TERMINI DI PRIVACY E SICUREZZA DEL FORNITORE

I presenti Termini di Privacy e Sicurezza stabiliscono i diritti e gli obblighi di Intesa e del Fornitore in materia di privacy, sicurezza e su questioni a queste correlate (i "**Termini**"). I presenti Termini sono integrati e diventano parte integrante del Contratto con il Fornitore (o accordo equivalente), che comprende gli le CGA, gli MPO, gli Ordini di Acquisto o altri documenti tra le nostre aziende che li citano (i "**Documenti d'Ordine**").

I presenti Termini sono costituiti da:

- Il presente documento,
- L'Appendice dei Dettagli del Trattamento allegata alla data di firma dei presenti Termini, che definisce le attività di trattamento dei dati da parte del Fornitore (per i Documenti d'Ordine successivi alla firma dei presenti Termini, a ciascun documento verrà allegata un'Appendice "Dettagli del Trattamento" separata che definirà le attività di trattamento specifiche del Fornitore in relazione a tale documento), e
- Le EU Standard Contractual Clauses, lo UK International Data Transfer Addendum (Appendice per il Trasferimento Internazionale dei Dati del Regno Unito) e il Supplier Transfer Impact Assessment (Valutazione dell'Impatto del Trasferimento del Fornitore), reperibili all'indirizzo http://www.intesa.it/fornitori/fornitori.html.

In caso di conflitto, i presenti Termini prevalgono sulle CGA, su qualsiasi accordo equivalente o Documento d'Ordine, inclusi gli accordi sul trattamento dei dati. Se il conflitto è tra questi Termini e gli accordi specifici concordati tra il Fornitore e Intesa per un Cliente Intesa, gli accordi specifici avranno la precedenza.

I termini con la prima lettera in maiuscolo hanno il significato attribuito loro nell'Articolo V dei presenti Termini o il significato che hanno in questi Termini o nel Documento d'Ordine o nel Contratto.

Articolo I. GOVERNANCE DEI DATI E AI

1.1. **Conformità alle leggi**. Il Fornitore si conformerà a tutte le leggi applicabili ai Servizi e ai Materiali, incluse le leggi relative alla protezione dei dati, alla sicurezza informatica e ai Sistemi AI. Il Fornitore informerà tempestivamente Intesa (e in ogni caso entro i termini previsti dalla legge e in modo tale da consentire a Intesa di adempiere ai propri obblighi legali) qualora il Fornitore determini di non poter più adempiere ai propri obblighi legali.

1.2. **Uso dei Dati.** Il Fornitore non:

(a) utilizzerà i Dati Intesa in alcuna forma, inclusi quelli aggregati, anonimizzati o di altro tipo, per scopi diversi dall'erogazione dei Servizi e dalla fornitura dei Materiali (a titolo esemplificativo, il Fornitore non è autorizzato a utilizzare o riutilizzare i Dati Intesa per valutare l'efficacia o sviluppare metodi per migliorare proprie offerte diverse dai Servizi o dai Materiali, per la ricerca e lo sviluppo per creare nuove offerte o per generare rapporti riguardanti le offerte del Fornitore);

(b) venderà o condividerà i Dati Intesa; o

(c) cercare di identificare nuovamente informazioni che potrebbero essere usate per dedurre informazioni su un Interessato o essere collegate a esso.

1.3. **Tecnologie di monitoraggio web**. Se il Fornitore o i suoi Subappaltatori, nell'erogazione dei Servizi o nella fornitura dei Materiali, raccolgono dati utilizzando tecnologie di tracciamento web (inclusi HTML5, archiviazione locale, tag o token di terze parti e web beacon), tali dati saranno considerati Dati Intesa e il Fornitore si atterrà ai propri obblighi in materia di Dati Intesa ai sensi dei presenti Termini.

1.4. **Non divulgazione**. Il Fornitore non divulgherà i Dati Intesa a terzi, se non ai Subresponsabili del trattamento approvati ai sensi dell'Articolo 2.5 o ai Subappaltatori approvati ai sensi dell'Accordo.

1.5. **Accesso governativo**. Se un governo, compreso un ente regolatore, richiede l'accesso ai Dati Intesa o se la divulgazione dei Dati Intesa è altrimenti richiesta dalla legge, il Fornitore informerà prontamente Intesa per iscritto di tale richiesta o obbligo e offrirà a Intesa una ragionevole opportunità di contestare qualsiasi divulgazione, a meno che non sia vietato dalla legge. Se la notifica è vietata dalla legge, il Fornitore adotterà le misure che ritiene ragionevolmente appropriate per contestare il divieto e la divulgazione dei Dati Intesa

attraverso un'azione giudiziaria o altri mezzi.

1.6. **Riservatezza**. Il Fornitore assicura a Intesa che: (a) solo i suoi dipendenti che necessitano di accedere ai Dati Intesa per erogare i Servizi o fornire i Materiali avranno tale accesso, e solo nella misura necessaria; e (b) ha vincolato i suoi dipendenti a obblighi di riservatezza che richiedono a tali dipendenti di utilizzare e divulgare i Dati Intesa solo come consentito dai presenti Termini.

1.7. **Restituzione o Cancellazione dei Dati Intesa**. Il Fornitore, a discrezione di Intesa, eliminerà o restituirà i Dati Intesa a Intesa alla risoluzione o alla scadenza del Documento d'Ordine o anche prima su richiesta di Intesa. Se Intesa richiede la cancellazione, il Fornitore, in conformità con il NIST SP 800-88 rev.1, renderà i dati illeggibili e non riassemblabili o ricostruibili e ne certificherà la cancellazione a Intesa su richiesta. Se Intesa richiede la restituzione dei Dati Intesa, il Fornitore provvederà a farlo in un formato comunemente utilizzato, secondo il calendario e le istruzioni ragionevoli di Intesa.

1.8. **Sistemi AI**

(a) Il Fornitore non utilizzerà Sistemi di Intelligenza Artificiale (AI) nell'erogazione dei Servizi o nella fornitura del Materiale da Consegnare, né includerà Sistemi AI nel Materiale da Consegnare, senza la previa autorizzazione scritta di Intesa in un Documento d'Ordine o nell'Accordo. Nel richiedere l'autorizzazione di Intesa, il Fornitore fornirà a Intesa per iscritto tutte le informazioni necessarie per valutare l'utilizzo dei Sistemi AI da parte del Fornitore (ad esempio, flussi di dati, modelli linguistici utilizzati, separazione dei dati).

(b) Il Fornitore dichiara e garantisce che: (i) l'input fornito da Intesa (compreso l'input fornito dai dipendenti o da qualsiasi altra terza parte ai sensi di un Documento d'Ordine) e l'output saranno classificati come Materiali Intesa, (ii) il Fornitore non utilizzerà i Materiali Intesa per addestrare o perfezionare il modello di base o altri elementi dei Sistemi AI, (iii) il Fornitore non conserverà i Materiali Intesa per un periodo superiore a quello necessario per erogare i Servizi, (iv) i Sistemi AI (compresi gli output e i dati di addestramento) saranno classificati come parte dei Servizi, e (v) nella misura consentita dalla legge applicabile, il Fornitore cede con la presente a Intesa tutti i suoi diritti, titoli e interessi sugli output dei Sistemi AI.

(c) Il Fornitore implementerà e manterrà un programma di governance e gestione dei rischi documentato per i Sistemi AI, che identifichi, verifichi, monitori e mitighi in modo ragionevole e appropriato i rischi noti e prevedibili, inclusi, a titolo esemplificativo, i rischi relativi all'etica, ai pregiudizi, alla sicurezza e alla protezione associati o derivanti dai Sistemi AI. Su richiesta, il Fornitore condividerà una copia del suo programma di governance e gestione dei rischi per i Sistemi AI. Il Fornitore notificherà tempestivamente a Intesa per iscritto qualsiasi rischio verificatosi o qualsiasi rischio materiale identificato in conformità con la disposizione di notifica concordata nel Documento d'Ordine, con una copia a cybersecurity@intesa.it.

Articolo II. PRIVACY

2.1. **Informazioni di Contatto Aziendali**. Intesa e il Fornitore possono Trattare le rispettive Informazioni di Contatto Aziendali (BCI) in conformità con le leggi applicabili sulla protezione dei dati, in qualità di Titolari del Trattamento dei Dati Personali autonomi, ovunque operino per fornire e ricevere i Materiali e i Servizi. Le Parti non agiscono in qualità di Titolari del Trattamento dei Dati Personali in relazione alle rispettive BCI. Se una delle Parti informa l'altra di eventuali richieste da parte di un Interessato in merito alle BCI dell'altra, l'altra Parte sarà responsabile di gestire tali richieste direttamente con l'Interessato. Ciascuna delle Parti ha implementato misure tecniche e organizzative appropriate per proteggere le BCI dell'altra. Per chiarezza, l'Articolo 3.12 (Incidenti di Sicurezza) si applica alle BCI.

2.2. **Fornitore come Responsabile del Trattamento**. Intesa nomina il Fornitore come Responsabile del Trattamento dei Dati Personali Intesa al solo scopo di fornire i Materiali ed erogare i Servizi in conformità con le istruzioni di Intesa, incluse quelle contenute nei presenti Termini, nel Contratto e in qualsiasi Documento d'Ordine correlato. Il Fornitore è un Responsabile del Trattamento dei Dati Personali Intesa. Se il Fornitore non agisce in conformità con le istruzioni di Intesa, impedendo a Intesa di conformarsi alla legge applicabile sulla protezione dei dati, Intesa può risolvere la parte interessata dei Servizi tramite comunicazione scritta. Qualora il Fornitore ritenga che un'istruzione violi una legge sulla protezione dei dati, il Fornitore informerà prontamente Intesa entro i termini previsti dalla legge.

2.3. **Misure Tecniche e Organizzative (TOMs)**. Il Fornitore implementerà e manterrà misure tecniche e organizzative

appropriate, incluse le misure di sicurezza di cui all'Articolo III, per garantire un livello di sicurezza adeguato al rischio associato all'erogazione dei Servizi e alla fornitura dei Materiali.

