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

ACCORDO PRINCIPALE PER IL TRATTAMENTO DI DATI PERSONALI – MASTER DATA PROCESSING AGREEMENT
(ex art. 28 del Regolamento UE 2016/679)

TRA

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

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

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

il soggetto indicato nel Contratto quale cliente (di seguito il "**Cliente**"), di

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

PREMESSO CHE

a) il Cliente ha sottoscritto uno o più contratti con il Fornitore (di seguito il "**Contratto**");
b) le Parti intendono disciplinare nel presente "*accordo principale per il trattamento dei dati personali – Master Data Processing Agreement*" (nel seguito "**MDPA**" o "**Accordo**") le condizioni e le modalità del trattamento dei dati personali eseguito dal Fornitore nell'ambito del Contratto e della erogazione delle Business Capability e 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 ciascuna Business Capability, nelle "*condizioni speciali di trattamento dei Dati Personali*" disponibili sul sito www.teamsystem.com/GDPR/DPA (di seguito "**DPA - Condizioni Speciali**") le quali costituiscono parte integrante ed essenziale del presente Accordo.

Tutto quanto sopra premessole Parti convengono quanto segue:

1. DEFINIZIONI E INTERPRETAZIONE

1.1. Le premesse costituiscono parte integrante del presente Accordo. Nell'Accordo i seguenti termini ed espressioni avranno il significato associato ad essi qui di seguito:
"Business Capability (o "BC")" significa ciascun prodotto, software, servizio o soluzione, indipendentemente dalla relativa tecnologia di erogazione (a titolo esemplificativo, modalità On-Premises, SaaS, IaaS, servizi e funzionalità basate su Sistemi di IA), reso disponibile nell'ambito dell'Ecosistema TeamSystem e messe a disposizione del Cliente. Una Business Capability può altresì essere funzionale a, o interoperare con, una o più

ulteriori Business Capability attivate dal Cliente;
"Data di Decorrenza dell'Accordo" indica la data in cui il Cliente sottoscrive o accetta il presente Accordo o, se anteriore, la data di decorrenza del Contratto a cui il presente Accordo è legato;
"Dati Personali" ha il significato di cui alla Legislazione in materia di Protezione dei Dati Personali e includerà, a titolo puramente esemplificativo, tutti i dati forniti, archiviati, inviati, ricevuti o altrimenti elaborati, o creati dal Cliente, o dall'Utente Finale attraverso l'Ecosistema TeamSystem e in relazione alla fruizione delle BC e 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 e/o PEC fornito/i dal Cliente nell'Ordine o fornito tramite altro canale ufficiale al Fornitore, a cui il Cliente intende ricevere le notifiche da parte del Fornitore;
"Istruzioni" indica le istruzioni scritte impartite dal Titolare nel presente Accordo (inclusivo dei relativi DPA – Condizioni Speciali) e, eventualmente, nel Contratto;
"Legislazione in materia di Protezione dei Dati Personali" indica il GDPR, e ogni eventuale ulteriore norma e/o regolamento sul trattamento dei dati personali emanati ai sensi del GDPR o comunque vigenti in Italia, incluso il Decreto Legislativo no. 196/2003, come modificato e integrato dal Decreto no. 101/2018, nonché ogni provvedimento vincolante che risulti emanato dalle autorità di controllo competenti in materia (es. Garante per la protezione dei dati personali) anche prima del 25 maggio 2018 e conservi efficacia vincolante;
"Ordine" significa il modulo o coupon, in formato elettronico o cartaceo, che specifica le Business Capability attivate dal Cliente e i termini e condizioni applicabili, e che costituisce parte integrante del Contratto una volta accettato da TeamSystem;
"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 i servizi di aggiornamento e sviluppo, assistenza tecnica, manutenzione e gli eventuali ulteriori servizi connessi alle Business Capability tempo per tempo pattuiti con il cliente e indicati nell'Ordine e/o descritti in eventuali allegati al Contratto;

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

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

1.2. I termini "ivi compreso/a/i/e" e "incluso/a/i/e" saranno interpretati come se fossero seguiti dall'espressione "a titolo puramente esemplificativo", così da fornire un elenco non esaustivo di esempi.

1.3. Per le finalità del presente Accordo, i termini "Interessato", "Trattamento", "Titolare del trattamento", "Responsabile del trattamento", "Trasferimento" e "Misure tecnico-organizzative adeguate" saranno interpretati in conformità alla Legislazione in materia di Protezione dei Dati Personali applicabile.

2. RUOLO DELLE PARTI

2.1. Le Parti riconoscono e convengono che il Fornitore agisce quale Responsabile del trattamento in relazione ai Dati Personali e il Cliente agisce di regola quale Titolare del trattamento dei Dati Personali.

2.2. Qualora il Cliente svolga operazioni di trattamento per conto di altro Titolare, il Cliente potrà agire come Responsabile del trattamento. In tal caso, il Cliente garantisce che le istruzioni impartite e le attività intraprese in relazione al trattamento dei Dati Personali, inclusa la nomina, da parte del Cliente, del Fornitore quale ulteriore Responsabile del trattamento derivante dalla stipulazione del presente Accordo è stata autorizzata dal relativo Titolare del trattamento e si impegna ad esibire al Fornitore, dietro sua semplice richiesta scritta, la documentazione attestante quanto sopra.

2.3. Ciascuna delle Parti si impegna a conformarsi, nel trattamento dei Dati Personali, ai rispettivi obblighi derivanti dalla Legislazione in materia di Protezione dei Dati Personali applicabile.

2.4. Il Fornitore ha nominato un Responsabile della protezione dei dati (DPO), domiciliato presso la sede di TeamSystem S.p.A., in via Sandro Pertini, 88 a Pesaro, che può essere contattato al seguente indirizzo: dpo@teamsystem.com o al numero 0721/42661.

3. TRATTAMENTO DEI DATI PERSONALI

3.1. Con la stipulazione del presente Accordo (inclusivo di ciascun DPA - Condizioni Speciali applicabile), il Cliente affida al Fornitore l'incarico di trattare i Dati Personali ai fini

dell'erogazione delle Business Capability attivate e dei Servizi, così come meglio dettagliato nel Contratto e nei DPA – Condizioni Speciali; i DPA – Condizioni Speciali sono disponibili tramite link al seguente indirizzo www.teamsystem.com/GDPR/DPA.

3.2. Il Fornitore si impegna a conformarsi alle Istruzioni, fermo restando che, qualora il Cliente richieda variazioni rispetto alle Istruzioni iniziali, il Fornitore valuterà gli aspetti di fattibilità e concorderà con il Cliente le predette variazioni ed i costi connessi.

3.3. Nei casi di cui all'art. 3.2 e in caso di richieste del Cliente che comportino il trattamento di Dati Personali che siano, ad avviso del Fornitore, in violazione della Legislazione in materia di Protezione dei Dati Personali, il Fornitore è autorizzato ad astenersi dall'eseguire tali Istruzioni e ne informerà prontamente il Cliente. In tali casi il Cliente potrà valutare eventuali variazioni alle Istruzioni impartite o contattare l'Autorità di controllo per verificare la liceità delle richieste avanzate.

4. LIMITAZIONI ALL'UTILIZZO DEI DATI PERSONALI

4.1. Nell'eseguire il trattamento dei Dati Personali ai fini dell'erogazione delle BC e 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 le Business Capability e i Servizi o per adempiere opportunamente i propri obblighi, previsti dal Contratto e dal presente Accordo ovvero imposti dalla legge o da un organo di vigilanza o controllo competente, ovvero da specifiche richieste del Cliente e/o dell'Utente Finale. In tale ultima circostanza il Fornitore ne informerà il Cliente (salvo il caso in cui ciò sia vietato dalla legge per ragioni di pubblico interesse) mediante comunicazione trasmessa all'Email di notifica;

4.1.2. in conformità alle Istruzioni del Cliente.

4.2 Il Personale del Fornitore che accede, o comunque tratta i Dati Personali, è preposto al trattamento di tali dati sulla base di idonee autorizzazioni e ha ricevuto la necessaria formazione anche in merito al trattamento dei dati personali. Tale personale è altresì vincolato da obblighi di riservatezza e dal Codice Etico aziendale e deve attenersi alle policy di riservatezza e di protezione dei dati personali adottate dal Fornitore.

5. AFFIDAMENTO A TERZI

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

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

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

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

5.1.4. Nei casi in cui il Fornitore ricorra a Responsabili Ulteriori del Trattamento per l'esecuzione di specifiche attività di trattamento dei Dati Personali, il Fornitore:

5.1.4.1. si impegna ad avvalersi di Responsabili Ulteriori del Trattamento che garantiscono misure tecniche e organizzative adeguate e garantisce che l'accesso ai Dati Personali, e il relativo trattamento, sarà effettuato esclusivamente nei limiti di quanto necessario per l'erogazione delle BC e dei servizi subappaltati;

5.1.4.2. almeno 15 (quindici) giorni prima della data di avvio delle operazioni di trattamento dei Dati Personali da parte del Responsabile Ulteriore del Trattamento informa il Cliente dell'affidamento al terzo (nonché dei dati identificativi del terzo, della sua ubicazione – ed eventualmente, dell'ubicazione dei server sui quali saranno conservati i dati, se applicabile - e delle attività affidate) mediante invio di Email di notifica o altro mezzo ritenuto idoneo dal Fornitore. Il Cliente potrà recedere dal Contratto entro 15 (quindici) giorni dal ricevimento della comunicazione, fermo restando l'obbligo di corrispondere al Fornitore gli importi dovuti alla data di cessazione del Contratto.

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

6. DISPOSIZIONI IN MATERIA DI SICUREZZA

6.1. *MISURE DI SICUREZZA DEL FORNITORE* – Nell'eseguire il trattamento dei Dati Personali ai fini dell'erogazione delle BC e 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 dell'Ecosistema TeamSystem del Fornitore, nonché misure per consentire il tempestivo ripristino degli accessi ai Dati Personali in caso di Violazione della Sicurezza dei Dati Personali, e misure per testare l'efficacia nel tempo di dette misure. Il Cliente dà atto ed accetta che, tenuto conto dello stato dell'arte, dei costi

di implementazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità di trattamento dei Dati Personali, le procedure e i criteri di sicurezza implementati dal Fornitore garantiscono un livello di protezione adeguato al rischio per quanto riguarda i suoi Dati Personali.

