CONDIZIONI GENERALI IAAS

DEFINIZIONI

Nelle presenti condizioni generali di contratto ("**Condizioni Generali**"), i termini e le espressioni di seguito elencati, quando riportati con iniziale maiuscola, devono intendersi con il significato ad essi attribuito nel presente paragrafo.

I termini indicati al singolare si intendono anche al plurale e viceversa.

Aggiornamento: indica qualunque aggiornamento, supplemento, adattamento, sviluppo, miglioria e/o modifica apportata ai Software da TeamSystem e/o da una delle società del Gruppo TeamSystem e/o dai terzi titolari e/o dal Distributore Ufficiale TeamSystem allo scopo di (i) correggere eventuali errori, vizi, *bug* o malfunzionamenti dei Software e/o (ii) dotare i Software di nuove o diverse funzionalità o rimuovere le funzionalità divenute obsolete e/o (iii) conformare i Software alle intervenute modifiche a livello fiscale, normativo e/o dell'ambiente tecnologico di riferimento.

Assistenza: indica la messa a disposizione di un servizio di *help desk* tecnico da remoto allo scopo di suggerire, ove possibile, soluzioni tecniche volte ad assicurare la corretta fruizione dei Software e/o delle Macchine Virtuali.

Cliente: significa la società indicata nell'Ordine.

Codice Etico: indica il codice etico adottato da TeamSystem e consultabile al sito https://www.teamsystem.com/compliance.

Codice di Condotta Anti-Corruzione: indica il codice di condotta anti-corruzione adottato da TeamSystem e consultabile al sito https://www.teamsystem.com/compliance.

Comunicazione di Ritiro: ha il significato di cui al paragrafo 10.1(b).

Condizioni Integrative: ha il significato di cui al paragrafo 1.1.

Connettività: significa la connessione all'Infrastruttura Cloud effettuata dal Cliente mediante collegamento a una rete di telecomunicazioni o a internet.

Contratto: significa le presenti Condizioni Generali, i relativi allegati (ivi incluso lo SLA), le Condizioni Integrative, l'Ordine, la documentazione tecnica eventualmente consegnata al Cliente, gli eventuali moduli di sottoscrizione e le eventuali istruzioni online per l'utilizzo delle Macchine Virtuali e dei Software.

Corrispettivi: ha il significato di cui al paragrafo 7.1.

Credenziali di Accesso: indica i sistemi di autenticazione attraverso i quali è possibile accedere e utilizzare le Macchine Virtuali e il Software per fruire delle Soluzioni Iaas, inclusi i codici di identificazione e le chiavi di accesso forniti da TeamSystem al Cliente ed associati a ciascun Utente e gli eventuali *token*.

Data Center: significa i centri servizi che ospitano i *server* interconnessi, di proprietà di TeamSystem o di terzi, sui quali risiede l'Infrastruttura Cloud.

Distributore Ufficiale TeamSystem: significa il soggetto che, in virtù di un valido contratto sottoscritto con TeamSystem, ha il diritto di commercializzare le Soluzioni Iaas e i Software.

GDPR: indica il Regolamento generale europeo sulla protezione dei dati del 27 aprile 2016 n. 679.

Gruppo TeamSystem: indica TeamSystem S.p.A. (con C.F. e P. IVA n. 01035310414) e tutte le società direttamente o indirettamente controllate da, o collegate a, TeamSystem ai sensi dell'art. 2359 c.c.

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

Licenza: ha il significato di cui al paragrafo 2.1.

Licenziante: indica, alternativamente, TeamSystem o la società appartenente al Gruppo TeamSystem indicata nell'Ordine o il Distributore Ufficiale TeamSystem indicato nell'Ordine.

Informazioni Confidenziali: ha il significato di cui al paragrafo 21.1.

Infrastruttura Cloud: indica il sistema *cloud* di titolarità di TeamSystem o di terzi che ospita i Software e le Macchine Virtuali.

Macchina Virtuale: indica ciascun ambiente virtuale indicato nell'Ordine e residente nell'Infrastruttura Cloud, accessibile da remoto dal Cliente, che emula il comportamento di un server attraverso l'utilizzo di risorse hardware dell'Infrastruttura Cloud.

MDPA: indica l'Accordo Principale per il Trattamento dei Dati Personali e il documento DPA – Condizioni Speciali applicabile, allegati al presente Contratto, presente all'Allegato C al presente Contratto.

Modello Organizzativo: indica il modello di organizzazione, gestione e controllo adottato da TeamSystem e consultabile al sito https://www.teamsystem.com/compliance.

Nuovo Prodotto: ha il significato di cui al paragrafo 10.1(b).

Ordine: significa il modulo o *coupon*, in formato elettronico o cartaceo, compilato e accettato (anche on-line) dal Cliente e contenente alcuni termini e le condizioni specificamente applicabili alle Soluzioni Iaas indicati nell'Ordine

medesimo. Resta inteso che, salvo diversamente concordato tra la Licenziante e il Cliente, in caso di discordanza tra i termini e le condizioni indicate nell'Ordine e le disposizioni delle Condizioni Generali e/o delle Condizioni Integrative, prevarranno le disposizioni dell'Ordine.

Paese Sanzionato: indica un qualsiasi 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 (come di seguito definita).

Parti: indica, congiuntamente, la Licenziante e il Cliente.

Prodotto Obsoleto: ha il significato di cui al paragrafo 10.1(a).

Proprietà Intellettuale: indica ogni diritto di proprietà intellettuale e/o industriale, registrato o non registrato, in tutto o in parte, ovunque nel mondo, quali - a titolo esemplificativo e non esaustivo - marchi, brevetti, modelli di utilità, disegni e modelli, nomi a dominio, know-how, opere coperte dal diritto d'autore, database e software (ivi inclusi, ma non limitatamente a, le sue derivazioni, il codice sorgente, il codice oggetto e le interfacce).

Servizi: indica, congiuntamente, i servizi aventi ad oggetto la fornitura al Cliente dell'Assistenza e degli Aggiornamenti.

Soluzione Iaas: indica, congiuntamente, i diritti concessi al Cliente con il Contratto per (i) l'accesso alle e l'utilizzo delle Macchine Virtuali ospitate sull'Infrastruttura Cloud; e per (ii) l'installazione e utilizzazione dei Software e/o di software di terze parti sulle Macchine Virtuali, ove compatibili con le caratteristiche tecniche di queste ultime.

Software: indica i prodotti software di titolarità di TeamSystem o di una società appartenente al Gruppo TeamSystem o di terzi indicati nell'Ordine e destinati ad essere installati sulle e utilizzati attraverso le Macchine Virtuali. Sono espressamente esclusi dalla definizione di "Software" tutti i software applicativi o programmi non indicati nell'Ordine o comunque non commercializzati da TeamSystem.

