Versione 28.09.2021

CONDIZIONI GENERALI SERVIZI DI ELABORAZIONE CEDOLINI

1 PREMESSE GENERALI ED AMBITO DI APPLICAZIONE

1.1 Le presenti condizioni generali di contratto (di seguito, le "**Condizioni Generali**") trovano applicazione con riferimento a tutti i contratti di appalto di Servizi (come di seguito definiti) tra (i) la società TeamSystem S.p.A, con sede legale in Pesaro, via Sandro Pertini 88, partita IVA 01035310414 (di seguito, il "**Fornitore**"), in qualità di appaltatore, e (ii) il Cliente (come di seguito definito), in qualità di committente. Le presenti Condizioni Generali non trovano applicazione solamente nel caso in cui sia stato stipulato tra il Fornitore e il Cliente uno specifico accordo scritto che disciplini dettagliatamente tutti i termini e le condizioni di appalto dei Servizi. In quest'ultimo caso, troveranno applicazione le previsioni dello specifico accordo scritto, limitatamente alle materie da esso disciplinate.

1.2 Le presenti Condizioni Generali rappresentano e contengono l'integrale regolamento dei rapporti contrattuali tra il Fornitore ed il Cliente e sono integrate solamente dal documento d'offerta comprensivo dei relativi allegati, sottoposto dal Cliente al Fornitore e accettato da quest'ultimo, e avente a oggetto l'identificazione dei Servizi nonché i termini e le condizioni commerciali e tecnici dell'appalto di Servizi (di seguito, il "**Documento d'Offerta**").

1.3 In caso di contrasto tra quanto previsto nelle Condizioni Generali e nel Documento d'Offerta troverà applicazione quanto previsto nel Documento d'Offerta.

1.4 Eventuali termini e condizioni - o, comunque, ogni altra clausola o previsione - che siano contenuti in documenti diversi dalle presenti Condizioni Generali e/o dal Documento d'Offerta, così come eventuali modifiche apportate unilateralmente dal Cliente alle presenti Condizioni Generali e/o al Documento d'Offerta che non siano espressamente accettate per iscritto dal Fornitore, non saranno mai vincolanti per il Fornitore, né potranno essere ritenute parte integrante delle presenti Condizioni Generali e/o nel Documento d'Offerta. Le presenti Condizioni Generali prevarranno sempre su eventuali condizioni generali e/o particolari del Cliente.

1.5 L'esecuzione delle prestazioni di cui al Contratto da parte del Fornitore a favore del Cliente non comporta e non potrà essere interpretata come accettazione, da parte del Fornitore, di termini e condizioni diversi dalle presenti Condizioni Generali e/o dal contenuto del Documento d'Offerta.

2 DEFINIZIONI

2.1 Ai fini dell'interpretazione delle presenti Condizioni Generali, ferme eventuali diverse definizioni contenute in altri articoli, si precisa di seguito il significato da attribuire ai termini seguenti:

(a) **Autorità Competente**: indica qualsiasi ente, autorità, dipartimento, ispettorato, ministro, ministero, pubblica amministrazione o ente pubblico, di natura locale, regionale, nazionale o sovranazionale, avente competenza in Italia o per l'Italia in relazione alle materie di volta in volta trattate dalle presenti Condizioni Generali;

(b) **Cliente**: indica il committente dell'appalto per la fornitura dei Servizi regolato dal Contratto, come individuato nel Documento d'Offerta;

(c) **Codice di Condotta Anti-Corruzione**: significa il codice di condotta anti-corruzione adottato da TeamSystem e consultabile al sito teamsystem.com;

(d) **Codice Etico**: significa il codice etico adottato da TeamSystem e consultabile al sito teamsystem.com;

(e) **Condizioni Generali**: ha il significato di cui al paragrafo 1.1;

(f) **Contratto**: indica il contratto di appalto di servizi tra il Fornitore e il Cliente regolato dal Documento d'Offerta e dalle Condizioni Generali, unitamente ai relativi allegati;

(g) **Controllate**: indica le società direttamente o indirettamente controllate dal Cliente ai sensi dell'articolo 2359, primo comma numeri 1 e 2 del codice civile eventualmente indicate nel Documento d'Offerta quali ulteriori destinatarie dei Servizi;

(h) **Corrispettivi**: ha il significato di cui al paragrafo 7.1;

(i) **Dati Personali di Terzi**: ha il significato di cui al paragrafo 13.3;

(j) **Documento d'Offerta**: ha il significato di cui al paragrafo 1.2;

(k) **Fornitore**: ha il significato di cui al paragrafo 1.1;

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

(m) **Gruppo TeamSystem**: indica il Fornitore e tutte le società direttamente o indirettamente controllate da, o collegate a, il Fornitore ai sensi dell'articolo 2359 del codice civile, ivi inclusa TeamSystem Service;

(n) **Informazioni Riservate**: ha il significato di cui al paragrafo 12.1;

(o) **Legislazione in materia di Protezione dei Dati Personali**: indica il GDPR, e ogni eventuale ulteriore norma e/o regolamento sul trattamento di 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

(p) **Modello Organizzativo**: significa il modello di organizzazione, gestione e controllo adottato da TeamSystem ai sensi del d.lgs. 231/2001 e consultabile al sito teamsystem.com;

(q) **Normativa Applicabile**: indica qualsiasi legge, regolamento, direttiva o altra fonte di diritto italiano o dell'Unione Europea, incluse le leggi regionali, locali, i provvedimenti emessi da ogni Autorità Competente, le norme CEI, le norme UNI e ogni altra normativa tecnica, che siano applicabili, tempo per tempo ed in ragione della materia di riferimento, al Contratto, ai Servizi, al Cliente e/o al Fornitore;

(r) **Parte/i**: ciascuno tra il Fornitore e il Cliente;

(s) **Responsabile**: ha il significato di cui al paragrafo 13.3;

(t) **Servizio/i**: indica i servizi di elaborazione delle retribuzioni e altre attività connesse riguardanti la gestione del personale individuati espressamente nel Documento d'Offerta, l'esecuzione dei quali è affidata dal Cliente al Fornitore ai sensi e per gli effetti del Contratto;

(u) **Sub-Responsabile:** : ha il significato di cui al paragrafo 13.3;

(v) **Tariffe**: ha il significato di cui al paragrafo 7.1;

(w) **TeamSystem Service:** indica TeamSystem Service S.r.l., con sede legale in Viale Giuseppe Ferro s.n.c., Campobasso, codice fiscale e partita IVA n. 01641790702;

(x) **Tempistiche Stimate**: ha il significato di cui al paragrafo 6.2.

