali, mentre le disposizioni contenute negli Ordini prevarranno sia sulle Condizioni Generali sia sulle Condizioni Integrative).

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 i Software (e gli eventuali Aggiornamenti e Sviluppi e gli eventuali Sistemi di AI**) **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**; (iii) essere consapevole e accettare che i termini e le condizioni del Contratto (ivi inclusi, ma non limitatamente a, i limiti temporali e di utilizzo applicabili alla Licenza, come di seguito definita) prevalgono su qualsiasi eventuale accordo di finanziamento e/o leasing stipulati tra il Cliente e terzi soggetti diversi dagli appartenenti alla Rete Commerciale TeamSystem.

1 LICENZA D'USO

1.1 La Licenziante concede in licenza d 'uso al Cliente, che accetta, il Software e la relativa documentazione ai termini e alle condizioni di cui al Contratto.

1.2 Il Software è concesso in licenza per (i) un'unica istanza ed un unico database per ogni prodotto indicato nell'Ordine (pertanto il Cliente potrà installare copia del Software utilizzandolo su un unico database) e (ii) un unico sistema multi-utente, nel rispetto del limite massimo di utenti eventualmente indicato nell'Ordine; e (iii) un utilizzo nel rispetto dei limiti eventualmente indicati nell'Ordine (ad esempi o con riferimento al numero massimo di documenti, transazioni, operazioni o dichiarazioni processabili o di anagrafiche clienti/dipendenti/altro gestibili). Eventuali richieste di ulteriori istanze o database per il medesimo cliente (es.: test, produzione o sviluppo) o di variazione dei suddetti limiti richiederanno l'acquisto di ulteriori licenze.

1.3 Il Cliente non potrà separare i componenti dei Software e installarli su dispositivi diversi salvo indicazioni esplicite riportate nella documentazione tecnica (es. circolari) relativa al Software.

1.4 La licenza d'uso concessa con il Contratto (la "**Licenza**") è da intendersi non esclusiva, onerosa, non sub licenziabile, non cedibile e comunque non utilizzabile da terzi ad alcun titolo, senza il preventivo consenso scritto della Licenziante.

1.5 A parziale deroga di quanto indicato nell'art. 1.4 che precede, il Cliente potrà concedere in sub-licenza d'uso il Software alle società direttamente o indirettamente controllate dal Cliente stesso ai sensi dell'art. 2359, primo comma, n. 1, c.c. eventualmente elencate nell'Ordine (le "**Controllate**"), restando inteso che, ai fini del presente art. 1.5:

(i) a fronte del diritto di sub-licenza concesso al Cliente, quest'ultimo dovrà corrispondere alla Licenziante, per ciascuna Controllata, il canone annuo aggiuntivo indicato nell'Ordine, ovvero determinato in base a separati accordi intervenuti tra il Cliente e la Licenziante;

(ii) le Controllate potranno utilizzare il Software esclusivamente sul database di cui al precedente art. 1.2;

(iii) in ogni caso il Cliente non potrà concedere l'utilizzo del Software ad un numero di utenti complessivamente superiore a quello

eventualmente indicato nell'Ordine o in separati accordi intervenuti tra le parti; e

(iv) il Cliente garantisce, anche promettendo il fatto del terzo ai sensi e per gli effetti dell'art. 1381 c.c., il rispetto da parte delle Controllate di tutti i termini e condizioni del Contratto; il Cliente è considerato esclusivo responsabile dell'operato di tali soggetti e garantisce altre sì il rispetto di tutte le normative applicabili, ivi incluse quelle in materia fiscale e civile;

(v) il Cliente si obbliga a tenere indenne e manlevata la Licenziante e gli altri soggetti appartenenti alla Rete Commerciale TeamSystem da eventuali conseguenze negative, danni, oneri, passività o richieste di terzi connesse all'uso o al non uso del Software da parte delle Controllate.

1.6 Il Cliente prende atto 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 dei Servizi (ivi inclusi gli Aggiornamenti e Sviluppi) e degli eventuali Sistemi di AI. Il Cliente sarà tenuto a verificare l'idoneità dei propri sistemi hardware, software e di rete ai fini dell'utilizzo del Software e della fruizione dei Servizi (ivi inclusi gli Aggiornamenti e Sviluppi) e degli eventuali Sistemi di AI e rinuncia sin d'ora a qualsiasi pretesa nei confronti della Licenziante e degli altri soggetti appartenenti alla Rete Commerciale TeamSystem collegata al mancato o non corretto funzionamento del Software e/o degli eventuali Sistemi di AI o alla mancata o non corretta erogazione dei Servizi conseguenti alla inidoneità dei propri sistemi hardware, software e/o di rete.

1.7 I Software oggetto del Contratto nonché le istruzioni per la loro installazione e configurazione sono resi disponibili per il download all'interno dello specifico portale che sarà indicato al Cliente, accessibile da parte di quest'ultimo previa creazione di apposite credenziali.

1.8 Il Cliente prende atto e accetta che i Software (e gli Aggiornamenti e Sviluppi e i Sistemi di AI) sono caratterizzati da una elevata complessità tecnica e che, di conseguenza, l'installazione e configurazione degli stessi richiede un supporto tecnico qualificato. Laddove il Cliente provvedesse all'installazione e configurazione dei Software (e dei relativi Aggiornamenti e Sviluppi e/o degli eventuali Sistemi di AI) avvalendosi di tecnici diversi da quelli della Licenziante o di un system integrator ufficiale TeamSystem, il Cliente prende atto ed accetta che la Licenziante (e in ogni caso TeamSystem) non potrà in nessun caso essere ritenuta responsabile per qualsivoglia malfunzionamento, blocco, errore e/o problema di sicurezza informatica dei Software o degli Aggiornamenti e Sviluppi o dei Sistemi di AI che dovessero derivare da una attività di installazione o configurazione degli stessi compiuta non in conformità con le relative istruzioni. Pertanto, il Cliente rinuncia sin da ora a qualsivoglia pretesa nei confronti della Licenziante (e in ogni caso di TeamSystem) con riferimento a quanto precede, impegnandosi a tenere quest'ultima indenne e manlevata da qualsiasi relati vo danno, spesa, passività, costo e/o conseguenza negativa che dovesse derivarle.

1.9 Attraverso apposita funzionalità del Software, ove prevista, il Cliente potrà creare e assegnare utenze secondarie (le "**Utenze Secondarie**") allo scopo di consentire a persone fisiche o giuridiche clienti del Cliente (gli "**Utenti Secondari**") di usufruire di specifiche e limitate funzionalità del Software e/o di consultare i documenti trattati dal Cliente per conto dell'Utente Secondario nell'ambito dell'utilizzo del Software con livelli di privilegio di volta in volta determinati dal Cliente medesimo, il tutto secondo quanto stabilito da TeamSystem a propria discrezione. Il Cliente prende atto ed accetta che la predetta funzionalità di attivazione delle Utenze Secondarie potrebbe non essere disponibile per tutti i Software oggetto del Contratto. Nel caso di attivazione delle Utenze Secondarie, la Licenziante si impegna a fornire agli Utenti Secondari le funzionalità disponibili del Software e il Cliente si impegna, anche ai sensi dell'art. 1381 c.c., a far sì che ciascun Utente Secondario utilizzi il Software nel rispetto delle Condizioni Generali e dei diritti di proprietà intellettuale e/o industriale di TeamSystem o di terzi.

1.10 TeamSystem si riserva la facoltà di rendere disponibili, a propria esclusiva discrezione, ed eventualmente dietro pagamento di appositi Corrispettivi, specifiche API e/o collegamenti tecnici tra i Software e applicativi terzi (le "**Piattaforme di Terzi**"), al fine di permettere lo scambio di dati e informazioni tra i Software e le Piattaforme di Terzi. Il Cliente accetta espressamente che tutti i diritti di proprietà intellettuale sulle API e/o collegamenti tecnici sono e rimangono di esclusiva titolarità di TeamSystem e/o dei relativi terzi proprietari eventualmente indicati nell'Ordine, nelle Condizioni Integrative o nella documentazione tecnica di supporto. Il Cliente prende atto e accetta che l'utilizzo mediante i Software delle Piattaforme di Terzi potrà essere subordinato all'eventuale preventivo completamento del processo di onboarding/iscrizione sulle Piattaforme di Terzi e /o all'accettazione delle condizioni contrattuali di tali terze parti, nonché al rispetto da parte del Cliente delle previsioni del Contratto e degli accordi presi con i predetti soggetti terzi.

1.11 Ferme restando le limitazioni di responsabilità a favore della Licenziante e di TeamSystem di cui all'articolo 13 delle Condizioni Generali, la Licenziante e TeamSystem, negli inderogabili limiti di legge, non potranno in alcun modo essere ritenute responsabili per danni diretti o indiretti e/o perdite, di qualunque natura o entità, che il Cliente o terzi dovessero subire in conseguenza di malfunzionamenti e/o elaborazioni errate dei Software che siano conseguenza di (i) errori e/o malfunzionamenti nell'elaborazione e/o nella trasmissione di dati e informazioni imputabili a ciascuna delle Piattaforme di Terzi e/o (ii) di uno scorretto utilizzo dell'API e/o collegamenti tecnici da parte del Cliente. Il Cliente, inoltre, prende atto ed accetta che le Piattaforme di Terzi sono gestite da terze parti estranee e diverse dalla Licenziante e TeamSystem e che, pertanto, in qualsiasi momento e senza alcun preavviso, anche per ragioni indipendenti dalla volontà della Licenziante/TeamSystem, le API e/o collegamenti tecnici con una o più Piattaforme di Terzi potrebbero non essere più disponibili o fruibili. A tal proposito, il Cliente rinuncia sin d'ora ad avanzare qualsivoglia pretesa nei confronti della Licenziante e di TeamSystem in relazione all'impossibilità e/o difficoltà di utilizzare le API e/o collegamenti tecnici tra i Software e le Piattaforme di Terzi conseguenti all'indisponibilità o a malfunzionamenti di queste ultime. La Licenziante e TeamSystem, infatti, non assumono alcuna responsabilità per eventuali malfunzionamenti, vizi e/o difetti, totali o parziali, delle Piattaforme di Terzi.

1.12 Con riferimento alle API di cui al paragrafo 1.10, il Cliente dichiara di essere consapevole della natura strategica e confidenziale delle API e si obbliga a:

a) utilizzare le API nei limiti ed utilizzi previsti dal presente Contratto, restando qualsiasi utilizzo diverso e ulteriore espressamente vietato;

b) non consentire in alcun modo l'accesso alle API da parte di terzi non espressamente autorizzati per iscritto da TeamSystem;

c) mantenere tutte le informazioni relative alle API e alla documentazione strettamente riservate, custodendole con modalità tali da escludere il rischio di accesso da parte di terzi non espressamente autorizzati per iscritto da TeamSystem;

d) adottare, rivalutare e aggiornare tempestivamente misure di sicurezza idonee a garantire le tutele di cui ai punti (b) e (c) del presente paragrafo;

e) non copiare, utilizzare (direttamente e/o indirettamente), in qualsivoglia modo, riprodurre e/o sfruttare (anche a titolo gratuito) qualsiasi informazione relativa alle API e/o ai relativi dettagli e/o alle specifiche tecniche;

f) impiegare le API in modo diligente e conforme ai principi di correttezza e buona fede, astenendosi da qualunque utilizzo massivo, continuativo, automatizzato o comunque eccedente i volumi di traffico ragionevolmente necessari per l'ordinario funzionamento delle integrazioni autorizzate;

g) monitorare costantemente l'utilizzo delle API al fine di prevenire, individuare e cessare tempestivamente eventuali chiamate anomale o eccessive, impegnandosi a collaborare prontamente con TeamSystem per l'adozione delle misure correttive che si rendessero necessarie.

1.13 La Licenziante e/o TeamSystem si riserva il diritto, a sua esclusiva discrezione e in qualsiasi momento, di sospendere o disabilitare, in tutto o in parte, l'accesso del Cliente alle API qualora rilevi (direttamente o indirettamente) un utilizzo anomalo, eccessivo o potenzialmente lesivo per la stabilità, la sicurezza, la disponibilità o le performance dei propri sistemi e/o dei Software e/o dei dati ivi trattati. Ove tecnicamente e commercialmente ragionevole, TeamSystem o la Licenziante informerà il Cliente dell'intervenuta sospensione, indicando le relative cause e, quando possibile, le azioni correttive da intraprendere.

2 ATTIVAZIONE OBBLIGATORIA

2.1 L'utilizzo del Software è subordinato alla sua attivazione, da parte del Cliente, mediante codici comunicati dalla Licenziante.

3 CONVALIDA

3.1 Il Cliente prende atto che la Licenziante e, in ogni caso, TeamSystem potranno effettuare, nel corso della durata del Contratto e senza nessun preavviso, verifiche sulla valida attivazione della Licenza e dei Servizi. Tali verifiche potranno essere effettuate anche con l'ausilio di programmi informatici (es. con l'invio in automatico da questi ultimi alla Licenziante dei dati identificativi delle licenze e delle informazioni necessarie a validare le stesse presenti sui sistemi dell'utilizzatore).

3.2 Il Cliente espressamente autorizza la Licenziante e, in ogni caso, TeamSystem ad utilizzare, ai fini della convalida, le informazioni raccolte nell'ambito delle attività di verifica di cui al precedente art. 3.1.

3.3 Qualora il Software non sia stato validamente attivato, non sia originale, sia contraffatto o il Cliente non disponga di una regolare licenza, la Licenziante potrà, senza alcun preavviso, inibire l'uso del Software e interrompere l'erogazione dei Servizi.

4 AGGIORNAMENTI E SVILUPPI

4.1 Gli Aggiornamenti e Sviluppi e le relative licenze d'uso saranno forniti dalla Licenziante al Cliente nell'ambito dell'erogazione dei Servizi e solo con riferimento ai Software concessi in Licenza ai sensi del Contratto.

4.2 Agli Aggiornamenti e Sviluppi, si applicano, in quanto compatibili, tutte le previsioni contrattuali relative al Software.

4.3 Il Cliente prende atto e accetta che, laddove ritenuto opportuno a insindacabile giudizio di TeamSystem o, se diverso, del titolare dei diritti di proprietà intellettuale e/o industriale sul Software, gli Aggiornamenti e Sviluppi possono determinare la modifica o l'eliminazione di alcune funzionalità dei Software oppure consistere in sostituzioni o migrazioni (anche parziali) dei Software.

4-BIS SISTEMI DI INTELLIGENZA ARTIFICIALE

4-bis.1 Fermo restando quanto indicato al paragrafo 5.3, TeamSystem si riserva la facoltà di integrare e/o fornire i Sistemi di Intelligenza Artificiale nei Software, ai termini e alle condizioni di cui al Contratto, nei limiti e forme di utilizzo eventualmente indicati dalla Licenziante o TeamSystem e a fronte dei Corrispettivi previsti.