2.4. **Diritti e Richieste degli Interessati**

(a) Il Fornitore informerà tempestivamente Intesa (in tempi che consentano a Intesa e agli Altri Titolari del Trattamento dei Dati Personali di adempiere ai propri obblighi legali e comunque non oltre 7 giorni) di qualsiasi richiesta da parte di un Interessato di esercitare i propri diritti (ad es. rettifica, cancellazione o blocco dei dati) in merito ai Dati Personali Intesa. Il Fornitore può anche indirizzare prontamente un Interessato ad inviare la richiesta a Intesa. Il Fornitore non risponderà ad alcuna richiesta da parte degli Interessati, a meno che non sia legalmente richiesto o richiesto da Intesa per iscritto.

(b) Se Intesa è obbligata a fornire informazioni in merito ai Dati Personali Intesa ad Altri Titolari del Trattamento dei Dati Personali o a terze parti (ad esempio, Interessati o regolatori), il Fornitore assisterà Intesa fornendo informazioni e intraprendendo le ragionevoli azioni richieste da Intesa, con un programma che consenta a Intesa di rispondere tempestivamente a tali Altri Titolari del Trattamento dei Dati Personali o terze parti.

2.5. **Subresponsabili**

(a) Intesa autorizza il Fornitore a collegarsi ai Subresponsabili elencati nelle rispettive Appendici dei Dettagli del Trattamento. Il Fornitore può inoltre avvalersi di Subresponsabili aggiuntivi o sostitutivi o ampliare l'ambito del Trattamento da parte di un Subresponsabile esistente, fermo restando quanto segue:

(i) Il Fornitore fornirà a Intesa un preavviso scritto di 30 giorni prima di procedere con tali modifiche.

(ii) Intesa può opporsi a qualsiasi nuovo Subresponsabile, o alla sua sostituzione, o all'ampliamento dell'ambito del trattamento per motivi ragionevoli; in tal caso, le Parti collaboreranno in buona fede per gestire l'obiezione di Intesa.

(iii) Fatto salvo il diritto di Intesa di opporsi in qualsiasi momento, il Fornitore può procedere con la modifica qualora Intesa non abbia sollevato obiezioni entro 30 giorni dal ricevimento dell'avviso scritto del Fornitore.

(b) Il Fornitore imporrà gli obblighi di protezione, sicurezza e certificazione dei dati stabiliti nei presenti Termini a ciascun Subresponsabile prima che un Subresponsabile tratti i Dati Personali Intesa. Il Fornitore è pienamente responsabile nei confronti di Intesa per l'adempimento degli obblighi di ciascun Subresponsabile.

2.6. **Trattamento dei Dati Transfrontaliero**

(a) Il Fornitore non trasferirà né divulgherà (anche tramite accesso remoto) alcun Dato Personale Intesa al di fuori dei confini nazionali, se non ai Subresponsabili approvati in conformità con l'Articolo 2.5. Se Intesa approva il trasferimento transfrontaliero di Dati Personali Intesa, le Parti coopereranno per conformarsi alle leggi applicabili sulla protezione dei dati. Se tali leggi richiedono le Clausole Contrattuali Standard (SCC), il Fornitore stipulerà tempestivamente le SCC come definite di seguito.

(b) **Spazio Economico Europeo**

(i) Se Intesa trasferisce Dati Personali soggetti al GDPR (General Data Protection Regulation) (2016/679) al di fuori dello Spazio Economico Europeo a un Fornitore non stabilito in un Paese Adeguato, il Fornitore stipula con la presente le EU Standard Contractual Clauses (Decisione della Commissione 2021/914), pre-firmate da Intesa e disponibili all'indirizzo ("**SCC UE**").

(ii) Nel caso in cui Intesa sia di fatto scomparsa, abbia cessato di esistere giuridicamente o sia diventata insolvente, gli Altri Titolari del Trattamento dei Dati Personali avranno il diritto di risolvere il Contratto e di incaricare il Fornitore di cancellare o restituire i Dati Personali Intesa.

(iii) La valutazione di Intesa sui trasferimenti di Dati Personali ai Fornitori, come richiesto dalle SCC UE, è pubblicata per la consultazione da parte del Fornitore all'indirizzo http://www.intesa.it/fornitori/fornitori.htm.

(iv) Il Fornitore fornirà dettagli sufficienti su ciascun Subresponsabile nelle Appendici dei Dettagli del Trattamento e nelle comunicazioni per soddisfare i propri obblighi come importatore di dati ai sensi della clausola 14(c) delle EU Standard Contractual Clauses, inclusi il nome del Subresponsabile, i luoghi di trattamento e le attività di trattamento.

(v) Il Fornitore agirà come Esportatore di Dati e stipulerà le SCC UE o un altro meccanismo di trasferimento appropriato con ciascun Subresponsabile approvato non stabilito in un Paese Adeguato.

(c) **Regno Unito.** Qualora i Dati Personali Intesa soggetti al Data Protection Act del Regno Unito (2018) vengano trasferiti al di fuori del Regno Unito verso un Paese non adeguato, il Fornitore sottoscrive con la presente

lo "UK International Data Transfer Addendum", pre-firmato da Intesa e disponibile all'indirizzo http://www.intesa.it/fornitori/fornitori.htm.

(d) **Svizzera**. Se i Dati Personali Intesa soggetti allo Swiss Federal Act on Data Protection (Legge Federale Svizzera sulla Protezione dei Dati) ("**FADP**") vengono trasferiti al di fuori della Svizzera verso un Paese Non Adeguato, il Fornitore sottoscrive con la presente le Clausole Contrattuali Standard UE, soggette alle seguenti modifiche:
   (i) i riferimenti al GDPR includeranno anche il riferimento alle disposizioni equivalenti del FADP;
   (ii) la Swiss Federal Data Protection Information Commission (Commissione Federale Svizzera per l'Informazione e la Protezione dei Dati) è l'autorità di vigilanza esclusiva ai sensi della Clausola 13 e dell'Allegato I.C delle Clausole Contrattuali Standard UE;
   (iii) la legge applicabile ai sensi della Clausola 17 delle Clausole Contrattuali Standard UE sarà la legge svizzera nel caso in cui il trasferimento di dati sia soggetto esclusivamente al FADP; e
   (iv) il termine "stato membro" non deve essere interpretato in modo da escludere gli interessati in Svizzera dalla possibilità di far valere i propri diritti nel luogo di residenza abituale (Svizzera) ai sensi della Clausola 18 delle Clausole Contrattuali Standard UE.

(e) **Brasile**. Qualora Intesa trasferisca Dati Personali soggetti alla Lei Geral de Proteção de Dados (LGPD) al di fuori del Brasile a un Fornitore non stabilito in un Paese adeguato, il Fornitore sottoscrive con la presente l'Allegato II della Resolução CD/ANPD nº 19/2024 ("Standard Contractual Clauses del Brasile" o "SCC del Brasile"), pre-firmato da Intesa e disponibile all'indirizzo http://www.intesa.it/fornitori/fornitori.htm ("**SCC del Brasile**").

(f) **Altri Paesi**. Qualora un trasferimento di Dati Personali Intesa sia soggetto alle leggi sulla protezione dei dati di un Paese in cui le Clausole Contrattuali Standard (SCC) locali non sono state pubblicate dall'Autorità di Vigilanza (ad esempio, la Legge sulla Protezione dei Dati del Perù, la Legge sulla Protezione dei Dati del Sudafrica) o l'Autorità di Vigilanza ha approvato l'uso delle EU Standard Contractual Clauses come garanzia sufficiente per il trasferimento transfrontaliero (ad esempio, la Legge sulla Protezione dei Dati dell'Argentina), le EU SCC regoleranno tale trasferimento, salvo le seguenti modifiche:
   (i) i riferimenti al GDPR includeranno anche il riferimento alle disposizioni equivalenti della legge locale sulla protezione dei dati;
   (ii) l'Autorità di Vigilanza locale è l'autorità di controllo esclusiva ai sensi della Clausola 13 e dell'Allegato I.C delle SCC UE;
   (iii) la legge applicabile ai sensi della Clausola 17 delle SCC UE sarà la legge locale sulla protezione dei dati; e
   (iv) il termine "stato membro" non deve essere interpretato in modo tale da escludere i soggetti interessati nel Paese dalla possibilità di far valere i propri diritti nel luogo di residenza abituale ai sensi della Clausola 18 delle SCC UE.

2.7. **Assistenza e Registri**

(a) Tenendo conto della natura del Trattamento, il Fornitore assisterà Intesa adottando adeguate Misure Tecniche e Organizzative ("**TOMs**") per adempiere agli obblighi associati alle richieste e ai diritti degli Interessati. Il Fornitore assisterà inoltre Intesa nel garantire la conformità agli obblighi relativi alla sicurezza del Trattamento, alla notifica e comunicazione di qualsiasi Incidente di Sicurezza e alla creazione di valutazioni d'impatto sulla protezione dei dati, inclusa la consultazione preventiva con l'autorità di controllo competente, se necessario, tenendo conto delle informazioni disponibili al Fornitore.

(b) Il Fornitore manterrà un registro aggiornato del nome e dei dettagli di contatto di ciascun Subresponsabile, inclusi i rappresentanti di ciascun Subresponsabile e il responsabile della protezione dei dati. Su richiesta, il Fornitore darà questo registro a Intesa secondo un programma che consentirà a Intesa di rispondere tempestivamente a qualsiasi richiesta da parte di un Cliente o di terze parti.