3 OGGETTO

3.1 Ai termini e alle condizioni di cui al Contratto, il Cliente affida al Fornitore, che accetta, l'esecuzione dei Servizi a fronte del pagamento dei Corrispettivi da parte del Cliente. Il Cliente prende atto ed accetta che i Servizi saranno erogati, in tutto o in parte, da TeamSystem Service.

3.2 Il Cliente e il Fornitore si danno reciprocamente atto e convengono che i Servizi di cui al Contratto sono esclusivamente quelli elencati nel Documento d'Offerta e che tali Servizi (i) saranno resi dal Fornitore (tramite TeamSystem Service) in conformità alla Normativa Applicabile e a quanto previsto nel Contratto, (ii) non sono soggetti ad autorizzazioni o concessioni; e (iii) non costituiscono attività riservata ai titolari di abilitazioni professionali. In ogni caso, il Fornitore dichiara al Cliente che né il Fornitore né TeamSystem Service sono iscritti agli albi di cui al D.Lgs. 139/2005 e alla L. 12/1979.

3.3 Salvo quanto diversamente previsto nel Documento d'Offerta, il Cliente e il Fornitore si danno reciprocamente atto e convengono che il Contratto ha a oggetto solo la fornitura dei Servizi, restando espressamente escluso dall'oggetto del Contratto tutto ciò che non sia espressamente ricompreso tra i Servizi, ivi compresi, a titolo meramente esemplificativo e non esaustivo: (i) la compravendita, la locazione o la concessione di qualsivoglia diritto d'uso, a qualsiasi titolo di *hardware* e/o di strutture informatiche di proprietà o comunque nella disponibilità del Fornitore o di terzi; (ii) la concessione di una licenza d'uso di soluzioni *software* di titolarità del Fornitore o di terzi; (iii) la prestazione da parte del Fornitore di servizi *cloud*, ivi inclusa, ma non limitatamente a, la concessione di licenze d'uso di applicativi *saas*; e/o (iv) la fornitura di servizi di connessione o di rete.

3.4 Ogni attività aggiuntiva o diversa rispetto ai Servizi espressamente individuati nel Documento d'Offerta (ivi incluse le eventuali richieste di modifica, anche parziali, avanzate dal Cliente in relazione alla prestazione di uno o più Servizi) dovrà essere oggetto di un autonomo e separato accordo scritto, da intendersi vincolante per il Fornitore solamente a seguito di espressa accettazione per iscritto da parte di quest'ultimo.

3.5 Trascorsi 15 (quindici) giorni dall'erogazione di ciascun Servizio, il Servizio prestato si considererà accettato senza riserve e il Cliente non avrà più nulla a pretendere nei confronti del Fornitore con riferimento alle attività svolte rinunciando, sin da ora, a qualsivoglia pretesa, azione, garanzia o diritto a qualsiasi titolo con riferimento alle stesse.

3.6 La prestazione dei Servizi sarà effettuata dal Fornitore sotto la propria responsabilità e secondo la propria organizzazione diretta del lavoro, con mantenimento della piena autonomia organizzativa e gestionale. Il Cliente non ha il diritto di impartire direttive al personale del Fornitore e di esercitare nei confronti di quest'ultimo poteri direttivi e/o gerarchici.

3.7 Il Cliente e il Fornitore si obbligano, ognuno per quanto di propria spettanza, ad evitare (i) ogni eventuale promiscuità funzionale tra il rispettivo personale e (ii) qualsiasi ingerenza reciproca nell'organizzazione e nella gestione aziendale dell'altra Parte.

4 SERVIZI

4.1 Il Cliente si impegna:

(a) a dotarsi autonomamente ed a proprie spese di materiale hardware e software adeguato e di una connettività adeguata al fine di poter fruire dei Servizi;

(b) a usare i Servizi in maniera conforme al Contratto ed esclusivamente per gli scopi cui essi sono destinati;

(c) a fornire al Fornitore tutte le informazioni necessarie per consentire al Fornitore 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 alle Controllate;

(d) a mettere a disposizione del Fornitore l'opportuno supporto logistico per l'espletamento delle eventuali attività che, per motivi di opportunità tecnica e logistica, potranno essere svolte dal Fornitore presso la sede del Cliente (in ogni caso, nel rispetto delle Normativa Applicabile, con particolare ma non esclusivo riferimento a quella in materia di sicurezza sul lavoro);

(e) a fare prendere visione e accettare a ciascuna Controllata le presenti Condizioni Generali.

5 ULTERIORI OBBLIGHI DEL CLIENTE

5.1 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 di (ii) voler utilizzare i Servizi nell'ambito della propria attività imprenditoriale, artigianale, commerciale o professionale e che, pertanto, non si applicano nei suoi confronti le disposizioni del D.Lgs. 206/2005 a protezione dei consumatori.

5.2 Il Cliente si impegna a far sì, anche ai sensi e per gli effetti di cui all'articolo 1381 del codice civile, che le disposizioni del Contratto siano rispettate da ciascuna Controllata, ivi inclusi i relativi dipendenti e/o collaboratori; il Cliente è, pertanto, considerato esclusivo responsabile dell'operato di tali soggetti e garantisce che questi ultimi rispetteranno tutta la Normativa Applicabile.

5.3 Ai fini dell'erogazione dei Servizi, laddove ritenuto opportuno dal Fornitore, sarà costituito uno specifico gruppo di lavoro composto da risorse del Fornitore e del Cliente che collaboreranno costantemente e in buona fede. Le risorse del team del Cliente dovranno avere specifiche competenze con riferimento a ciascun processo gestionale interessato. Il Cliente prende atto e accetta che una continua e fattiva collaborazione sua e dei membri del suo team è essenziale ai fini di una corretta e completa erogazione dei Servizi da parte del Fornitore.