4-bis. 2 Fermo restando quanto indicato al paragrafo. 4-bis.1, la Licenziante e/o TeamSystem si riserva la facoltà, a propria esclusiva discrezione, di mettere a disposizione i Sistemi di AI a titolo gratuito per un periodo di tempo determinato, eventualmente sottoposto all'accettazione di termini e condizioni integrative indicate nell'Ordine e/o in sede di attivazione del periodo d'uso gratuito (il "**Periodo d'Uso Gratuito**"). Con l'attivazione da parte del Cliente del Periodo d'Uso Gratuito, il Cliente è consapevole e accetta sin d'ora che, salvo diversamente indicato dalla Licenziante e/o TeamSystem, in caso di mancata disdetta/disattivazione dei Sistemi di Intelligenza Artificiale entro il termine del Periodo d'Uso Gratuito o il diverso termine indicato dalla Licenziante e/o TeamSystem e con le modalità indicate da quest'ultima, troveranno applicazione le presenti Condizioni Generali e il Cliente sarà tenuto al pagamento dei corrispettivi connessi ai Sistemi di AI come previsti dal Contratto, ovvero come indicati dalla Licenziante e/o TeamSystem all'avvio del Periodo d'Uso Gratuito. La concessione del Periodo d'Uso Gratuito non comporta alcun obbligo per la Licenziante e/o TeamSystem di rendere permanentemente disponibile tale opzione. Il Periodo d'Uso Gratuito può essere concesso una sola volta per ciascun Cliente, salvo diversa indicazione scritta della Licenziante e/o TeamSystem.

4-bis. 3 Il Cliente prende atto e accetta che i Corrispettivi dovuti dal Cliente per l'utilizzo dei Sistemi di AI potranno essere calcolati anche sulla base di un sistema interno di conteggio che misura gli utilizzi dei Sistemi di AI, quali a titolo meramente esemplificativo, le interazioni con i Sistemi di AI e/o le operazioni e/o elaborazioni effettuate tramite Sistemi di AI e/o altra unità di elaborazione e/o automazione, così come individuati dalla Licenziante e/o da TeamSystem per ciascun Sistema di AI reso disponibile(i "**Consumi AI**"). Le informazioni sulla tipologia/natura dei Consumi AI, sul numero di Consumi AI effettuati, le tariffe applicate ai Consumi AI e i corrispettivi di volta in volta dovuti dal Cliente a seconda dei Consumi AI effettuati tramite l'utilizzo dei Sistemi di AI, verranno indicati nell'Ordine e/o nell'apposita sezione del Software e/o della Soluzione dell'Ecosistema TS.

4-bis. 4 Il Cliente prende atto e accetta che i Sistemi di Intelligenza Artificiale sono caratterizzati da tecnologie e da modelli tecnologici, normativi e di business in continua evoluzione; in conseguenza di ciò, sorge periodicamente la necessità di effettuare attività di aggiornamento, adattamento e adeguamento, tanto a livello tecnologico quanto organizzativo e di pricing. Pertanto, il Cliente è consapevole e accetta che TeamSystem si riserva il diritto, ai sensi e con le modalità di cui all'articolo 20 delle presenti Condizioni Generali, di modificare i Corrispettivi dovuti dal Cliente e/o la struttura degli stessi, il meccanismo di determinazione dei corrispettivi nonché le metriche e i criteri di imputazione e misurazione dell'utilizzo dei Sistemi di AI, se del caso anche in considerazione dell'introduzione di modifiche connesse agli adeguamenti apportati ai Sistemi di AI e/o ai Software e/o alle Soluzioni dell'Ecosistema TS e/o dei livelli di utilizzo e consumo del Cliente dei prodotti e servizi offerti.

4-bis. 5 Il Cliente prende atto e accetta che le tipologie di Output rese disponibili, così come le caratteristiche degli Output offerti di volta in volta, potranno essere incrementate, modificate o ridotte, a insindacabile giudizio di TeamSystem, anche in base alle proprie esigenze di mercato.

4-bis. 6 Il Cliente, ai fini della fruizione dei Sistemi di AI, autorizza espressamente TeamSystem a svolgere, anche attraverso altre società del gruppo TeamSystem, attività di analisi, interconnessione e aggregazione dei dati, anche di natura personale, immessi dal Cliente nei Software e/o nelle Soluzioni dell'Ecosistema TS. Il Cliente autorizza altresì TeamSystem, anche attraverso altre società del gruppo TeamSystem, a trattare le informazioni e i dati, anche di natura personale, relativi a terze parti quali, a titolo esemplificativo, fornitori, partner commerciali, clientela e dipendenti del Cliente, immessi da quest'ultimo nei Software e/o nelle Soluzioni dell'Ecosistema TS, in conformità a quanto previsto nel MDPA di cui all'Allegato B. Con riferimento al trattamento dei dati o informazioni di terzi attraverso i Software e/o le Soluzioni dell'Ecosistema TS, il Cliente prende atto e accetta che tutti gli adempimenti previsti dalla Legislazione in materia di Protezione dei Dati Personali, ivi incluso ove applicabile l'obbligo di informativa e l'individuazione di un'adeguata base giuridica, nonché gli ulteriori adempimenti informativi previsti dalla normativa in materia di intelligenza artificiale, sono a esclusivo carico del Cliente stesso, impegnandosi quest'ultimo a tenere TeamSystem e le società del gruppo TeamSystem indenni e manlevate da qualsiasi pretesa, danno, spesa, costo e/o onere connesso alla violazione di quanto qui previsto.

4-bis. 7 Fermi restando gli inderogabili limiti di legge e le limitazioni di responsabilità di cui al presente Contratto, da intendersi come applicabili anche ai Sistemi di AI, il Cliente prende atto e riconosce espressamente che:

(a) i Sistemi di AI sono altamente innovativi e i risultati prodotti dall'utilizzo dei Sistemi di AI stessi potrebbero essere erronei, in toto o in parte, o comunque

non completamente affidabili. Il Cliente riconosce e accetta che l'uso dei Sistemi di AI avviene a proprio rischio e sotto l'esclusiva responsabilità del Cliente medesimo, che rimane l'unico responsabile per l'uso dei Sistemi di AI e per qualsiasi decisione presa sulla base delle elaborazioni fornite.

(b) Il Cliente resterà esclusivo responsabile della correttezza, veridicità e completezza dei dati, contenuti, informazioni immessi nei Software e/o nelle Soluzioni dell'Ecosistema TS, esonerando sin da ora TeamSystem e/o le società del gruppo TeamSystem per l'eventuale non correttezza delle elaborazioni effettuate attraverso i Sistemi di AI conseguente a erroneità, falsità o incompletezza dei dati immessi dal Cliente nei Software e/o nelle Soluzioni dell'Ecosistema TS.

(c) TeamSystem e/o le società del gruppo TeamSystem non saranno responsabili per qualsiasi uso improprio o illecito dei Sistemi di AI da parte del Cliente, nonché dell'eventuale utilizzo degli stessi in violazione di diritti di terzi, ivi inclusi senza limitazione diritti di proprietà intellettuale e/o industriale.

(d) TeamSystem e le società del gruppo TeamSystem non forniscono servizi di consulenza di alcun genere e che, pertanto, il Cliente resta l'unico responsabile (i) dell'assunzione delle eventuali informazioni necessarie al fine di effettuare le proprie determinazioni, inclusa l'eventuale validazione o correzione e utilizzo degli Output, e (ii) del puntuale rispetto della normativa tempo per tempo applicabile alla propria attività imprenditoriale nonché di qualsivoglia misura adottata in relazione al, o a seguito del, l'utilizzo dei Sistemi di AI, non assumendo TeamSystem né le società del gruppo TeamSystem alcuna responsabilità con riferimento a quanto precede.

(e) TeamSystem e/o le società del gruppo TeamSystem si riservano il diritto di effettuare manutenzioni, aggiornamenti o modifiche ai Sistemi di AI.

4-bis. 8 L'utilizzo dei Sistemi di AI è soggetto a un uso legittimo, equo e ragionevole da parte del Cliente, come eventualmente indicato nell'Ordine e/o nell'apposita sezione del Software o nell'apposita sezione delle Soluzioni dell'Ecosistema TS o comunque in fase di attivazione dei Sistemi di AI e come tempo per tempo definito da TeamSystem anche in ragione di quanto previsto al paragrafo 4-bis.4. La Licenziante e/o TeamSystem si riserva il diritto di sospendere l'accesso e l'utilizzo del Software (ivi inclusi i Sistemi di AI) a ciascun Cliente e/o utente e/o e/o Utente Secondario, nel caso in cui rilevi picchi anomali di utilizzo che possano compromettere la sicurezza, la stabilità o la disponibilità dei Sistemi di AI, salva la facoltà di risolvere il Contratto ai sensi del successivo paragrafo 12.3.

4-bis. 9 La Licenziante, al fuori di quanto previsto nel MDPA, non assume alcuna responsabilità per le attività di trattamento di dati personali condotte dal Cliente in qualità di titolare del trattamento, mediante i Sistemi di AI.

5 USO DEL SOFTWARE E DEI SISTEMI DI AI

5.1 Il Cliente prende atto e riconosce che ogni diritto di proprietà industriale e/o intellettuale sul Software e sulla relativa documentazione, nonché sugli eventuali Sistemi di AI, ivi inclusi i diritti di sfruttamento economico, in tutto e in parte, ovunque nel mondo, è e rimane di esclusiva titolarità di TeamSystem e/o dei suoi danti causa (fatte salve eventuali diverse indicazioni contenute nella documentazione tecnica relativa al Software) e, con il Contratto, non viene in alcun modo ceduto al Cliente. Il Software è concesso in Licenza nei limiti, alle condizioni e per la durata prevista dal Contratto. Pertanto, il Cliente potrà utilizzare il Software e gli eventuali Sistemi di AI esclusivamente nei modi espressamente consentiti dal Contratto e dovrà attenersi a qualsiasi limitazione tecnica presente nel Software e/o nei Sistemi di AI che gli consenta di utilizzarli solo in determinati modi. A titolo esemplificativo e non esaustivo, il Cliente non potrà:

(i) aggirare le limitazioni tecniche e le misure tecnologiche presenti nel Software e/o nei Sistemi di AI;

(ii) decodificare, decompilare o disassemblare il Software e/o i Sistemi di AI, salvo che tali attività siano espressamente consentite da previsioni di legge e comunque nei limiti di tali previsioni;

(iii) riprodurre, modificare, adattare, personalizzare il Software e/o gli Aggiornamenti e Sviluppi e/o i Sistemi di AI o crearne lavori derivati;

(iv) eseguire copie del Software, salvo quanto previsto dall'art. 7 delle presenti Condizioni Generali o stabilito, in maniera inderogabile, dalla legge e/o eseguire copie dei Sistemi di AI, salvo quanto stabilito in maniera inderogabile dalla legge;

(v) pubblicare il Software e/o i Sistemi di AI, anche per consentirne la duplicazione da parte di terzi;

(vi) commercializzare, a qualsiasi titolo, il Software e/o gli Aggiornamenti e Sviluppi e/o i Sistemi di AI;

(vii) utilizzare il Software e/o i Sistemi di AI in contrasto con norme di legge.

5.2 Il Cliente prende atto che il Software può contenere e/o necessitare l'uso di software cosiddetti open source e si impegna ad osservare i termini e le condizioni ad essi specificamente applicabili. Ove necessario, tali condizioni verranno rese idoneamente conoscibili al Cliente da parte della Licenziante.

5.3 Il Cliente prende atto e accetta che: (i) determinate funzionalità di alcuni o tutti i Software oggetto degli Ordini, nonchè i Sistemi di AI, potrebbero essere disponibili, a esclusiva discrezione di TeamSystem, solamente mediante l'interfacciamento e l'interazione tra i Software e determinati applicativi cloud e/o piattaforme online facenti parte delle Soluzioni dell'Ecosistema TS o di terzi, il cui utilizzo è oggetto di specifici e separati accordi, previo completamento da parte del Cliente delle procedure di *onboarding* sulle Soluzioni dell'Ecosistema TS interessate e accettazione del relativo contratto; e (ii) TeamSystem si riserva il diritto, previa informativa al Cliente e a propria esclusiva discrezione, di migrare moduli e funzionalità di uno o più Software in ambiente *cloud*. Il Cliente, pertanto, prende atto e accetta che: (a) dati, documenti e/o informazioni trattati e/o processati dal Cliente attraverso l'utilizzo dei Software (i "**Dati**") potrebbero essere migrati, trasmessi, trattati su Soluzioni dell'Ecosistema TS e/o archiviati, in tutto o in parte, anche su server di titolarità di o comunque utilizzati da TeamSystem e/o da altra società appartenente al gruppo TeamSystem (i "**Server**") per le finalità di fruizione del Software; e (b) con riferimento ai moduli e alle funzionalità dei Software e i Sistemi di AI disponibili e/o migrate in ambiente *cloud*, troverà applicazione quanto segue.

5.4 Nelle ipotesi di cui al paragrafo 5.3 che precede, ferma restando la disciplina specificamente applicabile all'utilizzo di ciascuna Soluzione dell'Ecosistema TS interessata e il fatto che ai software cloud facenti parte delle Soluzioni dell'Ecosistema TS troveranno applicazione, ove compatibili, le previsioni delle Condizioni Generali riferite al Software, le parti si danno reciprocamente atto e accettano che troveranno applicazione anche le seguenti previsioni:

(a) è fatto espresso divieto al Cliente di utilizzare i Software e/o le Soluzioni dell'Ecosistema TS e/o i Sistemi di AI al fine di immettere, conservare, inviare, pubblicare, trasmettere e/o condividere Dati che (i) siano in contrasto o violino i diritti di proprietà intellettuale di titolarità della Licenziante, di TeamSystem e/o di terzi; (ii) abbiano contenuti discriminatori, diffamatori, calunniosi o minacciosi; (iii) contengano materiale pornografico, pedopornografico, osceno o comunque contrario alla pubblica morale; (iv) contengano virus, worm, trojan horse o, comunque, altri elementi informatici di contaminazione o distruzione; (v) costituiscano attività di spamming, phishing e/o simili; (vi) siano in ogni caso in contrasto con le disposizioni normative e/o regolamentari applicabili. In caso di violazione di quanto precede, la Licenziante si riserva il diritto di interdire al Cliente l'utilizzo del Software e/o dei Sistemi di AI e/o della Soluzione dell'Ecosistema TS interessata (anche solo parzialmente) e/o l'accesso ai Dati e di risolvere il Contratto ai sensi dell'articolo 1456 c.c.;

(b) salvo che ciò sia necessario per adempiere a disposizioni di legge e/o a richieste dell'autorità giudiziaria, la licenziante e/o TeamSystem e/o le società appartenenti al gruppo TeamSystem non sono tenute in alcun modo alla verifica dei Dati (ivi inclusi quelli immessi nei Sistemi di AI) e, pertanto, non potranno in alcun modo essere ritenute responsabili per danni e/o perdite, diretti o indiretti e di qualsiasi natura, derivanti da errori e/o omissioni di tali Dati o connessi alla loro natura e/o caratteristiche;

(c) la Licenziante e/o TeamSystem si riservano altresì di sospendere o interrompere l'accesso ai Dati: (i) qualora ricorrano ragioni di sicurezza e/o riservatezza; (ii) in caso di violazione degli obblighi di legge in materia di utilizzo dei servizi informatici e della rete internet; (iii) nel caso in cui si verifichino problematiche ai Server e/o ai Software e/o alle Soluzioni dell'Ecosistema TS che non siano rimediabili senza sospendere l'accesso ai Dati, in ogni caso previo avviso scritto al Cliente circa le ragioni della sospensione e le tempistiche di intervento previste;

(d) in caso di cessazione dell'efficacia del Contratto, per qualsiasi ragione intervenuta, il Cliente avrà la facoltà di estrarre copia dei propri dati, documenti e/o contenuti tramite le funzionalità del Software per un periodo di 60 (sessanta) giorni dalla data di cessazione del Contratto. In alternativa, la restituzione di tali dati, documenti e/o contenuti potrà essere richiesta dal Cliente attraverso modalità di consegna automatizzata da concordare, a fronte del pagamento di corrispettivi specificamente previsti. Fatti salvi diversi accordi fra le parti, laddove il Cliente non abbia provveduto a scaricare o richiedere la restituzione dei Dati nel termine che precede, la Licenziante e/o TeamSystem e/o la società appartenente al gruppo TeamSystem provvederà a cancellarli in maniera permanente nel rispetto degli obblighi di legge rilevanti.