2.8. **Termini richiesti per Paese**

(a) **Giappone**

i) Per le BCI dei Soggetti Interessati situati in Giappone, il Fornitore si atterrà alle disposizioni dei presenti Termini, applicabili al Fornitore in qualità di Responsabile del Trattamento.

ii) La definizione di "Incidente di Sicurezza" nei presenti Termini è qui modificata per includere violazioni ragionevolmente sospette dei Dati Personali Intesa relativi agli Interessati situati in Giappone.

iii) Il Fornitore garantisce di non avere motivo di ritenere che le leggi e le pratiche di qualsiasi Paese in cui il Fornitore o i suoi Subresponsabili tratteranno i Dati Personali Intesa impediscano al Fornitore di adempiere ai suoi obblighi ai sensi dei presenti Termini. Il Fornitore notificherà a Intesa se, dopo aver accettato i Termini e per la durata dei Termini, il Fornitore ha motivo di ritenere di non poter adempiere al suo obbligo ai sensi dei Termini. In tal caso, le parti coopereranno in buona fede per identificare misure appropriate da adottare per affrontare la situazione. Qualora non fosse possibile implementare misure appropriate, Intesa valuterà se sospendere il trasferimento dei Dati Personali Intesa.

(b) **California**. Laddove il Fornitore, in qualità di Responsabile del Trattamento, tratti i Dati Personali Intesa degli Interessati situati nello Stato della California, (i) Intesa divulgherà i Dati Personali Intesa al Fornitore solo per le finalità commerciali limitate e specifiche selezionate nella relativa Appendice dei Dettagli del Trattamento, (ii) Intesa potrà, previa notifica, adottare misure ragionevoli e appropriate per interrompere il Trattamento non autorizzato o per garantire che il Trattamento da parte del Fornitore sia coerente con gli obblighi di Intesa ai sensi delle leggi applicabili sulla protezione dei dati, e (iii) il Fornitore non conserverà, utilizzerà o divulgherà i Dati Personali Intesa al di fuori del rapporto commerciale diretto tra Intesa e il Fornitore.

(c) **Canada**.

i) Per le BCI degli Interessati situati in Canada, il Fornitore si conformerà alle disposizioni delle presenti Condizioni d'Uso, applicabili al Fornitore in qualità di Responsabile del trattamento, nella misura in cui siano considerate Dati Personali.

ii) Per maggiore precisione, il richiamo alle leggi sulla protezione dei dati include tutte le linee guida vincolanti e le best practice emanate da un'Autorità di Vigilanza canadese avente giurisdizione, nelle versioni di volta in volta aggiornate o sostituite, come previsto dalle presenti Condizioni d'Uso.

iii) Il Fornitore non utilizzerà i Dati Intesa per creare un database di caratteristiche e/o misurazioni biometriche a scopo di identificazione personale.

iv) Il Fornitore eseguirà ogni valutazione d'impatto sulla privacy o sul trasferimento richiesta dalle leggi del Canada, fornendone copia su richiesta e notificando a Intesa senza indebito ritardo eventuali misure supplementari.

v) In caso di disaccordo sui risultati delle valutazioni del Fornitore, Intesa e il Fornitore collaboreranno per trovare una soluzione fattibile. In assenza di accordo, Intesa si riserva il diritto di sospendere o interrompere i servizi interessati senza alcun indennizzo.

vi) Il Fornitore collaborerà con Intesa fornendo le ulteriori informazioni ragionevolmente richieste per consentire a Intesa di valutare, in conformità con le leggi sulla protezione dei dati del Canada, se le Condizioni d'Uso assicurino una protezione dei Dati Personali adeguata.

Articolo III. SICUREZZA GENERALE

3.1. Policy di Sicurezza

(a) **Policy.** Le procedure di sicurezza informatica del Fornitore devono essere formalizzate, ricevere l'approvazione della direzione apicale e risultare allineate alle prassi standard internazionali quali il National Institute of Standards and Technology (NIST) e/o l'International Organization for Standardization (ISO). Le policy di sicurezza informatica del Fornitore saranno riviste e valutate dal Fornitore almeno annualmente e tempestivamente dopo qualsiasi modifica sostanziale apportata alle policy, per confermarne la continua applicabilità ed efficacia. Il Fornitore non apporterà modifiche alle policy che degraderebbero la sicurezza del Fornitore rispetto ai Materiali Intesa, ai Materiali o ai Servizi.

(b) **Test.** Il Fornitore definirà e manterrà un processo per testare regolarmente l'efficacia delle sue misure tecniche e organizzative per garantire la sicurezza dei Materiali Intesa, dei Materiali e dei Servizi.

(c) **Gestione dei Rischi**. Il Fornitore eseguirà valutazioni di rischio di sicurezza informatica appropriate come parte di un programma di governance del rischio continuo con i seguenti obiettivi: (i) identificare i rischi di sicurezza informatica relativi ai Materiali Intesa, ai Materiali e ai Servizi; (ii) valutare l'impatto di tali rischi; e (iii) laddove vengano identificate o giustificate strategie di riduzione o mitigazione del rischio,

implementare misure per mitigare e gestire efficacemente tali rischi, riconoscendo che il panorama delle minacce cambia costantemente.

3.2. Sicurezza del Personale

(a) **Formazione sulla sicurezza**. Il Fornitore assicurerà, almeno annualmente, un'adeguata sensibilizzazione, addestramento e formazione sulla sicurezza e sulla privacy a tutto il Personale del Fornitore che ha accesso o abbia la possibilità di accedere ai Materiali Intesa, ai Materiali o ai Servizi.

(b) **Controllo dei Precedenti**. Il Fornitore manterrà e seguirà i requisiti standard e obbligatori di verifica dell'impiego per tutte le nuove assunzioni di dipendenti ed estenderà tali requisiti a tutto il Personale del Fornitore e al Personale delle filiali controllate dal Fornitore. Tali requisiti includeranno controlli sui precedenti penali, nella misura consentita dalle leggi locali, la convalida della prova dell'identità e controlli aggiuntivi che il Fornitore ritenga necessari. Il Fornitore ripeterà e riconvaliderà periodicamente questi requisiti, come ritenuto necessario.

3.3. Gestione degli Asset

(a) **Inventario degli Asset**. Il Fornitore manterrà un inventario degli asset di tutte le apparecchiature su cui sono archiviati i Materiali Intesa. Il Fornitore limiterà l'accesso a tali apparecchiature solo al Personale del Fornitore autorizzato. Il Fornitore impedirà l'accesso non autorizzato, la copia, la modifica o la rimozione dei Materiali Intesa. Il Fornitore manterrà misure atte a prevenire l'accesso, la copia, la modifica o la cancellazione non autorizzati dei Materiali Intesa.

(b) **Sicurezza dei Componenti Software**. Il Fornitore si impegna a inventariare adeguatamente tutti i componenti software (compresi i software open source) utilizzati nell'ambito dell'erogazione dei Servizi e nello sviluppo e nella fornitura dei Materiali. Il Fornitore valuterà se tali componenti software presentano difetti di sicurezza e/o vulnerabilità che potrebbero portare alla divulgazione o all'accesso non autorizzato ai Materiali Intesa, ai Materiali o ai Servizi. Il Fornitore eseguirà tale valutazione prima della consegna o della concessione dell'accesso di Intesa ai Servizi e ai Materiali e, successivamente, in modo continuativo per la durata del Documento d'Ordine. Il Fornitore si impegna a correggere tempestivamente qualsiasi difetto di sicurezza o vulnerabilità in tali componenti software di cui il Fornitore venga a conoscenza. Il Fornitore risponderà prontamente a qualsiasi richiesta di Intesa relativa al fatto che un difetto di sicurezza o una vulnerabilità in tali componenti software sia conosciuto dal Fornitore e/o sia stato corretto dal Fornitore.

3.4. Policy di Controllo degli Accessi.

Il Fornitore manterrà una Policy di controllo degli accessi basata sui ruoli appropriata e misure tecniche di controllo degli accessi appropriate, coerenti con le Procedure Standard del Settore, per limitare l'accesso ai Materiali e alle risorse del Fornitore utilizzate per fornire i Servizi esclusivamente al Personale Autorizzato del Fornitore, e limitare tale accesso al livello minimo richiesto per fornire e supportare i Servizi e i Materiali. Tali accessi saranno registrati secondo i requisiti elencati nell'Articolo 3.10(f).

3.5. Autorizzazione

(a) Il Fornitore manterrà procedure di creazione e cancellazione degli account utente per concedere e revocare tempestivamente (e in ogni caso entro ventiquattro (24) ore) l'accesso a tutti i Materiali Intesa e a tutte le applicazioni e risorse interne del Fornitore utilizzate nell'erogazione dei Servizi e nella fornitura dei Materiali. Il Fornitore assegnerà a un'autorità appropriata l'approvazione della creazione e della revoca degli account utente o di livelli di accesso più elevati o ridotti per gli account esistenti, compresa la cessazione del rapporto di lavoro, del contratto, dell'incarico o di altro accordo del Personale con il Fornitore o di una modifica del ruolo se tale Personale non necessiti più tali diritti di accesso.

(b) Il Fornitore manterrà e aggiornerà i registri del Personale del Fornitore autorizzato ad accedere ai sistemi e alle risorse su cui sono archiviati, o da cui è possibile accedere ai Materiali Intesa e ai Materiali, o che sono utilizzati per erogare i Servizi, e riesaminerà tali registri almeno una volta a semestre. Il Personale di supporto amministrativo e tecnico sarà autorizzato ad accedere a tali sistemi, Materiali Intesa e Materiali solo quando richiesto e a condizione che tale Personale rispetti le misure tecniche e organizzative applicabili del Fornitore.

(c) Il Fornitore garantirà che gli account utente che hanno accesso a tali sistemi e risorse siano univoci e limitati da password e che gli account utente non siano condivisi.

3.6. Autenticazione

(a) Il Fornitore monitorerà i tentativi di accesso ripetuti ai sistemi informativi e agli asset.

(b) Il Fornitore manterrà pratiche di protezione delle password coerenti con le Procedure Standard del Settore e progettate per mantenere la riservatezza e l'integrità delle password generate, assegnate, distribuite e archiviate in qualsiasi forma. Il Fornitore genererà o richiederà all'utente di creare e utilizzare una password o passphrase complessa, generata casualmente e robusta, o alternative adeguate, come certificati digitali, schede/token hardware o dati biometrici.