5.4 Il Cliente prende atto e accetta che il Fornitore potrà affidare, in tutto o in parte, l'erogazione dei Servizi a soggetti terzi individuati a esclusiva discrezione del Fornitore, ivi inclusa TeamSystem Service.

5.5 È fatto divieto al Cliente di utilizzare i Servizi 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 del Fornitore e/o di alcuna società del Gruppo TeamSystem e/o di terzi; (b) abbiano contenuti discriminatori, diffamatori, calunniosi o minacciosi; (c) contengano materiali pornografico, pedopornografico, osceno o comunque contrario alla pubblica morale; (d) contengano *virus*, *worm*, *trojan horse* o, comunque, altri elementi informatici di contaminazione o distruzione; (e) costituiscano attività di *spamming*, *phishing* e/o simili; (f) siano in ogni caso in contrasto con la Normativa Applicabile.

5.6 Il Fornitore si riserva il diritto di sospendere 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 alla Normativa Applicabile. In tal caso, il Fornitore 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 8.4.

6 EFFICACIA E STIMA DELLE TEMPISTICHE

6.1 Fatto salvo quanto diversamente previsto nel Documento d'Offerta, il Contratto è valido ed efficace dalla data dell'accettazione del Documento d'Offerta da parte del Fornitore.

6.2 Resta inteso che, fatto salvo per le tempistiche eventualmente richiamate dal Fornitore in uno specifico allegato al Documento d'Offerta, le tempistiche indicate nella documentazione eventualmente prodotta dal Fornitore a seguito delle attività di analisi (a titolo meramente esemplificativo e non esaustivo documenti di analisi, diagrammi di gantt, etc.) (di seguito, le "**Tempistiche Stimate**"), nonché le eventuali ulteriori tempistiche per la prestazione dei Servizi, ivi incluse le tempistiche eventualmente richieste dal Cliente, sono indicative, non costituiscono termini essenziali e costituiscono il frutto di una stima che si basa sui dati comunicati e/o a disposizione del Fornitore alla data in cui la stima è stata formulata. Il Cliente prende atto che i Servizi hanno un alto livello di complessità tecnica e che l'erogazione degli stessi potrà subire dei rallentamenti o dei ritardi rispetto

alle Tempistiche Stimate in funzione di numerosi fattori quali, a mero titolo esemplificativo:

(i) variazione, su richiesta del Cliente, delle attività previste;

(ii) eventi imprevedibili alla data della stima (a titolo meramente esemplificativo e non esaustivo problematiche connesse ai sistemi *hardware*, *software*, *cloud* e di rete del Cliente; fatto del Cliente o di un terzo; etc.);

(iii) fattori o dati tecnici non conosciuti dal Fornitore alla data della stima delle tempistiche.

Il Fornitore, pertanto: (a) non rilascia dichiarazioni o garanzie espresse o implicite sul fatto che le Tempistiche Stimate saranno rispettate o, alla data in cui vengono formulate, siano corrette e/o sufficienti ai fini del raggiungimento degli obiettivi del Cliente; (b) salvo il caso in cui il ritardo derivi da dolo o colpa grave, non potrà essere ritenuto in alcun modo responsabile di eventuali danni, passività o conseguenze negative di qualsivoglia natura derivati al Cliente o a terzi in conseguenza di interruzioni, sospensioni, ritardi o malfunzionamenti dovuti al fatto del Cliente o di terzi, cause di forza maggiore, eventi imprevedibili, fattori tecnici o a elementi di cui il Fornitore non fosse a conoscenza.

7 CORRISPETTIVI, AGGIORNAMENTO DEI CORRISPETTIVI E PAGAMENTI

7.1 A fronte della fornitura dei Servizi, il Cliente è tenuto a corrispondere al Fornitore i corrispettivi (di seguito, i "**Corrispettivi**") determinati in base alle tariffe indicate nel Documento d'Offerta (di seguito, le "**Tariffe**") oppure in base a separati accordi scritti intervenuti tra il Cliente e il Fornitore, nonché a rimborsare al Fornitore le spese vive sostenute per la prestazione dei Servizi.

7.2 Il Fornitore avrà diritto alla revisione dei Corrispettivi ove il Cliente, successivamente alla sottoscrizione del Documento d'Offerta, richieda delle modifiche tecniche o degli emendamenti delle condizioni contrattuali pattuite.

7.3 Il Cliente prende atto e accetta espressamente che le Tariffe (e pertanto di conseguenza i Corrispettivi) sono soggette ad aggiornamento annuale nella misura del 100% della variazione in aumento dell'indice ISTAT dei prezzi della produzione dei servizi, calcolato come media degli ultimi dodici mesi.

7.4 Il Cliente prende atto che i Servizi sono soggetti, per loro stessa natura, ad una costante evoluzione normativa che richiede continue e onerose attività di aggiornamento. In ragione di quanto precede, il Fornitore avrà il diritto di modificare i Corrispettivi anche in misura superiore all'indice ISTAT con le modalità di cui all'articolo 18.

7.5 Fermo restando quanto previsto ai precedenti paragrafi, qualora durante l'esecuzione del Contratto dovessero verificarsi circostanze imprevedibili tali da rendere maggiormente onerosa l'erogazione dei Servizi da parte del Fornitore, quest'ultima avrà diritto di percepire un equo compenso *una tantum* ovvero di modificare unilateralmente i Corrispettivi.

7.6 Fatto salvo quanto eventualmente previsto nel Documento d'Offerta, i Corrispettivi, così come tutte le Tariffe, si intendono al netto di IVA e di ogni ulteriore imposta e/o onere fiscale eventualmente applicabile.