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

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

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

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

6.1.4.2. conformandosi agli obblighi di cui al punto 6.3.

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

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

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

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

6.2.2. Il Cliente si impegna altresì ad adottare tutte le misure idonee per proteggere le credenziali di autenticazione, i sistemi e i dispositivi utilizzati dal Cliente o dai fruitori presso l'Utente Finale per accedere all'Ecosistema TeamSystem e fruire

delle Business Capability e dei Servizi, e per effettuare i salvataggi e backup dei Dati Personali al fine di garantire il ripristino dei Dati Personali nel rispetto delle norme di legge.

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

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

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

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

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

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

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

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

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

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

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

7.2. Se, ai fini della conservazione o del trattamento dei Dati Personali da parte di un Responsabile Ulteriore del trattamento, è necessario effettuare il trasferimento dei Dati Personali fuori dallo SEE in un paese che non gode di una decisione di adeguatezza da parte della Commissione Europea ai sensi dell'art. 45 del GDPR, il Fornitore potrà adottare altre modalità di trasferimento dei Dati Personali conformi a quanto previsto dalla Legislazione in materia di Protezione dei Dati Personali, anche alla luce delle indicazioni fornite dalla Corte di Giustizia della Unione Europea nella causa C-311/18 e dal Comitato Europeo per la Protezione dei dati ("**EDPB**") nelle "Raccomandazioni 01/2020 sulle misure che integrano gli strumenti di trasferimento per garantire il rispetto del livello di protezione dei dati personali nell'UE" e nelle "Raccomandazioni 2/2020 relative alle garanzie essenziali europee per le misure di sorveglianza".

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

7.4. Qualora Titolare del trattamento sia l'Utente Finale, il Cliente si impegna a informare l'Utente Finale di tale trasferimento e dichiara che l'autorizzazione ad avvalersi del Responsabile Ulteriore del Trattamento situato fuori dallo SEE equivale al mandato di cui sopra. Parimenti, nel caso in cui il trasferimento dei Dati Personali al di fuori dello SEE sia subordinato alla attivazione da parte dell'Utente Finale di specifiche funzionalità delle Business Capability, l'attivazione di detta funzionalità equivale al mandato di cui sopra.

8. VERIFICHE E CONTROLLI

8.1. Il Fornitore sottopone ad audit periodici la sicurezza dei sistemi e degli ambienti di elaborazione dei Dati Personali dallo stesso utilizzati per l'erogazione dele Business Capability e dei Servizi e le sedi in cui avviene tale trattamento. Il Fornitore avrà la facoltà di incaricare dei professionisti indipendenti selezionati dal Fornitore per lo svolgimento di audit secondo standard internazionali e/o *best practice*, i cui esiti saranno riportati in specifici report ("**Report**"). Tali Report, che costituiscono informazioni confidenziali del Fornitore, potranno essere resi disponibili al Cliente per consentirgli di verificare la conformità del Fornitore agli obblighi di sicurezza di cui al presente Accordo.

8.2. Nei casi previsti dall'art. 8.1, il Cliente concorda che il proprio diritto di verifica sarà esercitato attraverso la verifica dei Report messi a disposizione dal Fornitore.

8.3. Il Fornitore riconosce il diritto del Cliente, con le modalità e nei limiti di seguito indicati, ad effettuare audit indipendenti per verificare la conformità del Fornitore agli obblighi previsti nel presente Accordo e nei rispettivi DPA – Condizioni Speciali, e di quanto previsto dalla normativa. Il Cliente potrà avvalersi per tali attività di proprio personale specializzato o di revisori esterni, purché tali soggetti siano previamente vincolati da idonei impegni alla riservatezza.

8.4. Nel caso di cui al precedente punto 8.2, il Cliente dovrà previamente inviare richiesta scritta al Responsabile della Protezione dei Dati (DPO) del Fornitore. Successivamente alla richiesta di audit o ispezione il Fornitore e il Cliente concorderanno, prima dell'avvio delle attività, i dettagli di tali verifiche (data di inizio e durata), le tipologie di controllo e l'oggetto delle verifiche, i vincoli di riservatezza a cui devono essere vincolati il Cliente e coloro che effettuano le verifiche e i costi che il Fornitore potrà addebitare per tali verifiche e che saranno determinati in relazione all'estensione e alla durata delle attività di verifica.

8.5. Il Fornitore potrà opporsi per iscritto alla nomina da parte del Cliente di eventuali revisori esterni che siano, ad insindacabile giudizio del Fornitore, non adeguatamente qualificati o indipendenti, siano concorrenti del Fornitore o che siano evidentemente inadeguati. In tali circostanze il Cliente sarà tenuto a nominare altri revisori o a condurre le verifiche in proprio.

8.6. Il Cliente si impegna a corrispondere al Fornitore gli eventuali costi calcolati dal Fornitore e comunicati al Cliente nella fase di cui al precedente punto 8.4, con le modalità e nei tempi ivi concordati. Restano a carico esclusivo del Cliente i costi delle attività di verifica dallo stesso commissionate a terzi.

8.7. Resta fermo quanto previsto in relazione ai diritti di ispezione del Titolare del trattamento e delle autorità nelle Clausole Contrattuali Tipo eventualmente sottoscritte ai sensi del precedente punto 7, che non potranno considerarsi modificate da alcuna delle previsioni contenute nel presente Accordo o nei relativi DPA – Condizioni Speciali.

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

8.9. Le attività di verifica che interessino eventuali Responsabili Ulteriori dovranno essere svolte nel rispetto delle regole di accesso e delle politiche di sicurezza dei Responsabili Ulteriori.

9. ASSISTENZA A FINI DI CONFORMITÀ

9.1. Il Fornitore presterà assistenza al Cliente e coopererà nei modi di seguito indicati al fine di consentire al Cliente il rispetto degli obblighi previsti dalla Legislazione in materia di Protezione dei Dati Personali.

9.2. Qualora il Fornitore riceva Richieste o reclami da un Interessato in relazione ai Dati

Personali, il Fornitore raccomanderà all'Interessato di rivolgersi al Cliente o all'Utente Finale, nel caso in cui quest'ultimo sia il Titolare del Trattamento. In tali casi il Fornitore informerà tempestivamente il Cliente del ricevimento della Richiesta mediante invio di Email di notifica e fornirà al Cliente le informazioni ad esso disponibili unitamente a copia della Richiesta o del reclamo. Resta inteso che tale attività di cooperazione sarà svolta in via eccezionale, in quanto la gestione dei rapporti con gli Interessati resta esclusa da quanto oggetto del Contratto ed è responsabilità del Cliente gestire eventuali reclami in via diretta e garantire che il punto di contatto per l'esercizio dei diritti da parte degli Interessati sia il Cliente stesso, o l'Utente Finale se Titolare del Trattamento. Sarà responsabilità del Cliente, o dell'Utente Finale qualora questi sia Titolare del Trattamento, provvedere a dar seguito a tali Richieste o reclami.

9.3. Il Fornitore provvederà a informare tempestivamente il Cliente, salvo il caso in cui ciò sia vietato dalla legge, con avviso all'Email di notifica di eventuali ispezioni o richieste di informazioni presentate da autorità di controllo e forze di polizia rispetto a profili che riguardano il trattamento dei Dati Personali.

9.4. Qualora, ai fini dell'evasione delle Richieste di cui ai precedenti punti, il Cliente abbia necessità di ricevere informazioni dal Fornitore circa il trattamento dei Dati Personali, il Fornitore presterà la necessaria assistenza nei limiti di quanto ragionevolmente possibile, a condizione che tali richieste siano presentate con congruo preavviso.

9.5. Il Fornitore, tenuto conto della natura dei Dati Personali e delle informazioni ad esso disponibili, fornirà ragionevole assistenza al Cliente nel rendere disponibili informazioni utili per consentire al Cliente l'effettuazione di valutazioni di impatto sulla protezione dei Dati Personali nei casi previsti dalla legge. In tal caso il Fornitore renderà disponibili informazioni di carattere generale in base alle Business Capability attivate, quali le informazioni contenute nel Contratto, nel presente Accordo e nei DPA - Condizioni Particolari relativi alle Business Capability interessate. Eventuali richieste di assistenza personalizzate potranno essere soggette al pagamento di un corrispettivo da parte del Cliente. Resta inteso che è responsabilità e onere esclusivo del Cliente, o dell'Utente Finale se Titolare del trattamento, procedere alla valutazione di impatto in base alle caratteristiche del trattamento dei Dati Personali dallo stesso posto in essere.

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

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

previsto dalla Legislazione in materia di Protezione dei Dati Personali.

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

10. OBBLIGHI DEL CLIENTE E LIMITAZIONI

10.1. Il Cliente si impegna a impartire Istruzioni conformi alla normativa e a utilizzare le Business Capability e i Servizi in modo conforme alla Legislazione in materia di Protezione dei Dati Personali e solo per trattare Dati Personali che siano stati raccolti in conformità alla Legislazione in materia di Protezione dei Dati Personali.

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

10.3. Il Cliente si impegna ad assolvere a tutti gli obblighi posti in capo al Titolare del Trattamento (e, nei casi in cui tali obblighi sono in capo all'Utente Finale, garantisce che analoghi obblighi sono imposti a carico dell'Utente Finale) dalla Legislazione in materia di Protezione dei Dati Personali, ivi inclusi gli obblighi di informativa nei confronti degli Interessati. Il Cliente si impegna inoltre a garantire che il trattamento dei Dati Personali effettuato mediante l'utilizzo delle Business Capability e dei Servizi avvenga solo in presenza di idonea base giuridica.