5.5 La Licenziante si riserva la facoltà di rendere disponibili, a propria esclusiva discrezione, una o più app mobile ("**App**") allo scopo di consentire al Cliente di fruire di determinate funzionalità del Software attraverso dispositivi mobili di proprietà o comunque nella disponibilità del Cliente. Il Cliente è consapevole e accetta che non tutte le funzionalità del Software potrebbero essere fruibili attraverso App e che il catalogo di tali funzionalità potrebbe essere variato dalla Licenziante a propria esclusiva discrezione in qualsiasi momento. Il Cliente prende atto ed accetta che l'utilizzo delle App è integralmente disciplinato dai termini e condizioni di cui al Contratto, restando inteso che la relativa Licenza avrà natura non esclusiva, non cedibile e temporanea.

5.6 Tutti i diritti di proprietà intellettuale relativi alle App sono e rimangono di esclusiva titolarità di TeamSystem e/o dei relativi terzi titolari indicati nell'Ordine, nelle Condizioni Integrative e/o nella documentazione tecnica di supporto.

5.7 Salvo ove diversamente previsto nell'Ordine, le App saranno rese disponibili presso uno o più app store (quali, a titolo esemplificativo, Google Play Store, Apple App Store, Huawei Store) selezionati ad esclusiva discrezione della Licenziante. La Licenziante compirà ogni ragionevole sforzo per garantire la disponibilità delle App sugli app store selezionati. Il Cliente, tuttavia, prende atto ed accetta che i predetti app store sono gestiti da terze parti estranee e diverse dalla Licenziante e che, pertanto, in qualsiasi momento e senza alcun preavviso, anche per ragioni connesse alle politiche di pubblicazione delle app sugli store imposte da tali terze parti e/o comunque indipendenti dalla volontà della Licenziante, le App potrebbero non essere più disponibili per il download dallo store o per l'utilizzo da parte del Cliente. Il Cliente rinuncia pertanto sin d'ora ad avanzare qualsivoglia pretesa nei confronti della Licenziante in relazione all'impossibilità di utilizzare e/o di scaricare e/o di aggiornare le App. La Licenziante non assume alcuna responsabilità per eventuali malfunzionamenti, totali o parziali, dell'App derivanti dal mancato rispetto dei requisiti tecnici minimi da parte del dispositivo mobile del Cliente. Tali requisiti tecnici minimi saranno indicati e resi disponibili sugli app store di riferimento.

5.8 Il Cliente rimane direttamente ed esclusivamente responsabile per qualsiasi azione compiuta dagli utenti, dagli Utenti Secondari, dalle Controllate e dai rispettivi dipendenti e collaboratori con riferimento ai Software e alle Soluzioni dell'Ecosistema TS e ai Sistemi di AI ivi incluse senza limitazione l'eventuale attivazione, laddove previsto, di funzionalità anche nell'ambito dei Sistemi di Intelligenza Artificiale. Il Cliente è consapevole e accetta che tali azioni da parte dai predetti soggetti si intendono compiute per conto dal Cliente e da questi direttamente compiute e autorizzate.

6 CORRISPETTIVI, AGGIORNAMENTO DEI CORRISPETTIVI E PAGAMENTI

6.1 A fronte della concessione in Licenza del Software e dei relativi Aggiornamenti e Sviluppi per la durata di cui al successivo art. 12 e della fornitura dei Servizi, il Cliente è tenuto a corrispondere alla Licenziante, il corrispettivo annuale indicato nell'Ordine sottoscritto dal Cliente ovvero determinato in base a separati accordi intervenuti tra il Cliente e la Licenziante, e, a fronte della fornitura degli eventuali Sistemi di AI, i corrispettivi connessi ai Sistemi di AI come indicati nell'Ordine o nel listino prezzi dedicato (i "**Corrispettivi**").

6.2 Il Cliente prende atto e accetta espressamente che tutti i Corrispettivi sono soggetti ad aggiornamento annuale nella misura del 100% della variazione tendenziale in aumento dell'indice ISTAT dei prezzi al consumo NIC per tipologia di prodotto.

6.3 Il Cliente prende atto che i Software e le attività prestate dalla Licenziante ai sensi del Contratto sono soggetti, 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 funzionalità dei Software e la corretta e completa erogazione dei Servizi. In ragione di quanto precede, la Licenziante avrà il diritto di modificare i Corrispettivi anche in misura superiore all'indice ISTAT con le modalità previste dall'art. 20 che segue.

6.4 Fermo restando quanto previsto al precedente paragrafo 6.2, qualora, nel corso della durata del Contratto, dovessero verificarsi circostanze imprevedibili tali da rendere maggiormente onerosa l'esecuzione delle prestazioni da parte della Licenziante, la stessa avrà il diritto di richiedere al Cliente un equo compenso *una tantum* ovvero una modifica dei Corrispettivi, con le modalità previste dall'art. 20 che segue.

6.5 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.

6.6 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 Licenziante. Salvo diversa indicazione nell'Ordine, i Corrispettivi annui dovuti in relazione ai Servizi ed al rinnovo della Licenza saranno calcolati pro quota nel caso di fruizione del servizio solamente per frazioni dell'anno.

6.7 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 Licenziante 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 Licenziante avrà diritto di: (i) sospendere immediatamente ogni prestazione dovuta ai sensi del Contratto (e, pertanto, anche di inibire l'uso del Software e sospendere la prestazione dei Servizi); e/o (ii) di risolvere anticipatamente il Contratto mediante semplice comunicazione scritta ai sensi dell'art. 1456 c.c.; e/o (iii) di sospendere altresì ogni prestazione dovuta ai sensi di eventuali altri contratti in essere con il Cliente (ivi incluso il diritto di inibire l'uso dei software licenziati ai sensi di tali contratti e di sospendere la prestazione di qualsivoglia servizio ad essi relativo), fatto salvo in ogni caso il diritto della Licenziante di recedere in qualsiasi momento da tali eventuali altri contratti.

6.8 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 art. 6.

7 DIVIETO DI CESSIONE E COPIATURA

7.1 Fatto espressamene salvo quanto previsto all'art. 1.5 che precede, il Cliente si impegna a non cedere ad alcun titolo né a far utilizzare ad alcun titolo a terzi il Software, né a eseguire o farne eseguire copie senza l'autorizzazione scritta della Licenziante anche dopo la scadenza del rapporto contrattuale, riconoscendo che un comportamento difforme oltre che costituire un inadempimento al Contratto, concreterebbe una violazione dei diritti di TeamSystem (o dell'eventuale diverso soggetto titolare dei medesimi diritti così come indicato nella documentazione tecnica, nell'Ordine o nelle Condizioni Integrative) sul Software e relativa documentazione e, più in generale, delle norme sul diritto d'autore.

7.2 In caso di utilizzo del Software in maniera non conforme alla previsione di cui al precedente art. 7.1, la Licenziante avrà il diritto di risolvere il Contratto e il Cliente dovrà corrispondere alla Licenziante, a titolo di penale e fatto comunque salvo il diritto della Licenziante di ottenere il risarcimento del maggior danno, un importo pari al corrispettivo che il Cliente avrebbe dovuto pagare alla Licenziante per l'uso del Software effettuato, moltiplicato per tre. Il Cliente riconosce la congruità della penale alla luce dell'interesse che la Licenziante ha all'utilizzo del Software in conformità alla previsione di cui al precedente art. 7.1 e, pertanto, dichiara la predetta penale non riducibile ai sensi dell'art. 1384 c.c.

8 COPIA DI BACK-UP

8.1 Qualora il Cliente abbia acquisito il Software su disco o altro supporto, è autorizzato a eseguire una copia di backup del supporto stesso. Il Cliente potrà utilizzare tale copia esclusivamente per reinstallare il Software sul dispositivo con Licenza.

8.2 L'utilizzo della copia di backup è subordinato alla sua attivazione secondo le modalità descritte al precedente art. 2.1 ed alle operazioni di convalida descritte al precedente art. 3.1.

9 VALIDITÀ DELLA LICENZA

9.1 La prova della validità della licenza sarà rappresentata dall'avvenuta attivazione e convalida della Licenza e dei Servizi secondo le modalità previste dal Contratto.

10 ESCLUSIONE DELLA GARANZIA

10.1 Il Cliente prende atto e accetta che il Software, compresi gli Aggiornamenti e Sviluppi e la documentazione relativa, nonché i Sistemi di AI sono forniti "così come sono" e che Licenziante e gli altri soggetti appartenenti alla Rete Commerciale TeamSystem non rilasciano dichiarazioni e garanzie espresse o implicite sul fatto che il Software e/o i Sistemi di AI siano adatti a soddisfare le esigenze del Cliente, che gli stessi siano esenti da errori o che abbiano funzionalità non previste nelle specifiche tecniche e nella documentazione relativa.

11 SERVIZI

11.1 La Licenziante fornisce al Cliente i Servizi indicati nell'Allegato A e gli eventuali ulteriori servizi pattuiti tempo per tempo con il Cliente, che saranno in ogni caso soggetti alla disciplina contenuta nelle presenti Condizioni Generali.

11.2 I Servizi decorrono dalla data di sottoscrizione del relativo Ordine o comunque della richiesta formulata dal Cliente e accettata dalla Licenziante e avranno la durata prevista dal successivo art. 12.

11.3 Fermo restando quanto previsto al successivo art. 12.5 con riferimento al recupero dei dati memorizzati, il Cliente riconosce e accetta che in caso di cessazione dei Servizi per qualsivoglia motivo, l'uso del Software potrà essere inibito e la Licenziante non interverrà più per correggere eventuali disfunzioni sopravvenute né metterà più a disposizione del Cliente alcun tipo di Aggiornamento e Sviluppo o di nuova versione del Software, né servizi di assistenza e manutenzione, non assumendosi alcuna responsabilità per danni che dovessero derivare da tale cessazione.

11.4 Nel caso in cui il Cliente, successivamente al mancato rinnovo dei Servizi, intendesse usufruire nuovamente dei servizi di aggiornamento, assistenza o manutenzione, dovrà stipulare con la Licenziante un nuovo contratto a condizioni da concordarsi di volta in volta. Saranno in ogni caso a carico del Cliente gli oneri aggiuntivi derivanti dalla riattivazione dei servizi medesimi.

11.5 In caso di richiesta di assistenza tecnica ed ai fini di una migliore esecuzione dei Servizi, il Cliente dovrà fornire alla Licenziante tutte le informazioni necessarie per individuare la causa della segnalazione dal medesimo effettuata, consentire alla Licenziante di eseguire al meglio i Servizi e a TeamSystem di migliorare e ottimizzare i propri prodotti. A tali fini, il Cliente (i) prende atto e acconsente che le informazioni relative al Cliente stesso ovvero ai dati del proprio sistema (quali a titolo esemplificativo e non esaustivo, informazioni tecniche, dati di configurazione, stato e diagnostica del Software e dei sistemi del Cliente) possano essere trasmesse alla Licenziante e/o a TeamSystem, ove necessario anche mediante l'utilizzo da parte della Licenziante e/o TeamSystem di appositi strumenti informatici di raccolta e comunicazione, e che, in mancanza della trasmissione, la capacità della Licenziante di fornire adeguatamente le prestazioni di cui al presente paragrafo potrebbe essere limitata o compromessa, e (ii) si impegna a fornire alla Licenziante e/o a TeamSystem, ove richiesto, l'assistenza di personale interno o altro supporto eventualmente necessario e l'accesso remoto ai propri sistemi, anche attraverso l'installazione e/o la configurazione dei predetti strumenti informatici sui sistemi del Cliente.

11.6 I Servizi resi dalla Licenziante saranno basati sulle dichiarazioni del Cliente in relazione ai sistemi e/o programmi utilizzati ed il Cliente assume piena ed esclusiva responsabilità in ordine a tali dichiarazioni. Il Cliente sarà il solo responsabile di ogni problema di compatibilità tra il Software oggetto del Contratto ed altro software applicativo o programma non aggiornato o, comunque, non commercializzato dalla Licenziante.

11.7 Il Cliente:

(i) dichiara di essere consapevole che gli interventi di assistenza e manutenzione posson o avere un alto grado di rischio per il funzionamento dei Software o per l'integrità di dati e/o informazioni e/o contenuti dallo stesso immessi e/o trattati attraverso il Software;

(ii) rimarrà responsabile esclusivo, ad eccezione delle misure di sicurezza che la Licenziate si impegna ad adottare nel MDPA di cui al successivo articolo 18, di un'adeguata protezione del proprio sistema e di tutti i dati e le informazioni in esso contenuti, anche in caso di accesso remoto della Licenziante o dei tecnici dalla medesima incaricati (a titolo esemplificativo, il Cliente sarà esclusivo responsabile per la scelta e l'implementazione di procedure relative alla sicurezza, alla crittografia, all'uso e alla trasmissione dei dati – inclusi dati personali –, il back up e il recupero dei dati memorizzati);

(iii) si impegna, ora per allora, a effettuare, prima dell'esecuzione dell'intervento, una copia di back up completa dei dati e del le informazioni dallo stesso immessi o trattati attraverso il Software.

11.8 Il Cliente prende atto e accetta che la Licenziante potrà affidare in tutto o in parte l'erogazione dei Servizi a soggetti terzi individuati dalla Licenziante medesima.

12 DURATA, RECESSO E RISOLUZIONE

12.1 Il Contratto, e la licenza d'uso del Software qui contenuta, 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 Licenza del Software e dei relativi Aggiornamenti e Sviluppi e la fornitura dei Servizi e, laddove presenti, degli eventuali Sistemi di AI si rinnoveranno automaticamente per successivi periodi di un anno. Al contrario, in caso di disdetta, la Licenza del Software e dei relativi Aggiornamenti e Sviluppi e l'obbligo della Licenziante di fornire i Servizi e gli eventuali Sistemi di AI cesseranno definitivamente di essere efficaci.

