CONDIZIONI GENERALI DI CONTRATTO

DEFINIZIONI

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

- **Adempimenti GDPR**: significa gli adempimenti richiesti per la *compliance* alle disposizioni del GDPR, espressamente identificati nella Scheda Servizio relativa al Servizio Privacy, per la gestione dei quali il Servizio Privacy è idoneo a fornire supporto al Cliente;
- **AgID**: significa l'Agenzia per l'Italia Digitale;
- **AliasLab**: significa la società Aliaslab S.p.A. (C.F. e P.IVA n. 13152000157), con sede legale in via Cornalia 11, (20124) Milano;
- **Atto di Affidamento**: significa il modulo allegato alle presenti Condizioni Generali (Allegato 1), mediante il quale il Terzo Beneficiario, ove necessario, affida a TeamSystem gli incarichi e le autorizzazioni necessarie al fine di permettere al Cliente di utilizzare i Servizi Agyo in nome e per conto del Terzo Beneficiario medesimo;
- **Atto di Delega**: significa, nel Servizio CCT, il modulo con il quale il Responsabile della Conservazione del Titolare dei Documenti delega a TeamSystem lo svolgimento di tutti gli adempimenti relativi al processo di conservazione dei Documenti di cui all'articolo 7, comma 1 del Regolamento Conservazione e in conformità a quanto concordato nell'Atto di Delega stesso;
- **CAD**: significa il codice dell'amministrazione digitale di cui al D.Lgs. n. 82 del 2005 e le sue successive modificazioni o integrazioni;
- **Cedente/Prestatore**: significa il soggetto che effettua, rispettivamente, la cessione del bene o la prestazione del servizio ai sensi dell'art. 21, comma 1, D.P.R. n. 633/72;
- **Cliente**: significa il soggetto, privato o pubblica amministrazione, identificato dalla procedura di certificazione nella Piattaforma Agyo, che può richiedere l'attivazione dei Servizi Agyo, per se stesso o, eventualmente, in favore di Terzi Beneficiari;
- **Codice di Condotta Anti-Corruzione**: significa il codice di condotta anti-corruzione adottato da TeamSystem e consultabile al sito *teamsystem.com*;
- **Condizioni del Certificatore**: ha il significato di cui al paragrafo 1.6.2.
- **Condizioni Generali**: significa i presenti termini e condizioni generali di contratto;
- **Connettività**: significa la connessione al Data Center effettuata dal Cliente mediante collegamento a una rete di telecomunicazioni o a internet;
- **Consorzio CBI**: significa le banche, gli istituti di pagamento e/o gli altri soggetti appartenenti al consorzio *Customer to Business Interaction*;
- **Contratto**: significa le presenti Condizioni Generali, i relativi allegati, i documenti ivi richiamati e le procedure online per l'accreditamento alla Piattaforma Agyo e l'attivazione dei Servizi Agyo, ivi incluse le Schede Servizio e le istruzioni online per il relativo utilizzo;
- **Contratto Nexi**: significa, nel Servizio Movimenti Bancari, il contratto che il Cliente deve sottoscrivere con Nexi per fruire del Servizio CBI al fine di consentire a TeamSystem di gestire i Flussi Bancari in Modalità Automatica nell'ambito del Servizio Movimenti Bancari;
- **Corrispettivi**: significa le somme, indicate nell'Ordine o, in mancanza dell'Ordine, nel listino prezzi pubblicato nell'apposita sezione della Piattaforma Agyo o, comunque, indicati al momento dell'attivazione online dei Servizi Hub, che il Cliente corrisponderà a TeamSystem o al soggetto appartenente alla Rete Vendite TS per l'attivazione e l'utilizzo di ciascuno dei Servizi Agyo effettivamente attivati e per gli eventuali ulteriori servizi a pagamento che il Cliente potrà richiedere a TeamSystem in relazione a ciascuno degli altri Servizi Agyo. Resta in ogni caso inteso che laddove uno o più Servizi Hub siano attivati nell'ambito di un'Offerta Integrata, i Corrispettivi per i Servizi Agyo attivati si intenderanno integralmente ricompresi nei corrispettivi complessivi previsti per l'Offerta Integrata, salvo ivi diversamente previsto;
- **Credenziali di Accesso**: significa il codice di identificazione e le chiavi di accesso forniti da TeamSystem, necessari per l'utilizzo della Piattaforma Agyo e dei Servizi Agyo attivati ed associati al Cliente;