10.4. Qualora il rilascio dell'informativa e l'ottenimento del consenso debbano avvenire per il tramite del prodotto oggetto del Contratto, il Cliente dichiara di aver valutato il prodotto e che esso risponde alle esigenze del Cliente. Resta altresì a carico del Cliente valutare se l'eventuale modulistica resa disponibile dal Fornitore per agevolare l'assolvimento degli obblighi di informativa e consenso (es. modello di privacy policy per App o informative presenti negli applicativi), quando disponibile, sia conforme alla Legislazione in materia di Protezione dei Dati Personali e adattare la stessa ove ritenuto opportuno.

10.5. E' altresì onere esclusivo del Cliente provvedere alla gestione dei Dati Personali in conformità alle Richieste avanzate dagli Interessati, e pertanto provvedere ad esempio agli eventuali aggiornamenti, integrazioni, rettifiche e cancellazioni dei Dati Personali.

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

10.7. Il Cliente prende atto che, ai sensi dell'art. 30 del GDPR, il Fornitore è tenuto a mantenere un registro delle attività di trattamento eseguite per conto dei Titolari (o Responsabili) del Trattamento e a raccogliere a tal fine i dati identificativi e di contatto di ciascun Titolare (e/o Responsabile) del Trattamento per conto del quale il Fornitore agisce e che tali informazioni devono essere rese disponibili all'autorità competente, su richiesta. Pertanto, quando richiesto, il Cliente si impegna a dare al Fornitore i dati identificativi e di contatto sopra indicati con le modalità individuate dal Fornitore nel tempo e a mantenere aggiornate tali informazioni tramite i medesimi canali.

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

11. DURATA

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

12. DISPOSIZIONI PER LA RESTITUZIONE O LA CANCELLAZIONEDEI DATI PERSONALI

12.1. Alla cessazione del Contratto, 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 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 Contratto, nei modi convenuti nel Contratto e conviene che è sua responsabilità provvedere all'estrazione totale o parziale dei soli Dati Personali che ritenga utile conservare e che tale estrazione dovrà essere effettuata prima della scadenza del termine di cui al punto 12.1.3.

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

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

13. RESPONSABILITA'

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

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

14. DISPOSIZIONI VARIE

14.1. Il presente Accordo sostituisce qualsiasi altro accordo, contratto o intesa tra le Parti con riferimento al suo oggetto nonché qualsivoglia istruzione fornita in qualsiasi forma dal Cliente al Fornitore precedentemente alla data del presente Accordo in merito ai Dati Personali trattati nell'ambito dell'esecuzione del Contratto.

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

14.3. In caso di conflitto tra le previsioni del presente Accordo e quanto previsto nel Contratto, o in documenti del Cliente non espressamente accettati dal Fornitore in deroga al presente Accordo e/o 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 Business Capability attivata:

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

A – BC 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. Il Fornitore mette a disposizione del Cliente la funzionalità di autenticazione multi-fattore (MFA) come misura di sicurezza tecnica aggiuntiva e opzionale per l'accesso al servizio. L'attivazione della MFA è a discrezione esclusiva del Cliente e fortemente raccomandata al fine di ottenere una maggiore tutela. Il Cliente è responsabile della gestione delle credenziali di accesso e dei dispositivi utilizzati per l'autenticazione multi-fattore. *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 – BC Iaas

Misure di sicurezza organizzative	*Data Center* – Il Fornitore fornisce, a seconda dei casi e delle specifiche pattuizioni contrattuali, le BC IaaS tramite i seguenti Data Center: - Aruba S.p.A., sito in Italia; - Microsoft Azure localizzato nelle regions West Europe e Italy North; - e TIM in Italia. Con riferimento alle misure di sicurezza fisica si prega di fare riferimento alle informazioni rese disponibili dai singoli provider, come di seguito indicate: • con riguardo ad Aruba S.p.A.: misure di sicurezza Aruba ; • con riguardo a Microsoft Azure: Sicurezza fisica dei data center di Azure • con riguardo a TIM: misure di sicurezza TIM Nei Data Center, l'ambiente di virtualizzazione (inclusa la SAN – Storage Area network) è presente su server ospitati in data center siti all'interno dell'Unione Europea, la cui gestione è demandata a fornitori certificati ISO 27001. *Certificazioni* – il Fornitore ha ottenuto le seguenti certificazioni/attestazioni: • ISO/IEC 27001: "Sicurezza delle informazioni""; • ISO/IEC 27017 "Sicurezza delle informazioni per i servizi Cloud" • ISO/IEC 27018 "Protezione dei dati personali nei servizi Public Cloud" • Per maggiori dettagli riguardo alle certificazioni ottenute dal Fornitore, si prega di fare riferimento al seguente link: Banche dati – Accredia: **Accredia banche dati** *Autorizzazione accessi logici* – Al momento della consegna delle Macchine Virtuali acquistate dal Cliente, il Fornitore consegna al Cliente le credenziali provvisorie di accesso alle stesse come Amministratore del sistema. In caso di mancata ricezione delle credenziali di accesso, è onere del Cliente attivarsi tempestivamente al fine di richiederle al Fornitore. Il Cliente ha l'obbligo di modificare le credenziali al primo accesso ed è l'unico responsabile dell'uso di tali credenziali, della gestione dei profili di accesso ed utenze e relative credenziali. Resta inteso che i profili di accesso alla macchina virtuale, aggiuntivi rispetto a quelli configurati al momento della consegna,

	devono essere definiti a cura del Cliente, sulla base delle proprie politiche di autorizzazione. Limitatamente a quanto di propria competenza, con riguardo all'infrastruttura di virtualizzazione, il Fornitore definisce i profili di accesso nel rispetto del *least privilege* necessari all'esecuzione delle mansioni assegnate. Tali profili sono oggetto di controlli periodici finalizzati alla verifica della sussistenza delle condizioni per la conservazione dei profili attribuiti. *Utenze* – Le VM sono configurate con modalità idonee a consentirne l'accesso unicamente a soggetti dotati di credenziali di autenticazione che ne consentono la loro univoca identificazione. *Sicurezza linee di comunicazione* – Per quanto di propria competenza, limitatamente all'infrastruttura di virtualizzazione, il Fornitore adotta protocolli di comunicazione sicuri e in linea con quanto la tecnologia rende disponibile in relazione al processo di autenticazione. *Risk management* – Il Fornitore conduce periodicamente un processo di analisi e trattamento dei rischi in ambito sicurezza delle informazioni volto alla prevenzione o riduzione dei possibili effetti indesiderati che potrebbero essere causati da minacce non correttamente indirizzate. *Change Management* – Per quanto di propria competenza, il Fornitore ha in essere una specifica procedura attraverso la quale regolamenta il processo di Change Management in considerazione dell'introduzione di eventuali innovazioni tecnologiche o cambiamenti della propria impostazione e della propria struttura organizzativa. Il Cliente è direttamente responsabile per procedure ed operazioni di Change Management aventi ad oggetto le Macchine Virtuali acquistate. *Formazione*: Il Fornitore eroga periodicamente ai propri dipendenti coinvolti nelle attività di trattamento corsi di formazione in ambito Information Security, Privacy & Data Protection e Cyber Security. *Protection from malware* – Le VM con sistema operativo Windows sono dotate di default di sistemi Antivirus/Antimalware nativi, la cui manutenzione e aggiornamento è onere e responsabilità del Cliente, coerentemente con il modello di servizio Iaas e con le condizioni generali di contratto. Resta, al riguardo, inteso che il Cliente è tenuto a valutare la congruità di tali soluzioni e la necessità di adottare, a propria cura e spese, sistemi di sicurezza e protezione ulteriori in base all'effettivo utilizzo della Macchina Virtuale ed alle proprie politiche di gestione dei rischi, nonché provvedere alla verifica periodica dell'effettivo aggiornamento dei predetti sistemi e – nel caso di fallimento di eventuali aggiornamenti automatici – di provvedere all'aggiornamento manuale dei sistemi di protezione qui descritti. *Backup & Restore* – Sono adottate idonee misure per garantire il back up dei dati ed il ripristino degli stessi in caso di danneggiamento o perdita, in conformità con le previsioni del Contratto. In tali evenienze,

	è previsto che il *restore* sia eseguito attraverso il ripristino dell'ultima copia di back up disponibile anteriormente al danneggiamento. È comunque demandata al Titolare del trattamento la facoltà di eseguire autonomamente il backup dei propri dati per l'intera durata del contratto, fermo restando la possibilità di ricevere, tramite richiesta al servizio di assistenza clienti, copia dei dati entro il termine di 60 giorni successivi al termine del contratto stesso. *Logging* – La piattaforma di virtualizzazione e la relativa consolle sono dotate di misure di tracciamento degli accessi e, ove appropriato, delle attività svolte in capo alle diverse tipologie di utenze (Amministratore, Super Utente, etc.) protetti da adeguate misure di sicurezza che ne garantiscono l'integrità. E' onere del Cliente adottare, se lo desidera, strumenti di logging delle attività svolte all'interno delle Macchine Virtuali diversi ed ulteriori a quelli forniti dal Sistema Operativo o singola applicazione installata nelle Macchine Virtuali. *Network & Security* - L'infrastruttura cloud che ospita le VM è dotata di sistemi di protezione, quali Firewall, nonché da sistema di protezione del traffico AntiDDOS dedicati alla protezione dell'intera infrastruttura (Region/data center). Resta inteso che, coerentemente con il modello di servizio Iaas ed in conformità alle Condizioni Generali di Contratto, il Cliente ha l'onere di proteggere con adeguati sistemi di sicurezza e protezione, inclusi eventuali sistemi AntiDDOS, la propria Macchina Virtuale. *Business Continuity & Disaster Recovery* – Il Cliente è responsabile dell'implementazione e gestione dei piani di Business Continuity e Disaster Recovery, salvo diverse pattuizioni a livello contrattuale. Ove gli accordi contrattuali lo prevedono, è posto in essere un piano di continuità operativa, integrato, ove necessario, con il piano di disaster recovery. Ciò garantisce la disponibilità e l'accesso ai sistemi anche nel caso di eventi negativi di portata rilevante che dovessero perdurare nel tempo. *Incident Management*– Per quanto di propria competenza, il Fornitore ha in essere una specifica procedura di Incident Management allo scopo di garantire il ripristino delle normali operazioni di servizio nel più breve tempo possibile in conformità a quanto previsto dal Contratto. E' onere del Cliente dotarsi di procedure di Incident Management per incidenti inerenti alla gestione delle Macchine Virtuali acquistate. *Attività di manutenzione sistemistica* – Nel caso il Cliente non abbia attivo un contratto di Manutenzione Sistemistica con il Fornitore, tutte le relative attività saranno di esclusivo onere e responsabilità del Cliente (tra cui, ad es. l'aggiornamento periodico delle patch di sicurezza, l'attivazione/creazione delle utenze user e amministrative

	della Macchina Virtuale, il monitoraggio degli indicatori di performance della Macchina Virtuale, etc.).