SLA: indica il *service level agreement* allegato alle presenti Condizioni Generali sub Allegato B.

TeamSystem: indica la società TeamSystem S.p.A. (C.F. e P. IVA n. 01035310414), con sede in via Sandro Pertini 88, 61122 – Pesaro (PU).

Utente: significa ciascun dipendente e/o collaboratore del Cliente, da quest'ultimo autorizzato ad utilizzare le Credenziali di Accesso per accedere alle Macchine Virtuali e utilizzare i Software.

1. Ambito di applicazione delle Condizioni Generali

1.1. Le presenti Condizioni Generali si applicano all'utilizzo, da parte del Cliente, delle Macchine Virtuali e dei Software oggetto delle Soluzioni Iaas identificati nell'Ordine. Le presenti Condizioni Generali si applicano, inoltre, a tutti gli aggiornamenti, supplementi, adattamenti, sviluppi, migliorie, personalizzazioni e modifiche in genere apportate ai Software e/o alle Macchine Virtuali, anche nell'ambito della fornitura dei Servizi, da parte della Licenziante, salvo essi non siano accompagnati da autonome condizioni contrattuali ("**Condizioni Integrative**").

1.2. 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 che sulle Condizioni Integrative. Le disposizioni del MDPA prevarranno su quanto diversamente concordato all'interno del Contratto.

1.3. TeamSystem 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 da TeamSystem 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.

1.4. Tutti i Diritti di Proprietà Intellettuale relativi alle App sono e rimangono di esclusiva titolarità della Licenziante e/o dei relativi terzi titolari indicati nell'Ordine, nelle Condizioni Integrative e/o nella documentazione tecnica di supporto.

1.5. Salvo 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 di TeamSystem. TeamSystem 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 da TeamSystem 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 di TeamSystem, 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.

2. Licenza d'uso delle Macchine Virtuali e del Software

2.1. Al solo scopo di consentire al Cliente di fruire delle Soluzioni Iaas esclusivamente mediante accesso autenticato all'Infrastruttura Cloud, la Licenziante concede al Cliente, che accetta, una licenza d'uso non

esclusiva, non cedibile, temporanea delle Macchine Virtuali e dei Software indicati nell'Ordine, limitatamente al numero massimo di Utenti, anch'essi specificati nell'Ordine ("**Licenza**").

3. Attivazione e convalida del Software

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

3.2. Il Cliente prende atto che la Licenziante (e, in ogni caso, TeamSystem) potrà 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 del Cliente).

3.3. 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 paragrafo.

3.4. 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 la prestazione dei Servizi.

4. Credenziali di Accesso

4.1. Il Cliente e/o ciascun Utente potranno accedere alle Macchine Virtuali e accedere ed utilizzare i Software mediante le Credenziali di Accesso che verranno fornite dalla Licenziante.

4.2. Il Cliente è consapevole del fatto che la conoscenza delle Credenziali di Accesso da parte di soggetti terzi consentirebbe a questi ultimi l'accesso non autorizzato all'Infrastruttura Cloud, alle Macchine Virtuali (e alle informazioni e ai dati ivi memorizzati) e l'utilizzo non autorizzato dei Software. Il Cliente sarà in ogni caso ritenuto esclusivo responsabile per ogni accesso e/o utilizzo, autorizzato o meno, dell'Infrastruttura Cloud, delle Macchine Virtuali e dei Software mediante le Credenziali di Accesso.

4.3. Il Cliente è tenuto a custodire e a far sì che ciascun Utente custodisca le Credenziali di Accesso con la massima riservatezza e con la massima diligenza, obbligandosi a non cederle né a consentirne l'uso a terzi non espressamente autorizzati.

4.4. La Licenziante e le società del Gruppo TeamSystem non potranno in alcun caso essere ritenute responsabili di qualsiasi danno, diretto e/o indiretto, che dovesse derivare al Cliente, a ciascun Utente e/o a terzi in conseguenza della mancata osservanza da parte del Cliente e/o di ciascun Utente delle previsioni di cui al presente articolo 4.

5. Aggiornamenti

5.1. Gli Aggiornamenti verranno forniti dalla Licenziante al Cliente nell'ambito della prestazione dei Servizi e solo con riferimento ai Software concessi in Licenza ai sensi del Contratto. Agli Aggiornamenti si applicano, in quanto compatibili, tutte le previsioni contrattuali che disciplinano l'uso del Software. Sono espressamente esclusi dagli Aggiornamenti forniti dalla Licenziante gli aggiornamenti relativi al sistema operativo della Macchina Virtuale e quelli relativi ai software applicativi o programmi non commercializzati dalla Licenziante, con riferimenti ai quali la Licenziante non assume alcun obbligo o responsabilità di sorta.

5.2. 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 sul Software, gli Aggiornamenti possono determinare la modifica o l'eliminazione di alcune funzionalità oppure consistere in sostituzioni o migrazioni (anche parziali) dei Software.

6. Servizi

6.1. 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.

6.2. In caso di richiesta di Assistenza 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 e dovrà fornire alla Licenziante, ove richiesto, l'assistenza di personale interno o altro supporto eventualmente necessario. Il Cliente acconsente ad inviare alla Licenziante e a TeamSystem le informazioni relative al Cliente stesso per consentire alla Licenziante di eseguire al meglio i Servizi e a TeamSystem di migliorare i propri prodotti.

6.3. 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.

6.4. Il Cliente è consapevole e accetta espressamente che i Servizi non includono servizi di aggiornamento del sistema operativo della Macchina Virtuale né servizi di aggiornamento di eventuali altri software applicativi o programmi non commercializzati dalla Licenziante. Dello svolgimento di tali attività e di qualsivoglia altra attività connessa all'utilizzo, gestione e manutenzione delle Macchine Virtuali, che non sia espressamente indicata fra quelle incluse nei Servizi a carico della Licenziante, il Cliente rimane l'esclusivo responsabile (in particolare, ad esempio, nel caso in cui il Cliente abbia disattivato le funzionalità di aggiornamento automatico del sistema operativo della Macchina Virtuale – e.g. di *windows* – e/o dei software applicativi o programmi di terze parti non commercializzati dalla Licenziante, abbia disinstallato il client antivirus, e/o

abbia disattivato il windows firewall della Macchina Virtuale), esonerando sin d'ora la Licenziante (e, in ogni caso, TeamSystem) da qualsivoglia responsabilità per eventuali danni (diretti o indiretti) o perdite, di qualunque natura o entità, subiti a seguito del mancato svolgimento delle predette attività.