7.7 Salvo ove diversamente previsto nel Documento d'Offerta, TeamSystem fatturerà al Cliente, con cadenza mensile, un dodicesimo dei Corrispettivi annuali previsti nel Documento d'Offerta. Resta inteso che, ove alla fine dell'anno di competenza, i Servizi effettivamente svolti dal Fornitore su richiesta del Cliente superino quelli preventivati nel Documento d'Offerta, il Fornitore provvederà a fatturare al Cliente l'eccedenza in base alle Tariffe concordate. In nessun caso sarà previsto il rimborso al Cliente dei Corrispettivi eventualmente già pagati.

7.8 I pagamenti dei Corrispettivi dovranno essere effettuati dal Cliente nel termine espressamente indicato nel Documento d'Offerta o, in mancanza di espressa previsione nel Documento d'Offerta, nel termine di 30 (trenta) giorni dal ricevimento della fattura emessa dal Fornitore.

7.9 In assenza di diverse indicazioni nel Documento d'Offerta, i pagamenti dovranno essere eseguiti presso la sede del Fornitore. In ogni caso non saranno ritenuti né validi, né efficaci, i pagamenti effettuati a mani di dipendenti del Fornitore o di terzi operanti per conto dello stesso che non siano in possesso di valida autorizzazione e delega scritta a riscuotere somme in nome e per conto del Fornitore medesimo.

7.10 Nel Documento d'Offerta il Fornitore potrà richiedere la prestazione di garanzie di pagamento a carico ed a spese del Cliente. La mancata prestazione, da parte del Cliente, delle garanzie richieste dal Fornitore legittimerà l'applicazione da parte del Fornitore della clausola risolutiva espressa di cui al paragrafo 8.4.

7.11 I termini di pagamento indicati in Contratto sono tassativi. 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, il Fornitore avrà diritto di (i) ai sensi dell'articolo 1460 del codice civile, sospendere le prestazioni a carico del Fornitore fino al ricevimento del versamento dovuto; (ii) avvalersi della clausola risolutiva espressa di cui al paragrafo 8.4; (iii) 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 (iv) recedere in qualsiasi momento da tali eventuali altri contratti.

7.12 Fermo restando l'obbligo per il Cliente di versare i Corrispettivi, il Fornitore si riserva altresì la facoltà di interrompere in ogni momento la fornitura dei Servizi in favore del Cliente e/o di ciascuna Controllata in caso di inadempimento di una delle obbligazioni assunte dal Cliente in uno qualsiasi degli eventuali ulteriori contratti conclusi tra il medesimo Cliente e il Fornitore (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 tale ipotesi, TeamSystem comunicherà al Cliente l'intenzione di interrompere la fornitura dei Servizi, invitando il Cliente, ove possibile, a porre rimedio all'inadempimento entro un determinato termine. Il Cliente rimane in ogni caso obbligato a versare quanto dovuto anche in caso di interruzione della fornitura dei Servizi.

7.13 Il Cliente sarà comunque tenuto ad effettuare tempestivamente i pagamenti dovuti, anche nel caso in cui abbia sollevato contestazioni per ritardi o per vizi o difetti nei confronti del Fornitore, atteso come in tali ipotesi il Fornitore avrà comunque la possibilità di adottare ogni rimedio necessario ad eliminare le ragioni alla base delle contestazioni, rispettando i termini e le condizioni del Contratto. Relativamente all'ipotesi indicata, in applicazione dell'articolo 1462 del codice civile, dovrà ritenersi pertanto rinunciata da parte del Cliente la facoltà di sollevare l'eccezione di inadempimento di cui all'articolo 1460 del codice civile.

8 DURATA, RECESSO E RISOLUZIONE

8.1 Fatto salvo quanto eventualmente e diversamente previsto nel Documento d'Offerta, 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.

8.2 Il solo Fornitore potrà recedere anzitempo dal Contratto nelle seguenti ipotesi:

(i) mediante semplice comunicazione scritta con effetto immediato, nel caso in cui siano state presentate a carico del Cliente istanze di fallimento o avviate altre procedure concorsuali, sequestri, pignoramenti, condanne civili o penali dei legali rappresentanti del Cliente che ne pregiudichino il buon nome o possano ostacolarne l'attività, nonché nel caso di fusione, liquidazione o cessione d'azienda da parte del Cliente o di mutamento nella compagine sociale del Cliente o della sua controllante finale, salvo che, in tali ultimi casi di mutamento, il Fornitore, previamente informato, abbia fornito il proprio consenso scritto alla prosecuzione del Contratto. Il Cliente si impegna ad informare tempestivamente il Fornitore in merito al verificarsi di uno degli eventi sopra menzionati;

(ii) in qualsiasi momento, mediante semplice comunicazione scritta al Cliente con un preavviso di 60 (sessanta) giorni.

Fatte salve le norme inderogabili limiti di legge e quanto previsto all'articolo 19, il Cliente rinuncia espressamente ad avvalersi di qualsiasi ipotesi di recesso eventualmente prevista dalle normative tempo per tempo applicabili al Contratto.

8.3 Il Fornitore si riserva altresì il diritto di recedere dal Contratto 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 il Fornitore (o una qualsiasi delle società del Gruppo TeamSystem o un distributore ufficiale TeamSystem), obbligazioni il cui inadempimento costituisca causa di risoluzione di tali eventuali ulteriori contratti.

8.4 Oltre a quanto stabilito in altre parti delle presenti Condizioni Generali, il Contratto si intenderà automaticamente risolto, ai sensi e per gli effetti di cui all'articolo 1456 del codice civile, mediante semplice comunicazione scritta in tal senso del Fornitore, nell'ipotesi di inadempimento, da parte del Cliente, delle obbligazioni di cui agli articoli 4 (Obblighi del Cliente in relazione ai Servizi), 5 (Ulteriori Obblighi del Cliente), 7 (Corrispettivi, aggiornamento dei Corrispettivi e pagamenti), 9 (Diritti di proprietà intellettuale), 12 (Riservatezza); 19.1 (Divieto di cessione del Contratto). È fatto comunque salvo il diritto del Fornitore di ottenere il risarcimento di tutti i danni subiti.

8.5 Alla cessazione del Contratto, il Cliente riceverà tutti gli elaborati oggetto della prestazione dei Servizi e quanto necessario alla gestione del servizio di elaborazione dati come previsto dalle procedure standard TeamSystem.