C – BUSINESS PROCESS OUTSOURCING (BPO)

Misure di sicurezza organizzative	*Certificazioni* – Il Fornitore ha ottenuto le seguenti certificazioni/attestazioni: • ISO/IEC 27001: "Sicurezza delle informazioni" • ISO/IEC 27017: "Sicurezza delle informazioni per i servizi Cloud" • ISO/IEC 27018: per la protezione dei dati personali nei servizi Public Cloud. • Per maggiori dettagli riguardo alle certificazioni ottenute dal Fornitore, si prega di fare riferimento al seguente link: Banche dati – Accredia: **Accredia Banche dati** *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 - la 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 – BC 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.

MASTER DATA PROCESSING AGREEMENT

Version 8 dated 6 July 2026

MASTER DATA PROCESSING AGREEMENT
(pursuant to Article 28 of Regulation EU 2016/679)

BETWEEN

This agreement for the protection of personal data is entered into between the Provider, as indicated below, and the client, which accepts this agreement. "**Provider**" refers to one or more of the following parties:

(i) TeamSystem S.p.A., with registered office in Pesaro (PU), via Sandro Pertini 88, tax identification and VAT number 01035310414; and/or

(ii) the company belonging to the group headed by TeamSystem whose name is indicated in the Agreement;

AND

the party referred to in the Agreement as the client (hereinafter the "**Client**"),

hereinafter collectively referred to as the "**Parties**" or individually as the "**Party**"

WHEREAS

a) The Client has entered into one or more agreements with the Provider ("**Agreement**");
b) In this "Master Data Processing Agreement" ("**MDPA**" or "**Master Agreement**") the Parties intend to establish the terms, conditions and methods according to which the Provider will process personal data in connection with the Agreement and the provision of the Business Capabilities and the Services, as well as the obligations relating to such processing, including the Provider's duties as the Data Processor under Article 28 of General Data Protection Regulation No. 679 of 27 April 2016 (the "**GDPR**");
c) The specific characteristics of the processing of the Personal Data for each Business Capability are detailed in the "Special Terms and Conditions for the Processing of Personal Data" available at www.teamsystem.com/GDPR/DPA (the "**DPA - Special Terms**") which are incorporated into this Agreement by this reference.

Now therefore, the Parties agree to the following:

1. DEFINITIONS AND INTERPRETATION

1.1. The above preliminary provisions are incorporated into this MDPA by this reference. As used in this MDPA the following words and expressions shall have the meanings set forth below:

"Adequacy Decision" means a decision of the European Commission, based on Article 45(3) of the GDPR, assessing that the laws of a certain country ensure an adequate level of protection, as required by the Applicable Data Protection Law.

"Applicable Data Protection Law" means the GDPR and any other law and/or regulation regarding the processing of personal data issued pursuant to the GDPR or that is in any case in force in Italy, including Legislative Decree No. 196/2003 as

amended and supplemented by Decree No. 101/2018, as well as any binding decision issued by the competent authorities (e.g. the "Garante", the Italian Personal Data Protection Authority), even before 25 May 2018, which remains binding and enforceable.

"Business Capability" (or "BC") means each product, software, service or solution, regardless of the technology through which it is delivered (by way of example, On-Premises, SaaS, IaaS, services and functionalities based on AI Systems), made available within the TeamSystem Ecosystem and provided to the Client. A Business Capability may also be functional to, or interoperate with, one or more further Business Capabilities activated by the Client.

"Business Days" means every calendar day other than a Saturday, Sunday and a day when the banks in Milan are not generally open for business.

"Data Sub-Processor" means any sub-contractor engaged by the Provider to perform any of its contractual obligations and which, during such performance, may be required to collect, access, receive, store or otherwise process the Personal Data.

"**Email Address**" means the email and/or certified email (PEC) address (or addresses) provided to the Provider by the Client in the Order or using another official means. It is the address where the Client wishes to receive notices from the Provider.

"**End User**" means the final user of the Business Capability, acting as Data Controller.

"Instructions" means the written instructions given by the Controller in this MDPA (including the relevant DPA – Special Terms) and, where applicable, in the Agreement.

"MDPA Effective Date" means the date when the Client signs or accepts this MDPA or, if earlier, the effective date of the Agreement to which this MDPA is connected.

"Order" means the form or coupon, in electronic or paper format, specifying the Business Capabilities activated by the Client and the applicable terms and conditions, and which forms an integral part of the Agreement once accepted by TeamSystem.

"**Personal Data**" has the meaning construed according to the Applicable Data Protection Law, whereby Personal Data include, without limitation, all data provided, stored, transmitted, received or otherwise processed or created by the Client or by the End User through the TeamSystem Ecosystem and in relation to the use of the BCs and the Services, to the extent that they are processed by the Provider under the Agreement. A list of the categories of Personal Data is included in the DPA – Special Terms.

"**Personal Data Breach**" means any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, the Personal Data that occurs in the systems operated by the Provider or that are in any case under its control.

"Personnel of the Provider" means the managers, employees, consultants and other personnel of the Provider, not including the personnel of any Data Sub-Processor.

"Request" means a request lodged by a Data Subject for access to or erasure or rectification of the Personal Data or for the exercise of another right laid down in the GDPR.

"Service(s)" means the updating and development, technical support and maintenance services and any further services connected to the Business Capabilities agreed from time to time with the Client and indicated in the Order and/or described in any exhibits to the Agreement.

1.2. The words "including" and "included" shall be construed as if they were accompanied by the expression "without limitation" so that any list that follows any of these words will consequently be composed of mere examples and will not be exhaustive.

1.3. For the purposes of this MDPA, the terms "Data Subject", "Processing", "Data Controller", "Data Processor", "Transfer" and "Appropriate Technical and Organizational Measures" shall be construed in compliance with the Applicable Data Protection Law.

2. ROLES OF THE PARTIES

2.1. The Parties acknowledge and agree that, in relation to the processing of the Personal Data, the Provider acts as the Data Processor and, as a general rule, the Client acts as the Data Controller.

2.2. If the Client is carrying out the processing on behalf of another Data Controller, the same Client may act as a Data Processor. In such event, the Client hereby warrants that all instructions given and activities carried out in relation to the processing of the Personal Data, including the Client's appointment of the Provider as a Data Sub-Processor, in connection with the execution of this MDPA, have been authorized by the relevant Data Controller and undertakes to show the Provider, upon its written request, the documentation attesting to the above.

2.3. In the processing of the Personal Data, each Party undertakes to comply with its obligations under the Applicable Data Protection Law.

2.4. The Provider has designated a Data Protection Officer (DPO) domiciled at the offices of TeamSystem S.p.A. in Pesaro, via Sandro Pertini, 88, who may be contacted by email at dpo@teamsystem.com or by telephone at +39 0721/42661.

3. PROCESSING OF PERSONAL DATA

3.1. By entering into this MDPA (and into any incorporated DPA – Special Terms), the Client entrusts the Provider with the processing of the Personal Data for the purposes of providing the activated Business Capabilities and the Services, as detailed in the

Agreement and in the DPA – Special Terms. The DPA – Special Terms are available through a link on the following website: www.teamsystem.com/GDPR/DPA.

3.2. The Provider hereby undertakes to comply with the Instructions, provided that, should the Client request changes to any initially given Instructions, the Provider shall examine the feasibility of the requested changes and agree with the Client such changes and the associated costs.

3.3. In the cases contemplated in paragraph 3.2 and if the Client's requests lead to the Personal Data processing infringing, in the opinion of the Provider, the Applicable Data Protection Law, the Provider is authorized to refrain from performing such Instructions and shall promptly inform the Client. In such case, the Client may decide whether to amend the Instructions given or to contact the Supervisory Authority to verify whether the requests are lawful.

4. RESTRICTIONS TO THE USE OF PERSONAL DATA

4.1. In the processing of Personal Data for the purposes of providing the BCs and the Services, the Provider undertakes to carry out such processing:

4.1.1. only to the extent and according to methods that are necessary for the provision of the Business Capabilities and the Services or to properly perform its obligations under the Agreement and this MDPA, that are laid down by the law or by a competent supervisory or control authority, or that arise from specific requests made by the Client and/or by the End User. In this last case, the Provider shall inform the Client (unless prevented from doing so by the law out of concern for the public interest) by sending a notice to the Email Address;

4.1.2. in accordance with the Client's Instructions.

4.2 The Personnel of the Provider with access to, or in any case processing, the Personal Data is entrusted with the processing of such data based on appropriate authorizations and has received the necessary training with respect to such processing. Furthermore, this personnel is bound to comply with confidentiality obligations and the company's Code of Ethics and must abide by the Provider's confidentiality and personal data protection policies.

5. PROCESSING ACTIVITIES ENTRUSTED TO THIRD PARTIES

5.1. With respect to the processing activities entrusted to Data Sub-Processors, the Parties agree as follows:

5.1.1. The Client expressly agrees that the Provider may entrust certain processing operations in relation to the Personal Data to other companies belonging to the TeamSystem group and/or to third parties specified in the DPA – Special Terms.

5.1.2. The Client further agrees that the Provider may entrust certain processing operations in relation to the Personal Data to other third parties, in accordance with paragraph 5.1.4.

5.1.3. The Parties agree that if the Client signs the Standard Contractual Clauses (as required by paragraph 7 for the transfer of the Personal Data abroad) with a Data Sub-Processor, this shall be deemed as consent to engaging that party for the processing operations.