(c) Il Fornitore utilizzerà l'autenticazione a più fattori, anche per l'accesso amministrativo al dominio e al portale cloud. L'autenticazione a più fattori può includere tecniche come l'uso di certificati crittografici, token di password monouso (OTP) o dati biometrici.

3.7. Crittografia

(a) **Policy**. Il Fornitore implementerà e manterrà policy e standard crittografici coerenti con le Procedure Standard del Settore per proteggere i Materiali Intesa, inclusi, ove appropriato, la pseudonimizzazione e la crittografia.

(b) **Crittografia**. Il Fornitore crittograferà i Materiali Intesa in transito e a riposo. Gli algoritmi di crittografia proteggeranno i dati a livelli di sicurezza coerenti con le Procedure Standard del Settore (come NIST SP 800-131a) e utilizzeranno funzioni di hashing riconosciute dal settore, che saranno almeno altrettanto protettive dello standard di crittografia Advanced Encryption Standard a 256 bit (AES 256) a riposo e TLS v1.2 in transito. Il Fornitore manterrà e seguirà policy e procedure di gestione delle chiavi coerenti con le Procedure Standard del Settore che definiscono i requisiti, la sicurezza, la rotazione e il ciclo di vita delle chiavi di crittografia, inclusi la creazione, la distribuzione, la revoca, l'archiviazione e la distruzione.

3.8. Sicurezza Fisica e Ambientale

(a) **Accesso alle Strutture**. Il Fornitore limiterà l'accesso alle Strutture al solo Personale autorizzato.

(b) **Protezione dalle Interruzioni**. Il Fornitore compirà sforzi ragionevoli per proteggere tali sistemi e risorse da interruzioni di corrente e altre interruzioni causate da guasti nei servizi di supporto.

(c) **Smaltimento o Riutilizzo Sicuro delle Apparecchiature**. Il Fornitore garantirà che tutti i Materiali Intesa siano stati eliminati o sovrascritti in modo sicuro dalle apparecchiature contenenti supporti di archiviazione, utilizzando processi conformi alle Procedure Standard del Settore, prima dello smaltimento o del riutilizzo di tali apparecchiature.

3.9. Sicurezza Operativa

(a) **Policy Operativa**. Il Fornitore manterrà procedure operative e di sicurezza appropriate e tali procedure saranno rese disponibili a tutto il Personale che ne abbia bisogno.

(b) **Protezioni da Malware**. Il Fornitore implementerà soluzioni antivirus e di gestione degli endpoint per mantenere i controlli anti-malware al fine di proteggere tali sistemi e asset da software dannoso, incluso software dannoso proveniente da reti pubbliche.

(c) **Gestione della Configurazione**. Il Fornitore definirà Policy che regolino l'installazione di software e utility da parte del Personale.

(d) **Gestione delle Modifiche**. Il Fornitore manterrà e implementerà procedure per garantire che solo versioni approvate e sicure del codice, delle configurazioni, dei sistemi e delle applicazioni vengano implementate negli ambienti di produzione.

(e) **Separazione Logica**. Il Fornitore manterrà un adeguato isolamento dei propri ambienti di produzione, non di produzione e altri, e, se i Materiali Intesa sono già presenti o vengono trasferiti in un ambiente non di produzione (ad esempio, per riprodurre un errore), il Fornitore garantirà che le protezioni di sicurezza e privacy nell'ambiente non di produzione siano uguali a quelle dell'ambiente di produzione.

3.10. Sicurezza delle Comunicazioni

(a) **Trasferimento delle Informazioni**. Il Fornitore limiterà l'accesso tramite crittografia ai Materiali Intesa archiviati su supporti fisicamente trasportati al di fuori delle Strutture. Il Fornitore assicurerà che sia possibile verificare e stabilire la misura in cui i Materiali Intesa sono stati o possano essere trasmessi o resi disponibili utilizzando apparecchiature di comunicazione dati.

(b) **Sicurezza dei Servizi di Rete**. Il Fornitore assicurerà che i controlli e le procedure di sicurezza siano implementati per tutti i servizi e i componenti di rete in conformità con le Procedure Standard del Settore, indipendentemente dal fatto che tali servizi siano forniti internamente o esternalizzati.

(c) **Rilevamento delle Intrusioni**. Il Fornitore implementerà sistemi e misure di rilevamento delle intrusioni o di prevenzione delle intrusioni per la prevenzione di attacchi DoS (denial of service) per tutti i sistemi utilizzati nell'erogazione dei Servizi e nella fornitura dei Materiali, tali misure includeranno anche la sorveglianza continua atta a intercettare e rispondere agli eventi di sicurezza man mano che vengono identificati e l'aggiornamento del database delle firme non appena saranno disponibili nuove versioni per la distribuzione commerciale.

(d) **Firewall**. Il Fornitore implementerà firewall che consentano l'utilizzo solo di porte e servizi documentati e approvati. Tutte le altre porte saranno in modalità "nega tutto".

(e) **Monitoraggio**. Il Fornitore monitorerà l'utilizzo degli accessi privilegiati e manterrà misure di gestione delle informazioni e degli eventi di sicurezza per: (i) identificare accessi e attività non autorizzati, (ii) facilitare una risposta tempestiva e appropriata a tali accessi e attività, e (iii) consentire audit da parte del Fornitore e di Intesa.

(f) **Registrazione**. Il Fornitore adotterà procedure per garantire che tutti i sistemi, inclusi firewall, router, switch di rete e sistemi operativi, registrino le informazioni nel rispettivo log di sistema o in un sistema di registrazione centralizzato, al fine di consentire gli audit di sicurezza di cui di seguito. Il Fornitore dovrà: (i) conservare i log per almeno 180 giorni, (ii) assicurarsi che nessun log contenga informazioni riservate, (iii) proteggere i log da modifiche o cancellazioni non autorizzate, (iv) eseguire backup giornalieri dei log e (v) monitorare i log per rilevare eventuali anomalie funzionali e rischi. Il Fornitore fornirà tali log a Intesa su richiesta.

3.11. *Acquisizione, Sviluppo e Manutenzione del Sistema*

3.11.1 Aggiornamento e Manutenzione

3.11.1.1 Il Fornitore si impegna ad effettuare, a proprie spese senza addebito di ulteriori costi e trasferte a carico di Intesa, tutte le operazioni di aggiornamento e manutenzione del Servizio e/o del Software necessarie per l'erogazione dello stesso secondo gli standard di sicurezza garantiti ad Intesa con il documento MPO.

3.11.1.2 Il Fornitore, inoltre, garantisce che ogni componente software fornita ad Intesa è conforme ai principi SSDLC (ciclo di sviluppo sicuro - Secure Software Development Lifecycle), così da assicurare la protezione dell'infrastruttura, dei dati e dei processi aziendali di Intesa. Tali obbligazioni costituiscono i requisiti minimi di sicurezza informatica che devono essere rispettati da tutti i fornitori di software e servizi che collaborano con Intesa.

3.11.1.3 In particolare, il Fornitore si impegna a rispettare le seguenti obbligazioni:

a) Obblighi di Sicurezza del Fornitore

Il Fornitore si impegna a garantire che ogni componente software o servizio fornito a Intesa rispetti i seguenti requisiti di sicurezza applicativa. In particolare, il fornitore deve eseguire le seguenti attività di verifica della sicurezza, almeno una volta all'anno e obbligatoriamente ad ogni major release, aggiornamento significativo del codice, modifica architetturale o rilascio funzionale:

- Penetration Test (PT)
- • Static Application Security Testing (SAST)
- • Dynamic Application Security Testing (DAST)
- • Software Composition Analysis (SCA)

I risultati di tali attività devono essere documentati in appositi report, completi di:

- • Metodologia utilizzata
- • Vulnerabilità identificate con servizi punteggio CVSS
- • Evidenze tecniche
- • Piano di remediation

I report devono essere consegnati a Intesa entro 10 giorni lavorativi dalla conclusione delle attività.

b) Vulnerability Assessment (VA) e Penetration test (PT)

Qualora il software venga installato sui sistemi di Intesa, l'attività di Vulnerability Assessment (VA) e Penetration Test (PT) sarà eseguita da Intesa stessa.

Nel caso in cui il software sia gestito, ospitato o distribuito dal Fornitore (es. modelli SaaS, cloud privato o pubblico), il Fornitore è responsabile anche della conduzione del VA, oltre a PT, SAST, DAST e SCA.

c) Ciclo di Sviluppo Sicuro (SSDLC)

Il Fornitore dovrà dimostrare l'adozione di pratiche sicure nello sviluppo del software, inclusi ma non limitati a:

- Analisi delle minacce (Threat Modeling)
- Validazione sicura dell'input
- Gestione sicura delle dipendenze
- Controlli di accesso e gestione delle identità
- Logging e tracciamento delle attività
- Protezione delle API e dei servizi esposti
- Testing di sicurezza automatizzato integrato nel CI/CD pipeline

Condividendo con INTESA le procedure adottate, senza indebito ritardo.

3.11.1.4 Vulnerabilità. Rispetto ad eventuali vulnerabilità che dovessero essere identificate nel corso dei servizi, il Fornitore dovrà porvi rimedio secondo le tempistiche di seguito indicate.

A. Nel caso in cui una vulnerabilità venga:

I. Identificata dal Fornitore stesso, nell'ambito della propria attività di monitoraggio e gestione della sicurezza;

II. Segnalata da INTESA in seguito ad un utilizzo ordinario del Servizio,

il Fornitore si impegna a porre rimedio entro i termini indicati nella tabella seguente, salvo che non sia diversamente concordato per iscritto tra le Parti:

Livello di gravità	Tempo massimo per la risoluzione
Critico	1 settimana
Alto	2 settimane
Medio	4 settimane
Basso	12 settimane

I livelli di gravità di cui alla precedente tabella, sono dettagliati come segue:

Livello di gravità: Critico

Le vulnerabilità che ottengono un punteggio nell'intervallo critico di solito hanno la maggior parte delle seguenti caratteristiche:

- Lo sfruttamento della vulnerabilità probabilmente comporta la compromissione a livello di root di server o dispositivi dell'infrastruttura.