12.2 La sola Licenziante 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 in caso di inadempimento di una delle obbligazioni assunte dal Cliente in uno qualsiasi degli eventuali ulteriori contratti conclusi tra il medesimo Cliente e la Licenziante (o una qualsiasi società del gruppo TeamSystem o un distributore ufficiale TeamSystem), obbligazioni il cui inadempimento costituisca causa di risoluzione di tali eventuali ulteriori contratti. È fatto comunque salvo il diritto della Licenziante di ottenere il risarcimento di tutti i danni subiti.

12.3 Ferme restando le ulteriori ipotesi di risoluzione previste dal Contratto (quali, a titolo esemplificativo, le clausole 6.7 (Mancato e ritardato pagamento), 7.2 (Divieto di cessione e copiatura), 16.1 (Divieto di storno)), la Licenziante 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: 1.2 (Limiti licenza del Software per un unico database o per sistema multi-utente), 1.3 (Divieto separazione componenti Software e installazione su dispositivi diversi), 1.4 (Divieto sub licenza, cessione e utilizzo da parte di terzi), 1.5 (Condizioni per la sub-licenza alle Controllate), 3.3. (Uso di Software contraffatto), 4-bis.7 e 4-bis.8 (Sistemi di AI), 5 (Limiti uso del Software), 8.1 (Limiti uso della copia di backup), 15 (Diritti di proprietà intellettuale), 17 (Riservatezza), 22 (Codice di Condotta Anti-Corruzione Codice Etico e Modello Organizzativo di TeamSystem), 22bis (Rispetto della legislazione in materia di restrizioni commerciali nei rapporti con l'estero).

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

12.4 Fermo restando l'obbligo per il Cliente di versare alla Licenziante i Corrispettivi di cui all'articolo 6, TeamSystem si riserva in ogni momento la facoltà di inibire al Cliente e/o a ciascuna Controllata l'uso del Software e dei relativi Aggiornamenti e Sviluppi e di interrompere la fornitura dei Servizi in favore del Cliente e/o di ciascuna Controllata in caso di (i) inadempimento del Cliente e/o di ciascuna Controllata ad una delle obbligazioni richiamate nel precedente paragrafo 12.3 e 6.6; (ii) inadempimento di una delle obbligazioni assunte dal Cliente in uno qualsiasi degli eventuali ulteriori contratti conclusi tra il medesimo Cliente e la Licenziante (o una qualsiasi società del gruppo TeamSystem o un distributore ufficiale TeamSystem), obbligazioni il cui inadempimento costituisca causa di risoluzione di tali eventuali ulteriori contratti. In tali ipotesi, la Licenziante comunicherà al Cliente l'intenzione di inibire l'utilizzo del Software e di interrompere la fornitura dei Servizi invitando, ove possibile, il Cliente a porre rimedio all'inadempimento entro un determinato termine. Il Cliente rimane in ogni caso obbligato a versare quanto dovuto anche in caso di inibizione all'uso del Software e dei relativi Aggiornamenti e Sviluppi e di interruzione nella fornitura dei Servizi.

12.5 Alla scadenza del Contratto o in caso di sua cessazione per qualsiasi ragione intervenuta, la Licenziante cesserà di fornire tutti i Servizi prestati in esecuzione del Contratto (compresa la fornitura di Aggiornamenti e Sviluppi) e la fornitura degli eventuali Sistemi di AI e l'uso dei Software e dei relativi Aggiornamenti e Sviluppi e dei Sistemi di AI sarà inibito al Cliente, fatta eccezione per la sola funzionalità di recupero dei dati memorizzati nei Software che resterà abilitata per un periodo di 90 giorni dalla data di cessazione del Contratto.

13 LIMITAZIONE DI RESPONSABILITÀ

13.1 Il Cliente prende atto che, salvi i casi di dolo o colpa grave, la Licenziante e, per quanto occorrer possa, gli altri soggetti appartenenti alla Rete Commerciale TeamSystem in nessun caso potranno essere ritenuti responsabili per qualsiasi danno dovesse derivare al Cliente stesso o a terzi in conseguenza dell'uso o del non uso del Software e/o dei Sistemi di AI, essendo il Cliente tenuto in ogni caso a verificare la correttezza delle elaborazioni eseguite mediante lo stesso.

13.2 In ogni caso, salvi i casi di dolo o colpa grave, la responsabilità della Licenziante non potrà mai eccedere l'ammontare di corrispettivi pagati dal Cliente ai sensi del Contratto nell'anno in cui si è verificato l'evento dal quale discende la responsabilità della Licenziante.

14 DANNO RISARCIBILE

14.1 Fatte salve le ipotesi di dolo o di colpa grave, la Licenziante e, per quanto occorrer possa, gli altri soggetti appartenenti alla Rete Commerciale TeamSystem non potranno essere ritenuti responsabili per eventuali danni da lucro cessante, mancato guadagno o danni indiretti, perdita o danneggiamento di dati, fermo fabbrica, perdita di opportunità commerciali o di benefici di altro genere, pagamento di penali, ritardi o altre responsabilità del Cliente verso terzi che dovessero derivare, in tutto o in parte dall'uso o dal mancato uso del Software e/o dei Sistemi di AI.

14.2 La Licenziante e, per quanto occorrer possa, gli altri soggetti appartenenti alla Rete Commerciale TeamSystem, fatti salvi gli inderogabili limiti di legge, non potranno in nessun caso essere ritenuti responsabili per qualsiasi danno (diretto o indiretto), costo, perdita e/o spesa che il Cliente e/o terzi dovessero subire in conseguenza di attacchi informatici, attività di hacking e, in generale, accessi abusivi e non autorizzati da parte di terzi ai sistemi informatici del Cliente e/o della Licenziante e/o di TeamSystem (ivi inclusi, ma non limitatamente a, i Server), dai quali possano derivare, senza pretesa di esaustività, le seguenti conseguenze: (i) mancata fruizione, totale o parziale del Software e/o dei Sistemi di AI, (ii) perdite di dati di titolarità o comunque nella disponibilità del Cliente (ivi inclusi i Dati), e (iii) danneggiamento dei sistemi hardware e/o software di titolarità o comunque in uso al Cliente.

15 DIRITTI DI PROPRIETÀ INTELLETTUALE

15.1 La titolarità di tutti i diritti di proprietà industriale e/o intellettuale, ivi inclusi i relativi diritti di sfruttamento economico, sul Software (ivi inclusi, ma non limitatamente a, i codici oggetto, i codici sorgente e le interfacce), nonché sui relativi lavori preparatori, sulla relativa documentazione, sugli Aggiornamenti e Sviluppi e sui lavori derivati, nonché sui Sistemi di AI e sulle API, sono e rimangono, in tutto e in parte e ovunque nel mondo, esclusivamente in capo a TeamSystem (o all'eventuale diverso soggetto titolare dei diritti sul Software e/o sui Sistemi AI così come eventualmente indicato nella documentazione tecnica, nell'Ordine o nelle Condizioni Integrative).

15.2 Restano altresì in capo a TeamSystem (o all'eventuale diverso soggetto titolare, come eventualmente indicato nella documentazione tecnica, nell'Ordine o nelle Condizioni Integrative) tutti i diritti sui marchi, loghi, nomi, e altri segni distintivi comunque associati al Software e/o ai Sistemi di AI, con la conseguenza che il Cliente non potrà in alcun modo utilizzarli senza la preventiva autorizzazione scritta di TeamSystem (o dell'eventuale diverso soggetto titolare dei diritti sul Software e/o sui Sistemi AI così come eventualmente indicato nella documentazione tecnica, nell'Ordine o nelle Condizioni Integrative).

16 DIVIETO DI STORNO

16.1 Durante la vigenza del Contratto e per un periodo di un anno successivo alla conclusione del rapporto contrattuale, il Cliente si impegna a non assumere, né a sollecitare l'assunzione, nonché a non instaurare rapporti di collaborazione, a qualsiasi titolo, anche di consulenza, con

qualsiasi dipendente o collaboratore della Licenziante.

16.2 In caso di violazione di quanto stabilito al comma che precede, la Licenziante avrà diritto di risolvere il Contratto mediante semplice comunicazione scritta. Il Cliente, inoltre, sarà tenuto a corrispondere alla Licenziante, a titolo di penale, una somma pari al 200% dell'ultima retribuzione annuale del dipendente/collaboratore, salvo il diritto al maggior danno eventualmente subito dalla Licenziante. Il Cliente riconosce la congruità della penale alla luce dell'interesse che la Licenziante ha al rispetto da parte del Cliente delle previsioni di cui all'art. 16.1 e, pertanto, dichiara la predetta penale non riducibile ai sensi dell'art. 1384 c.c.

17 Riservatezza

17.1 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.

18 Trattamento dei dati personali

18.1 Le Parti riconoscono e si danno reciprocamente atto che la sottoscrizione del presente Contratto e l'esecuzione dei Servizi comporteranno la raccolta e il trattamento di dati personali del Cliente (nonché di parti ad essi correlate, quali procuratori, legali rappresentanti, etc.) da parte di TeamSystem per le finalità necessarie all'esecuzione del predetto Contratto e in conformità alla Legislazione in materia di protezione dei Dati Personali e alle altre eventuali previsioni di legge applicabili. TeamSystem, in qualità di titolare del trattamento, si impegna a trattare tali dati secondo quanto riportato nell'informativa rilasciata da TeamSystem ai sensi dell'articolo 13 del GDPR e disponibile sul sito web aziendale.

18.2 Con riferimento al trattamento dei dati personali di soggetti terzi immessi o comunque trattati dal Cliente attraverso il Software ("**Dati Personali di Terzi**"), ai sensi del Regolamento generale europeo sulla protezione dei dati del 27 aprile 2016 n. 679 ("**GDPR**"), le parti si danno atto e accettano di conformarsi a quanto previsto nell' "Accordo Principale per il Trattamento di Dati Personali" ("**MDPA**") allegato al presente Contratto (Allegato B).

18.3 Il Cliente dovrà manlevare e tenere indenne la Licenziante da qualunque pregiudizio, onere, sanzione o pretesa che la Licenziante dovesse subire o ricevere in ragione della violazione da parte del Cliente degli obblighi stabiliti dal MDPA (ivi incluso per ciò che attiene ad eventuali pretese o richieste degli interessati o di terzi ed i relativi costi legali di difesa). La Licenziante, in ogni caso, non potrà essere ritenuta responsabile per l'eventuale carenza, lacunosità o non correttezza delle istruzioni impartite dal Cliente in merito al trattamento dei Dati Personali di Terzi o per la mancata adozione di misure di sicurezza tecnico-organizzative relative al proprio personale.

18.4 Fermo restando quanto previsto all'articolo 4-bis, il Cliente ha, in ogni caso, la facoltà di esercitare i propri diritti ai sensi della Legislazione in materia di Protezione dei Dati Personali, quali ad esempio, i diritti di rettifica e cancellazione dei propri dati personali ovvero di opporsi al trattamento degli stessi come previsto nell'informativa sul trattamento dei dati personali.

19 Legge applicabile e foro esclusivamente competente

19.1 Il Contratto è soggetto alla legge italiana.

19.2 Qualsiasi controversia inerente al, o derivante dal Contratto, fatta eccezione per i procedimenti d'ingiunzione di cui agli artt. 633 ss. c.p.c. e le relative fasi di opposizione, sarà devoluta alla cognizione di un collegio di tre arbitri, nominati in conformità al Regolamento della Camera Arbitrale di Milano, che deciderà secondo diritto.

20 Modifiche unilaterali del Contratto

20.1 Considerata l'elevata complessità tecnica e normativa del settore in cui TeamSystem opera e dei prodotti e servizi offerti da quest'ultima, considerato altresì che tale settore è caratterizzato da continue evoluzioni tecnologiche, normative e delle esigenze di mercato, e considerato infine che, in conseguenza di quanto sopra, sorge periodicamente la necessità che TeamSystem adegui la propria organizzazione e/o struttura tecnica e funzionale dei prodotti e servizi offerti alla propria clientela (anche nell'interesse di quest'ultima), il Cliente accetta che il Contratto potrà essere modificato da TeamSystem in qualsiasi momento, dandone semplice comunicazione scritta (anche via e-mail o con l'ausilio di programmi informatici) al Cliente. Le modifiche potranno consistere in: (i) modifiche connesse agli adeguamenti apportati alla struttura tecnica e/o funzionale dei prodotti e servizi offerti; (ii) modifiche connesse agli adeguamenti apportati alla struttura organizzativa di TeamSystem; (iii) modifiche relative ai corrispettivi dovuti dal Cliente, nonché alla struttura degli stessi, che tengano conto degli adeguamenti di cui ai punti (i) e (ii) che precedono.

20.2 In tal caso, il Cliente avrà il diritto di recedere dal Contratto con comunicazione scritta inviata a TeamSystem a mezzo raccomandata con ricevuta di ritorno nel termine di 15 giorni dal ricevimento della comunicazione scritta da parte di TeamSystem di cui al paragrafo che precede.

20.3 In mancanza di esercizio della facoltà di recesso da parte del Cliente, nei termini e nei modi sopra indicati, le modifiche al Contratto si intenderanno da quest'ultimo definitivamente conosciute e accettate e diverranno definitivamente efficaci e vincolanti.

21 Ritiro dal mercato e sostituzione di Software e Servizi

21.1 Il Cliente prende atto che i Software e gli ambienti nei quali essi operano sono soggetti, per loro natura, ad una costante evoluzione tecnologica che può determinare la loro obsolescenza e, in alcuni casi, l'opportunità di un ritiro dal mercato e, eventualmente, di una sostituzione con nuove soluzioni tecnologiche. Pertanto, TeamSystem potrebbe decidere, a suo insindacabile giudizio, nel corso della durata del presente Contratto, di ritirare dal mercato i Software e/o i relativi Servizi e/o i Sistemi di AI (eventualmente sostituendoli con nuove soluzioni tecnologiche). In tal caso:

(i) la Licenziante dovrà comunicare per iscritto (es. a mezzo email) al Cliente, con un preavviso di almeno sei mesi, che TeamSystem intende ritirare dal mercato uno o più Software e/o Servizi e/o Sistemi di AI (ciascuno di essi il "**Prodotto Obsoleto**");

(ii) la comunicazione di cui al punto (i) che precede (la "**Comunicazione di Ritiro**") dovrà contenere una descrizione dell'eventuale nuovo prodotto o servizio (il "**Nuovo Prodotto**") che sostituirà ciascun Prodotto Obsoleto, restando inteso che il Nuovo Prodotto potrà basarsi su tecnologie diverse rispetto a quelle su cui si basa il Prodotto Obsoleto;

(iii) laddove il Prodotto Obsoleto non fosse sostituito da alcun Nuovo Prodotto, il contratto cesserà di produrre effetti con riferimento al Prodotto Obsoleto nella data che sarà indicata nella stessa Comunicazione di Ritiro (comunque non precedente all'ultimo giorno del sesto mese successivo alla data della Comunicazione di Ritiro); a partire da tale data, il Prodotto Obsoleto cesserà, a seconda del caso, di funzionare o di essere erogato e il Cliente avrà diritto alla restituzione della quota di corrispettivo eventualmente già pagata per il periodo in cui non potrà godere del Prodotto Obsoleto;

(iv) laddove il Prodotto Obsoleto fosse sostituito con un Nuovo Prodotto, il Cliente avrà il diritto, esercitabile entro 15 giorni dalla data della Comunicazione di Ritiro, di recedere dal Contratto con riferimento al Prodotto Obsoleto con efficacia dall'ultimo giorno del sesto mese successivo alla data della Comunicazione di Ritiro (data dalla quale, il Prodotto Obsoleto cesserà, a seconda del caso, di funzionare o di essere erogato) restando inteso che, in caso contrario, il Contratto continuerà ad esplicare i propri effetti (fatta espressa eccezione per quanto specificatamente indicato nella Comunicazione di Ritiro) con riferimento al Nuovo Prodotto e ogni riferimento al Prodotto Obsoleto dovrà intendersi riferito al Nuovo Prodotto.