5.1.4. In those cases when the Provider uses Data Sub-Processors for the performance of specific processing activities in relation to the Personal Data, the Provider:

5.1.4.1. undertakes to engage Data Sub-Processors that guarantee adequate technical and organizational measures and ensure that the access to Personal Data, and the related processing, shall be limited to only necessary for the provision of the BCs and the sub-contracted services.

5.1.4.2. shall inform the Client that it has engaged a Data Sub-Processor at least 15 (fifteen) days before the start of the processing operations on the Personal Data by such Data Sub-Processor (and such notice shall include information identifying the third party, its location and, if applicable, the location of the servers where the data will be stored and, if applicable, where the entrusted activities will be carried out) by writing to the Email Address or using another means as deemed appropriate by the Provider. The Client shall be entitled to withdraw from the Agreement within 15 (fifteen) days from receipt of the notice, without prejudice to its obligation to pay any amounts due to the Provider at the date of termination of the Agreement.

5.1.5. Additional information concerning the list of Data Sub-Processors, the processing activities entrusted to such parties and the place where they are located shall be indicated in the DPA – Special Terms relating to the Services activated by the Client.

6. SECURITY

6.1. *PROVIDER'S SECURITY MEASURES* – When processing the Personal Data for the purposes of providing the BCs and the Services, the Provider undertakes to implement appropriate technical and organizational measures to prevent unlawful or unauthorized processing, accidental or unlawful corruption, damage, accidental loss, alteration and unauthorized disclosure of, or access to, the Personal Data, as described in Exhibit 1 to this MDPA ("**Security Measures**").

6.1.1. Exhibit 1 to the MDPA sets forth appropriate measures for the protection of data files. These measures are proportionate to the risk level of the Personal Data and are aimed at ensuring the confidentiality, integrity, availability and resilience of

the Provider's systems and the TeamSystem Ecosystem. Exhibit 1 also contains measures for the rapid restoration of access to the Personal Data in the event of a Personal Data Breach and measures for testing the effectiveness of such measures over time. The Client acknowledges and agrees that, considering the state of the art, the implementation costs and the nature, scope, context and purposes of the Personal Data processing, the security procedures and principles that have been adopted by the Provider ensure a level of protection that is appropriate to the risk in relation to the Personal Data.

6.1.2. The Provider may update and change the Security Measures indicated above over time, provided that such updates and changes do not reduce the overall level of security of the TeamSystem Ecosystem and the BCs. The Client shall be informed of any such updates and changes by notice sent to the Email Address.

6.1.3. If the Client requests additional security measures beyond the Security Measures, the Provider reserves the right to assess the feasibility of such additional security measures and may charge the Client for additional implementation costs.

6.1.4. The Client acknowledges and agrees that the Provider, considering the nature of the Personal Data and the information available to the Provider based on that specifically set out in the relevant DPA – Special Terms, shall assist the Client in ensuring compliance with the security obligations pursuant to Articles 32 to 34 of the GDPR as follows:

6.1.4.1. implementing and updating the Security Measures in accordance with the provisions of paragraphs 6.1.1, 6.1.2 and 6.1.3;

6.1.4.2. complying with the obligations specified in paragraph 6.3.

6.1.5. The Parties agree that, in the Agreements concerning products installed at the premises of the Client or any of its providers ("on-premises products"), the Security Measures indicated above shall only apply in connection with Services that require the processing of the Personal Data by the Provider or by any of its delegated parties (e.g. remote support and assistance, migration services).

6.1.6. If the product can be integrated with third-party applications, the Provider shall not be liable for the implementation of the Security Measures in relation to the components of such third parties or for the product's operating modes consequent to such integration by the third parties.

6.2. *CLIENT'S SECURITY MEASURES* – Without prejudice to the Provider's obligations under paragraph 6.1, the Client acknowledges and agrees that, when using the BCs and the Services, it remains an exclusive duty of the Client to have its personnel and those that it has authorized to access such BCs and Services implement appropriate security measures in connection with the use of the BCs and the Services.

6.2.1. To this end, the Client undertakes to use the BCs, the Services and the features for the processing of the Personal Data always ensuring a level of security appropriate to the actual risk.

6.2.2. The Client further undertakes to implement all appropriate measures for the protection of the authentication credentials, systems and devices used by the Client or by the users of the End User to access the TeamSystem Ecosystem and use the Business Capabilities and the Services. The Client also undertakes to save and make backup copies of the Personal Data in order to ensure that they can be restored in accordance with the provisions of the law.

6.2.3. The Provider shall have no obligation and shall bear no liability for the protection of the Personal Data that the Client or the End User, if applicable, stores or transfers outside the systems used by the Provider or by the Data Sub-Processors engaged by the Provider (for example, in paper archives or data centers, as in the case of Agreements concerning on-premises products).

6.3. *DATA BREACHES* – Except for the Agreements concerning on-premises products, to which this paragraph 6.3 does not apply, the Provider, if it becomes aware of a Personal Data Breach, shall:

6.3.1. inform the Client without undue delay by notice sent to the Email Address.

6.3.2. take reasonable measures to mitigate any possible damage and protect the Personal Data.

6.3.3. provide the Client with a description of the Personal Data Breach, to the extent possible, including the measures taken to prevent or mitigate the potential risks and the activities recommended by the Provider to the Client for the management of the Personal Data Breach.

6.3.4. consider as confidential pursuant to the Agreement all information concerning any Personal Data Breaches, the related documents, communications and notices, and refrain from disclosing any data and information without the Controller's prior written consent unless strictly necessary to meet the Client's obligations arising from the Applicable Data Protection Law.

6.4. In the cases contemplated under paragraph 6.3 above, the Client shall be exclusively responsible for the performance, in the cases required by the Applicable Data Protection Law, of any obligations to inform third parties (the End User if the Client is a Data Processor) of a Personal Data Breach and, if the Client is the Data Controller, any obligations to inform the Supervisory Authority and the Data Subjects.

6.5. The Parties agree that the notification of a Personal Data Breach or the implementation of measures to manage a Personal Data Breach do not imply acknowledgement by the Provider of a breach or liability in relation to the Personal Data Breach.

6.6. The Client shall promptly inform the Provider of any misuse of the accounts or the authentication credentials or of any Personal Data Breaches of which it may have become aware in relation to the BCs and/or the Services.

7. RESTRICTIONS TO THE TRANSFER OF THE PERSONAL DATA TO COUNTRIES OUTSIDE THE EUROPEAN ECONOMIC AREA (EEA)

7.1. The Provider shall not transfer the Personal Data to countries that are outside the EEA except if agreed with the Client.

7.2. Should, for the storage or processing of the Personal Data by a Data Sub-Processor, it be necessary to transfer the Personal Data outside the EEA to a country without a decision of adequacy by the European Commission pursuant to Article 45 of the GDPR, the Provider may use other methods for the transfer of the Personal Data, provided that they are compliant with the requirements of the Applicable Data Protection Law and considering the guidance given by the Court of Justice of the European Union in Case C-311/18 and by the European Data Protection Board ("**EDPB**") in the "Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data" and the "Recommendations 02/2020 on the European Essential Guarantees for surveillance measures".

7.3. In the cases described in paragraph 7.2, with this MDPA, the Client expressly gives the Provider the authority to execute the standard contractual clauses referred to in point (c) of Article 46(2) of the GDPR for the transfer of personal data to other processors located in third countries ("**Standard Contractual Clauses**") with the Data Sub-Processors mentioned in the related DPA – Special Terms, and to adopt any further measures that may be reasonably required to allow the transfer of the personal data outside the EEA in compliance with the requirements established in the GDPR.

7.4. If the End User is the Data Controller, the Client undertakes to inform such End User of the transfer and hereby states and declares that the authorization given to use a Data Sub-Processor outside the EEA is the equivalent of the authority given above. Similarly, if the transfer of the Personal Data outside the EEA requires the activation of specific feature(s) of the Business Capabilities by the End User, the activation of such feature(s) is the equivalent of the authority given above.

8. AUDITS AND CONTROLS

8.1. The Provider shall have regular audits conducted on the security of the Personal Data processing systems and environments that it uses to provide the Business Capabilities and the Services as well as the premises where the processing is carried out. The Provider may decide to select and engage independent experts to perform audits in accordance with international standards and/or best practices, the findings of which shall be described in specific reports ("**Reports**"). These Reports, which constitute confidential information of the Provider, may be made available to the Client so that the latter may verify the Provider's compliance with the security obligations set forth in this MDPA.

8.2. In the cases contemplated in paragraph 8.1, the Client hereby agrees that its right to verification shall be exercised by checking the Reports made available to it by the Provider.

8.3. The Provider acknowledges that the Client is entitled, according to the methods and limits specified below, to carry out independent audits in order to verify the Provider's compliance with the obligations of this MDPA and the respective DPA – Special Terms and with the provisions of law. The Client may use its own specialized personnel or independent auditors to carry out these activities, provided that they are previously bound by appropriate confidentiality obligations.

8.4. In the cases contemplated in paragraph 8.2 above, the Client must send a prior written request to the Provider's Data Protection Officer (DPO). Following the request for an audit or inspection, the Provider and the Client shall agree, before the activities begin, the details of the audit activities (start date and duration), the types of controls and the scope of the checks, the confidentiality obligations to which the Client and those performing the activities must be bound and the costs that the Provider may charge for such audit activities, which shall be calculated in proportion to the extension and duration of the activities.

8.5. The Provider is entitled to object in writing to the Client's appointment of any external auditors that, in the Provider's indisputable judgement, do not adequately meet qualification or independence requirements, are competitors of the Provider or are clearly unfit. In such circumstances, the Client must appoint other auditors or carry out the audits on its own.

8.6. The Client undertakes to pay the Provider any costs as may be calculated by the Provider and reported to the Client in the phase under paragraph 8.4, according to the methods and terms established therein. The Client shall fully and exclusively bear all costs relating to any audit activities entrusted by the Client to third parties.

8.7. All the above is without prejudice to the inspection rights of the Data Controller and the authorities as established in the Standard Contractual Clauses, if any have been signed pursuant to paragraph 7, which shall not be affected by any provisions set forth in this MDPA or in the related DPA – Special Terms.