6.5. Il Cliente:

(a) dichiara di essere consapevole che i Servizi possono avere un alto grado di rischio per il funzionamento dei Software e delle Macchine Virtuali o per l'integrità di dati e/o informazioni e/o contenuti immessi e/o trattati attraverso i Software e le Macchine Virtuali;

(b) rimarrà responsabile esclusivo di un'adeguata protezione dei sistemi utilizzati per accedere alle Macchine Virtuali e utilizzare i Software e di tutti i dati e le informazioni in essi contenuti e/o memorizzati, anche in caso di accesso remoto della Licenziante o dei tecnici dalla medesima incaricati;

(c) si impegna, ora per allora, a effettuare periodicamente e comunque prima dell'esecuzione di Servizi una copia di back up completa dei dati e delle informazioni di cui al paragrafo che precede.

7. Corrispettivi e pagamenti

7.1. A fronte della fornitura delle Soluzioni Iaas e dei Servizi, il Cliente si impegna a corrispondere alla Licenziante i corrispettivi indicati nell'Ordine ("**Corrispettivi**"), secondo le modalità e le tempistiche ivi previste. In mancanza di espressa previsione nell'Ordine, i Corrispettivi dovranno essere corrisposti entro trenta giorni dal ricevimento di regolare fattura emessa dalla Licenziante.

7.2. Tutti i Corrispettivi devono intendersi al netto di I.V.A. e degli eventuali altri oneri di legge.

7.3. 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.

7.4. Il Cliente prende atto che l'Infrastruttura Cloud, le Macchine Virtuali e i Software sono soggetti, per loro stessa natura, ad una costante evoluzione tecnologica e normativa che richiede continue e onerose attività di aggiornamento, sviluppo e, in alcuni casi, di sostituzione, necessarie al fine di garantire la loro funzionalità. In ragione di quanto precede, la Licenziante avrà il diritto di modificare i Corrispettivi anche in misura superiore all'indice ISTAT con le modalità di cui all'articolo 15.

7.5. Fermo restando quanto previsto al paragrafo che precede, qualora, durante l'esecuzione del Contratto, dovessero verificarsi circostanze imprevedibili tali da rendere maggiormente onerosa l'erogazione delle Soluzioni Iaas da parte della Licenziante, quest'ultima avrà diritto di percepire un equo compenso *una tantum* ovvero di modificare unilateralmente i Corrispettivi con le modalità di cui all'articolo 15.

7.6. 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 sulle somme dovute matureranno interessi di mora nella misura prevista dal d.lgs. 231/2002. In tal caso, fermo quanto previsto dai successivi paragrafi 18.1 e 18.2, la Licenziante avrà altresì diritto di (i) sospendere 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) e/o (ii) recedere in qualsiasi momento da tali eventuali altri contratti.

7.7. Il Cliente rinuncia a proporre eccezioni senza avere preventivamente adempiuto alle proprie obbligazioni di pagamento ai sensi del presente articolo 7.

8. Obblighi del Cliente

8.1. Con il Contratto, fermi restando gli obblighi previsti nelle presenti Condizioni Generali, il Cliente si impegna a:

(a) corrispondere alla Licenziante i Corrispettivi dovuti ai sensi dell'articolo 7;

(b) dotarsi autonomamente di materiale *hardware* e *software*, nonché di una Connettività adeguata al fine di poter accedere all'Infrastruttura Cloud e utilizzare le Macchine Virtuali e i Software;

(c) adottare autonomamente, con riferimento alle Macchine Virtuali e ai Software, tutte le misure di sicurezza e di protezione informatica adeguate all'utilizzo degli stessi;

(d) adeguare autonomamente le caratteristiche dei propri sistemi informatici e della Connettività alle modifiche, alle sostituzioni e ai correttivi eventualmente apportati all'Infrastruttura Cloud, ai Software e alle Macchine Virtuali successivamente alla conclusione del Contratto;

(e) usare i Software e/o le Macchine Virtuali in maniera conforme alla Licenza ed esclusivamente per gli scopi cui essi sono destinati

(f) non alterare le utenze tecniche presenti sulla Macchina Virtuale al momento della sottoscrizione del Contratto (quali, a titolo esemplificativo e non esaustivo, quelle denominate "ts-admin", "ts-zabbix", "vbck", "bck", "postgres" o "teamsy") necessarie per far funzionare correttamente il Software, gestire l'attività di backup della Macchina Virtuale e consentire l'erogazione dell'Assistenza e dei Servizi da parte della Licenziante;

(g) fornire alla Licenziante tutte le informazioni necessarie per consentire alla Licenziante un corretto e completo adempimento delle obbligazioni assunte ai sensi del presente Contratto, nonché a

comunicare immediatamente le eventuali relative variazioni, ivi inclusa qualsiasi variazione relativa agli Utenti;

(h) fare prendere visione a ciascun Utente delle presenti Condizioni Generali.

9. Proprietà Intellettuale

9.1. Tutti i diritti di Proprietà Intellettuale, ivi inclusi i relativi diritti di sfruttamento economico sull'Infrastruttura Cloud, sul Software, sulle Soluzioni Iaas, sulle Macchine Virtuali, sulla documentazione, sugli Aggiornamenti, sui lavori preparatori e sui relativi lavori derivati sono e rimangono, in tutto e in parte e ovunque nel mondo, di esclusiva titolarità di TeamSystem e/o dei relativi terzi proprietari (ivi incluse, eventualmente, le altre società del Gruppo TeamSystem) indicati nell'Ordine, nelle Condizioni Integrative o nella documentazione tecnica di supporto.

9.2. Restano altresì in capo a TeamSystem e/o ai terzi titolari tutti i diritti sui marchi, loghi, nomi, nomi a dominio e altri segni distintivi comunque associati all'Infrastruttura Cloud, alle Soluzioni Iaas, alle Macchine Virtuali, ai Software e agli Aggiornamenti, con la conseguenza che il Cliente non potrà in alcun modo utilizzarli senza la preventiva autorizzazione scritta di TeamSystem o del terzo titolare.