22 CODICE DI CONDOTTA ANTI-CORRUZIONE, CODICE ETICO E MODELLO ORGANIZZATIVO DI TEAM SYSTEM

22.1 Il Cliente dichiara (i) di essere a conoscenza delle disposizioni del D. Lgs. 231/2001 ss.mm.ii. in materia di responsabilità amministrativa degli enti, (ii) di non essere incorso in alcuna violazione che possa determinare una sua responsabilità ai sensi di quanto previsto dal D. Lgs. 231/2001 e (iii) di non essere a conoscenza di indagini in corso da parte dell'autorità competente a tal riguardo.

22.2 Il Cliente dichiara di essere a conoscenza del fatto che TeamSystem ha adottato:

(i) un Modello di Organizzazione, gestione e controllo ai sensi del D. Lgs. 231/2001 ("**Modello Organizzativo**"), nonché

(ii) un codice anticorruzione ("**Codice di Condotta Anti-Corruzione**"), e

(iii) un codice etico ("**Codice Etico**")

e che tali documenti sono disponibili sul sito www.teamsystem.com.

22.3 Il Cliente riconosce e accetta il Modello Organizzativo, il Codice Etico e il Codice di Condotta Anti-Corruzione quale parte integrante del Contratto.

22.4 Il Cliente, pertanto, si impegna ad operare in maniera conforme a quanto richiesto dalla vigente normativa e dalle regole di condotta del Modello Organizzativo, del Codice Etico e del Codice di Condotta Anti-Corruzione e a non porre in essere – ed a far sì che i propri dipendenti e/o collaboratori non pongano in essere - alcuna condotta che possa determinare una responsabilità ai sensi del D. Lgs. 231/2001, sia essa a favore proprio, di TeamSystem o di terzi. Al riguardo, con riferimento all'esecuzione delle attività oggetto del Contratto, il Cliente si impegna ulteriormente a:

(i) utilizzare nell'esecuzione del Contratto solo pratiche etiche e a non utilizzare, autorizzare, coinvolgere o tollerare alcuna pratica commerciale che non rispetti le dichiarazioni e gli impegni che precedono;

(ii) rispettare le leggi contro la corruzione vigenti, tra cui a titolo esemplificativo e non esaustivo le leggi in materia di corruzione e gli ulteriori reati contro la PA previsti dal Codice Penale italiano, le disposizioni in materia di corruzione tra privati, il Foreign Corrupt Practices Act e il UK Bribery Act, i trattati internazionali anticorruzione, quali la Convenzione dell'Organizzazione per la Cooperazione e lo Sviluppo Economico sulla lotta alla corruzione dei pubblici ufficiali stranieri nelle operazioni economiche internazionali e la Convenzione delle Nazioni Unite contro la corruzione;

(iii) astenersi, nel rispetto delle norme anticorruzione vigenti, dal pagare, offrire o promettere di pagare, o autorizzare il paga mento, diretto o indiretto, in favore di pubblici ufficiali, enti pubblici, partiti politici, persone fisiche o giuridiche, nonché in favore di soggetti terzi indicati da pubblici ufficiali o membri di enti pubblici e/o di partiti politici, e in generale di qualsivoglia terzo, che possano in qualsiasi modo influenzare un atto o decisione idonea a ottenere, mantenere o indirizzare affari;

(iv) astenersi dal dare o promettere denaro, provvigioni, emolumenti e altre utilità ad amministratori, sindaci, dipendenti o collaboratori di società appartenenti al gruppo facente capo a TeamSystem, ivi compresi regali, intrattenimenti, viaggi o qualsiasi altro tipo di beneficio, anche non patrimoniale, in violazione di quanto previsto dal Codice Etico e dal Codice di Condotta Anti -Corruzione del gruppo facente capo a TeamSystem.

22.5 Il Cliente si impegna a segnalare a TeamSystem eventuali casi di violazioni dei principi contenuti nel Modello Organizzativo, nel Codice Etico e nel Codice di Condotta Anti-Corruzione, secondo le modalità ivi indicate.

22.6 In caso di inosservanza, anche parziale, da parte del Cliente al presente art. 22 e/o nel caso in cui le dichiarazioni rese dal medesimo si rivelino errate, non vere o non corrette, TeamSystem e/o la Licenziante potrà risolvere di diritto ex art. 1456 c.c. il Contratto, salvo in ogni caso il diritto di agire per il risarcimento di ogni danno patito.

22 BIS RISPETTO DELLA LEGISLAZIONE IN MATERIA DI RESTRIZIONI COMMERCIALI NEI RAPPORTI CON L'ESTERO

22bis.1 Il Cliente dichiara, garantisce, e si impegna a, che l'esecuzione del Contratto non violi e non violerà, in nessun caso, direttamente e/o indirettamente, le misure restrittive e/o divieti nel commercio con l'estero e/o le misure restrittive e/o divieti nei confronti di determinate persone fisiche, persone giuridiche e/o enti (i "**Soggetti Sanzionati**") adottati dall'Unione Europea e/o implementati dall'Office of Foreign Assets Control ("**OFAC**") degli Stati Uniti d'America e/o dalle Autorità del Regno Unito (la "**Legislazione in materia di Restrizioni nei Rapporti con l'Estero**").

22bis.2 Il Cliente dichiara e garantisce di non essere un Soggetto Sanzionato, né di essere controllato, direttamente e/o indirettamente, da un Soggetto Sanzionato e/o, comunque, di non agire, direttamente o indirettamente, per e/o nell'interesse di un Soggetto Sanzionato.

22bis.3 Il Cliente si impegna a non intrattenere alcun rapporto, direttamente e/o indirettamente, con Soggetti Sanzionati.

22bis.4 Il Cliente dichiara e garantisce, e si impegna a, che il Software (ivi inclusi i Sistemi di AI) e i Servizi, così come i diritti nascenti dal presente Contratto, non sono, né saranno mai, destinati, direttamente e/o indirettamente, a nessun Soggetto Sanzionato e/o a nessun paese il cui governo e/o qualsiasi suo organo sono soggetti alle restrizioni imposte dalla Legislazione in materia di Restrizioni nei Rapporti con l'Estero ("**Paese Sanzionato**").

22bis.5 Il Cliente si impegna a non fare in modo che il Software (ivi inclusi i Sistemi di AI) e i Servizi, così come i diritti nascenti dal presente Contratto, siano e saranno, direttamente e/o indirettamente, messi a disposizione nella Federazione Russa e/o nella Repubblica Bielorussa o per l'utilizzo nella Federazione Russa e/o nella Repubblica Bielorussa e/o, più in generale, messi a disposizione o destinati all'utilizzo in nessuno dei Paesi Sanzionati.

22bis.6 Il Cliente dichiara e garantisce di aver approntato un sistema di compliance per assicurare che l'utilizzo del Software (ivi inclusi i Sistemi di AI) e dei Servizi, l'esecuzione del Contratto e, più in generale, la propria attività di impresa siano conformi alla Legislazione in materia di Restrizioni nei Rapporti con l'Estero.

22bis.7 Il Cliente dichiara e garantisce di essere, e si impegna a tenersi costantemente, aggiornato in merito al contenuto della Legislazione in materia di Restrizioni nei Rapporti con l'Estero e, in particolare, in merito all'elenco dei Soggetti Sanzionati e/o dei Paesi Sanzionati.

22bis.8 Il Cliente si obbliga, a semplice richiesta di TeamSystem, entro il termine indicato da TeamSystem, a consegnare a TeamSystem tutta la documentazione richiesta al fine di verificare il rispetto da parte del Cliente delle garanzie e degli obblighi di cui al presente articolo.

22bis.9 Il Cliente si obbliga ad informare, senza dilazione alcuna, TeamSystem nel caso in cui l'esecuzione del presente Contratto possa determinare una violazione della Legislazione in materia di Restrizioni nei Rapporti con l'Estero.

22bis.10 In caso di violazione delle dichiarazioni, garanzie, impegni ed obblighi di cui al presente articolo, TeamSystem avrà il diritto, a sua discrezione, di:

a) sospendere, senza preavviso, l'esecuzione del Contratto;

b) recedere, senza preavviso, dal presente Contratto; e/o

c) risolvere di diritto, ex art. 1456 c.c., il presente Contratto con effetto immediato a decorrere dalla dichiarazione scritta inviata da TeamSystem, fermo restando in ogni caso il diritto di TeamSystem al risarcimento del danno.

22bis.11 Resta inteso che in caso di sospensione e/o recesso ai sensi del paragrafo che precede, il Cliente dichiara, ora per allora, di rinunciare a qualsiasi pretesa nei confronti di TeamSystem.

22bis.12 Il Cliente si obbliga a tenere manlevato ed indenne TeamSystem e/o le società del gruppo TeamSystem in relazione a qualsiasi pregiudizio, ivi incluso il danno alla reputazione commerciale di TeamSystem, che TeamSystem e/o le società del gruppo TeamSystem dovessero subire in caso di violazione, nel corso dell'esecuzione del Contratto, della Legislazione in materia di Restrizioni nei Rapporti con l'Estero e/o, comunque, in caso di violazione da parte del Cliente delle garanzie e degli impegni previsti nel presente articolo.

23 DISPOSIZIONI FINALI

23.1 Il Cliente non ha diritto di trasferire o cedere i suoi diritti e/o le obbligazioni derivati dal Contratto senza il preventivo consenso scritto della Licenziante. Il Cliente prende, inoltre, atto del fatto che, laddove la Licenziante fosse un distributore ufficiale TeamSystem, il rapporto tra la Licenziante e TeamSystem avente ad oggetto il diritto della Licenziante di distribuire i Software potrebbe cessare nel corso della durata del presente Contratto e che, in tal caso:

(i) TeamSystem comunicherà al Cliente la cessazione del rapporto contrattuale intercorrente tra la medesima TeamSystem e la Licenziante;

(ii) a decorrere dalla data di ricezione della comunicazione di cui al punto (i) che precede, il Cliente dovrà pagare i Corrispettivi direttamente a TeamSystem secondo i termini e le modalità indicate nella medesima comunicazione;

(iii) ogni contratto intercorrente tra il Cliente e la Licenziante con riferimento ai Software sarà ceduto, ai sensi e per gli effetti dell'art. 1406 c.c., dalla Licenziante a TeamSystem;

(iv) il Cliente presta sin da ora, ai sensi e per gli effetti dell'art. 1407 c.c., il proprio consenso alla cessione di cui al punto (iii) che precede.

23.2 Nel caso in cui una qualsiasi delle clausole delle presenti Condizioni Generali sia o diventi invalida o inefficace, tale invalidità o inefficacia non vizia la validità o l'efficacia delle altre clausole delle Condizioni Generali, che pertanto rimarranno in vigore tra le parti. Le parti concordano di sostituire le clausole invalide o inefficaci con clausole valide e efficaci, che siano il più possibile aderenti alla volontà delle parti.

23.3 Il mancato esercizio da parte della Licenziante di qualsiasi diritto ad essa riconosciuto dalle presenti Condizioni Generali non costituisce una rinuncia a tale diritto, né deve essere interpretato come tale.

ALLEGATO A

SERVIZI DI AGGIORNAMENTO, ASSISTENZA TECNICA E MANUTENZIONE

SERVIZI COMPRESI

- rilascio di Aggiornamenti e Sviluppi resi necessari dalla modifica, integrazione o emissione leggi, decreti, regolamenti, direttive, ordini o decisioni, italiani, comunitari o stranieri che, a insindacabile giudizio della Licenziante, non abbiano un impatto significativo sull'operatività e/o sui costi della Licenziante;
- rilascio di Aggiornamenti e Sviluppi derivanti da nuove versioni (c.d. "*Release*") del Software;
- assistenza tecnica tramite IVR (o tramite ulteriori eventuali sistemi che saranno tempo per tempo sviluppati e implementati) entro il numero massimo di ticket eventualmente indicato nell'Ordine;
- teleassistenza con dispositivi Sw.

SERVIZI NON COMPRESI

- ore di viaggio per interventi di assistenza tecnica;
- ripristino delle normali condizioni operative a seguito dell'uso di accessori non forniti dalla Licenziante ovvero a seguito di negligenza, incuria, dolo o eventuali tentativi da parte del cliente di effettuare modifiche;
- ripristino delle normali condizioni operative a seguito di cambio dell'hardware;
- ripristino delle normali condizioni operative a seguito di alluvioni, incendi manomissione dolosa, atti di teppismo, danneggia menti in seguito a furti o tentativo di furto e altri eventi di forza maggiore;
- fornitura di supporti (dischi, toner, etc.);
- installazione del Software e/o di Aggiornamenti e Sviluppi;
- aggiornamenti, sviluppi o attività in genere resi necessari dalla modifica, integrazione o emissione leggi, decreti, regolamenti, direttive, ordini o decisioni, italiani, comunitari o stranieri che, a insindacabile giudizio della Licenziante, abbiano un impatto significativo sull'operatività e/o sui costi della Licenziante;
- rimozione VIRUS e assistenza helpdesk su gestione di package software non prodotti da TeamSystem se rientranti nelle sue competenze;
- personalizzazioni su programmi e stampe standard (da analizzare preventiva mente);
- interventi di assistenza o manutenzione che siano resi necessari a causa di (i) manomissioni o interventi di manutenzione e/o assistenza eseguiti da parte di personale non incaricato dalla Licenziante, (ii) incidenti provocati da eventi politici, atti vandalici o comunque dal fatto doloso di dipendenti del cliente o di terzi; (iii) negligenza, incuria, impiego non corretto o non conforme alle eventuali istruzioni d ella Licenziante o di TeamSystem; (iv) interruzioni o fluttuazioni dell'energia elettrica; (v) allagamenti, incendi, fenomeni atmosferic i, calamità naturali o altre cause accidentali;
- ogni altra attività non espressamente compresa nei Servizi.