8.8. This paragraph 8 shall not apply to the Agreements concerning on-premises products.

8.9. The audit activities involving any Data Sub-Processors shall be carried out in compliance with such Data Sub-Processors' access rules and security policies.

9. ASSISTANCE IN ENSURING COMPLIANCE

9.1. The Provider shall assist the Client and provide cooperation as specified below to enable the Client to comply with its obligations under the Applicable Data Protection Law.

9.2. Should the Provider receive a Request or claim from a Data Subject concerning the Personal Data, it shall invite the Data Subject to address such Request or claim to the

Client or to the End User if this latter is the Data Controller. In any such event, the Provider shall promptly inform the Client of receipt of the Request using the Email Address, and shall provide the Client with all the available information, together with a copy of the Request or claim. The Parties agree that this cooperation shall be carried out by way of an exception to the general rule that the relationships with the Data Subjects fall outside the scope of the Agreement and that the responsibility for handling claims directly and serving as a contact for Data Subjects in the exercise of their rights lies directly with the Client or with the End User, if this latter is the Data Controller. The Client, or the End User if this latter is the Data Controller, shall respond to any such Requests or complaints.

9.3. The Provider shall promptly inform the Client, unless it is prohibited by the law to do so, by sending a notice to the Email Address, of any inspections or requests to provide information that it receives from any supervisory or police authorities in relation to the processing of Personal Data.

9.4. If, in order to comply with a Request as per the paragraphs above, the Client needs to receive information from the Provider about the processing of the Personal Data, the Provider shall provide the necessary assistance to the extent that is reasonably possible, provided that such requests were made with adequate notice.

9.5. Considering the nature of the Personal Data and the information available to the Provider, this latter shall give reasonable assistance to the Client in making available useful information to enable the Client to carry out the impact assessments on the protection of the Personal Data when so required by the law. In such cases, the Provider shall make general information available, based on the activated Business Capabilities, such as the information included in the Agreement, in this MDPA and in the DPA – Special Terms relating to the concerned Business Capabilities. The Client may be charged for any requests for personalized assistance. It is the exclusive responsibility of the Client, or the End User if this latter is the Data Controller, to carry out the impact assessment based on the characteristics of the Personal Data processing performed by the same.

9.6. The Provider undertakes to provide the Business Capabilities and the Services based on the principles of minimization of the processing (privacy by design & by default), without prejudice to the fact that it is the exclusive responsibility of the Client, or the End User if this latter is the Data Controller, to ensure that the processing is then effectively carried out in compliance with such principles and to verify that the technical and organizational measures meet the compliance requirements, including the requirements established by the Applicable Data Protection Law.

9.7. The Client acknowledges that, in the event of a Request by respective Data Subjects for the portability of the Personal Data, and solely with reference to the BCs generating the Personal Data that are relevant in this respect, the Provider shall assist the Client

by making available the information needed for retrieval of the required data in a format that is compliant with the Applicable Data Protection Law.

9.8. Paragraphs 9.5 and 9.7 shall not apply in the event of any Agreements concerning on-premises products.

10. OBLIGATIONS OF THE CLIENT AND RESTRICTIONS

10.1. The Client undertakes to give Instructions in compliance with the regulations and to use the Business Capabilities and the Services in compliance with the Applicable Data Protection Law and for the exclusive purpose of processing the Personal Data that have been collected in compliance with the Applicable Data Protection Law.

10.2. Any processing of Personal Data under Articles 9 and 10 of the GDPR shall be allowed only if expressly established in the DPA – Special Terms. Outside such cases, any processing of such Personal Data shall be permitted exclusively upon prior written agreement between the Parties in compliance with the provisions of paragraph 3.2.

10.3. The Client undertakes to fulfil all the obligations placed upon the Data Controller pursuant to the Applicable Data Protection Law (and, in the event that such obligations are placed upon the End User, it ensures that the End User commits to equivalent obligations), including the obligations to provide certain information to the Data Subjects. The Client further undertakes to ensure that the processing of the Personal Data through the use of the Business Capabilities and the Services shall always be carried out with a suitable legal basis.

10.4. If a data processing notice must be given and consent collected by means of the product contemplated in the Agreement, the Client states and declares that it has evaluated the product and that the product meets its needs. The Client shall also be responsible for assessing whether any forms made available by the Provider to facilitate the Client in meeting its obligations to inform and to obtain consent (e.g., the privacy policy for apps or the data processing policy notices in software), where available, comply with the Applicable Data Protection Law, and for editing such forms if deemed appropriate.

10.5. The Client shall further bear full and exclusive responsibility for managing the Personal Data in compliance with the Requests submitted by the Data Subjects and, therefore, for carrying out, for example, any updates, integrations, rectification and erasure of the Personal Data.

10.6. The Client is responsible for keeping the account associated with the Email Address active and updated.

10.7. The Client acknowledges that, pursuant to Article 30 of the GDPR, the Provider is required to keep a log of the processing activities performed on behalf of the Data Controllers (or Processors) and to collect, for this purpose, the identification and contact data of each Data Controller (and/or Processor) on behalf of which the Provider operates and that such information must be made available to the competent

authority upon request. Therefore, when so requested, the Client undertakes to give the Provider the identification and contact data mentioned above, in the manner specified by the Provider at any time, and to update such information through the same means.

10.8. Therefore, the Client states and declares that the processing of the Personal Data, as described in the Agreements, in this MDPA and in the relevant DPA – Special Terms, is lawful.

11. DURATION

11.1. This MDPA shall enter into force on the MDPA Effective Date and automatically terminate at the date of erasure of all the Personal Data by the Provider, as provided for in this MDPA and, where applicable, in the relevant DPA – Special Terms.

12. PROVISIONS ON THE RETURN OR ERASURE OF THE PERSONAL DATA

12.1. Upon termination of the Agreement, regardless of the reason, the Provider shall:

12.1.1. erase the Personal Data (including any copies) from the Provider's systems or those under its control, within the term established in the Agreement, unless the Provider is required or permitted to retain the data in order to comply with any provisions of the Italian or European laws;

12.1.2. destroy any Personal Data stored on paper in its possession, unless the Provider is required or permitted to retain the data in order to comply with any provisions of the Italian or European laws; and

12.1.3. make the Personal Data available to the Client for retrieval during the period set forth in the Agreement. Where no specific term is specified in the Agreement, the Provider shall keep the Personal Data available to the Client for a period of 60 (sixty) days following termination of the Agreement.

12.2. The Client acknowledges that it has the right, after termination of the Agreement, to retrieve the Personal Data as specified in the Agreement and agrees that it will be its responsibility to retrieve all or part of the Personal Data to the extent that it deems appropriate to retain, and that such retrieval must be completed within the term specified in paragraph 12.1.3.

12.3. The Parties agree that the provisions in paragraphs 12.1 and 12.2 shall not apply to Agreements concerning on-premises products. In these cases, the Client is responsible for retrieving the Personal Data that it deems appropriate to retain, by and no later than the term established in the Agreement. The Client acknowledges that the Personal Data may no longer be accessible after the end of this term. Furthermore, in the cases contemplated in this paragraph 12.3, it is also the Client's responsibility to erase the Personal Data as required by the law.

12.4. The above is without prejudice to any other different or additional provisions concerning the erasure of the Personal Data that may be set forth in the Agreement and in the respective DPA – Special Terms.

13. LIABILITY

13.1. Each Party is liable for the fulfilment of its obligations under this MDPA, the related DPA – Special Terms and the Applicable Data Protection Law.

13.2. Without prejudice to any mandatory limitations established by law, the Provider shall compensate the Client in case of breach of this MDPA and/or the related DPA – Special Terms up to the maximum amount agreed in the Agreement.

14. MISCELLANEOUS

14.1. This MDPA supersedes and replaces any other agreement, contract or understanding between the Parties with respect to its subject matter, as well as any instructions given, in any form, by the Client to the Provider prior to the date of this MDPA with reference to the Personal Data processed in the framework of the performance of the Agreement.

14.2. The Provider may amend this MDPA by sending written notice to the Client (including via email or using computer programs). In this case, the Client shall be entitled to withdraw from the Agreement by written notice sent to the Provider by registered letter with receipt of delivery within 15 days from receipt of the Provider's notice. If the Client does not exercise its right of withdrawal within the terms and in the manners described above, the amendments to this MDPA shall be deemed as acknowledged and accepted by the Client and shall become definitively enforceable and binding on the Parties.

14.3. In the event of any inconsistency between the provisions of this MDPA and those set forth in the Agreement or in any documents of the Client that have not been expressly accepted by the Provider in a departure from this MDPA and/or from the respective DPA – Special Terms, the provisions of this MDPA and the relevant DPA – Special Terms shall prevail.