9 DIRITTI DI PROPRIETÀ INTELLETTUALE

9.1 Il Cliente prende atto e riconosce espressamente che tutti i diritti di proprietà industriale e/o intellettuale, ivi inclusi i relativi diritti di sfruttamento economico, sui Servizi, sulla documentazione, sui software eventualmente sviluppati nell'erogazione dei Servizi e gli eventuali lavori derivati (ivi inclusi, ma non limitatamente a, i relativi codici oggetto, codici sorgente, interfacce e documentazione di supporto) saranno, in tutto e in ogni loro parte e ovunque nel mondo, di esclusiva titolarità del Fornitore, di TeamSystem Service e/o dei relativi terzi proprietari indicati nel Documento d'Offerta.

9.2 Restano altresì in capo al Fornitore - o alla società del Gruppo TeamSystem che ne sia titolare - tutti i diritti sui marchi, loghi,

nomi, e altri segni distintivi comunque associati ai Servizi, con la conseguenza che il Cliente non potrà in alcun modo utilizzarli senza la preventiva autorizzazione scritta del Fornitore.

9.3 Il Cliente dichiara e garantisce di avere ottenuto tutte le licenze e le autorizzazioni necessarie a consentire al Fornitore di prestare i Servizi, e che, pertanto, le attività oggetto dei Servizi, ivi inclusa, ma non limitatamente a, le eventuali attività di sviluppo e personalizzazione di software di terzi, non violano in alcun modo alcun diritto di proprietà industriale e/o intellettuale di terzi, ovunque nel mondo.

10 MANLEVA

10.1 Il Cliente si impegna a manlevare e tenere indenne il Fornitore da eventuali danni, oneri o costi (ivi inclusi quelli per consulenza e assistenza legale) di qualunque tipo, diretti o indiretti, attuali o potenziali, che il Fornitore dovesse sostenere in conseguenza di qualsivoglia azione o pretesa di terzi derivante dall'utilizzo dei Servizi da parte del Cliente in violazione di quanto previsto nel Contratto, o comunque connessa a detto indebito utilizzo.

11 DIVIETO DI STORNO

11.1 Durante la vigenza del Contratto e per un periodo di un anno successivo alla cessazione dello stesso, 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, direttamente o indirettamente, con qualsiasi dipendente o collaboratore del Fornitore o di qualsiasi altra società del Gruppo TeamSystem.

11.2 In caso di violazione di quanto stabilito al comma che precede, il Fornitore avrà diritto di risolvere il Contratto mediante semplice comunicazione scritta. Il Cliente, inoltre, sarà tenuto a corrispondere al Fornitore, a titolo di penale, una somma pari al 200% dell'ultima retribuzione annuale del dipendente / collaboratore, salvo il diritto al maggior danno eventualmente subito dal Fornitore. Il Cliente riconosce la congruità della penale alla luce dell'interesse che il Fornitore ha al rispetto da parte del Cliente delle previsioni di cui al presente articolo 11.

12 RISERVATEZZA

12.1 Le Parti riconoscono e si danno reciprocamente atto che tutte le informazioni di cui verranno a conoscenza nell'esecuzione del Contratto (di seguito, le "**Informazioni Riservate**") hanno natura confidenziale e riservata e, pertanto, si impegnano a non utilizzarle o divulgarle a terzi, in qualunque modo e con qualunque mezzo, per finalità diverse da quelle di cui al Contratto, salvo per quanto richiesto dalla Normativa Applicabile e/o sulla base di un legittimo ordine da parte dell'Autorità Competente e/o per tutelare un proprio diritto anche nei confronti di terzi, fermo restando in ogni caso l'obbligo di preventiva comunicazione all'altra Parte, in modo da permettere a quest'ultima di richiedere le necessarie misure a tutela della segretezza delle informazioni. Tale obbligo di riservatezza rimane in vigore per tu a la durata del presente Contratto e successivamente per un periodo di tre (3) anni, qualunque sia la causa della sua cessazione. L'obbligo di riservatezza che precede non riguarda le informazioni che sono di dominio pubblico.

12.2 Resta possibile per il Fornitore citare il Cliente ed il servizio erogato nei tempi e nei modi descritti nel Contratto come referenza per eventuali bandi, gare e service/software selection.

13 TRATTAMENTO DEI DATI PERSONALI

13.1 Le Parti riconoscono e si danno reciprocamente atto che la sottoscrizione del presente Contratto e l'esecuzione dei Servizi comporteranno la raccolta e il trattamento di dati personali del Cliente (nonché di parti ad essi correlate, quali procuratori, legali rappresentanti, etc.) da parte del Fornitore per le finalità necessarie all'esecuzione del predetto Contratto e in conformità alla Legislazione in materia di protezione dei Dati Personali e alle altre eventuali previsioni di legge applicabili. Il Fornitore, in qualità di titolare del trattamento, si impegna a trattare tali dati secondo quanto riportato nell'informativa rilasciata dal Fornitore ai sensi dell'articolo 13 del GDPR consultabile al link https://tc.teamsystem.com/InformativaPrivacy.pdf.

13.2 Ad ogni modo, il Fornitore potrà trattare le informazioni cui avrà accesso in ragione dell'utilizzo dei Servizi da parte del Cliente per finalità di ricerca finalizzata al miglioramento dei servizi secondo le modalità descritte nella propria informativa sul trattamento dei dati personali.

13.3 Resta inteso che il Cliente è titolare del trattamento ai sensi del GDPR rispetto ai dati personali di terzi soggetti (i "**Dati Personali di Terzi**") a cui il Fornitore avrà accesso per la fornitura dei Servizi. Rispetto a tali dati il Fornitore agirà quale responsabile del trattamento ai sensi dell'art. 28 del GDPR (il "**Responsabile**") e le Parti accettano di conformarsi a quanto previsto nel MDPA allegato al presente Contratto (Allegato A). Qualora il Cliente agisca, a propria volta, quale responsabile del trattamento dei dati per conto di un terzo titolare, il Cliente garantisce che quest'ultimo ha autorizzato il ricorso al Fornitore quale sub-responsabile del trattamento (il "**Sub-Responsabile**") ai sensi degli artt. 28 e 29 GDPR.