ALLEGATO B

MDPA

ACCORDO PRINCIPALE PER IL TRATTAMENTO DI DATI PERSONALI – MASTER DATA PROCESSING AGREEMENT

(ex art. 28 del Regolamento UE 2016/679)

TRA

Il presente accordo per la protezione di dati personali è concluso tra il Fornitore, come di seguito definito, e il cliente che accetta il presente accordo. Per "**Fornitore**" si intende uno o più 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; e/o

(ii) la società appartenente al gruppo facente capo a TeamSystem e indicata nel Contratto;

E

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 principale per il trattamento dei dati personali – Master Data Processing Agreement*" (nel seguito "**MDPA**" o "**Accordo**") le condizioni e le modalità del trattamento dei dati personali eseguito dal Fornitore nell'ambito del Contratto e della prestazione dei Servizi 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**");

c) le caratteristiche specifiche del trattamento dei Dati Personali sono descritte, con riferimento a ciascun Servizio, nelle "*condizioni speciali di trattamento dei Dati Personali*" disponibili sul sito www.teamsystem.com/GDPR/DPA (di seguito "**DPA - Condizioni Speciali**") le quali costituiscono parte integrante ed essenziale del presente Accordo.

Tutto quanto sopra premessole 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:

"Data di Decorrenza dell'Accordo" indica la data in cui il Cliente sottoscrive o accetta il presente Accordo o, se anteriore, la data di decorrenza del Contratto a cui il presente Accordo è legato;
"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, o dall'Utente Finale in relazione alla fruizione dei Servizi, nella misura in cui siano oggetto di trattamento da parte del Fornitore, sulla base del Contratto. Un elenco delle categorie di Dati Personali è riportata nei DPA – Condizioni Speciali;
"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 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;
"Istruzioni" indica le istruzioni scritte impartite dal Titolare nel presente Accordo (inclusivo dei relativi DPA – Condizioni Speciali) e, eventualmente, nel Contratto;

"Legislazione in materia di Protezione dei Dati Personali" indica il GDPR, e ogni eventuale ulteriore norma e/o regolamento sul trattamento dei dati personali emanati ai sensi del GDPR o comunque vigenti in Italia, incluso il Decreto Legislativo no. 196/2003, come modificato e integrato 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) anche prima del 25 maggio 2018 e conservi efficacia vincolante;

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

"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;

"**Utente Finale**" si intende l'eventuale fruitore finale del Servizio, Titolare del Trattamento; e

"**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 TeamSystem S.p.A., in via Sandro Pertini, 88 a Pesaro, che può essere contattato al seguente indirizzo: dpo@teamsystem.com o al numero 0721/42661.

3. TRATTAMENTO DEI DATI PERSONALI

3.1. Con la stipulazione del presente Accordo (inclusivo di ciascun DPA - Condizioni Speciali applicabile), il Cliente affida al Fornitore l'incarico di trattare i Dati Personali ai fini della prestazione dei Servizi, così come meglio dettagliato nel Contratto e nei DPA – Condizioni Speciali; i DPA – Condizioni Speciali sono disponibili tramite link al seguente indirizzo www.teamsystem.com/GDPR/DPA.

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:

4.1.1. 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, ovvero da specifiche richieste del Cliente e/o dell'Utente Finale. 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;

4.1.2. 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 dal Codice Etico aziendale 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:

5.1.1. il Cliente acconsente espressamente che alcune operazioni di trattamento di Dati Personali siano affidate dal Fornitore ad altre società del gruppo TeamSystem e/o a soggetti terzi individuati nei DPA – Condizioni Speciali.

5.1.2. Il Cliente acconsente altresì all'affidamento di operazioni di Trattamento dei Dati Personali a ulteriori soggetti terzi secondo le modalità previste al successivo articolo 5.1.4.

5.1.3. Resta inteso che la sottoscrizione delle Clausole Contrattuali Tipo (prevista dal successivo punto 7 in caso di trasferimento all'estero dei Dati Personali) da parte del Cliente con un Responsabile Ulteriore del trattamento deve intendersi quale consenso all'affidamento al terzo delle operazioni di trattamento.

5.1.4. 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:

5.1.4.1. 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;

5.1.4.2. almeno 15 (quindici) giorni prima della data di avvio delle operazioni di trattamento dei Dati Personali da parte del Responsabile Ulteriore del Trattamento informa il Cliente dell'affidamento al terzo (nonché dei dati identificativi del terzo, della sua ubicazione – ed

eventualmente, dell'ubicazione dei server sui quali saranno conservati i dati, se applicabile - e delle attività affidate) mediante invio di Email di notifica o altro mezzo ritenuto idoneo dal Fornitore. Il Cliente potrà recedere dal Contratto entro 15 (quindici) giorni dal ricevimento della comunicazione, fermo restando l'obbligo di corrispondere al Fornitore gli importi dovuti alla data di cessazione del Contratto.

5.1.5. Eventuali informazioni aggiuntive sull'elenco dei Responsabili Ulteriori del Trattamento, dei trattamenti loro affidati e della loro ubicazione, sono contenuti nei DPA - Condizioni Speciali relativi ai Servizi attivati dal Cliente.

6. DISPOSIZIONI IN MATERIA DI SICUREZZA

6.1. *MISURE DI SICUREZZA DEL FORNITORE* – Nell'eseguire il trattamento dei Dati Personali ai fini della prestazione dei Servizi il Fornitore si impegna ad adottare misure tecnico-organizzative adeguate 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 di, o l'accesso ai, Dati Personali, come descritte nell'Allegato 1 al presente Accordo ("**Misure di Sicurezza**").

6.1.1. L'Allegato 1 all'Accordo contiene misure di protezione degli archivi dati commisurate al livello dei rischi presenti con riferimento ai Dati Personali per consentire la riservatezza, integrità, disponibilità e la resilienza dei sistemi e dei Servizi del Fornitore, nonché misure per consentire il tempestivo ripristino degli accessi ai Dati Personali in caso di Violazione della Sicurezza dei Dati Personali, e misure per testare l'efficacia nel tempo di dette misure. Il Cliente dà atto ed accetta che, tenuto conto dello stato dell'arte, dei costi di implementazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità di trattamento dei Dati Personali, le procedure e i criteri di sicurezza implementati dal Fornitore garantiscono un livello di protezione adeguato al rischio per quanto riguarda i suoi Dati Personali.

6.1.2. Il Fornitore potrà aggiornare e modificare nel tempo le Misure di Sicurezza sopra indicate, fermo restando che tali aggiornamenti e modifiche non potranno comportare una riduzione del livello di sicurezza complessivo dei Servizi. Di tali aggiornamenti e modifiche sarà fornita notifica al Cliente mediante invio di comunicazione all'Email di notifica.

6.1.3. Qualora il Cliente richieda di adottare misure di sicurezza aggiuntive rispetto alle Misure di Sicurezza, il Fornitore si riserva il diritto di valutarne la fattibilità e potrà applicare costi aggiuntivi a carico del Cliente per tale implementazione.

6.1.4. Il Cliente riconosce e accetta che il Fornitore, tenuto conto della natura dei Dati Personali e delle informazioni disponibili al Fornitore stesso secondo quanto specificamente riportato nei relativi DPA – Condizioni Particolari, presterà assistenza al Cliente nel garantire il rispetto degli obblighi di sicurezza di cui agli artt. 32-34 del GDPR nei modi seguenti:

6.1.4.1. implementando e mantenendo aggiornate le Misure di Sicurezza secondo quanto previsto ai precedenti punti 6.1.1, 6.1.2, 6.1.3;

6.1.4.2. conformandosi agli obblighi di cui al punto 6.3.

6.1.5. Resta inteso che, nei Contratti aventi ad oggetto prodotti installati presso il Cliente o presso fornitori del Cliente (installazioni *on premises)*, le Misure di Sicurezza sopra indicate troveranno applicazione esclusivamente in relazione ai Servizi che prevedono il Trattamento dei Dati Personali da parte del Fornitore o di suoi affidatari (es. supporto e assistenza da remoto, servizi di migrazione).

6.1.6. Qualora il prodotto consenta l'integrazione con applicativi di terze parti, il Fornitore non sarà responsabile dell'applicazione delle Misure di Sicurezza relative alle componenti delle terze parti o delle modalità di funzionamento del prodotto derivanti dall'integrazione effettuata dalle terze parti.

6.2. *MISURE DI SICUREZZA DEL CLIENTE* – Fermi restando gli obblighi di cui al precedente punto 6.1 in capo al Fornitore, il Cliente riconosce e accetta che, nella fruizione dei Servizi, rimane responsabilità esclusiva del Cliente l'adozione di adeguate misure di sicurezza in relazione alla fruizione dei Servizi da parte del proprio personale e di coloro che sono autorizzati ad accedere a detti Servizi.

6.2.1. A tal fine il Cliente si impegna ad utilizzare i Servizi e le funzionalità di trattamento dei Dati Personali in modo da garantire un livello di protezione adeguato al rischio effettivo.

6.2.2. Il Cliente si impegna altresì ad adottare tutte le misure idonee per proteggere le credenziali di autenticazione, i sistemi e i dispositivi utilizzati dal Cliente o dai fruitori presso l'Utente Finale per accedere ai Servizi, e per effettuare i salvataggi e backup dei Dati Personali al fine di garantire il ripristino dei Dati Personali nel rispetto delle norme di legge.

6.2.3. Resta escluso qualsiasi obbligo o responsabilità in capo al Fornitore circa la protezione dei Dati Personali che il Cliente o l'Utente Finale, se applicabile, conservino o trasferiscano fuori dai sistemi utilizzati dal Fornitore e dai suoi Responsabili Ulteriori del Trattamento (ad esempio, in archivi cartacei, o presso propri data center, come nel caso di Contratti aventi ad oggetto prodotti installati presso il Cliente o presso fornitori del Cliente).

6.3. *VIOLAZIONI DI SICUREZZA* – Fatta eccezione per il caso di Contratti aventi ad oggetto prodotti installati presso il Cliente o presso fornitori del Cliente per i quali non trova applicazione il presente punto 6.3, qualora il Fornitore venga a conoscenza di una Violazione di Sicurezza dei Dati Personali, lo stesso:

6.3.1. informerà senza ingiustificato ritardo il Cliente mediante comunicazione inoltrata all'Email di notifica;

6.3.2. adotterà misure ragionevoli per limitare i possibili danni e la sicurezza dei Dati Personali;

6.3.3. fornirà al Cliente, per quanto possibile, una descrizione della Violazione della Sicurezza dei Dati Personali ivi incluse le misure adottate per evitare o mitigare i potenziali rischi e le attività raccomandate dal Fornitore al Cliente per la gestione della Violazione di Sicurezza;

6.3.4. considererà informazioni confidenziali ai sensi di quanto previsto nel Contratto, le informazioni attinenti alle eventuali Violazioni della Sicurezza, i relativi documenti, comunicati e avvisi e non comunicherà a terzi dati informazioni, fuori dai casi strettamente necessari all'assolvimento degli obblighi del Cliente derivanti dalla Legislazione in materia di Protezione dei Dati Personali senza il previo consenso scritto del Titolare del Trattamento.

6.4. Nei casi di cui al precedente punto 6.3, è responsabilità esclusiva del Cliente adempiere, nei casi previsti dalla Legislazione in materia di Trattamento di Dati Personali, agli obblighi di notificazione della Violazione di Sicurezza ai terzi (all'Utente Finale qualora il Cliente sia un Responsabile del Trattamento) e, se il Cliente è Titolare del Trattamento, all'Autorità di controllo e agli interessati.

6.5. Resta inteso che la notificazione di una Violazione di Sicurezza o l'adozione di misure volte a gestire una Violazione di Sicurezza non costituisce riconoscimento di inadempimento o di responsabilità da parte del Fornitore in relazione a detta Violazione di Sicurezza.

6.6. Il Cliente dovrà comunicare tempestivamente al Fornitore eventuali utilizzi impropri degli account o delle credenziali di autenticazione oppure eventuali Violazioni di Sicurezza di cui abbia avuto conoscenza riguardanti i Servizi.

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

7.1. Il 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 potrà adottare altre modalità di trasferimento dei Dati Personali conformi a quanto previsto dalla Legislazione in materia di Protezione dei Dati Personali, anche alla luce delle indicazioni fornite dalla Corte di Giustizia della Unione Europea nella causa C-311/18 e dal Comitato Europeo per la Protezione dei dati ("**EDPB**") nelle "Raccomandazioni 01/2020 sulle misure che integrano gli strumenti di trasferimento per garantire il rispetto del livello di protezione dei dati personali nell'UE" e nelle "Raccomandazioni 2/2020 relative alle garanzie essenziali europee per le misure di sorveglianza".

7.3. Nei casi di cui al precedente punto 7.2 con il presente Accordo il Cliente conferisce espressamente mandato al Fornitore a sottoscrivere le clausole contrattuali tipo di cui all'articolo 46, comma 2, lettera c) del GDPR, per il trasferimento di dati personali a incaricati del trattamento stabiliti in paesi terzi (le "**Clausole Contrattuali Tipo**") con i Responsabili Ulteriori del Trattamento riportati nei relativi DPA – Condizioni Particolari, nonché ad adottare tutte le eventuali misure supplementari che si rendano ragionevolmente necessarie per consentire il trasferimento dei dati personali al di fuori dello SEE in conformità ai requisiti previsti dal GDPR .

7.4. 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. Parimenti, nel caso in cui il trasferimento dei Dati Personali al di fuori dello SEE sia subordinato alla attivazione da parte dell'Utente Finale di specifiche funzionalità del/i Servizio/i, l'attivazione di detta funzionalità 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 in specifici report ("**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 nei rispettivi DPA – Condizioni Speciali, 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 o nei relativi DPA – Condizioni Speciali.

8.8. Il presente punto 8 non è applicabile ai Contratti aventi ad oggetto prodotti installati presso il Cliente o presso fornitori del Cliente.

8.9. 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 Email 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 garantire che il punto di contatto per l'esercizio dei diritti da parte degli Interessati sia il Cliente stesso, o l'Utente Finale se Titolare del Trattamento. Sarà responsabilità del Cliente, o dell'Utente Finale qualora questi sia Titolare del Trattamento, 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, nel presente Accordo e nei DPA - Condizioni Particolari relativi ai Servizi interessati. 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, o dell'Utente Finale se Titolare del trattamento, procedere alla valutazione di impatto in base alle caratteristiche del trattamento dei Dati Personali dallo stesso posto in essere nel contesto dei Sevizi.

9.6. Il Fornitore si impegna a rendere Servizi improntati ai principi di minimizzazione del trattamento (*privacy by design & by default*), fermo restando che è responsabilità esclusiva del Cliente, o dell'Utente Finale, se Titolare del Trattamento, assicurare che il trattamento sia condotto poi concretamente nel rispetto di detti principi e verificare che le misure tecniche e organizzative di un Servizio soddisfano i requisiti di conformità della Società, ivi inclusi i requisiti previsti dalla Legislazione in materia di protezione dei dati personali.

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.