*****

Exhibit 1

Technical and organisational measures

In addition to the security measures set forth in the Agreement and in the MDPA, the Data Processor applies the following organizational security measures based on the type of Business Capability activated:

A – BC SaaS
B – BC IaaS
C – BPO (Business Process Outsourcing)
D – BPI (Business Process Insourcing)
E – BC On-premises

A – BC SaaS

Organizational Security Measures	*User Policies and Regulations* – The Provider has adopted detailed policies and regulations, with which all users having access to information systems must comply, so that users' behaviour ensures compliance with the principles of data confidentiality, availability and integrity in the use of IT resources. *Logical access authorization* – The Provider defines access profiles in accordance with the principle of least privilege required to carry out the assigned duties. The authorisation profiles are identified and configured before the processing begins and in such a manner that access is limited to only the data necessary for the processing operations. The profiles are subject to regular audits aimed at assessing whether the requirements to maintain the assigned profiles are still met. *Technical support* – Technical support work is governed to ensure that only the activities provided for by contract are performed and to prevent any excessive processing of personal data for which the Client or End User is Controller. *Data Protection Impact Assessment (DPIA)* – In compliance with Articles 35 and 36 of the GDPR and based on the document WP248 – Guidelines on Data Protection Impact Assessment, adopted by the Working Party

	set up in accordance with Article 29, the Provider has prepared its own methodology for the analysis and assessment of processing that, considering the nature, scope, context and purposes of the processing, presents a high risk for the rights and freedoms of natural persons, in order to carry out an impact assessment on the protection of personal data before beginning the processing. *Incident Management* – The Provider has implemented a specific incident management procedure to restore normal service operations at the soonest while maintaining the best service levels. *Data Breaches* – The Provider has implemented a specific procedure for the management of events and incidents that could have a potential impact on personal data. This procedure defines the roles and responsibilities, the process for detection of a (suspected or actual) incident/breach, the implementation of counter-actions, the response to, and containment of, the incident/breach as well as the methods for informing the Client of personal data breaches. *Training:* The Provider periodically delivers training courses on the proper management of personal data to its employees involved in the processing activities
Technical Security Measures	*Firewalls, IDPS* – Personal data are protected against the risk of intrusion as described in Article 615-*quinquies* of the Italian Criminal Code by means of intrusion detection and prevention systems (IDPS), which are updated with the best available technologies. *Security of communication lines* – Insofar as it is responsible, the Provider has implemented secure communication protocols that are in line with the available technology. *Protection from malware* – The systems are protected against the risks of intrusion and program actions through the activation of the appropriate electronic tools that are periodically updated. Antivirus tools are in use and constantly updated. *Authentication Credentials* – The systems are configured in such a manner that access is granted exclusively to users with authentication

	credentials allowing unique identification of the user. This includes a code associated with a secret password known only to the user and an authentication device held by the user for the user's exclusive use and which may be associated with an ID code or password. The Provider makes multi-factor authentication (MFA) available to the Client as an additional and optional technical security measure for access to the service. The activation of MFA is at the Client's sole discretion and is strongly recommended in order to obtain greater protection. The Client is responsible for managing the access credentials and the devices used for multi-factor authentication. *Password* – Passwords are managed in accordance with best practices in terms of their basic features, i.e., the obligation to change them at the first access, their minimum length, the absence of elements that may be easily inferred from their holder, complexity rules, expiration, history, contextual strength assessment, display and storage. Users assigned credentials also receive detailed instructions concerning the measures to take to ensure that such credentials remain secret. *Logging* – The systems may be configured in such a manner as to track access and, where appropriate, the activities carried out by the different types of users (Administrator, Super User, etc.). The logs are protected by appropriate security measures ensuring their integrity. *Backup & Restore* – Appropriate measures are taken to ensure that data access can be restored in the event of damage to the data or electronic tools, within terms that are certain and consistent with the rights of the data subjects. If so required by contractual agreements, an operational continuity plan is implemented and, where necessary, integrated with the disaster recovery plan. These plans ensure the availability of, and access to, the systems, even in the event of serious adverse events that may persist in time. *Vulnerability Assessment & Penetration Test* – The Provider regularly conducts vulnerability analyses aimed at assessing the level of exposure to known vulnerabilities, in relation to both infrastructures and operations, not only considering already operating systems but also systems that are under development.

	When deemed appropriate in relation to the potential risks that have been identified, the above assessments and tests are periodically supplemented with special penetration tests, which simulate breaches in various scenarios of attack, with the aim of checking the level of security of applications/systems/networks through activities that exploit detected vulnerabilities to circumvent the physical/logical security mechanisms and gain access. The results of the tests are examined thoroughly and in detail to identify areas for improvement and take the actions necessary to ensure the high level of security that is required. *System Administrators* – All users operating as System Administrators are indicated in a list that is regularly updated, and the duties assigned to them are duly defined in special documents of appointment. The activities performed by System Administrators are tracked by means of a log management system and the data in the log are stored in an immutable manner to allow monitoring after the activities. The work of the System Administrators is audited to verify compliance with the organizational, technical and security measures in relation to the processing of personal data as required by current regulations. *Data Centers* – Physical access to the Data Center is restricted to authorized persons only. For further details on the security measures adopted for the data center services provided by the Data Sub-Processors, as specified in the DPA – Special Terms, please refer to the descriptions of such security measures prepared by the same Data Sub-Processors and made available in their respective official sites at the following addresses (or at the addresses made available in the future by the same Data Sub-Processors): For the Data Center services provided by Amazon Web Services: https://aws.amazon.com/it/compliance/data-center/controls/ For the Data Center services provided by Microsoft: https://www.microsoft.com/en-us/trustcenter

B – BC IaaS

Organizational Security Measures	*Data centers* – The Provider provides, depending on the circumstances and the specific contractual arrangements, the BC IaaS through the following Data Centers: - Aruba S.p.A., located in Italy; - Microsoft Azure located in West Europe e Italy North regions; - TIM located in Italy. With reference to physical security measures, please refer to the information made available by the individual providers, as set out below: • with regard to Aruba S.p.A.: misure di sicurezza Aruba ; • with regard to Microsoft Azure: Sicurezza fisica dei data center di Azure • with regard to TIM: misure di sicurezza TIM In the Data Centers, the virtualization environment (including the SAN – Storage Area Network) resides on servers hosted in data centers located within the European Union, which are managed by ISO 27001-certified providers. *Certifications* – The Provider has obtained the following certifications/attestations: • ISO/IEC 27001: "Information security" • ISO/IEC 27017 "Information security for Cloud services" • ISO/IEC 27018 "Protection of personal data in Public Cloud services" • For further details on the certifications obtained by the Provider, please refer to the following link: Banche dati – Accredia: Accredia databases. *Logical access authorization* – Upon delivery of the virtual machines purchased by the Client, the Provider provides the Client with

	temporary access credentials granting access to such Virtual Machines as the System Administrator. If the login credentials are not received, it is the Client's responsibility to promptly request them from the Provider. Any additional access profiles other than those that are configured upon delivery, must be defined by the Client based on its own authorization policies. With reference to the virtualization infrastructure, the Provider, insofar as it is responsible, shall define the access profiles based on the principle of the least privilege necessary to carry out the assigned duties. The profiles are subject to regular audits aimed at assessing whether the requirements to maintain the assigned profiles are still met. *User Profiles* – The VMs are configured in such a manner that allows access exclusively to people with authentication credentials allowing unique identification of the user. *Security of communication lines* – Insofar as it is responsible and with exclusive reference to the virtualization infrastructure, the Provider implements secure communication protocols that are in line with the available technology in relation to the authentication process. *Change Management* – Insofar as it is responsible, the Provider has a specific procedure to govern the change management process in view of the introduction of any technological innovations or modifications to its model and organizational structure. The Client is directly responsible for all change management procedures and operations concerning the virtual machines purchased by the Client. *Training*: The Provider periodically delivers cyber security, data protection and information security training courses to its employees involved in the processing activities. *Protection from malware* – The VMs with a Windows operating system are equipped by default with native antivirus/antimalware systems, the maintenance and updating of which must be carried out by the Client who bears full responsibility for it, in line with the IaaS service model and in compliance with the general terms and conditions. In this respect, it is hereby agreed that the Client is responsible for assessing the adequacy of these solutions and considering whether it is necessary to adopt, at its own care and expense, additional security

	and protection systems based on the actual use of the VMs and the Client's risk management policies, as well as periodically verifying that the aforementioned systems are effectively updated and – should any automatic updates fail – manually updating the protection systems described herein. Risk management Supplier periodically conducts analysis and management of risks relating to information security information aimed at preventing or reducing the possible undesirable effects that could be caused by threats that are not properly addressed. *Backup & Restore* – Appropriate measures are taken to ensure the backup and recovery of data in the event of damage or loss, in compliance with the Agreement. In such cases, the data may be restored by recovering the last available back-up copy before the corruption. However, the Data Controller is responsible for deciding whether to independently back up its data for the entire duration of the Agreement, without prejudice to the possibility of obtaining a copy of the data within the 60-day term following termination of such Agreement by sending a request to customer service. *Logging* – The virtualization platform and related console have logs in place to track access and, where appropriate, the activities carried out by the different types of user profiles (Administrator, Super User, etc.). The logs are protected by appropriate security measures ensuring their integrity. The Client is responsible for implementing, should it decide to do so, additional logging tools to track the activities carried out in the Virtual Machines other than those provided by the operating system or a single application installed on the Virtual Machines. *Network and security* – The cloud infrastructure used to host the VMs is equipped with security systems, such as firewalls, and with a system protecting traffic from DDOS attacks for the protection of the infrastructure as a whole (region/data center). However, the Parties agree that, in line with the IaaS service model and in compliance with the general terms and conditions of the Agreement, the Client is responsible for protecting its own VM with adequate security and protection systems, including systems that protect against DDoS attacks.

	Business Continuity & Disaster Recovery –Client is responsible for implementing and managing Business Continuity and Disaster Recovery plans, unless otherwise agreed in the contract. Where contractual agreements so provide, a business continuity plan is put in place, integrated, where necessary, with the disaster recovery plan. This ensures the availability of and access to systems even in the event of significant adverse events that may persist over time. *Incident Management* – Insofar as it is responsible, the Provider has implemented a specific incident management procedure to restore normal service operations at the soonest in accordance with the Agreement. The Client is responsible for setting up incident management procedures for incidents relating to the management of the purchased VMs. *System Maintenance Activities* – If the Client has not entered into a system maintenance agreement with the Provider, all such system maintenance activities (including, without limitation, periodic updates of security patches, activation/creation of profiles for VM users and administrators, monitoring VM performance indicators, etc.) shall exclusively be the Client's duty and responsibility.

C – BUSINESS PROCESS OUTSOURCING (BPO)

Organizational Security Measures	*Certifications* – The Provider has obtained the following certifications/attestations: • ISO/IEC 27001: "Information security". • ISO/IEC 27017: "Information security for Cloud services" • ISO/IEC 27018: for the protection of personal data in Public Cloud services. • For further details on the certifications obtained by the Provider, please refer to the following link: Banche dati – Accredia: Accredia databases.