13.4 Rispetto ai Dati Personali di Terzi, il Cliente resterà pienamente responsabile dell'adempimento nei confronti degli interessati di tutti gli obblighi previsti dal GDPR e dalla Legislazione in materia di protezione dei Dati Personali ad esso applicabili in qualità di titolare del trattamento. Il Fornitore non assume alcuna responsabilità in merito alle conseguenze derivanti dall'inosservanza da parte del Cliente degli obblighi sul medesimo gravanti in qualità di titolari del trattamento, se non per effetto e nei limiti di eventuali violazioni commesse dal Fornitore stesso in qualità di responsabile del trattamento ovvero violazioni dell'MDPA.

14 RESPONSABILITÀ DEL FORNITORE

14.1 Il Fornitore non rilascia dichiarazioni e garanzie espresse o implicite sul fatto che i Servizi siano adatti a soddisfare le specifiche esigenze del Cliente.

14.2 Il Fornitore non potrà essere ritenuto responsabile per danni, diretti o indiretti, di qualsiasi natura ed entità, che dovessero derivare al Cliente e/o alle Controllate e/o a terzi: (i) in conseguenza della mancata continua e fattiva collaborazione del Cliente e delle sue risorse e/o dell'incompetenza di quest'ultime ai sensi del paragrafo 5.3, e/o (ii) in conseguenza di perdite di dati, documenti e/o informazioni contenute nei sistemi informatici del Cliente derivanti dalla prestazione dei Servizi.

14.3 Qualora il Cliente utilizzi in tutto o in parte i Servizi per predisporre o elaborare autonomamente ulteriore documentazione integrata da dati e informazioni non generati dai Servizi (di seguito, le "**Elaborazioni**"), in nessun caso il Fornitore potrà essere ritenuto responsabile per eventuali danni o perdite, di qualunque natura o entità, derivanti dalle Elaborazioni, essendo in ogni caso il Cliente tenuto a verificare la correttezza e accuratezza di tali Elaborazioni e del loro utilizzo.

14.4 Salvo che ciò sia necessario per adempiere a disposizioni di legge e/o a richieste dell'autorità giudiziaria, il Fornitore non è tenuto in alcun modo alla verifica dei dati e dei contenuti forniti dal Cliente e e/o da ciascuna Controllata per l'erogazione dei Servizi e, pertanto, non potrà in alcun modo essere ritenuto 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.

14.5 Il Fornitore, fatti salvi gli inderogabili limiti di legge, non potrà in nessun caso essere ritenuto 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 ai sistemi informatici del Cliente e/o del Fornitore, dai quali possano derivare, senza pretesa di esaustività, le seguenti conseguenze: (i) mancata fruizione dei Servizi; (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.

14.6 Salvo il caso di dolo o colpa grave, la responsabilità del Fornitore non potrà mai eccedere l'ammontare dei Corrispettivi pagati dal Cliente ai sensi del presente Contratto nell'anno in cui si è verificato l'evento dal quale discende la responsabilità di TeamSystem. Il Fornitore non potrà essere ritenuto 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 e/o delle Controllate verso terzi.

15 LEGGE APPLICABILE, COMPOSIZIONE DELLE CONTROVERSIE E FORO COMPETENTE

15.1 Il Contratto è regolato dalla e deve essere interpretato in conformità alla legge italiana.

15.2 Il Fornitore e il Cliente si impegnano a porre in essere ogni misura necessaria od opportuna per risolvere in buona fede e amichevolmente qualsiasi controversia dovesse sorgere in relazione all'interpretazione ed esecuzione del Contratto.

15.3 Ove entro 30 (trenta) giorni dall'insorgenza della controversia le Parti non abbiano raggiunto una soluzione amichevole, la controversia sarà risolta mediante arbitrato secondo il Regolamento della Camera Arbitrale di Milano, che le Parti dichiarano di conoscere e accettare integralmente. Il Collegio Arbitrale sarà composto da un collegio di 3 (tre) arbitri (di nazionalità italiana), nominati in conformità al predetto regolamento. Gli arbitri procederanno in via rituale e secondo diritto. L'arbitrato avrà sede in Milano nel luogo indicato dal presidente del Tribunale Arbitrale. La presente clausola compromissoria non opererà con riferimento a qualsiasi controversia che, a norma di legge, non sia compromettibile in arbitrato, nonché per i procedimenti d'ingiunzione di cui agli articoli 633 e seguenti del codice di procedura civile, le relative fasi di opposizione e i procedimenti in materia di proprietà industriale e/o intellettuale, che saranno devoluti alla giustizia ordinaria e alla esclusiva competenza del Foro di Milano.

16 CODICE ETICO, CODICE DI CONDOTTA ANTI-CORRUZIONE E MODELLO ORGANIZZATIVO

16.1 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.

16.2 Il Cliente dichiara di essere a conoscenza del fatto che il Fornitore ha adottato il Modello Organizzativo, il Codice di Condotta

Anti-Corruzione, e il Codice Etico e che tali documenti sono disponibili sul sito www.teamsystem.com.

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

16.4 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, del Fornitore 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.

16.5 Il Cliente si impegna a segnalare al Fornitore 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.

16.6 In caso di inosservanza, anche parziale, da parte del Cliente al presente articolo e/o nel caso in cui le dichiarazioni rese dal medesimo si rivelino errate, non vere o non corrette, il Fornitore 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.

17 SALUTE E SICUREZZA

17.1 Le Parti si impegnano a cooperare e coordinarsi allo scopo di adempiere le obbligazioni previste all'articolo 26 del D. Lgs n. 81/2008, così come modificato e integrato tempo per tempo. Al riguardo, il Fornitore è tenuto ad informare il Cliente circa i rischi propri relativi alle attività oggetto dei Servizi nonché a impegnarsi alla costante e continua collaborazione e cooperazione per l'individuazione di rischi e l'adozione di misure preventive e protettive da parte del proprio personale operativo negli ambienti di lavoro del Cliente.