9.8. I precedenti punti 9.5 e 9.7 non sono applicabili in caso di Contratti aventi ad oggetto prodotti installati presso il Cliente o presso fornitori del Cliente.

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. L'eventuale trattamento di Dati Personali di cui agli artt. 9 e 10 del GDPR sarà consentito solo ove espressamente previsto nel DPA - Condizioni Particolari; fuori da tali casi, l'eventuale trattamento di tali Dati Personali sarà consentito solo previo accordo scritto tra le Parti ai sensi di quanto previsto al punto 3.2.

10.3. Il Cliente si impegna ad assolvere a tutti gli obblighi posti in capo al Titolare del Trattamento (e, nei casi in cui tali obblighi sono in capo all'Utente Finale, garantisce che analoghi obblighi sono imposti a carico dell'Utente Finale) 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.

10.4. 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. Resta altresì a carico del Cliente valutare se l'eventuale modulistica resa disponibile dal Fornitore per agevolare l'assolvimento degli obblighi di informativa e consenso (es. modello di privacy policy per App o informative presenti negli applicativi), quando disponibile, sia conforme alla Legislazione in materia di Protezione dei Dati Personali e adattare la stessa ove ritenuto opportuno.

10.5. E' 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.

10.6. E' onere del Cliente mantenere l'account collegato all'Email di notifica attivo ed aggiornato.

10.7. 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.

10.8. Il Cliente dichiara pertanto che le attività di trattamento dei Dati Personali, come descritte nei Contratti, nel presente Accordo e nei relativi DPA – Condizioni Particolari, sono lecite.

11. DURATA

11.1. 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 e, se previsto, nei relativi DPA – Condizioni Particolari.

12. DISPOSIZIONI PER LA RESTITUZIONE O LA CANCELLAZIONEDEI DATI PERSONALI

12.1. Alla cessazione del Servizio, per qualunque causa intervenuta, il Fornitore

12.1.1. 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 o consentita al fine di assolvere ad una disposizione di legge italiana o europea;

12.1.2. 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

12.1.3. manterrà a disposizione del Cliente i Dati Personali per l'estrazione per il periodo di previsto dal Contratto. Ove il Contratto non preveda un termine specifico, il Fornitore manterrà a disposizione del Cliente i Dati Personali per l'estrazione per il periodo di 60 (sessanta) giorni successivi alla cessazione del Contratto.

12.2. 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 12.1.3.

12.3. Resta inteso che quanto previsto ai punti 12.1e 12.2 non si applica ai Contratti aventi ad oggetto prodotti installati presso il Cliente o presso fornitori del Cliente. In tali casi, è responsabilità del Cliente estrarre, entro e non oltre il termine previsto dal Contratto, i Dati Personali che ritenga utile conservare; il Cliente riconosce che successivamente al predetto termine i Dati Personali potrebbero non essere più accessibili. Nei casi di cui al presente punto 12.3 resta altresì responsabilità del Cliente provvedere alla cancellazione dei Dati Personali nel rispetto delle norme di legge.

12.4. Restano ferme eventuali ulteriori o diverse disposizioni circa la cancellazione dei Dati Personali previste dal Contratto e nei rispettivi DPA – Condizioni Speciali.

13. RESPONSABILITA'

13.1. Ciascuna Parte è responsabile per l'adempimento dei propri obblighi previsti dal presente Accordo e dai relativi DPA –Condizioni Particolari e dalla Legislazione in materia di protezione dei Dati Personali.

13.2. Fatti salvi i limiti inderogabili di legge, il Fornitore sarà tenuto a risarcire il Cliente in caso di violazione del presente Accordo e/o dei relativi DPA – Condizioni Particolari entro i limiti massimi convenuti nel Contratto.

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 dal Fornitore dandone 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 al Fornitore a mezzo raccomandata con ricevuta di ricevimento nel termine di 15 giorni dal ricevimento della comunicazione del Fornitore. In mancanza di esercizio del diritto di recesso da parte del Cliente, nei termini e nei modi sopra indicati, le modifiche al presente Accordo si intenderanno da questi definitivamente conosciute e accettate e diverranno definitivamente efficaci e vincolanti.

14.3. In caso di conflitto tra le previsioni del presente Accordo e quanto previsto nel Contratto per la prestazione dei Servizi, o in documenti del Cliente non espressamente accettati dal Fornitore in deroga al presente Accordo e/ ai rispettivi DPA – Condizioni Speciali, prevarrà quanto previsto nel presente Accordo e nelle clausole dei relativi DPA – Condizioni Speciali.

****

Allegato1

Misure tecnico-organizzative

In aggiunta alle misure di sicurezza previste nel Contratto e nel MDPA il Responsabile del Trattamento applica le seguenti misure di sicurezza organizzative a seconda della tipologia di Servizio con cui viene erogato o licenziato il prodotto:

A – Cloud SaaS
B – Servizi Iaas
C – BPO (Business Process Outsourcing)
D – BPI (Business Process Insourcing)
E – On premises

A – CLOUD SaaS

Misure di sicurezza 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. *Valutazione d'impatto sulla protezione dei dati (DPIA)* – In conformità agli artt. 35 e 36 del GDPR e sulla base del documento WP248 – Linee guida sulla valutazione d'impatto nella protezione dei dati adottate dal Gruppo di lavoro ex art. 29, il Fornitore ha predisposto una propria metodologia per l'analisi e la valutazione dei trattamenti che, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, presentino un rischio elevato per i diritti e le libertà delle persone fisiche allo scopo di procedere con la valutazione dell'impatto sulla protezione dei dati personali prima di iniziare il trattamento. *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. *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. *Formazione*: Il Fornitore eroga periodicamente ai propri dipendenti coinvolti nelle attività di trattamento corsi di formazione sulla corretta gestione dei dati personali
Misure di sicurezza tecniche	*Firewall, IDPS* - I dati personali sono protetti contro il rischio d'intrusione di cui all'art. 615-quinquies del codice penale mediante sistemi di Intrusion Detection & Prevention, mantenuti aggiornati in relazione alle migliori tecnologie disponibili. *Sicurezza linee di comunicazione*- Per quanto di propria competenza, sono adottati dal Fornitore protocolli di comunicazione sicuri e in linea con quanto la tecnologia rende disponibile.

Protection from malware– I sistemi sono protetti contro il rischio di intrusione e dell'azione di programmi mediante l'attivazione di idonei strumenti elettronici aggiornati con cadenza periodica.
Sono in uso strumenti antivirus mantenuti costantemente aggiornati.

Credenziali di autenticazione – I sistemi sono configurati con modalità idonee a consentirne l'accesso unicamente a soggetti dotati di credenziali di autenticazione che ne consentono la loro univoca identificazione. Fra questi, codice associato a una parola chiave, riservata e conosciuta unicamente dallo stesso; dispositivo di autenticazione in possesso e uso esclusivo dell'utente, eventualmente associato a un codice identificativo o a una parola chiave.

Parola chiave – Relativamente alle caratteristiche di base ovvero obbligo di modifica al primo accesso, lunghezza minima, assenza di elementi riconducibili agevolmente al soggetto, regole di complessità, scadenza, history, valutazione contestuale della robustezza, visualizzazione e archiviazione, la parola chiave è gestita conformemente alle best practice. Ai soggetti ai quali sono attribuite le credenziali sono fornite puntuali istruzioni in relazione alle modalità da adottare per assicurarne la segretezza.

Logging – I sistemi sono configurabili con modalità che consentono il tracciamento degli accessi e, ove appropriato, delle attività svolte in capo alle diverse tipologie di utenze (Amministratore, Super Utente, etc.) protetti da adeguate misure di sicurezza che ne garantiscono l'integrità.

Backup & Restore – Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati.
Ove gli accordi contrattuali lo prevedono è posto in uso un piano di continuità operativa integrato, ove necessario, con il piano di disaster recovery; essi garantiscono la disponibilità e l'accesso ai sistemi anche nel caso di eventi negativi di portata rilevante che dovessero perdurare nel tempo.

Vulnerability Assessment & Penetration Test – Il Fornitore effettua periodicamente attività di analisi delle vulnerabilità finalizzate a rilevare lo stato di esposizione alle vulnerabilità note, sia in relazione agli ambiti infrastrutturali sia a quelli applicativi, considerando i sistemi in esercizio o in fase di sviluppo.
Ove ritenuto appropriato in relazione ai potenziali rischi identificati, tali verifiche sono integrate periodicamente con apposite tecniche di Penetration Test, mediante simulazioni di intrusione che utilizzano diversi scenari di attacco, con l'obiettivo di verificare il livello di sicurezza di applicazioni/sistemi/reti attraverso attività che mirano a sfruttare le vulnerabilità rilevate per eludere i meccanismi di sicurezza fisica/logica ed avere accesso agli stessi.
I risultati delle verifiche sono puntualmente e dettagliatamente esaminati per identificare e porre in essere i punti di miglioramento necessari a garantire l'elevato livello di sicurezza richiesto.

Amministratori di Sistema – Relativamente a tutti gli utenti che operano in qualità di Amministratori di Sistema, il cui elenco è mantenuto aggiornato e le cui funzioni attribuite sono opportunamente definite in appositi atti di nomina, è gestito un sistema di log management finalizzato al puntuale tracciamento delle attività svolte ed alla conservazione di tali dati con modalità inalterabili idonee a consentirne ex post il monitoraggio. L'operato degli Amministratori di Sistema è sottoposto ad attività di verifica in modo da controllarne la rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previsti dalle norme vigenti.

Data Center – L'accesso fisico al Data Center è limitato ai soli soggetti autorizzati.
Per il dettaglio delle misure di sicurezza adottate con riferimento ai servizi di data center erogati dai Responsabili Ulteriori del Trattamento, così come individuati nei DPA Condizioni Speciali, si fa rinvio alle misure di sicurezza indicate descritte dai medesimi Responsabili Ulteriori e rese disponibili nei relativi siti istituzionali ai seguenti indirizzi (o a quelli che saranno successivamente resi disponibili dai Responsabili Ulteriori):

Per i servizi di Data Center erogati da Amazon Web Services:

	https://aws.amazon.com/it/compliance/data-center/controls/ Per i servizi di Data Center erogati da Microsoft: https://www.microsoft.com/en-us/trustcenter

B – Servizi Iaas

Misure di sicurezza organizzative	*Data Center* – Il Fornitore fornisce, a seconda dei casi e delle specifiche pattuizioni contrattuali, i servizi IaaS tramite i seguenti Data Center: - Aruba S.p.A., sito in Italia; - Microsoft Azure localizzato nelle regions West Europe e Italy North; - e TIM in Italia. Con riferimento alle misure di sicurezza fisica si prega di fare riferimento alle informazioni rese disponibili dai singoli provider, come di seguito indicate: • con riguardo ad Aruba S.p.A.: misure di sicurezza Aruba ; • con riguardo a Microsoft Azure: Sicurezza fisica dei data center di Azure • con riguardo a TIM: misure di sicurezza TIM Nei Data Center, l'ambiente di virtualizzazione (inclusa la SAN – Storage Area network) è presente su server ospitati in data center siti all'interno dell'Unione Europea, la cui gestione è demandata a fornitori certificati ISO 27001. *Certificazioni* – il Fornitore ha ottenuto le seguenti certificazioni/attestazioni: • ISO/IEC 27001:2022: "Erogazione dei servizi di progettazione e gestione dell'infrastruttura ICT, di gestione delle applicazioni interne al Gruppo e di gestione dell'infrastruttura Cloud (IaaS)"; • ISO/IEC 27017:2015 "Sicurezza delle informazioni per i servizi Cloud" • ISO/IEC 27018:2019 "Protezione dei dati personali nei servizi Public Cloud" *Autorizzazione accessi logici* – Al momento della consegna delle Macchine Virtuali acquistate dal Cliente, il Fornitore consegna al Cliente le credenziali provvisorie di accesso alle stesse come Amministratore del sistema. In caso di mancata ricezione delle credenziali di accesso, è onere del Cliente attivarsi tempestivamente al fine di richiederle al Fornitore. Il Cliente ha l'obbligo di modificare le credenziali al primo accesso ed è l'unico responsabile dell'uso di tali credenziali, della gestione dei profili di accesso ed utenze e relative credenziali. Resta inteso che i profili di accesso alla macchina virtuale, aggiuntivi rispetto a quelli configurati al momento della consegna, devono essere definiti a cura del Cliente, sulla base delle proprie politiche di autorizzazione. Limitatamente a quanto di propria competenza, con riguardo all'infrastruttura di virtualizzazione, il Fornitore definisce i profili di accesso nel rispetto del *least privilege* necessari all'esecuzione delle mansioni assegnate. Tali profili sono oggetto di controlli periodici finalizzati alla verifica della sussistenza delle condizioni per la conservazione dei profili attribuiti. *Utenze* – Le VM sono configurate con modalità idonee a consentirne l'accesso unicamente a soggetti dotati di credenziali di autenticazione che ne consentono la loro univoca identificazione. *Sicurezza linee di comunicazione* – Per quanto di propria competenza, limitatamente all'infrastruttura di virtualizzazione, il Fornitore adotta protocolli di comunicazione sicuri e in linea con quanto la tecnologia rende disponibile in relazione al processo di autenticazione.

Risk management – Il Fornitore conduce periodicamente un processo di analisi e trattamento dei rischi in ambito sicurezza delle informazioni volto alla prevenzione o riduzione dei possibili effetti indesiderati che potrebbero essere causati da minacce non correttamente indirizzate.

Change Management – Per quanto di propria competenza, il Fornitore ha in essere una specifica procedura attraverso la quale regolamenta il processo di Change Management in considerazione dell'introduzione di eventuali innovazioni tecnologiche o cambiamenti della propria impostazione e della propria struttura organizzativa. Il Cliente è direttamente responsabile per procedure ed operazioni di Change Management aventi ad oggetto le Macchine Virtuali acquistate.

Formazione: Il Fornitore eroga periodicamente ai propri dipendenti coinvolti nelle attività di trattamento corsi di formazione in ambito Information Security, Privacy & Data Protection e Cyber Security.

Protection from malware – Le VM con sistema operativo Windows sono dotate di default di sistemi Antivirus/Antimalware nativi, la cui manutenzione e aggiornamento è onere e responsabilità del Cliente, coerentemente con il modello di servizio Iaas e con le condizioni generali di contratto. Resta, al riguardo, inteso che il Cliente è tenuto a valutare la congruità di tali soluzioni e la necessità di adottare, a propria cura e spese, sistemi di sicurezza e protezione ulteriori in base all'effettivo utilizzo della Macchina Virtuale ed alle proprie politiche di gestione dei rischi, nonché provvedere alla verifica periodica dell'effettivo aggiornamento dei predetti sistemi e – nel caso di fallimento di eventuali aggiornamenti automatici – di provvedere all'aggiornamento manuale dei sistemi di protezione qui descritti.