9.3. Il Cliente si impegna, anche ai sensi dell'art. 1381 c.c. per ciascun Utente, ad utilizzare l'Infrastruttura Cloud, i Software, le Macchine Virtuali, le Soluzioni Iaas e gli Aggiornamenti negli stretti limiti della Licenza e nel rispetto dei diritti di Proprietà Intellettuale di TeamSystem o di terzi. Pertanto, a titolo esemplificativo e non esaustivo e fatti in ogni caso salvi gli inderogabili limiti di legge, il Cliente non potrà:

(a) aggirare le limitazioni tecniche e le misure tecnologiche di protezione presenti nell'Infrastruttura Cloud, nelle Macchine Virtuali, nel Software e/o negli Aggiornamenti, ivi incluso il sistema di autenticazione;

(b) decodificare, decompilare o disassemblare le Macchine Virtuali, il Software e/o gli Aggiornamenti;

(c) riprodurre, modificare, adattare, personalizzare il Software e/o gli Aggiornamenti o crearne lavori derivati;

(d) eseguire o far eseguire copie delle Macchine Virtuali, del Software e/o degli Aggiornamenti;

(e) pubblicare o far pubblicare il Software e/o gli Aggiornamenti;

(f) commercializzare a qualsivoglia titolo le Macchine Virtuali, le Soluzioni Iaas, il Software e/o gli Aggiornamenti e Sviluppi;

(g) utilizzare l'Infrastruttura Cloud oltre i limiti dimensionali e operativi eventualmente specificati nell'Ordine.

10. Ritiro dal mercato e sostituzione

10.1. 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 (eventualmente sostituendoli con nuove soluzioni tecnologiche). In tal caso:

(a) la Licenziante comunicherà per iscritto (anche a mezzo email) al Cliente, con un preavviso di almeno sei mesi, che intende ritirare dal mercato uno o più Software (ciascuno di essi il "**Prodotto Obsoleto**");

(b) la comunicazione di cui al punto (a) che precede ("**Comunicazione di Ritiro**") conterrà una descrizione dell'eventuale nuovo Software (il "**Nuovo Prodotto**") che sostituirà ciascun Prodotto Obsoleto, restando inteso che il Nuovo Prodotto potrà basarsi su tecnologie diverse rispetto a quelle del Prodotto Obsoleto;

(c) 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 dalla Licenziante nella 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 di essere fornito e il Cliente avrà diritto alla restituzione della quota dei Corrispettivi eventualmente già pagata per il periodo in cui non potrà godere del Prodotto Obsoleto;

(d) 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 solo Prodotto Obsoleto con efficacia dall'ultimo giorno del sesto mese successivo alla data della Comunicazione di Ritiro (data dalla quale il Prodotto Obsoleto cesserà di essere fornito) 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.

11. Responsabilità della Licenziante

11.1. La Licenziante (e in ogni caso TeamSystem) non rilascia dichiarazioni e garanzie espresse o implicite sul fatto che le Soluzioni Iaas, le Macchine Virtuali, il Software e/o gli Aggiornamenti siano adatti a soddisfare le specifiche esigenze del Cliente, che siano esenti da errori o che abbiano funzionalità non previste nelle specifiche tecniche e nella documentazione relativa.

11.2. La Licenziante (e, in ogni caso, TeamSystem) non potrà essere ritenuta responsabile per danni, diretti o indiretti, di qualsiasi natura ed entità, che dovessero derivare al Cliente e/o a ciascun Utente e/o a terzi in conseguenza dell'uso delle Soluzioni Iaas, delle Macchine Virtuali, del Software e/o degli Aggiornamenti in maniera non conforme a quanto previsto dal Contratto e/o dalle leggi vigenti. Inoltre, la Licenziante (e, in ogni caso, TeamSystem) non potrà essere ritenuta responsabile per danni, diretti o indiretti, di qualsiasi natura ed entità, che dovessero derivare al Cliente e/o a ciascun Utente e/o a terzi in conseguenza del mancato o non corretto svolgimento da parte del Cliente delle attività di utilizzo, gestione e manutenzione delle Macchine Virtuali previste a suo carico dal presente Contratto.

11.3. La Licenziante (e, in ogni caso, TeamSystem) non sarà in alcun modo responsabile di eventuali malfunzionamenti e/o mancata fruizione delle Soluzioni Iaas, delle Macchine Virtuali, del Software e/o degli Aggiornamenti che derivino da una Connettività inadeguata rispetto alle relative caratteristiche tecniche.

11.4. In nessun caso la Licenziante (e, in ogni caso, TeamSystem) potrà essere ritenuta responsabile per eventuali danni o perdite, di qualunque natura o entità, derivanti dalle elaborazioni effettuate dal Cliente e/o da ciascun Utente e mediante le Soluzioni Iaas, le Macchine Virtuali, il Software e/o gli Aggiornamenti, essendo in ogni caso il Cliente e/o l'Utente tenuto a verificare la correttezza di tali elaborazioni.

11.5. Salvo che ciò sia necessario per adempiere a disposizioni di legge e/o a richieste dell'autorità giudiziaria, TeamSystem non è tenuta in alcun modo alla verifica dei dati e dei contenuti immessi dal Cliente e/o da ciascun Utente e nell'Infrastruttura Cloud attraverso le Soluzioni Iaas e, pertanto, non potrà in alcun modo essere ritenuta responsabile 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.

11.6. TeamSystem, fatti salvi gli inderogabili limiti di legge, non potrà in nessun caso essere ritenuta responsabile 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 all'Infrastruttura Cloud, alle Macchine Virtuali, ai Software e, in generale, ai sistemi informatici del Cliente e/o di TeamSystem, dai quali possano derivare, senza pretesa di esaustività, le seguenti conseguenze: (i) mancata fruizione delle Soluzioni Iaas; (ii) perdite di dati di titolarità o comunque nella disponibilità del Cliente; e (iii) danneggiamento dei sistemi hardware e/o software e/o alla Connettività del Cliente.

11.7. Salvo il caso di dolo o colpa grave, la responsabilità della Licenziante (e, in ogni caso, di TeamSystem) non potrà mai eccedere l'ammontare dei Corrispettivi annuali pagati dal Cliente ai sensi del presente Contratto nell'anno in cui si è verificato l'evento dal quale discende la responsabilità della Licenziante. La Licenziante (e, in ogni caso, TeamSystem) non potrà essere ritenuta responsabile 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.

12. Responsabilità e dichiarazioni del Cliente

12.1. 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 le Macchine Virtuali e i Software (nonché gli eventuali Aggiornamenti) esclusivamente ad uso interno e 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 tutela 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) prevalgono su qualsiasi eventuale contratto, pattuizione e/o accordo collegato al Contratto, ivi inclusi, a titolo esemplificativo e non esaustivo, eventuali accordi di finanziamento e/o leasing stipulati dal Cliente con terzi soggetti.

12.2. Il Cliente si impegna a far sì che le disposizioni del Contratto siano rispettate da ciascun Utente. Anche ai sensi dell'art. 1381 c.c., il Cliente è considerato esclusivo responsabile dell'operato di tali soggetti e garantisce altresì il rispetto di tutte le normative applicabili, ivi incluse quelle in materia fiscale e civile.