- Lo sfruttamento è solitamente semplice, nel senso che l'attaccante non ha bisogno di particolari credenziali di autenticazione o conoscenza delle singole vittime e non ha bisogno di convincere un utente bersaglio, ad esempio tramite l'ingegneria sociale, a svolgere funzioni speciali.

Disponibilità di una versione correttiva, di una patch o comunque di una soluzione entro e non oltre 1 settimana, salvo che non sia diversamente concordato per iscritto tra le Parti.

Livello di gravità: Alto

Le vulnerabilità che ottengono un punteggio nella fascia alta di solito hanno alcune delle seguenti caratteristiche:

- La vulnerabilità è difficile da sfruttare.

- Lo sfruttamento potrebbe comportare privilegi elevati.

- Lo sfruttamento potrebbe comportare una significativa perdita di dati o tempi di inattività.

Disponibilità di una versione correttiva, di una patch o comunque di una soluzione entro e non oltre 2 settimane, salvo che non sia diversamente concordato per iscritto tra le Parti.

Livello di gravità: Medio

Le vulnerabilità con un punteggio medio di solito hanno alcune delle seguenti caratteristiche:

- Vulnerabilità che richiedono all'attaccante di manipolare le singole vittime tramite tattiche di ingegneria sociale.

- Vulnerabilità Denial of Service difficili da impostare.

- Exploit che richiedono a un utente malintenzionato di risiedere sulla stessa rete locale della vittima.

- Vulnerabilità in cui lo sfruttamento fornisce solo un accesso molto limitato.

- Vulnerabilità che richiedono privilegi utente per essere sfruttate con successo.

Disponibilità di una versione correttiva, di una patch o comunque di una soluzione entro e non oltre 4 settimane, salvo che non sia diversamente concordato per iscritto tra le Parti.

Livello di gravità: Basso

Le vulnerabilità nella fascia bassa in genere hanno un impatto minimo sull'attività di un'organizzazione. Lo sfruttamento di tali vulnerabilità di solito richiede l'accesso al sistema locale o fisico.

Disponibilità di una versione correttiva, di una patch o comunque di una soluzione entro e non oltre 12 settimane, salvo che non sia diversamente concordato per iscritto tra le Parti.

B) Nel caso in cui una vulnerabilità venga individuata a seguito di un'attività di assessment tecnico formalmente richiesta da Intesa (es. Penetration Test, Vulnerability Assessment, SAST, DAST, SCA), il Fornitore si impegna a porre rimedio entro i termini indicati nella tabella seguente, sulla base del livello di gravità assegnato secondo le linee guida CVSS.

Livello di Gravità	Descrizione	Tempo massimo per la risoluzione
Critico	Vulnerabilità con impatto massimo (es. RCE, escalation privilegi da remoto, senza autenticazione).	1 settimana
Alto	Potenziale perdita di dati o privilegio elevato, richiede condizioni più complesse.	2 settimane
Medio	Richiede interazione utente o accesso alla stessa rete locale.	8 settimane
Basso	Impatto minimo. Exploit locali o fisici difficili da realizzare.	12 settimane

Nell'ipotesi in cui il Fornitore non adempia alle obbligazioni dei punti A) e B) del presente articolo entro i termini ivi previsti, Intesa avrà il diritto di applicare, per ogni giorno di ritardo, una penale pari al 2% del valore del PO applicabile, fatto salvo in ogni caso il diritto per Intesa di risolvere il PO applicabile e/o il Contratto, secondo quanto previsto dalle CGA, configurandosi in tale ipotesi un inadempimento grave da parte del Fornitore.

3.11.2 (a) Consolidamento dell'Applicazione

i) Il Fornitore manterrà e implementerà policy, procedure e standard di sviluppo di applicazioni sicure, coerenti con le Procedure Standard del Settore, come le Tecniche di Sviluppo per la Sicurezza SANS Top 25 o il progetto OWASP Top Ten.

ii) Tutto il Personale del Fornitore responsabile della progettazione, sviluppo, configurazione, test e distribuzione di applicazioni sicure sarà qualificato per eseguire i Servizi e sviluppare i Materiali e riceverà una formazione adeguata sulle pratiche di sviluppo di applicazioni sicure del Fornitore.

3.11.2 (b) Consolidamento del sistema

iii) Il Fornitore implementerà e garantirà l'uso di configurazioni standard sicure dei sistemi operativi. Le immagini dovranno rappresentare versioni consolidate del sistema operativo sottostante e delle applicazioni installate sul sistema. Il consolidamento include la rimozione di account non necessari (inclusi gli account di servizio), la disabilitazione o la rimozione di servizi non necessari, l'applicazione di

patch, la chiusura di porte di rete aperte e inutilizzate e l'implementazione di sistemi di rilevamento delle intrusioni e/o sistemi di prevenzione delle intrusioni. Queste immagini dovranno essere convalidate regolarmente per aggiornare la loro configurazione di sicurezza, ove necessario. Il Fornitore implementerà strumenti e processi di applicazione di patch sia per le applicazioni che per il software del sistema operativo. Laddove, su sistemi obsoleti, non possano più essere installate patch, il Fornitore provvederà ad aggiorna tali sistemi all'ultima versione del software applicativo. Il Fornitore rimuoverà software obsoleto, non supportato e inutilizzato dal sistema.

iv) Il Fornitore limiterà i privilegi amministrativi solo a quel personale che ha sia la conoscenza necessaria per amministrare il sistema operativo sia un'esigenza aziendale di modificare la configurazione del sistema operativo sottostante.

3.11.2 (c) Scansione delle Vulnerabilità dell'Infrastruttura.

Il Fornitore effettuerà mensilmente la scansione dei propri ambienti interni (ad es. server, dispositivi di rete, ecc.) relativi ai Servizi e ai Materiali, e settimanalmente la scansione degli ambienti esterni relativi ai Servizi e ai Materiali. Il Fornitore avrà un processo definito e documentato con tempistiche specifiche per affrontare eventuali rilevamenti commisurati al rischio posto e al livello di gravità.

3.11.2 (d) Valutazione delle Vulnerabilità delle Applicazioni.

Il Fornitore effettuerà una valutazione delle vulnerabilità della sicurezza delle applicazioni prima di ogni nuova release pubblica. Il Fornitore avrà un processo definito e documentato per affrontare eventuali risultati commisurati al rischio posto.

3.11.2 (e) Test di Penetrazione e Valutazioni di Sicurezza.

Il Fornitore incaricherà una terza parte indipendente riconosciuta nel settore per l'esecuzione di un test di penetrazione completo e di una valutazione della sicurezza di tutti i sistemi coinvolti nella fornitura dei Servizi e dei Materiali, su base ricorrente e con frequenza non inferiore a una volta all'anno. Il Fornitore avrà un processo definito e documentato per affrontare eventuali risultati commisurati al rischio posto. Su richiesta scritta di Intesa, ma non più di una volta all'anno, il Fornitore fornirà un'attestazione che confermi che è stato completato un test di penetrazione indipendente di terze parti e che il Fornitore ha implementato un processo per affrontare quanto rilevato secondo una valutazione dei rischi. Il Fornitore fornirà un riepilogo dei rilevamenti, incluso il numero di sistemi o applicazioni testati, le date dei test, la metodologia di test e il numero di risultati critici, alti, medi e bassi.

3.11.2 (f) Disaster Recovery.

Per l'intera durata dell'Accordo, il Fornitore manterrà una soluzione di disaster recovery ("**DR**") o di alta disponibilità ("**HA**") e un piano correlato per i Servizi e i Materiali, coerenti con le Procedure Standard del Settore. Il Fornitore testerà la soluzione DR o HA e il piano correlato almeno una volta all'anno. Inoltre, la soluzione e il piano garantiranno:

i) che i sistemi installati utilizzati per erogare i Servizi e fornire i Materiali saranno ripristinati in caso di interruzione,

ii) la capacità del Fornitore di ripristinare la disponibilità e l'accesso ai Materiali Intesa in modo tempestivo in caso di incidente fisico o tecnico, e

iii) la continua riservatezza, integrità, disponibilità e resilienza dei sistemi utilizzati dal Fornitore per erogare i Servizi e fornire i Materiali.

3.12. Continuità delle operazioni aziendali

Il Fornitore garantisce di avere e mantenere un piano di continuità delle operazioni aziendali e procedure di test della continuità delle operazioni aziendali che includeranno, a titolo esemplificativo e non esaustivo, le aree della pianificazione di disaster recovery, della pianificazione in caso di pandemia e della sicurezza informatica. I programmi di sicurezza informatica devono includere, come minimo, disposizioni atte a prevenire e rilevare incidenti di sicurezza informatica e rispondere agli stessi. Il Fornitore accetta di fornire gli obiettivi specifici di ripristino del piano di continuità delle operazioni aziendali e di riesaminare, aggiornare e sottoporre a test annualmente il piano di continuità delle operazioni aziendali e, su richiesta di Intesa, il Fornitore dovrà fornire un riepilogo del piano di continuità delle operazioni aziendali e dei risultati dei test. Intesa può, di tanto in tanto, fornire feedback in merito al piano e richiedere al Fornitore che i commenti di Intesa vengano tenuti in considerazione durante l'aggiornamento dello stesso. Tuttavia, il Fornitore rimane l'unico responsabile dell'adempimento delle proprie responsabilità ai sensi

del Contratto e dell'adeguatezza del piano di continuità delle operazioni aziendali, indipendentemente dal fatto che Intesa abbia riesaminato o fatto commenti sul piano.

3.13. Incidenti di Sicurezza

(a) Il Fornitore implementerà e seguirà un programma di risposta agli incidenti di sicurezza delle informazioni conforme alle Procedure Standard del Settore, incluse procedure documentate per l'indagine e la gestione degli incidenti di sicurezza delle informazioni. Il programma di risposta agli incidenti di sicurezza delle informazioni tratterà argomenti quali la definizione delle priorità degli incidenti, i ruoli e le responsabilità, le procedure di escalation interne, il tracciamento e la segnalazione, il contenimento e il ripristino. Il programma di gestione degli incidenti di sicurezza delle informazioni sarà testato, rivisto e approvato periodicamente, ma almeno annualmente.