Backup & Restore – Sono adottate idonee misure per garantire il back up dei dati ed il ripristino degli stessi in caso di danneggiamento o perdita, in conformità con le previsioni del Contratto. In tali evenienze, è previsto che il *restore* sia eseguito attraverso il ripristino dell'ultima copia di back up disponibile anteriormente al danneggiamento. È comunque demandata al Titolare del trattamento la facoltà di eseguire autonomamente il backup dei propri dati per l'intera durata del contratto, fermo restando la possibilità di ricevere, tramite richiesta al servizio di assistenza clienti, copia dei dati entro il termine di 60 giorni successivi al termine del contratto stesso.

Logging – La piattaforma di virtualizzazione e la relativa consolle sono dotate di misure di tracciamento degli accessi e, ove appropriato, delle attività svolte in capo alle diverse tipologie di utenze (Amministratore, Super Utente, etc.) protetti da adeguate misure di sicurezza che ne garantiscono l'integrità. E' onere del Cliente adottare, se lo desidera, strumenti di logging delle attività svolte all'interno delle Macchine Virtuali diversi ed ulteriori a quelli forniti dal Sistema Operativo o singola applicazione installata nelle Macchine Virtuali.

Network & Security - L'infrastruttura cloud che ospita le VM è dotata di sistemi di protezione, quali Firewall, nonché da sistema di protezione del traffico AntiDDOS dedicati alla protezione dell'intera infrastruttura (Region/data center). Resta inteso che, coerentemente con il modello di servizio Iaas ed in conformità alle condizioni generali di Contratto, il Cliente ha l'onere di proteggere con adeguati sistemi di sicurezza e protezione, inclusi eventuali sistemi AntiDDOS, la propria Macchina Virtuale.

Business Continuity & Disaster Recovery –
Il Cliente è responsabile dell'implementazione e gestione dei piani di Business Continuity e Disaster Recovery, salvo diverse pattuizioni a livello contrattuale.
Ove gli accordi contrattuali lo prevedono, è posto in essere un piano di continuità operativa, integrato, ove necessario, con il piano di disaster recovery. Ciò garantisce la disponibilità e l'accesso ai sistemi anche nel caso di eventi negativi di portata rilevante che dovessero perdurare nel tempo.

	Incident Management– Per quanto di propria competenza, il Fornitore ha in essere una specifica procedura di Incident Management allo scopo di garantire il ripristino delle normali operazioni di servizio nel più breve tempo possibile in conformità a quanto previsto dal Contratto. E' onere del Cliente dotarsi di procedure di Incident Management per incidenti inerenti alla gestione delle Macchine Virtuali acquistate. *Attività di manutenzione sistemistica* – Nel caso il Cliente non abbia attivo un contratto di Manutenzione Sistemistica con il Fornitore, tutte le relative attività saranno di esclusivo onere e responsabilità del Cliente (tra cui, ad es. l'aggiornamento periodico delle patch di sicurezza, l'attivazione/creazione delle utenze user e amministrative della Macchina Virtuale, il monitoraggio degli indicatori di performance della Macchina Virtuale, etc.).

C – BUSINESS PROCESS OUTSOURCING (BPO)

Misure di sicurezza organizzative	*Certificazioni* – Il Fornitore ha ottenuto le seguenti certificazioni/attestazioni: • ISO/IEC 27001:2013: "Erogazione dei servizi di progettazione e gestione dell'infrastruttura ICT, di gestione delle applicazioni interne al Gruppo e di gestione dell'infrastruttura Cloud (IaaS)". • ISO/IEC 27018:2014 per la protezione dei dati personali nei servizi Public Cloud. *Policy e Disciplinari utenti* – Sono in essere dettagliate policy e disciplinari, ai quali tutta l'utenza con accesso ai sistemi informativi ha l'obbligo di conformarsi, 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* necessario 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* – Il Fornitore regolamenta la gestione degli interventi di assistenza allo scopo di garantire l'esecuzione delle sole attività disciplinate contrattualmente e impedire il trattamento eccessivo di dati personali la cui titolarità è in capo al Cliente o all'Utente Finale. *Change Management* – Il Fornitore ha in essere una specifica procedura attraverso la quale regolamenta il processo di Change Management in considerazione dell'introduzione di eventuali innovazioni tecnologiche o cambiamenti della propria impostazione e della propria struttura organizzativa. *Valutazione d'impatto sulla protezione dei dati (DPIA)* – In conformità agli artt. 35 e 36 del GDPR e sulla base del documento WP248 – Linee guida sulla valutazione d'impatto nella protezione dei dati adottate dal Gruppo di lavoro ex art. 29, il Fornitore ha predisposto una propria metodologia per l'analisi e la valutazione dei trattamenti che, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, presentino un rischio elevato per i diritti e le libertà delle persone fisiche allo scopo di procedere con la valutazione dell'impatto sulla protezione dei dati personali prima di iniziare il trattamento. *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. *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. *Formazione*: Il Fornitore eroga periodicamente ai propri dipendenti coinvolti nelle attività di trattamento, corsi di formazione sulla corretta gestione dei dati personali.
Misure di sicurezza tecniche	*Alta affidabilità* – Il Fornitore garantisce l'alta affidabilità nei seguenti termini: • L'architettura Server è completamente basata sull'utilizzo della soluzione di virtualizzazione VMWare applicata mediante duplicazione fisica e virtuale dei singoli sistemi, al fine di garantire la tolleranza ai guasti e l'eliminazione dei single point of failure. In particolare in caso di failure di un sistema, il software di gestione dell'ambiente virtuale è in grado di ridistribuire le attività in corso verso gli altri sistemi (high availabilty e load balancing), riducendo al minimo i disservizi e garantendo la persistenza delle connessioni esistenti. • Ciascun Server è attestato su una SAN mediante connessione iSCSI ad alta velocità. • Tutte le componenti dell'infrastruttura, tra i quali server, apparati di rete e sicurezza, sistemi Storage ed infrastruttura SAN, sono completamente ridondate per eliminare ogni single point of failure. • L'architettura di rete è progettata per proteggere i sistemi di front-end da Internet e dalle reti interne mediante l'utilizzo di una DMZ protetta da due livelli di firewalling distinti (defense-in-depth): un firewall di frontiera connesso ad Internet ed un secondo firewall, che integra anche funzionalità di Intrusion Prevention e antimalware, di proprietà dell'organizzazione, è messo a protezione della DMZ e dei sistemi di backend. *Hardening* – Sono in essere apposite attività di hardening finalizzate a prevenire il verificarsi di incidenti di sicurezza minimizzando le debolezze architetturali dei sistemi operativi, delle applicazioni e degli apparati di rete considerando - in particolare - le diminuzione dei rischi connessi alle vulnerabilità di sistema, la diminuzione dei rischi connessi al contesto applicativo presente sui sistemi e l'aumento dei livelli di protezione dei servizi erogati dai sistemi stessi. *Firewall, IDS/IPS* – I sistemi anti-intrusione, quali Firewall e IDS/IPS, sono posizionati all'interno del segmento di rete che collega l'infrastruttura cloud con Internet, al fine di intercettare ogni eventuale azione malevola volta a degradare, parzialmente o totalmente, l'erogazione del servizio. Nello specifico gli apparati adottati sono del tipo UTM SourceFire (Cisco), che includono sia la componente Firewall sia la componente IDS/IPS. *Sicurezza linee di comunicazione* - Per quanto di propria competenza, sono adottati dal Fornitore protocolli di comunicazione sicuri e in linea con quanto la tecnologia rende disponibile. *Protection from malware* – Le VM sono protette contro il rischio di intrusione e dell'azione di programmi mediante l'attivazione di idonei strumenti elettronici aggiornati con cadenza periodica. Tutte le VM sono gestite tramite funzionalità antivirus (sia a livello hypervisor che infrastrutturale). *Credenziali di autenticazione* – I sistemi sono configurati con modalità idonee a consentirne l'accesso unicamente a soggetti dotati di credenziali di autenticazione che ne consentono la loro univoca identificazione. Fra questi, codice associato a una parola chiave, riservata e conosciuta unicamente dallo stesso; dispositivo di autenticazione in possesso e uso esclusivo dell'utente, eventualmente associato a un codice identificativo o a una parola chiave.. *Parola chiave* – Relativamente alle caratteristiche di base ovvero, obbligo di modifica al primo accesso, lunghezza minima, assenza di elementi riconducibili agevolmente al soggetto, regole di complessità, scadenza, history, valutazione contestuale della robustezza, visualizzazione e archiviazione, la parola chiave è gestita conformemente

alle best practice. Ai soggetti ai quali sono attribuite le credenziali sono fornite puntuali istruzioni in relazione alle modalità da adottare per assicurarne la segretezza.

Logging – I sistemi sono configurabili con modalità che consentono il tracciamento degli accessi e, ove appropriato, delle attività svolte in capo alle diverse tipologie di utenze (Amministratore, Super Utente, etc.) protetti da adeguate misure di sicurezza che ne garantiscono l'integrità.

Backup & Restore – Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati.
È comunque demandata al Titolare la facoltà di eseguire autonomamente il backup dei propri dati per l'intera durata del contratto e per i 60 giorni successivi al termine dello stesso.
Ove gli accordi contrattuali lo prevedono è posto in uso un piano di continuità operativa integrato, ove necessario, con il piano di disaster recovery i quali garantiscono la disponibilità e l'accesso ai sistemi anche nel caso di eventi negativi di portata rilevante che dovessero perdurare nel tempo.

Vulnerability Assessment & Penetration Test – Il Fornitore effettua periodicamente attività di analisi delle vulnerabilità finalizzata a rilevare lo stato di esposizione alle vulnerabilità note, sia in relazione agli ambiti infrastrutturali sia a quelli applicativi, considerando i sistemi in esercizio o in fase di sviluppo.
Ove ritenuto appropriato in relazione ai potenziali rischi identificati, tali verifiche sono integrate periodicamente con apposite tecniche di Penetration Test, mediante simulazioni di intrusione che utilizzano diversi scenari di attacco, con l'obiettivo di verificare il livello di sicurezza di applicazioni / sistemi / reti attraverso attività che mirano a sfruttare le vulnerabilità rilevate per eludere i meccanismi di sicurezza fisica / logica ed avere accesso agli stessi.
I risultati delle verifiche sono puntualmente e dettagliatamente esaminati per identificare e porre in essere i punti di miglioramento necessari a garantire l'elevato livello di sicurezza richiesto.

Amministratori di Sistema – Relativamente a tutti gli utenti che operano in qualità di Amministratori di Sistema, il cui elenco è mantenuto aggiornato e le cui funzioni attribuite sono opportunamente definite in appositi atti di nomina, è gestito un sistema di log management finalizzato al puntuale tracciamento delle attività svolte ed alla conservazione di tali dati con modalità inalterabili idonee a consentirne ex post il monitoraggio. L'operato degli Amministratori di Sistema è sottoposto ad attività di verifica in modo da controllarne la rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previsti dalle norme vigenti.

Data Center – L'ambiente di virtualizzazione (inclusa la SAN – Storage Area network) è presente su server ospitati in un data center sito in Italia la cui gestione è demandata ad un fornitore certificato ISO 27001. In particolare le misure di sicurezza fisica poste a protezione del Data Center sono di seguito elencate:

- Perimetro di sicurezza esterno:
  - ✓ recinzione perimetrale che delimita il confine di proprietà composta da una protezione passiva anti scavalcamento con altezza minima di 3 m;
  - ✓ le aree esterne sono monitorate da barriere infrarossi e/o sistemi di videoanalisi e sistemi di videosorveglianza con videoregistrazione;
  - ✓ accesso pedonale selettivo/singolo;
  - ✓ accesso veicolare selettivo;
  - ✓ ronda armata.
- Perimetro di sicurezza interno:
  - ✓ presidio di vigilanza per controlli aree interne ed esterne, supervisione;
  - ✓ allarmi, gestione visitatori con consegna badge in osservanza a disposizioni aziendali e specifiche per i Data Center;
  - ✓ presidio di reception per la gestione degli accessi;
  - ✓ tornelli a braccio triplice prospicienti al locale del presidio vigilanza e reception.
- Perimetro di massima sicurezza interno:
  - ✓ varco di accesso sala sistemi dotato di protezione passiva interbloccato;
  - ✓ sistema di controllo accessi con gestione delle liste ABILITATI;

	✓ sensori magnetici stato porta in grado di rilevare lo stato della porta; ✓ uscite d'emergenza dotate di sensori stato porta. Tutti gli allarmi sono remotizzati al presidio di vigilanza.

D - BPI – BUSINESS PROCESS INSOURCING

Misure di sicurezza organizzative	*Policy e Disciplinari utenti* – Sono in essere dettagliate policy e disciplinari, ai quali tutta l'utenza con accesso ai sistemi informativi ha l'obbligo di conformarsi, 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 el rispetto del least privilege necessario 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. *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. *Formazione*: Il Fornitore eroga periodicamente ai propri dipendenti coinvolti nelle attività di trattamento corsi di formazione sulla corretta gestione dei dati personali.
Misure di sicurezza tecniche	*Sicurezza linee di comunicazione* - Per quanto di propria competenza, sono adottati dal Fornitore protocolli di comunicazione sicuri e in linea con quanto la tecnologia rende disponibile in relazione al processo di autenticazione. *Backup & Restore* – Ove previsto dagli accordi contrattuali, sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati.

E – ON PREMISES

Misure di sicurezza organizzative	*Policy e Disciplinari utenti* – Sono in essere dettagliate policy e disciplinari, ai quali tutta l'utenza con accesso ai sistemi informativi ha l'obbligo di conformarsi, finalizzate a garantire comportamenti idonei ad assicurare, in fase di assistenza tecnica, 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* necessario 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* – Il Fornitore regolamenta la gestione degli interventi di assistenza allo scopo di garantire l'esecuzione delle sole attività previste contrattualmente e impedire il trattamento eccessivo di dati personali la cui titolarità è rivestita dal Cliente. *Incident Management & 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.

	Formazione: Il Fornitore eroga periodicamente ai propri dipendenti coinvolti nelle attività di trattamento corsi di formazione sulla corretta gestione dei dati personali
Misure di sicurezza tecniche	*Sicurezza linee di comunicazione*- Per quanto di propria competenza, in fase di gestione di interventi di assistenza, sono adottati dal Fornitore protocolli di comunicazione sicuri e in linea con quanto la tecnologia rende disponibile. *Protection from malware*– Le postazioni di lavoro adottate in fase di Assistenza tecnica, sono protette contro il rischio di intrusione e dell'azione di programmi mediante l'attivazione di idonei strumenti elettronici aggiornati con cadenza periodica. Tutte le VM sono gestite tramite funzionalità antivirus (sia a livello hypervisor che infrastrutturale). *Amministratori di Sistema* – Relativamente a tutti gli utenti che operano in qualità di Amministratori di Sistema, il cui elenco è mantenuto aggiornato e le cui funzioni attribuite sono opportunamente definite in appositi atti di nomina, è gestito un sistema di log management finalizzato al puntuale tracciamento delle attività svolte ed alla conservazione di tali dati con modalità inalterabili idonee a consentirne ex post il monitoraggio. L'operato degli Amministratori di Sistema è sottoposto ad attività di verifica in modo da controllarne la rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previsti dalle norme vigenti.