12.3. È fatto divieto di utilizzare le Soluzioni Iaas, l'Infrastruttura Cloud, i Software e/o gli Aggiornamenti al fine di depositare, conservare, inviare, pubblicare, trasmettere e/o condividere dati, applicazioni o documenti informatici che:

(a) siano in contrasto o violino i diritti di Proprietà Intellettuale di titolarità di TeamSystem, della Licenziante e/o di terzi;

(b) abbiano contenuti discriminatori, diffamatori, calunniosi o minacciosi;

(c) contengano materiali pornografico, pedopornografico, osceno o comunque contrario alla pubblica morale, all'ordine pubblico e/o al buon costume;

(d) contengano *virus*, *worm*, *trojan horse*, *malware* o, comunque, altri elementi informatici di contaminazione o distruzione;

(e) costituiscano attività di *spamming*, *phishing* e/o simili;

(f) consentano di effettuare attività di *mining* di criptovalute o attività similari, utilizzando le capacità di calcolo e infrastrutturali dell'Infrastruttura Cloud;

(g) siano in ogni caso in contrasto con le disposizioni normative e/o regolamentari applicabili.

12.4. La Licenziante si riserva il diritto di sospendere l'accesso all'Infrastruttura Cloud, alle Macchine Virtuali e ai Software, nonché la fornitura dei Servizi, qualora venga a conoscenza di una violazione di quanto previsto nel presente articolo e/o venga avanzata espressa richiesta in tal senso da un organo giurisdizionale o amministrativo in base alle norme vigenti. In tal caso, la Licenziante provvederà a comunicare al Cliente le motivazioni dell'adozione della sospensione all'accesso, salva la facoltà di risolvere il Contratto ai sensi del successivo articolo 18.

12.5. Il Cliente prende atto che l'Infrastruttura Cloud, le Macchine Virtuali, i Software e gli Aggiornamenti possono contenere e/o necessitare l'uso di software di terze parti (anche *open source*) e si impegna, anche ai sensi dell'art. 1381 c.c. per ciascun Utente, ad osservare i termini e le condizioni ad essi specificamente applicabili. Ove necessario, tali condizioni verranno rese idoneamente conoscibili al Cliente da parte di TeamSystem.

12.6. Il Cliente prende atto e accetta che la Licenza del Software è concessa per (i) un'unica istanza ed un unico database per ogni Software indicato nell'Ordine e (ii) un'unica Macchina Virtuale multi-utente, nel rispetto del limite massimo di utenti indicato nell'Ordine. Eventuali richieste di ulteriori istanze o database per il medesimo cliente (es.: test, produzione o sviluppo) richiederanno l'acquisto di ulteriori licenze.

12.7. Il Cliente prende atto e accetta che, fatto salvo quanto espressamente incluso nei Servizi svolti dalla Licenziante, egli sarà l'esclusivo responsabile dell'uso o del non uso in generale, della gestione e della manutenzione delle Macchine Virtuali oggetto della Licenza (ivi incluso dell'attività di navigazione sul web svolta attraverso le Macchine Virtuali) e sarà tenuto, tra l'altro, a: (i) verificare costantemente l'adeguatezza delle misure di sicurezza informatica inerenti alle Macchine Virtuali e ai Software rispetto al loro utilizzo; (ii) adottare ed implementare le eventuali misure di protezione informatica più idonee all'utilizzo delle Macchine Virtuali e dei Software (e.g. antivirus, procedure aziendali in materia di sicurezza informatica, formazione specifica degli Utenti, firewall a livello della Macchina Virtuale).

13. Manleva

13.1. Il Cliente si impegna a manlevare e tenere indenne la Licenziante (e, in ogni caso, TeamSystem) da qualsiasi danno, pretesa, responsabilità e/o onere, diretti o indiretti e comprese le ragionevoli spese legali, che la Licenziante (e, in ogni caso, TeamSystem) dovesse subire o sopportare in conseguenza dell'inadempimento, da parte del Cliente e/o di ciascun Utente, anche di uno solo degli obblighi previsti ai seguenti paragrafi: 3 (Attivazione e convalida del Software); 4 (Credenziali di Accesso); 6 (Servizi); 8 (Obblighi del Cliente); 9 (Proprietà Intellettuale); 10 (Ritiro dal mercato e sostituzione); 12 (Responsabilità e dichiarazioni del Cliente); 20 (Divieto di storno); 21 (Confidenzialità); 22 (Codice Etico, Codice di Condotta Anti-corruzione e Modello Organizzativo di TeamSystem); 22bis (Rispetto della legislazione in materia di restrizioni commerciali nei rapporti con l'estero) e 25 (Cessione del Contratto autorizzazione preventiva alla cessione).

14. Sospensione e interruzione

14.1. TeamSystem compirà ogni ragionevole sforzo per garantire la massima disponibilità della Soluzione di Iaas in conformità allo SLA. Il Cliente, tuttavia, prende atto ed accetta che la Licenziante potrà sospendere e/o interrompere l'accesso all'Infrastruttura Cloud, alle Macchine Virtuali e/o ai Software, previa comunicazione scritta al Cliente, qualora si dovessero rendere necessari interventi di manutenzione ordinaria o straordinaria all'Infrastruttura Cloud, alle Macchine Virtuali e/o ai Software. In tali casi, TeamSystem si impegna a ripristinare la disponibilità della Soluzione di Iaas nel minor tempo possibile.

14.2. Fatto salvo quanto previsto ai paragrafi 12.4 e 18.2, la Licenziante si riserva altresì la facoltà di sospendere o interrompere l'accesso alla Soluzione di Iaas:

(a) in caso di mancato o ritardato pagamento, totale o parziale, dei Corrispettivi;

(b) qualora ricorrano ragioni di sicurezza e/o riservatezza;

(c) in caso di violazione, da parte del Cliente e/o di ciascun Utente, agli obblighi di legge in materia di utilizzo dei servizi informatici e della rete internet;

(d) nel caso in cui si verifichino problematiche all'Infrastruttura Cloud e/o alle Macchine Virtuali e/o ai Software che non siano rimediabili senza sospendere il relativo accesso, ivi inclusa l'ipotesi di relativa sostituzione e/o migrazione anche parziale, in ogni caso previo avviso scritto al Cliente circa le ragioni della sospensione e le tempistiche di intervento previste.

15. Modifiche unilaterali

15.1. 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 dalla Licenziante 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, che tengano conto degli adeguamenti di cui ai punti (i) e (ii) che precedono.