(b) Il Fornitore informerà prontamente (e in nessun caso oltre le 24 ore) Intesa dopo essere venuto a conoscenza di un Incidente di Sicurezza, inviando un'e-mail a cybersecurity@intesa.it. In relazione a un Incidente di Sicurezza, il Fornitore dovrà prontamente:

i) fornire a Intesa le informazioni ragionevolmente richieste su tale incidente, sull'indagine a riguardo del Fornitore e sullo stato delle attività di ripristino e rimedio del Fornitore. A titolo di esempio, le informazioni ragionevolmente richieste possono includere i risultati fattuali relativi alla natura, alla causa e all'impatto dell'incidente, i log che dimostrano l'accesso privilegiato, amministrativo e di altro tipo a Dispositivi, sistemi, servizi o applicazioni, i riepiloghi basati su immagini forensi di Dispositivi, sistemi o applicazioni e altri elementi simili, nella misura in cui siano rilevanti per l'incidente o per le attività di mitigazione, rimedio e ripristino del Fornitore;

ii) assicurare che il Personale del Fornitore appropriato con conoscenza dell'incidente partecipi alle conferenze telefoniche richieste da Intesa;

iii) coinvolgere esperti di terze parti in materia di risposta agli incidenti, gestione degli incidenti di violazione dei dati, analisi forensi e scoperta elettronica, su ragionevole richiesta di Intesa;

iv) fornire a Intesa ragionevole assistenza per soddisfare eventuali obblighi legali (inclusi gli obblighi di notifica alle autorità di regolamentazione, agli Interessati, ai Clienti o ad altre terze parti) di Intesa, delle affiliate di Intesa e dei Clienti (e dei loro clienti e affiliate); e

v) mitigare e porre rimedio tempestivamente e adeguatamente agli effetti dell'Incidente di Sicurezza e implementare controlli e processi aggiuntivi per ridurre il rischio di incidenti simili in futuro, tenendo in debita considerazione qualsiasi contributo di Intesa su tali mitigazioni e rimedi.

(c) Il Fornitore è responsabile di tutti i costi e le spese sostenute dal Fornitore nell'indagare, rispondere, mitigare e porre rimedio a un Incidente di Sicurezza. Fatta salva la limitazione di responsabilità prevista dall'Accordo, il Fornitore è anche responsabile di tutti i costi e le spese vive sostenute da Intesa e dai Clienti (e dai loro clienti e affiliate) in relazione all'indagine, alla risposta, alla mitigazione e alla risoluzione dell'Incidente di Sicurezza. I costi e le spese di rimedio dell'Incidente di Sicurezza possono includere i costi relativi al rilevamento e all'indagine di un Incidente di Sicurezza, alla determinazione delle responsabilità ai sensi di leggi e regolamenti, al ricaricamento dei dati, alla correzione dei difetti del prodotto (anche tramite Codice Sorgente o altro sviluppo), all'ingaggio di terze parti per assistere con quanto sopra o altre attività pertinenti e altri costi e spese necessari per rimediare agli effetti dannosi dell'Incidente di Sicurezza.
In caso di Incidente di Sicurezza che coinvolga Dati Personali Intesa, il Fornitore è responsabile di tutti i costi da esso sostenuti e rimborserà a Intesa tutti i costi e le spese sostenute da Intesa in relazione alla notifica dell'Incidente di Sicurezza alle autorità di regolamentazione competenti, ad altri enti governativi e agenzie di autoregolamentazione del settore pertinenti, ai media (se richiesto dalla legge applicabile), agli Interessati, ai Clienti e ad altri;

(d) Il Fornitore non rivelerà a terzi che Intesa è stata colpita da un Incidente di Sicurezza, a meno che Intesa non lo approvi per iscritto o se richiesto dalla legge. Il Fornitore informerà Intesa per iscritto prima di distribuire qualsiasi notifica legalmente richiesta a terzi che riveli, direttamente o indirettamente, l'identità di Intesa.

(e) Il Fornitore informerà anche tempestivamente Intesa di qualsiasi minaccia effettiva o imminente di violazione dei presenti Termini o delle sue Policy di sicurezza, procedure di sicurezza o Policy di utilizzo accettabile relative alla fornitura di un Materiale da Consegnare o all'erogazione dei Servizi.

3.14. Relazioni con i Fornitori

(a) **Subappaltatori**. Il Fornitore è responsabile della conformità ai presenti Termini anche se utilizza un Subappaltatore. Il Fornitore si impegnerà contrattualmente a far sì che tali Subappaltatori proteggano i Materiali di Intesa attraverso termini non meno completi o rigorosi di quelli applicabili al Fornitore nei

Termini. Il Fornitore è responsabile nei confronti di Intesa dell'esecuzione delle prestazioni di ciascun Subappaltatore.

(b) **Controllo Qualità e Gestione della Sicurezza**. Il Fornitore si farà carico della supervisione del controllo qualità e della gestione della sicurezza dello sviluppo software esternalizzato a un Subappaltatore.

(c) **Informazioni Precontrattuali**. Il Fornitore dichiara e garantisce che tutte le informazioni materiali fornite durante le discussioni precontrattuali con Intesa relative alla privacy, alla sicurezza e alla governance dei dati, ai sensi dei presenti Termini o altrimenti, sono accurate in tutti gli aspetti materiali e non sono, per omissione o altro, fuorvianti.

3.15. Verifica, Cooperazione, Conformità alla Sicurezza e Valutazione.

(a) **Verifica.** Il Fornitore manterrà una documentazione verificabile che dimostri la conformità ai presenti Termini.

(i) Intesa, da sola o con l'ausilio di un revisore esterno, potrà, con preavviso scritto di 30 giorni al Fornitore, verificare il rispetto da parte del Fornitore dei presenti Termini, anche, per tale scopo, accedendo a una qualsiasi Struttura, sebbene Intesa non accederà ad alcun data center in cui il Fornitore Tratti Dati Intesa a meno che non abbia in buona fede motivo di ritenere che ciò fornirebbe informazioni pertinenti. Il Fornitore collaborerà nelle verifiche di Intesa anche rispondendo tempestivamente e pienamente alle richieste di informazioni, attraverso documenti, altri registri, colloqui con il Personale del Fornitore, o simili. Il Fornitore può fornire la prova dell'adesione a un codice di condotta approvato oppure a una certificazione del settore o fornire in altro modo informazioni per dimostrare la conformità ai presenti Termini, a titolo oneroso da parte di Intesa.

(ii) Le verifiche non avverranno con una cadenza inferiore ai 12 mesi, a meno che: (A) Intesa non stia verificando i rimedi messi in atto dal Fornitore rispetto ai timori risultanti da una verifica precedente e più recente di 12 mesi o (B) sia stata rilevata un Incidente di Sicurezza e Intesa desideri verificare il rispetto degli obblighi in relazione a tale incidente. In entrambi i casi, Intesa fornirà lo stesso preavviso scritto di 30 giorni come specificato al comma (i) precedente, ma l'urgenza di far fronte a un Incidente di Sicurezza potrà richiedere a Intesa di effettuare una verifica con preavviso scritto inferiore a 30 giorni.

(iii) Un organismo regolatore o un Altro Titolare del Trattamento dei Dati Personali potrà esercitare gli stessi diritti di Intesa di cui ai commi (ii) e (iii), con la consapevolezza che un organismo regolatore potrà esercitare tutti i diritti aggiuntivi di cui dispone ai sensi della legge.

(iv) Qualora Intesa disponesse di basi ragionevoli per concludere che il Fornitore non è conforme con i presenti Termini (indipendentemente dal fatto che tali basi derivino da una verifica ai sensi dei presenti Termini o altro), il Fornitore rimedierà prontamente a tale non conformità.

(v) Il presente Articolo si applica in aggiunta alla clausola "Tenuta dei Registri e Diritti di Audit" o altra clausola di Audit simile nell'Accordo.

(b) **Cooperazione**. Se Intesa ha motivo credere che alcuni Servizi o Materiali possano aver contribuito, stiano contribuendo o contribuiranno a qualsiasi problema di sicurezza informatica, il Fornitore collaborerà a rispondere a qualsiasi domanda di Intesa relativa a tale timore, rispondendo tempestivamente e pienamente alle richieste di informazioni, attraverso documenti, altri registri, colloqui con il Personale del Fornitore, o simili.

(c) **Conformità alla Sicurezza**. Il Fornitore otterrà (i) una certificazione di conformità alla ISO 27001, da una società di revisione pubblica indipendente, (ii) un rapporto di una società di revisione pubblica indipendente che dimostri la revisione dei sistemi, dei controlli e delle operazioni del Fornitore in conformità con un SOC 2 Type 2, che includerà come minimo i Principi di Servizio di Fiducia di Sicurezza (noti anche come Criteri Comuni), Disponibilità e Riservatezza, e (iii) un rapporto di una società di revisione pubblica indipendente che dimostri la revisione dei sistemi, dei controlli e delle operazioni del Fornitore in conformità con un SOC 1 Type 2, se i Servizi influenzano i rapporti finanziari di Intesa. Il Fornitore si atterrà alle future linee guida relative alla SSAE18 emesse dall'AICPA, dall'IAASB, dalla Securities and Exchange Commission o dalla Public Company Accounting Oversight Board. Su richiesta, il Fornitore fornirà tempestivamente a Intesa una copia di ciascun certificato e rapporto che il Fornitore è obbligato a ottenere.