	User Policies and Regulations – Detailed policies and regulations are in place, with which all users having access to information systems must comply, so that users' conduct is appropriate to ensure compliance with the principles of confidentiality, availability and integrity of data in the use of IT resources. *Logical access authorization* – The Provider defines access profiles in accordance with the principle of the least privilege required to carry out the assigned duties. The authorisation profiles are identified and configured before the processing begins and in such a manner that access is limited to only the data necessary for the processing operations. The profiles are subject to regular audits aimed at assessing whether the requirements to maintain the assigned profiles are still met. *Technical support* – The Provider governs the management of technical support work to ensure that only the activities provided for by contract are performed and to prevent any excessive processing of personal data for which the Client or End User is Controller. *Change Management* – The Provider has implemented a specific procedure to regulate the Change Management process in view of the introduction of any technological innovations or changes in its set-up and organizational structure. *Data Protection Impact Assessment (DPIA)* – In compliance with Articles 35 and 36 of the GDPR and based on the document WP248 – Guidelines on Data Protection Impact Assessment, adopted by the Working Party set up in accordance with Article 29, the Provider has prepared its own methodology for the analysis and assessment of processing that, considering the nature, scope, context and purposes of the processing, presents a high risk for the rights and freedoms of natural persons, in order to carry out an impact assessment on the protection of personal data before beginning the processing. *Incident Management* – The Provider has implemented a specific incident management procedure to restore normal service operations at the soonest while maintaining the best service levels.

	Data Breaches – The Provider has implemented a specific procedure for the management of events and incidents that could have a potential impact on personal data. This procedure defines the roles and responsibilities, the process for detection of a (suspected or actual) incident/breach, the implementation of counter-actions, the response to, and containment of, the incident/breach as well as the methods for informing the Client of personal data breaches. *Training*: The Provider periodically delivers training courses on the proper management of personal data to its employees involved in the processing activities.
Technical Security Measures	*High Reliability* – The Provider ensures high reliability in the following terms: • The server architecture is completely based on the VMWare virtualization solution applied by creating physical and virtual redundancies of each individual system, in order to ensure fault-tolerance and removal of single points of failure. In particular, in the event of a system failure, the virtual environment management software can reallocate current activities to other systems (principles of high availability and load balancing), minimizing service inefficiencies and ensuring persistence of existing connections. • Each server is placed on a SAN connected via high-speed iSCSI. • All infrastructure components, including servers, security and network equipment, storage systems and SAN infrastructure, are completely redundant, in order to eliminate every single point of failure. • The network architecture has been designed to protect front-end systems from the internet and from internal networks using a DMZ shielded by means of two layers of separate firewalls (defence-in-depth strategy): a boundary firewall connected to the internet and a second firewall with intrusion prevention and anti-malware features, which is proprietary to the organization and has been set up to protect the DMZ and back-end systems. *Hardening* – Specially designed hardening activities are in place to prevent security incidents by minimizing the architectural weaknesses of the operating systems, the applications and the network equipment, considering, in particular, the reduction of risks relating to system

	vulnerabilities, the reduction of risks relating to the applications installed in the systems and the higher protection levels of the services provided. *Firewalls, IDS/IPS* – The anti-intrusion systems, such as firewalls and IDS/IPS, are positioned in the network segment connecting the cloud infrastructure with the internet in order to intercept any malicious activity aimed at completely or partially compromising the provision of the service. In this specific case, the equipment used is type UTM SourceFire (Cisco), which includes both the firewall and the IDS/IPS components. *Security of communication lines* – Insofar as it is responsible, the Provider has implemented secure communication protocols that are in line with the available technology. *Protection from malware* – The VMs are protected against the risks of intrusion and program actions through the activation of appropriate electronic tools that are periodically updated. All VMs are managed with antivirus features (at both hypervisor and infrastructure level). *Authentication Credentials* – The systems are configured in such a manner that access is granted exclusively to users with authentication credentials allowing unique identification of the user. This includes a code associated with a secret password known only to the user and an authentication device held by the user for the user's exclusive use and which may be associated with an ID code or password. *Password* – Passwords are managed in accordance with best practices in terms of their basic features, i.e., the obligation to change them at the first access, their minimum length, the absence of elements that may be easily inferred from their holder, complexity rules, expiration, history, contextual strength assessment, display and storage. Users assigned credentials also receive detailed instructions concerning the measures to take to ensure that such credentials remain secret. *Logging* – The systems may be configured in such a manner as to track access and, where appropriate, the activities carried out by the

	different types of users (Administrator, Super User, etc.). The logs are protected by appropriate security measures ensuring their integrity. *Backup & Restore* – Appropriate measures are taken to ensure that data access can be restored in the event of damage to the data or electronic tools, within terms that are certain and consistent with the rights of the data subjects. However, the Controller is responsible for deciding whether to independently back up its data for the entire duration of the Agreement and for the 60-day term following termination of the same. If so required by contractual agreements, an operational continuity plan is implemented and, where necessary, integrated with the disaster recovery plan. These plans ensure the availability of, and access to, the systems, even in the event of serious adverse events that may persist in time. *Vulnerability Assessment & Penetration Test* – The Provider regularly conducts vulnerability analyses aimed at assessing the level of exposure to known vulnerabilities, in relation to both infrastructures and operations, considering not only already operating systems but also systems that are under development. When deemed appropriate in relation to the potential risks that have been identified, the above assessments and tests are periodically supplemented with special penetration tests, which simulate breaches in various scenarios of attack, with the aim of checking the level of security of applications/systems/networks through activities that exploit detected vulnerabilities to circumvent the physical/logical security mechanisms and gain access. The results of the tests are examined thoroughly and in detail to identify areas for improvement and take the actions necessary to ensure the high level of security that is required. *System Administrators* – All users operating as System Administrators are indicated in a list that is regularly updated, and the duties assigned to them are duly defined in special documents of appointment. The activities performed by System Administrators are tracked by means of a log management system and the data in the log are stored in an immutable manner to allow monitoring after the activities. The work of the System Administrators is audited to verify compliance with the

	organizational, technical and security measures in relation to the processing of personal data as required by current regulations. *Data centers* – The virtualization environment (including the storage area network (SAN)) is hosted on servers at a data center in the European Union, which is managed by an ISO 27001-certified provider. In particular, the security measures implemented to protect the Data Center are listed below: • Exterior perimeter security: ✓ External fence marking the boundary of the property not lower than 3 meters' height, equipped with passive anti climb protection ✓ Monitoring of external areas by means of infrared barriers and/or video analysis systems and by video surveillance with recording systems ✓ Restricted/individual pedestrian access ✓ Restricted vehicle access ✓ Armed patrols • Interior perimeter security: ✓ Surveillance room for the control of internal and external areas, supervision ✓ Use of alarms, management of visitors by delivering badges according to company policies and to specific regulations for data centres ✓ Reception desk for entry control ✓ Three-arm turnstiles placed opposite to the surveillance room and reception desk • High security inner perimeter: ✓ Interlocked access to system rooms equipped with passive protection ✓ Entry control system based on lists of "AUTHORIZED" people ✓ Magnetic sensors detecting the state of doors ✓ Emergency exits with sensors detecting the door status. All alarms are remotely linked to the surveillance room.

D - BPI – BUSINESS PROCESS INSOURCING

Organizational Security Measures	*User Policies and Regulations* – Detailed policies and regulations are in place, with which all users having access to information systems must comply, so that users' conduct is appropriate to ensure compliance with the principles of confidentiality, availability and integrity of data in the use of IT resources. *Logical access authorization* – The Provider defines access profiles in accordance with the principle of the least privilege required to carry out the assigned duties. The authorisation profiles are identified and configured before the processing begins and in such a manner that access is limited to only the data necessary for the processing operations. The profiles are subject to regular audits aimed at assessing whether the requirements to maintain the assigned profiles are still met. *Data Breaches* – The Provider has implemented a specific procedure for the management of events and incidents that could have a potential impact on personal data. This procedure defines the roles and responsibilities, the process for detection of a (suspected or actual) incident/breach, the implementation of counter-actions, the response to, and containment of, the incident/breach as well as the methods for informing the Client of personal data breaches. *Training*: The Provider periodically delivers training courses on the proper management of personal data to its employees involved in the processing activities.
Technical Security Measures	*Security of communication lines* – Insofar as it is responsible, during the technical support phase, the Provider implements secure communication protocols that are in line with the available technology. *Backup & Restore* – Where required by contractual agreements, appropriate measures are taken to restore access to data in the event of damage to such data or to IT tools, within certain amounts of time compatible with the rights of the data subjects.

E – BC ON PREMISES

Organizational Security Measures	*User Policies and Regulations* – Detailed policies and regulations are in place, with which all users having access to information systems must comply, so that users' conduct is appropriate to ensure, during the technical support phase, compliance with the principles of confidentiality, availability and integrity of data in the use of IT resources. *Logical access authorization* – The Provider defines access profiles in accordance with the principle of the least privilege required to carry out the assigned duties. The authorisation profiles are identified and configured before the processing begins and in such a manner that access is limited to only the data necessary for the processing operations. The profiles are subject to regular audits aimed at assessing whether the requirements to maintain the assigned profiles are still met. *Technical support* – The Provider governs the management of technical support work to ensure that only the activities provided for by contract are performed and to prevent any excessive processing of personal data for which the Client is Controller. *Incident Management & Data Breaches* – The Provider has implemented a specific procedure for the management of events and incidents that could have a potential impact on personal data. This procedure defines the roles and responsibilities, the process for detection of a (suspected or actual) incident/breach, the implementation of counter-actions, the response to, and containment of, the incident/breach as well as the methods for informing the Client of personal data breaches. *Training:* The Provider periodically delivers training courses on the proper management of personal data to its employees involved in the processing activities
Technical Security Measures	*Security of communication lines* – Insofar as it is responsible, during the technical support phase, the Provider implements secure communication protocols that are in line with the available technology. *Protection from malware* – Workstations used during the technical support phase are protected against the risks of intrusion and program

	actions through the activation of the appropriate electronic tools that are periodically updated. All VMs are managed with antivirus features (at both hypervisor and infrastructure level). *System Administrators* – All users operating as System Administrators are indicated in a list that is regularly updated, and the duties assigned to them are duly defined in special documents of appointment. The activities performed by System Administrators are tracked by means of a log management system and the data in the log are stored in an immutable manner to allow monitoring after the activities. The work of the System Administrators is audited to verify compliance with the organizational, technical and security measures in relation to the processing of personal data as required by current regulations.