17.2 In presenza di rischi di interferenza, e fatte salve le esclusioni previste dall'articolo 26 del D. Lgs n. 81/2008 (ad esempio, con riguardo alle prestazioni di natura intellettuale), le Parti sono tenute alla elaborazione di un DUVRI (Documento unico di valutazione dei rischi interferenziali) su iniziativa del Cliente e all'attuazione di misure preventive congiunte. Resta inteso che, allorquando l'interferenza, preventivamente esclusa dalle Parti, dovesse emergere nello svolgimento dei Servizi, le Parti dovranno informarsi reciprocamente e immeditatamente agire al fine di correttamente ottemperare alle disposizioni di legge vigenti.

17.3 Allo stato, essendo assenti rischi interferenziali, non vi sono costi relativi alla predisposizione di misure volte a eliminare o ridurre al minimo i suddetti rischi medesimi.

17.4 Il Cliente, inoltre, dichiara e garantisce di rispettare le prescrizioni inderogabili di legge di cui al summenzionato D. Lgs n. 81/2008; altresì è tenuto - prima dell'avvio delle attività oggetto del presente Contratto - a comunicare ai lavoratori del Fornitore eventuali disposizioni di sicurezza e misure generali di prevenzione e protezione, nonché a garantire la capacità di risposta alle emergenze di incendio e sanitarie.

18 MODIFICHE UNILATERALI DEL CONTRATTO

18.1 Considerata l'elevata complessità tecnica e normativa del settore in cui TeamSystem opera e dei prodotti e servizi offerti da quest'ultima, considerato altresì che tale settore è caratterizzato da continue evoluzioni tecnologiche, normative e delle esigenze di mercato, e considerato infine che, in conseguenza di quanto sopra, sorge periodicamente la necessità che TeamSystem adegui la propria organizzazione e/o struttura tecnica e funzionale dei prodotti e servizi offerti alla propria clientela (anche nell'interesse di quest'ultima), il Cliente accetta che il Contratto potrà essere modificato da TeamSystem in qualsiasi momento, dandone semplice comunicazione scritta (anche via e-mail o con l'ausilio di programmi informatici) al Cliente. Le

modifiche potranno consistere in: (i) modifiche connesse agli adeguamenti apportati alla struttura tecnica e/o funzionale dei prodotti e servizi offerti; (ii) modifiche connesse agli adeguamenti apportati alla struttura organizzativa di TeamSystem; (iii) modifiche relative ai corrispettivi dovuti dal Cliente, che tengano conto degli adeguamenti di cui ai punti (i) e (ii) che precedono.

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

18.3 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.

19 DISPOSIZIONI FINALI

19.1 Il Cliente non ha diritto di trasferire o cedere il presente Contratto, né i suoi diritti e/o obbligazioni derivati dal Contratto, senza il preventivo consenso scritto del Fornitore.

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

19.3 Durante l'esecuzione del Contratto, la tolleranza del Fornitore circa comportamenti del Cliente non conformi ad una o più delle prescrizioni contenute nelle presenti Condizioni Generali, nel Documento d'Offerta o nella Normativa Applicabile, non implica la rinuncia a fare valere in qualunque momento i propri diritti.

19.4 Nelle presenti Condizioni Generali, tutti i termini espressi in giorni devono intendersi quali giorni di calendario.

Versione 28.09.2021

Allegato "A"

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 Committente che accetta il presente accordo. Per "Fornitore" si intende uno o più dei seguenti soggetti:

TeamSystem S.p.A., con sede legale in Pesaro (PU), via Sandro Pertini 88, codice fiscale e partita IVA n. 01035310414

e

il soggetto indicato nel Contratto quale committente (di seguito il "Committente"),

di seguito, congiuntamente, le "Parti" o disgiuntamente la "Parte"

PREMESSO CHE

a) Il Committente 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 e riportate in calce al presente accordo (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 Committente sottoscrive o accetta il presente Accordo;
"Dati Personali" ha il significato di cui alla Legislazione in materia di Protezione dei Dati Personali e includerà, a titolo puramente esemplificativo, tutti i dati forniti, archiviati, inviati, ricevuti o altrimenti elaborati, o creati dal Committente, 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 Committente, all'atto della sottoscrizione del Servizio o fornito tramite altro canale ufficiale al Fornitore, a cui il Committente 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 Committente 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 Committente agisce di regola quale Titolare del trattamento dei Dati Personali.

2.2. Qualora il Committente svolga operazioni di trattamento per conto di altro Titolare, il Committente potrà agire come Responsabile del trattamento. In tal caso, il Committente garantisce che le istruzioni impartite e le attività intraprese in relazione al trattamento dei Dati Personali, inclusa la nomina, da parte del Committente, 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 fornire 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: privacy@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 Committente 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 Committente richieda variazioni rispetto alle Istruzioni iniziali, il Fornitore valuterà gli aspetti di fattibilità e concorderà con il Committente le predette variazioni ed i costi connessi.

3.3. Nei casi di cui all'art. 3.2 e in caso di richieste del Committente 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 Committente. In tali casi il Committente 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 Committente (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 Committente.

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 Committente 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 Committente 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 Committente 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 Committente 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 Committente 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 Committente.

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 Committente 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 Committente mediante invio di comunicazione all'Email di notifica.

6.1.3. Qualora il Committente 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 Committente per tale implementazione.

6.1.4. Il Committente 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 Committente 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 Committente o presso fornitori del Committente (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 COMMITTENTE – Fermi restando gli obblighi di cui al precedente punto 6.1 in capo al Fornitore, il Committente riconosce e accetta che, nella fruizione dei Servizi, rimane responsabilità esclusiva del Committente 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 Committente 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 Committente si impegna altresì ad adottare tutte le misure idonee per proteggere le credenziali di autenticazione, i sistemi e i dispositivi utilizzati dal Committente 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 Committente, 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 Committente o presso fornitori del Committente).