(d) **Valutazione di Conformità di Intesa**. Su ragionevole richiesta di Intesa, ma non più di una volta in un periodo di 12 mesi per ciascun singolo Servizio o Materiale da Consegnare, il Fornitore compilerà in modo accurato e tempestivo (entro un massimo di 14 giorni) un questionario per verificare la conformità del Fornitore ai suoi obblighi di sicurezza informatica e governance dei dati ai sensi del Contratto e dei presenti Termini ("**Valutazione di Conformità**"). Se, dopo il completamento della Valutazione di Conformità, Intesa determina

ragionevolmente che le pratiche e le procedure di sicurezza e governance dei dati del Fornitore non soddisfano gli obblighi del Fornitore, Intesa notificherà al Fornitore le carenze. Se il Fornitore concorda con la valutazione delle carenze di Intesa, il Fornitore, senza ingiustificato ritardo: (i) correggerà tali carenze a proprie spese entro un periodo di tempo concordato con Intesa sulla base di una valutazione del rischio; e (ii) fornirà a Intesa, o ai suoi rappresentanti debitamente autorizzati, ragionevole documentazione e informazioni che confermino la risoluzione delle carenze. Se il Fornitore non riesce a risolvere le carenze classificate come elevate o critiche entro il periodo di tempo concordato, Intesa ha il diritto di risolvere immediatamente per inadempimento sostanziale il Contratto o PO applicabili previa notifica al Fornitore. Intesa non divulgherà la documentazione a terzi diversi dai propri revisori senza il consenso scritto del Fornitore. Se il Fornitore non concorda con la valutazione delle carenze di Intesa, il Fornitore fornirà tempestivamente a Intesa una spiegazione scritta che ne dettagli i suoi motivi e, se Intesa non accetta i motivi del Fornitore, le parti si rivolgeranno ai rispettivi Responsabili della Privacy, Responsabili della Sicurezza delle Informazioni o a un dirigente con ambito e autorità simili per una risoluzione tempestiva. Se eventuali carenze sono causate dall'uso dei Servizi da parte di Intesa, il Fornitore fornirà un ragionevole supporto tecnico per assistere Intesa nell'uso appropriato dei Servizi per risolvere tali carenze.

Articolo IV. ACCESSO ALLE RETI INTESA

Questo Articolo si applica se i dipendenti del Fornitore avranno accesso ad un qualsiasi Sistema Aziendale.

4.1. Condizioni Generali

(a) Intesa determinerà se autorizzare i dipendenti del Fornitore ad accedere ai Sistemi Aziendali. Se Intesa lo autorizza, il Fornitore rispetterà e farà anche in modo che i propri dipendenti con tale accesso rispettino i requisiti di questo Articolo.

(b) Intesa identificherà i mezzi con cui i dipendenti del Fornitore potranno accedere ai Sistemi Aziendali, incluso se tali dipendenti accederanno ai Sistemi Aziendali tramite Dispositivi forniti da Intesa o dal Fornitore.

(c) I dipendenti del Fornitore possono accedere ai Sistemi Aziendali e utilizzare i Dispositivi autorizzati da Intesa per tale accesso, al fine di erogare i Servizi, che saranno un Dispositivo fornito da Intesa ("Dispositivo Intesa") o un Dispositivo fornito dal Fornitore ("Dispositivo del Fornitore").

(d) I dipendenti del Fornitore non copieranno i Materiali Intesa accessibili tramite un Sistema Aziendale senza la previa approvazione scritta di Intesa (e non copieranno mai alcun Materiale Intesa su un dispositivo di archiviazione portatile, come una USB, un disco rigido esterno o altri elementi simili).

(e) Su richiesta, il Fornitore confermerà, tramite il nome del dipendente, i Sistemi Aziendali specifici a cui i suoi dipendenti sono autorizzati ad accedere e hanno avuto accesso, in qualsiasi periodo di tempo identificato da Intesa.

(f) Il Fornitore informerà Intesa entro ventiquattro (24) ore dal momento in cui un dipendente del Fornitore con accesso a un Sistema Aziendale non è più: (i) impiegato dal Fornitore o (ii) impegnato in attività che richiedono tale accesso. Il Fornitore collaborerà con Intesa per garantire che l'accesso per tali dipendenti precedenti o attuali venga immediatamente revocato.

(g) Il Fornitore segnalerà immediatamente a Intesa qualsiasi incidente di sicurezza effettivo o sospetto (come la perdita di un Dispositivo Intesa o di un Dispositivo Fornitore o l'accesso non autorizzato a un Dispositivo Intesa o a un Dispositivo Fornitore o a dati, materiali o altre informazioni di qualsiasi tipo) e collaborerà con Intesa nelle indagini su tali incidenti.

(h) Il Fornitore non può consentire ad alcun agente, appaltatore indipendente o dipendente del subappaltatore di accedere a qualsiasi Sistema Aziendale, senza il previo consenso scritto di Intesa; se Intesa fornisce tale consenso, il Fornitore impegnerà contrattualmente tali persone e i relativi datori di lavoro al rispetto dei requisiti del presente Articolo come se tali persone fossero dipendenti del Fornitore e sarà responsabile nei confronti di Intesa per tutte le azioni e le omissioni ad agire di tale persona o datore di lavoro rispetto a tale accesso al Sistema Aziendale.

(i) Intesa potrà revocare l'accesso ai Sistemi Aziendali in qualsiasi momento, per qualsiasi dipendente del Fornitore o per tutto il Personale del Fornitore, senza preavviso al Fornitore, a qualsiasi dipendente del Fornitore o ad altri, se Intesa ritiene che ciò sia necessario ai fini della sicurezza.

(j) I diritti di Intesa non sono bloccati, diminuiti o limitati in alcun modo da alcuna disposizione del Documento d'Ordine, dal Contratto tra le Parti o da qualsiasi altro accordo tra le parti, inclusa qualsiasi disposizione che possa richiedere di ubicare dati, materiali o altre informazioni di qualsiasi tipo solo in una o più posizioni selezionate o che possa richiedere che solo le persone di una o più sedi selezionate accedano a tali dati,

materiali o altre informazioni.

4.2. Software del Dispositivo

(a) Il Fornitore istruirà il proprio Personale a installare tempestivamente il software sui Dispositivi Intesa e sui Dispositivi del Fornitore, richiesto da Intesa per facilitare l'accesso ai Sistemi Aziendali in modo sicuro. Né il Fornitore né il suo Personale interferiranno con il funzionamento di tale software o con le funzionalità di sicurezza abilitate dal software.

(b) Il Fornitore e il suo Personale rispetteranno le regole di configurazione per i Dispositivi Intesa e i Dispositivi del Fornitore stabilite da Intesa e collaboreranno con Intesa per garantire che il software funzioni come previsto da Intesa. Ad esempio, il Fornitore non sostituirà il blocco del sito Web del software o le funzionalità di applicazione automatizzata delle patch.

(c) Il Personale del Fornitore non può condividere nomi utente, password o simili per i Dispositivi Intesa e i Dispositivi del Fornitore con altre persone.

(d) Se Intesa autorizza il Personale del Fornitore ad accedere ai Sistemi Aziendali utilizzando i Dispositivi del Fornitore, il Fornitore installerà ed eseguirà su tali Dispositivi un sistema operativo approvato da Intesa ed eseguirà l'aggiornamento a una nuova versione di tale sistema operativo o di un nuovo sistema operativo entro un tempo ragionevole dall'indicazione a fare ciò da parte di Intesa.

4.3. Dispositivi Intesa

(a) I dipendenti del Fornitore non possono utilizzare i Dispositivi Intesa per fornire servizi a terzi o altre entità, né per accedere a sistemi IT, reti, applicazioni, siti web, strumenti di posta elettronica, strumenti di collaborazione o simili del Fornitore o di terze parti, per o in relazione ai Servizi. I dipendenti del Fornitore non possono utilizzare i Dispositivi Intesa per motivi personali (ad esempio, i dipendenti del Fornitore non possono archiviare file personali come musica, video, immagini o altri elementi simili su tali Dispositivi Intesa e non possono utilizzare Internet da tali Dispositivi Intesa per motivi personali). I dipendenti del Fornitore non possono condividere i Dispositivi Intesa che utilizzano per accedere ai Sistemi Aziendali con altri dipendenti del Fornitore.

(b) Intesa ha il diritto incondizionato per monitorare e porre rimedio a potenziali intrusioni e altre minacce alla sicurezza informatica in qualunque modo, da qualunque luogo e utilizzando qualsiasi mezzo che Intesa ritenga necessario o appropriato, senza preavviso al Fornitore, a qualsiasi dipendente del Fornitore o ad altri. A titolo di esempio di tali diritti, Intesa può, in qualsiasi momento, (i) eseguire un test di sicurezza su qualsiasi Dispositivo Intesa, (ii) monitorare, recuperare tramite mezzi tecnici o di altro tipo e rivedere comunicazioni (incluse e-mail da qualsiasi account di posta elettronica sui Dispositivi Intesa), log, file e altri elementi archiviati in qualsiasi Dispositivo Intesa o trasmessi tramite qualsiasi Sistema Aziendale, e
(iii) acquisire un'immagine forense completa di qualsiasi Dispositivo Intesa. Se Intesa necessita della collaborazione del Fornitore per esercitare i suoi diritti, il Fornitore soddisferà pienamente e tempestivamente le richieste di Intesa per tale collaborazione (incluse, ad esempio, richieste di configurare in modo sicuro qualsiasi Dispositivo Intesa, installare software di monitoraggio o altro su qualsiasi Dispositivo Intesa, condividere i dettagli di connessione a livello di sistema, intraprendere misure di risposta agli incidenti su qualsiasi Dispositivo e fornire accesso fisico a qualsiasi Dispositivo Intesa affinché Intesa ottenga un'immagine forense completa o altro, e richieste simili e correlate).

(c) Intesa manterrà il titolo di proprietà di tutti i Dispositivi Intesa, con il Fornitore che si assume il rischio di perdita dei Dispositivi Intesa, anche a causa di furto, vandalismo o negligenza. Il Fornitore non effettuerà né consentirà alcuna alterazione dei Dispositivi Intesa senza previo consenso scritto di Intesa, dove per alterazione si intende qualsiasi modifica ad un Dispositivo, inclusa qualsiasi modifica al software, alle applicazioni, alla progettazione della sicurezza, alla configurazione della sicurezza o alla progettazione fisica, meccanica o elettrica del Dispositivo.