15.2. In tal caso, il Cliente avrà la facoltà di recedere dal Contratto con comunicazione scritta inviata alla Licenziante a mezzo raccomandata A/R nel termine di 15 giorni dal ricevimento della comunicazione scritta da parte della Licenziante di cui al paragrafo che precede.

15.3. 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.

16. Durata

16.1. Fatto salvo quanto eventualmente e diversamente previsto nelle Condizioni Integrative o nell'Ordine, il Contratto rimarrà efficace tra le Parti fino al 31 dicembre dell'anno di sottoscrizione e si intenderà automaticamente rinnovato alla scadenza per successivi periodi di un anno ciascuno, salvo disdetta da inviarsi 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 della scadenza.

17. Recesso

17.1. La Licenziante potrà recedere dal Contratto nelle seguenti ipotesi:

(a) in qualsiasi momento, con un preavviso scritto al Cliente di 6 mesi;

(b) mediante semplice comunicazione scritta con effetto immediato, qualora il Cliente divenga insolvente, sia posto in liquidazione, sia assoggettato ad una qualsiasi procedura concorsuale;

(c) 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 un distributore ufficiale TeamSystem o una qualsiasi delle società del Gruppo 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.

18. Clausola risolutiva espressa

18.1. Fatto salvo il risarcimento del danno e ferme restando le altre ipotesi di risoluzione del Contratto previste nelle presenti Condizioni Generali, la Licenziante si riserva il diritto di risolvere il Contratto ai sensi dell'art. 1456 c.c. a seguito di invio di semplice comunicazione scritta a mezzo PEC ovvero lettera raccomandata A/R in caso di mancato adempimento da parte del Cliente anche di una sola delle previsioni: 2 (Licenza d'uso delle Macchine Virtuali e del Software); 4.3 (Credenziali di Accesso); 6.2-6.3-6.4 (Servizi); 7.1-7.5 (Corrispettivi e pagamenti); 8 (Obblighi del Cliente); 9 (Proprietà Intellettuale); 10 (Ritiro dal mercato e sostituzione); 12.1-12.2-12.3-12.6 (Responsabilità e dichiarazioni del Cliente); 13 (Manleva); (Divieto di storno); 21 (Confidenzialità); 22 (Codice Etico, Codice di Condotta Anti-corruzione e Modello Organizzativo di TeamSystem); 22bis (Rispetto della legislazione in materia di restrizioni commerciali nei rapporti con l'estero) e 25 (Cessione del Contratto e autorizzazione preventiva alla cessione).

18.2. Fermo restando l'obbligo per il Cliente di versare i Corrispettivi di cui all'articolo 7.1, la Licenziante si riserva altresì la facoltà di interrompere in ogni momento l'accesso del Cliente all'Infrastruttura Cloud, alle Macchine Virtuali e ai Software, nonché la prestazione dei Servizi in caso di (i) inadempimento del Cliente e/o di ciascun Utente ad una delle obbligazioni di cui al paragrafo 18.1; (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 procedere a quanto sopra invitando il Cliente, ove possibile, a porre rimedio all'inadempimento entro un determinato termine.

19. Effetti della cessazione

19.1. In caso di cessazione del Contratto, per qualsiasi causa intervenuta, TeamSystem cesserà immediatamente e definitivamente la fornitura delle Soluzioni Iaas e dei Servizi al Cliente.

19.2. Fermo restando quanto previsto al paragrafo 19.1, a seguito della cessazione del Contratto, per qualsiasi ragione intervenuta, il Cliente avrà la facoltà di effettuare il download dei propri dati, documenti e/o contenuti 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 ovvero su appositi supporti ottici, a fronte del pagamento di corrispettivi specificamente previsti.

19.3. Fatti salvi diversi accordi fra le Parti e gli inderogabili limiti di legge, laddove il Cliente non abbia scaricato o richiesto la restituzione dei dati, documenti e/o contenuti nel termine di cui al paragrafo 19.2, TeamSystem avrà la facoltà di cancellarli in maniera permanente.

19.4. Resta in ogni caso inteso che le seguenti previsioni sopravvivranno alla cessazione del Contratto, per qualsiasi causa intervenuta: 1 (Ambito di applicazione delle Condizioni Generali); 7 (Corrispettivi e pagamenti); 9 (Proprietà Intellettuale); 11 (Responsabilità della Licenziante); 12 (Responsabilità e

dichiarazioni del Cliente); 13 (Manleva); 20 (Divieto di storno); 21 (Confidenzialità); 22 (Codice Etico, Codice di Condotta Anti-corruzione e Modello Organizzativo di TeamSystem); 22bis (Rispetto della legislazione in materia di restrizioni commerciali nei rapporti con l'estero); 23 (Comunicazioni); 24 (Legge applicabile e foro esclusivo); 26 (Effetto novativo); 27 (Tolleranza) e 28 (invalidità e inefficacia parziale).

20. Divieto di storno

20.1. 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 e, in generale, di TeamSystem.

20.2. 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 al paragrafo 20.1 e, pertanto, dichiara la predetta penale non riducibile ai sensi dell'art. 1384 c.c.

21. Confidenzialità

21.1. Tutte le informazioni relative al presente Contratto, alle Soluzioni Iaas, all'Infrastruttura Cloud, alle Macchine Virtuali, ai Software e ai Servizi ("**Informazioni Confidenziali**") sono da considerarsi strettamente riservate e, pertanto, le Parti si impegnano reciprocamente, anche ai sensi dell'art. 1381 c.c. per ciascun Utente e per i propri dipendenti e collaboratori, a non divulgarle, a non utilizzare per finalità diverse da quelle di cui al Contratto e ad adottare ogni misura adeguata a mantenere la confidenzialità delle Informazioni Confidenziali.

21.2. Le disposizioni previste al paragrafo che precede non si applicano alle Informazioni Confidenziali che la Parte ricevente possa dimostrare documentalmente che:

(a) fossero già note o comunque legittimamente in possesso della Parte ricevente anteriormente e indipendentemente dalla comunicazione delle stesse da parte della Parte divulgante;

(b) divengano di pubblico dominio, salvo che ciò derivi da una violazione del Contratto;

(c) debbano essere divulgate ad un qualsiasi organismo statale o Autorità o Tribunale competenti per forza di legge, regolamento o ordine di un Tribunale, a condizione che la richiesta da parte di tale organismo statale o Autorità o Tribunale sia notificata senza indugio per iscritto alla Parte divulgante prima di dare esecuzione all'ordine ricevuto, affinché la Parte divulgante possa individuare e attuare le misure che riterrà più opportune per mantenere la riservatezza delle Informazioni Confidenziali chiedendone eventualmente la segretazione. Tale notifica deve includere, senza limitazione, l'identificazione delle informazioni da divulgare ed una copia dell'ordine. In ogni caso, la Parte ricevente dovrà divulgare solo le informazioni strettamente necessarie ad adempiere agli obblighi ad essa imposta e prenderà tutti i provvedimenti che si renderanno opportuni per limitare l'ulteriore divulgazione delle informazioni in questione da parte del suddetto organismo statale o Autorità o Tribunale, fermo restando che gli obblighi di segretezza in virtù del presente Contratto per tali informazioni non verranno meno.