6.3. VIOLAZIONI DI SICUREZZA – Fatta eccezione per il caso di Contratti aventi ad oggetto prodotti installati presso il Committente o presso fornitori del Committente 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 Committente 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 Committente, 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 Committente per la gestione della Violazione di Sicurezza;

6.3.4. considererà informazioni confidenziali ai sensi di quanto previsto nel Contratto, le informazioni attinenti le 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 Committente 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 Committente 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 Committente sia un Responsabile del Trattamento) e, se il Committente 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 Committente 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 Committente.

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:

7.2.1. farà in modo che il Responsabile Ulteriore del trattamento stipuli le clausole contrattuali tipo previste nella Decisione della Commissione europea 2010/87/UE, del 5 febbraio 2010, per il trasferimento di dati personali a incaricati del trattamento stabiliti in paesi terzi (le "Clausole Contrattuali Tipo"), o loro equivalente, se modificate nel tempo. Copia delle Clausole Contrattuali Tipo sottoscritte dal Fornitore per conto del Committente saranno rese disponibili al Committente; e/o

7.2.2. potrà proporre al Committente altre modalità di trasferimento dei Dati Personali conformi a quanto previsto dalla Legislazione in materia di Protezione dei Dati Personali (es. Privacy Shield in caso di Responsabili Ulteriori del trattamento situati negli Stati Uniti e per cui sia verificabile l'aderenza tramite i canali e registri ufficiali, o trasferimenti infragruppo del Responsabile Ulteriore

del Trattamento che sia parte di un gruppo societario che ha ottenuto l'approvazione delle BCR per i Responsabili del trattamento).

7.3. Nei casi di cui al precedente punto 7.2.1 con il presente Accordo il Committente conferisce espressamente mandato al Fornitore a sottoscrivere le Clausole Contrattuali Tipo con i Responsabili Ulteriori del Trattamento riportati nei relativi DPA – Condizioni Particolari. Qualora Titolare del trattamento sia l'Utente Finale, il Committente si impegna a informare l'Utente Finale di tale trasferimento e dichiara che l'autorizzazione ad avvalersi del Responsabile Ulteriore del Trattamento situato fuori dallo SEE equivale al mandato di cui sopra.

8. VERIFICHE E CONTROLLI

8.1. Il Fornitore sottopone ad audit periodici la sicurezza dei sistemi e degli ambienti di elaborazione dei Dati Personali dallo stesso utilizzati per l'erogazione dei Servizi e le sedi in cui avviene tale trattamento. Il Fornitore avrà la facoltà di incaricare dei professionisti indipendenti selezionati dal Fornitore per lo svolgimento di audit secondo standard internazionali e/o best practice, i cui esiti saranno riportati in specifici report ("Report"). Tali Report, che costituiscono informazioni confidenziali del Fornitore, potranno essere resi disponibili al Committente 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 Committente concorda che il proprio diritto di verifica sarà esercitato attraverso la verifica dei Report messi a disposizione del Fornitore.

8.3. Il Fornitore riconosce il diritto del Committente, 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 Committente 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 8.3 il Committente 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 Committente 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 Committente 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 Committente 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 Committente sarà tenuto a nominare altri revisori o a condurre le verifiche in proprio.

8.6. Il Committente si impegna a corrispondere al Fornitore gli eventuali costi calcolati dal Fornitore e comunicati al Committente nella fase di cui al precedente punto 8.4, con le modalità e nei tempi ivi concordati. Restano a carico esclusivo del Committente 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 Committente o presso fornitori del Committente.

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 Committente e coopererà nei modi di seguito indicati al fine di consentire al Committente 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 Committente o all'Utente Finale, nel caso in cui quest'ultimo sia il Titolare del Trattamento. In tali casi il Fornitore informerà tempestivamente il Committente del ricevimento della Richiesta mediante invio di Email di notifica e fornirà al Committente 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 Committente gestire eventuali reclami in via diretta e garantire che il punto di contatto per l'esercizio dei diritti da parte degli Interessati sia il Committente stesso, o l'Utente Finale se Titolare del Trattamento. Sarà responsabilità del Committente, 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 Committente, 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 Committente 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 Committente nel rendere disponibili informazioni utili per consentire al Committente 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 Committente. Resta inteso che è responsabilità e onere esclusivo del Committente, 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 Committente, 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, ivi inclusi i requisiti previsti dalla Legislazione in materia di protezione dei dati personali.

9.7. Il Committente 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 Committente 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 Committente o presso fornitori del Committente.

10. OBBLIGHI DEL COMMITTENTE E LIMITAZIONI

10.1. Il Committente 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 Committente 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 Committente 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 Committente dichiara di aver valutato il prodotto e che esso risponde alle esigenze del Committente. Resta altresì a carico del Committente 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 Committente 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 Committente mantenere l'account collegato all'Email di notifica, attivo ed aggiornato.

10.7. Il Committente 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 Committente 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 Committente 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 Committente 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 Committente 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 Committente. In tal caso, il Committente 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 Committente, 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 Committente 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 27018:2014 per la protezione dei dati personali nei servizi Public Cloud. Autorizzazione accessi logici – Il Fornitore definisce i profili di accesso all'infrastruttura 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. 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. 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.

Misure di sicurezza tecniche	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. 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 sono sono dotate di default di sistemi Antivirus/Antimalware/WebReputation preconfigurati a livello infrastrutturale, aggiornati con cadenza periodica. Resta inteso che, coerentemente con il modello di servizio iaas ed in conformità alle condizioni generali di Contratto, è onere il Cliente 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. 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 e per i 60 giorni successivi al termine dello 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. Firewall, IDS/IPS - L'infrastruttura cloud che ospita le VM è dotata di sistemi anti-intrusione, quali Firewall, nonché da sistema di protezione del traffico AntiDDOS. 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 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. Alta affidabilità – il Fornitore garantisce l'alta affidabilità nei seguenti termini: L'architettura di rete è disegnata per proteggere i sistemi che erogano il servizio IaaS da Internet mediante l'utilizzo di un Firewall perimetrale e sistemi anti DDOS; l'architettura di rete è disegnata per proteggere le VM dei clienti IaaS da Internet attraverso l'utilizzo di una coppia di Firewall. Le VM dei clienti IaaS sono segregate le une dalle altre attraverso sistemi di microsegmentazione fornite dall'Hypervisor. 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.

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.