(d) Il Fornitore restituirà tutti i Dispositivi Intesa entro 5 giorni lavorativi dal termine della necessità di tali Dispositivi per l'erogazione dei Servizi e, se richiesto da Intesa, distruggerà contestualmente tutti i dati, i materiali e altre informazioni di qualsiasi tipo presenti su tali Dispositivi, senza conservarne alcuna copia, attenendosi agli standard NIST per eliminare definitivamente tutti questi dati, materiali e altre informazioni. Il Fornitore impacchetterà e restituirà, a proprie spese nel luogo identificato da Intesa, i Dispositivi Intesa nelle stesse condizioni in cui sono stati consegnati al Fornitore, a parte una ragionevole usura. La mancata osservanza da parte del Fornitore di qualsiasi obbligo di cui al presente comma (d) costituisce una violazione sostanziale del Contratto e del relativo Documento d'Ordine e di qualsiasi accordo correlato tra le parti, con la consapevolezza che un accordo è "correlato" se l'accesso a qualsiasi Sistema Aziendale facilita le attività

del Fornitore o altre attività ai sensi di tale accordo.

(e) Intesa fornirà supporto per i Dispositivi Intesa (incluse l'ispezione e la manutenzione preventiva e correttiva dei Dispositivi). Il Fornitore informerà tempestivamente Intesa della necessità di un servizio di rimedio.

(f) Per i programmi software che Intesa possiede o su cui ha il diritto di licenza, Intesa concede al Fornitore un diritto temporaneo di utilizzare, archiviare e fare copie sufficienti per supportare il proprio utilizzo autorizzato dei Dispositivi Intesa. Il Fornitore non potrà trasferire programmi ad alcuno, fare copie delle informazioni sulla licenza del software o disassemblare, decompilare, decodificare o altrimenti tradurre qualsiasi programma se non espressamente consentito dalla legge applicabile senza incorrere in una deroga contrattuale

Articolo V. DEFINIZIONI

5.1. **Paese Adeguato** indica un Paese che fornisce un livello adeguato di protezione dei dati rispetto al trasferimento pertinente ai sensi delle normative applicabili sulla protezione dei dati o in base alle decisioni di organismi regolatori.

5.2. **Sistema AI** indica un sistema basato su macchina progettato per operare con livelli variabili di autonomia e che può manifestare adattabilità dopo la sua implementazione, e che, per obiettivi espliciti o impliciti, deduce, dall'input che riceve, come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali.

5.3. **Informazioni di Contatto Aziendali** ("**BCI**") indicano i Dati Personali impiegati per entrare in contatto, identificare o autenticare un individuo in ambito lavorativo o aziendale unicamente per scopi di amministrazione e gestione contrattuale (ad esempio, fatturazione e gestione dell'account, calcolo degli incentivi dei partner, reporting interno e modellazione aziendale come previsioni, entrate e pianificazione della capacità). In genere, le BCI includono il nome di una persona, l'indirizzo e-mail aziendale, l'indirizzo fisico, il numero di telefono o attributi simili. Ad esempio, i nomi e gli indirizzi e-mail utilizzati per contattare il Personale del Fornitore per i servizi di supporto sono BCI, tuttavia, i nomi e gli indirizzi e-mail inclusi nei dati di supporto diagnostico sono Dati Personali Intesa.

5.4. **Servizio Cloud** indica qualsiasi offerta "as a service" che il Fornitore ospita o gestisce, comprese le offerte "software as a service", "platform as a service" e "infrastructure as a service".

5.5. **Titolare del Trattamento dei Dati Personali** indica la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del Trattamento dei Dati Personali.

5.6. **Sistema Aziendale** indica un sistema IT, una piattaforma, un'applicazione, una rete o simili su cui Intesa fa affidamento per la propria attività, compresi quelli che si trovano o sono accessibili tramite la rete Intranet, Internet o altro.

5.7. **Cliente** indica un cliente di Intesa.

5.8. **Importatore di Dati** indica un Responsabile del Trattamento o un Subresponsabile che non si trova in un Paese Adeguato.

5.9. **Interessato** si intende una persona fisica che può essere identificata, direttamente o indirettamente.

5.10. **Giorno** o **Giorni** indicano i giorni solari, a meno che non venga specificato giorno "lavorativo".

5.11. **Dispositivo** indica una postazione di lavoro, un laptop, un tablet, uno smartphone o un assistente digitale personale fornito da Intesa o dal Fornitore.

5.12. **Strutture** indicano una sede fisica in cui il Fornitore ospita, accede o altrimenti Elabora Materiali o Materiali Intesa.

5.13. **Procedure Standard del Settore** indica le pratiche raccomandate o richieste dal National Institute of Standards and Technology ("**NIST**") o dall'International Organization for Standardization ("**ISO**"), o da qualsiasi altro ente o organizzazione di simile reputazione e sofisticazione.

5.14. **Dati Intesa** indica tutti i dati, file, materiali, testi, audio, video, immagini o altri dati, inclusi i Dati Personali Intesa, le Informazioni di Contatto Aziendali (BCI) Intesa e i Dati non Personali Intesa, che vengono forniti o resi accessibili al Fornitore (inclusi, a titolo esemplificativo, tramite un Servizio Cloud) in relazione all'erogazione dei Servizi o alla fornitura dei Materiali, indipendentemente dal fatto che siano forniti o resi accessibili da Intesa, dal Personale Intesa, da un Cliente, da un dipendente o collaboratore del Cliente, o da qualsiasi altra persona o entità.

5.15. **Materiale Intesa** indica qualsiasi Dato Intesa e Tecnologia Intesa.

5.16. **Dati Personali Intesa** indica i Dati Personali, escluso le BCI Intesa, che Intesa fornisce o rende accessibili al Fornitore per l'erogazione dei Servizi o la fornitura dei Materiali. I Dati Personali Intesa includono i Dati

Personali di cui Intesa è titolare del trattamento e i Dati Personali che Intesa Tratta per conto di Altri Titolari del Trattamento dei Dati Personali.

5.17. **Tecnologia Intesa** indica il Codice Sorgente, altro codice, testi descrittivi, firmware, software, tool, progetti, schemi, rappresentazioni grafiche, chiavi incorporate, certificati e altre informazioni, materiali, asset, documenti e tecnologia che Intesa ha direttamente o indirettamente concesso in licenza o che ha altrimenti reso disponibile al Fornitore secondo quanto descritto in un Documento d'Ordine o ai sensi di un Accordo.

5.18. **Paese Non Adeguato** indica un Paese che non è considerato adeguato ai sensi delle leggi applicabili sulla protezione dei dati o di una decisione di un organo regolatore competente.

5.19. **Altri Titolari del Trattamento dei Dati Personali** indica qualsiasi entità diversa da Intesa che sia un Titolare del Trattamento dei Dati Intesa, come ad esempio un'affiliata Intesa, un Cliente o una sua affiliata.

5.20. **Software On-Premise** indica il software fornito dal Fornitore come Materiale da Consegnare, che Intesa o un subappaltatore di Intesa esegue, installa o gestisce sui server o sistemi di Intesa o del subappaltatore.

5.21. **Dati Personali** indicano qualsiasi informazione relativa a un Interessato e qualsiasi altra informazione che può essere classificata come "dati personali" o simili in base a qualsiasi normativa sulla protezione dei dati.

5.22. **Personale** indica le persone che sono dipendenti di Intesa o del Fornitore, agenti di Intesa o del Fornitore, appaltatori indipendenti incaricati da Intesa o dal Fornitore o forniti a una delle parti da un subappaltatore.

5.23. **Trattare** o **Trattamento** indica qualsiasi operazione o insieme di operazioni eseguite sui Dati Intesa, inclusa l'archiviazione, l'utilizzo, l'accesso e la lettura.

5.24. **Responsabile del Trattamento** indica una persona fisica o giuridica che Tratta Dati Personali per conto di un Titolare del Trattamento e include "fornitore di servizi" o termini sostanzialmente simili ai sensi di qualsiasi legge sulla protezione dei dati.

5.25. **Incidente di sicurezza** indica (a) un evento che effettivamente o imminentemente mette a rischio la riservatezza, l'integrità o la disponibilità di qualsiasi Materiale Intesa o di un sistema informativo utilizzato dal Fornitore o dai suoi Subappaltatori per erogare i Servizi o fornire i Materiali, (b) una violazione della sicurezza che porta alla distruzione, perdita, alterazione, divulgazione non autorizzata o accesso accidentale o illecito ai Dati Intesa trasmessi, archiviati o altrimenti Trattati, o (c) l'accesso o l'uso non autorizzato del Codice Sorgente utilizzato dal Fornitore o dai suoi Subappaltatori nell'erogazione dei Servizi o nella fornitura di un Materiale da Consegnare o ad essa correlata.

5.26. **Vendere** (o **Vendita**) indica il noleggio, il rilascio, la divulgazione, la diffusione, il rendere disponibile, trasferire o altrimenti comunicare oralmente, per iscritto o con mezzi digitali o di altro tipo, dati in cambio di un corrispettivo in moneta o altro valore.

5.27. **Standard Contractual Clauses** ("**SCCs**") indica le clausole contrattuali richieste dalle leggi applicabili sulla protezione dei dati per il trasferimento di Dati Personali a Titolari del Trattamento dei Dati Personali o Responsabili del Trattamento che non sono stabiliti in un Paese Adeguato.

5.28. **Codice sorgente** indica il codice di programmazione leggibile da persone o codice che può essere convertito in forma leggibile da persone, che gli sviluppatori utilizzano nella creazione, sviluppo o manutenzione di un prodotto, ma che non viene reso pubblico nel normale corso della distribuzione o dell'uso commerciale del prodotto.

5.29. **Subresponsabile** indica qualsiasi Subappaltatore del Fornitore, incluso un'affiliata del Fornitore, che tratta i Dati Personali Intesa.

5.30. **Autorità di Vigilanza** indica un ente pubblico indipendente responsabile della supervisione dell'applicazione delle leggi sulla protezione dei dati all'interno di un paese o regione specifica.