22. Codice Etico, Codice di Condotta Anti-corruzione e Modello Organizzativo di TeamSystem

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:

(a) il Modello Organizzativo;

(b) il Codice di Condotta Anti-Corruzione; e

(c) il 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:

(a) 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;

(b) 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;

(c) astenersi, nel rispetto delle norme anticorruzione vigenti, dal pagare, offrire o promettere di pagare, o autorizzare il pagamento, 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;

(d) astenersi dal dare o promettere denaro, provvigioni, emolumenti e altre utilità ad amministratori, sindaci, dipendenti o collaboratori di società del Gruppo 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 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 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.

Art. 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 le Soluzioni Iaas 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 Sanzionato.

22bis.5. Il Cliente si impegna a non fare in modo che le Soluzioni Iaas 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 delle Soluzioni Iaas 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. Comunicazioni

23.1. Tutte le comunicazioni al Cliente inerenti al Contratto potranno essere effettuate all'indirizzo email comunicato dal Cliente medesimo nell'Ordine. Resta inteso che sarà cura e responsabilità del Cliente comunicare ogni variazione in relazione all'indirizzo email identificato dal Cliente per tutte le comunicazioni.

24. Legge applicabile e foro esclusivo

24.1. Il presente Contratto è regolato e deve essere interpretato in conformità alla legge italiana.

24.2. Sarà devoluta alla cognizione di un collegio di tre arbitri, nominati in conformità al regolamento della camera arbitrale di Milano, che deciderà secondo diritto, qualsiasi controversia inerente al, o derivante dal Contratto, fatta eccezione per (*i*) i procedimenti d'ingiunzione di cui agli artt. 633 ss. c.p.c. e le relative fasi di opposizione e (*ii*) i procedimenti, cautelari o di merito, relativi alla violazione dei diritti di Proprietà Intellettuale di titolarità di TeamSystem e/o di altre società appartenenti al Gruppo TeamSystem, per i quali sarà esclusivamente competente il Foro di Milano.

25. Cessione del Contratto e autorizzazione preventiva alla cessione

25.1. Salva preventiva autorizzazione scritta di TeamSystem, è fatto divieto al Cliente di cedere, in tutto o in parte, il Contratto.

25.2. Nel caso in cui la Licenziante sia un Distributore Ufficiale TeamSystem, il Cliente prende atto e accetta che il rapporto contrattuale intercorrente tra TeamSystem e tale Distributore Ufficiale TeamSystem avente ad oggetto la commercializzazione delle Soluzioni Iaas potrebbe cessare nel corso della durata del presente Contratto e che, in tal caso:

(a) TeamSystem comunicherà al Cliente la cessazione del rapporto contrattuale intercorrente tra la medesima TeamSystem e il Distributore Ufficiale TeamSystem;

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

(c) ogni contratto intercorrente tra il Cliente e il Distributore Ufficiale TeamSystem con riferimento alle Soluzioni Iaas sarà ceduto, ai sensi e per gli effetti dell'art. 1406 c.c., dal Distributore Ufficiale TeamSystem a TeamSystem;

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

26. Effetto novativo

26.1. È escluso qualsiasi rilievo di eventuali precedenti accordi individuali tra le Parti con riferimento a quanto forma oggetto del Contratto, che si intendono assorbiti ed esaustivamente superati dalla disciplina del Contratto.

27. Tolleranza

27.1. L'eventuale omissione di far valere uno o più dei diritti previsti dal Contratto non potrà comunque essere intesa come definitiva rinuncia a tali diritti e non impedirà, quindi, di esigerne in qualsiasi altro momento il puntuale e rigoroso adempimento.

28. Invalidità e inefficacia parziale

28.1. L'eventuale invalidità o inefficacia di una qualsiasi delle pattuizioni del Contratto lascerà intatte le altre pattuizioni giuridicamente e funzionalmente indipendenti, salvo quanto previsto dall'art. 1419, primo comma, c.c.

29. Trattamento dei dati personali

29.1. Le Parti convengono che la Licenziante potrà procedere all'elaborazione e utilizzo di informazioni puramente statistiche, su base aggregata, raccolte in relazione all'utilizzo delle Soluzioni Iaas da parte del Cliente, ivi incluse informazioni relative ai meta-dati associati ai documenti, a fini di studio e statistici. Il Cliente concede a tal fine al Licenziante una licenza non esclusiva, perpetua, irrevocabile, valida in tutto il mondo e a titolo gratuito, ad utilizzare tali informazioni per dette finalità.

29.2. Con riferimento al trattamento dei dati personali di soggetti terzi immessi o comunque trattati dal Cliente con riferimento alle Soluzioni Iaas, ai sensi del GDPR, le Parti si danno atto e accettano di conformarsi a quanto previsto nel MDPA allegato al presente Contratto (Allegato C).

29.3. Resta inteso che la Licenziante non assume alcuna responsabilità in merito alle conseguenze derivanti dall'inosservanza da parte del Cliente degli obblighi sul medesimo gravante in qualità di titolare del trattamento ai sensi della normativa in materia di protezione dei dati personali. Il Cliente si impegna a 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 di tali obblighi.

ALLEGATO A

SERVIZI COMPRESI

- rilascio di Aggiornamenti dei Software resi necessari dalla modifica, integrazione o emissione di 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 derivanti da nuove versioni (c.d. "*Release*") dei Software;
- Assistenza 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 software;
- interventi di Assistenza consistenti: (i) nel ripristino di Macchine Virtuali e/o database degli applicativi TeamSystem in conseguenza di problematiche legate a guasti dei Data Center e/o dell'Infrastruttura Cloud e/o guasti hardware dei server che ospitano le Macchine Virtuali; (ii) nel *reset* delle Credenziali di Accesso relative alle Macchine Virtuali;
- gestione ordinaria dell'Infrastruttura Cloud (e.g. gestione del firewall dell'Infrastruttura Cloud e/o della RAM, esecuzione dei backup pianificati).

SERVIZI NON COMPRESI

- rilascio di Aggiornamenti dei Software o attività in genere resi necessari dalla modifica, integrazione o emissione di 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 su software diversi dai Software (come sopra definiti);
- personalizzazioni su programmi e stampe standard (da analizzare preventivamente);
- installazione di software applicativi o programmi (inclusi i Software, come sopra definiti) e dei relativi aggiornamenti (inclusi gli Aggiornamenti, come sopra definiti);
- aggiornamenti del sistema operativo della Macchina Virtuale e/o di software applicativi o programmi diversi dai Software (come sopra definiti);
- gestione del firewall e delle configurazioni di sicurezza a livello della Macchina Virtuale;
- interventi di Assistenza (ivi inclusi quelli per ripristino Macchine Virtuali e/o database degli applicativi TeamSystem) che siano resi necessari a causa di (i) incidenti provocati da eventi politici, atti vandalici o comunque dal fatto doloso di dipendenti del cliente o di terzi (inclusi attacchi informatici, virus, hacker, etc.); (ii) negligenza, incuria, impiego del Software e/o delle Macchine Virtuali e/o dell'Infrastruttura Cloud in maniera non corretta o non conforme al Contratto e/o alle eventuali istruzioni della Licenziante o di TeamSystem; (iii) allagamenti, incendi, fenomeni atmosferici, calamità naturali o altre cause di forza maggiore;
- ogni altra attività non espressamente compresa nei Servizi.

ALLEGATO B

1. Oggetto e scopo

Obiettivo del presente "*service level agreement*" (in seguito per brevità "**SLA**") è quello di definire i parametri di riferimento per l'erogazione dei servizi di accesso ed utilizzo dell'Infrastruttura Cloud e per il monitoraggio del livello di qualità effettivamente erogato.

Sono esclusi dallo SLA i servizi non attinenti all'Infrastruttura Cloud tra cui, *inter alia*, i Servizi relativi ai Software.

2. SLA di funzionalità operativa

La Licenziante, farà ogni ragionevole sforzo per garantire la massima disponibilità dell'Infrastruttura Cloud e, contestualmente, l'osservanza dei parametri di funzionalità operativa riportati di seguito.

I livelli minimi di servizio che la Licenziante si impegna a rispettare sono i seguenti:

(i) risorse del Data Center attraverso il quale viene erogato il servizio di accesso ed utilizzo dell'Infrastruttura Cloud:

- *uptime* del 99,98% su base annuale per alimentazione elettrica e/o climatizzazione ambientale;
- *uptime* del 99,95% su base annuale, di accessibilità tramite rete internet alla Infrastruttura Cloud.

(ii) Infrastruttura Cloud:

- *uptime* del 99,95% su base annuale, per la disponibilità dei nodi fisici (*server*) che ospitano l'Infrastruttura Cloud.

3. Manutenzione programmata

Il tempo di manutenzione programmata non viene conteggiato ai fini del calcolo degli *uptime*. La manutenzione programmata riguarda le attività svolte regolarmente dalla Licenziante per mantenere la funzionalità delle risorse del Data Center attraverso il quale viene erogato il servizio di accesso ed utilizzo dell'Infrastruttura Cloud e dei nodi fisici che ospitano l'Infrastruttura Cloud; essa è ordinaria e straordinaria.

L'esecuzione degli interventi di manutenzione sarà comunicata dalla Licenziante al Cliente con un preavviso minimo di 24 (ventiquattro) ore a mezzo e-mail inviata all'indirizzo di posta elettronica indicato in fase d'ordine. La Licenziante impegna a compiere ogni ragionevole sforzo per eseguire le attività di manutenzione programmata in orari di minimo impatto.

4. Rilevamento guasti e/o anomalie

Eventuali guasti e/o anomalie alle infrastrutture attraverso le quali viene erogato il servizio di accesso ed utilizzo dell'Infrastruttura Cloud saranno segnalate dal Cliente alla Licenziante secondo le modalità definite dalla Licenziante; ai fini del calcolo degli *uptime* saranno tuttavia presi in considerazione soltanto i disservizi confermati anche dal sistema di monitoraggio.

Il monitoraggio viene effettuato tramite software specifici.

5. Limiti di applicabilità dello SLA

Qui di seguito sono riportate le condizioni in presenza delle quali gli eventuali disservizi non saranno conteggiati ai fini del calcolo degli *uptime*:

(i) cause di forza maggiore e cioè eventi che, oggettivamente, impediscano alla Licenziante di intervenire (in via meramente esemplificativa e non esaustiva: scioperi e manifestazioni con blocco delle vie di comunicazione; incidenti stradali; guerre e atti di terrorismo; catastrofi naturali quali alluvioni, tempeste, uragani etc);

(ii) interventi straordinari da effettuarsi con urgenza a insindacabile giudizio della Licenziante per evitare pericoli alla sicurezza e/o stabilità e/o riservatezza e/o integrità dell'Infrastruttura Cloud e dei dati e/o informazioni in essa contenuti.

(iii) indisponibilità o blocchi dell'Infrastruttura Cloud imputabili a:

- errato utilizzo, errata configurazione o comandi di spegnimento, volontariamente o involontariamente, eseguiti dal Cliente;
- anomalie e malfunzionamenti dei software applicativi/gestionali forniti da terze parti;
- inadempimento o violazione del Contratto imputabile al Cliente;

(iv) anomalia o malfunzionamento del servizio di accesso ed utilizzo dell'Infrastruttura Cloud, ovvero loro mancata o ritardata rimozione o eliminazione imputabili ad inadempimento o violazione del Contratto da parte del Cliente ovvero ad un cattivo uso da parte sua;

(v) mancato collegamento della/e infrastruttura/e virtuale/i alla rete pubblica per volontà o per fatto del Cliente;

(vi) cause che determinano l'inaccessibilità, totale o parziale, dell'Infrastruttura Cloud imputabili a guasti nella rete internet esterna al perimetro della Licenziante e comunque fuori dal suo controllo.

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	*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 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. 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.

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 sulla corretta gestione dei dati personali.

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, ferma 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.

Firewall, IDS/IPS - 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.

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.

	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. Più precisamente, a seconda dei casi e delle specifiche pattuizioni contrattuali, i data center di riferimento sono quelli di Aruba S.p.A. in Italia e quello di Microsoft Azure nella regione "West Europe". Per le misure di sicurezza fisica si prega di fare riferimento alle informazioni rese disponibili dai singoli provider: con riguardo ad Aruba S.p.A.: - https://www.datacenter.it/home.aspx con riguardo a Microsoft Azure: • https://docs.microsoft.com/it-it/azure/security/fundamentals/physical-security *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.