- **Data Center**: significa i centri servizi che ospitano i server interconnessi, di proprietà di TeamSystem o di terzi, che gestiscono ed archiviano le Fatture Elettroniche, i Documenti e i dati trasmessi dal Cliente in occasione dell'uso della Piattaforma Agyo e dei Servizi Agyo attivati;
- **Digital Box**: significa l'area dedicata della Piattaforma Agyo, accedendo alla quale il Terzo Beneficiario ha la facoltà di consultare i documenti (ivi incluse, senza limitazione, le Fatture Elettroniche) trattati dal Cliente per conto del Terzo Beneficiario nell'ambito di uno specifico Servizio Agyo. È espressamente inteso che il Digital Box potrebbe non essere disponibile per tutti i Servizi Agyo attivati dal Cliente;
- **Dipendenti o Collaboratori**: significa, nel Servizio di Firma Digitale, i dipendenti o i collaboratori del Cliente, da quest'ultimo espressamente autorizzati e in favore dei quali viene richiesto l'emissione di un certificato qualificato al fine di fruire del Servizio di Firma Digitale;
- **Documentazione FEA**: significa, nel Servizio di FEA, la documentazione disponibile nell'apposita sezione della Piattaforma Hub che il Cliente ha la facoltà di utilizzare allo scopo di ottenere il consenso del terzo all'utilizzo del Servizio di FEA ai fini della sottoscrizione dei documenti informatici trattati nell'ambito del rapporto tra il Cliente e il terzo;
- **Documenti**: significa, nel Servizio CCT, i documenti informatici, i fascicoli informatici e le aggregazioni documentali informatiche (e i meta-dati ed essi associati) del Cliente o del Terzo Beneficiario, che costituiscono il pacchetto di versamento di input che viene poi trasformato secondo lo standard UNI SInCRO dal Servizio CCT nel pacchetto di versamento di cui all'articolo 4, comma 1, lett. a) del Regolamento Conservazione;
- **Emissione per Conto Terzi**: significa, nel Servizio Fatturazione Elettronica, l'affidamento a TeamSystem da parte del Cedente/Prestatore dell'emissione delle Fatture Elettroniche tramite l'apposizione della firma digitale, nelle modalità previste dall'articolo 21, terzo comma, del D.P.R. n. 633/72;
- **Fattura Elettronica**: significa la fattura scambiata in modalità elettronica da un Cedente/Prestatore con un destinatario/acquirente attraverso il Servizio Fatturazione Elettronica, in formato XML secondo il tracciato definito nella relativa Scheda Servizio;
- **FEA**: significa firma elettronica avanzata, in conformità alla definizione di cui agli artt. 1, n. 11 e 26 del Regolamento eIDAS;
- **FEA Grafometrica**: significa la soluzione di FEA basata sull'acquisizione dinamica dei dati della firma autografa del sottoscrittore mediante speciali tavolette di acquisizione (*tablet* grafometrici) o dispositivi *tablet* equipaggiati con opportuni sensori e *software*;
- **FEA in Mobilità**: significa la soluzione di FEA basata sul sistema dell'inserimento di una OTP (*one time password*) nel corso di una chiamata ad un numero verde effettuata attraverso la SIM card del sottoscrittore;
- **Firma Digitale**: significa il particolare tipo di firma qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare della firma, tramite la chiave privata, e al destinatario, tramite la chiave pubblica, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici, in conformità agli articoli 1 lett. s) e 24 del CAD;
- **Firma Digitale Automatica**: significa la procedura di apposizione automatica di Firma Digitale su uno o più documenti informatici senza la necessità che tali documenti informatici siano sottoposti al firmatario prima dell'apposizione della firma, eseguita previa autorizzazione del titolare della firma che mantiene il controllo esclusivo delle proprie chiavi di firma, in assenza di presidio puntuale e continuo da parte di questo, ai sensi del combinato disposto di cui agli articoli 1 lett. r) del D.C.P.M. del 22 febbraio 2013 e 35, 3° comma del CAD;
- **Firma Digitale Remota**: significa la procedura di apposizione di Firma Digitale su un documento informatico nel quale la chiave privata del firmatario è conservata, unitamente al relativo certificato di firma, dal certificatore accreditato in un HSM, dispositivo remoto sicuro, e nel quale la Firma Digitale è generata dal firmatario, consentendo di garantire il controllo esclusivo delle chiavi private da parte dei titolari delle stesse, mediante l'utilizzo di strumenti di autenticazione indicati nella relativa Scheda Servizio o successivamente adottati da TeamSystem e comunicati al Cliente, ai sensi degli articoli 1 lett. q) e 3, comma 4 del D.C.P.M. del 22 febbraio 2013;
- **Flussi Bancari**: significa, congiuntamente, i Flussi Dispositivi e i Flussi Informativi;
- **Flussi Dispositivi**: significa i flussi di dati di natura dispositiva predisposti dal Cliente e trasmessi a Nexi attraverso il Servizio Movimenti Bancari;
- **Flussi Informativi**: significa i flussi di dati di natura informativa trasmessi alla Piattaforma Agyo (i) da Nexi, in caso di fruizione del Servizio Movimenti Bancari in Modalità Automatica previa sottoscrizione del Contratto Nexi, ovvero (ii) dal Cliente, in caso di fruizione del Servizio Movimenti Bancari in Modalità Semiautomatica;

- **GDPR**: significa il Regolamento (UE) n. 2016/679 del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE;
- **Incaricato alla Registrazione**: significa, nel Servizio di Firma Digitale, il soggetto che effettua, per conto del certificatore accreditato, le operazioni di riconoscimento del richiedente e di inserimento dei dati necessari alla generazione dei certificati qualificati nell'apposita maschera messa a disposizione nell'ambito della Piattaforma Agyo;
- **Legislazione in materia di Protezione dei Dati Personali**: indica il GDPR, e ogni eventuale ulteriore norma e/o regolamento di attuazione emanati ai sensi del GDPR o comunque vigenti in Italia, nonché ogni provvedimento vincolante che risulti emanato dalle autorità di controllo competenti in materia (es. Garante per la protezione dei dati personali) e conservi efficacia vincolante (ivi inclusi i requisiti delle Autorizzazioni generali al trattamento dei dati sensibili e giudiziari, se applicabili e ove mantengano la propria efficacia vincolante successivamente al 25 maggio 2018);
- **Manuale della Conservazione**: significa, nel Servizio CCT, il documento, redatto ai sensi del Regolamento Conservazione e della procedura di accreditamento AgID, che illustra l'organizzazione, i soggetti coinvolti e i ruoli svolti dagli stessi, il modello di funzionamento, la descrizione del processo, la descrizione delle architetture e delle infrastrutture utilizzate, le misure di sicurezza adottate e ogni altra informazione utile alla gestione e alla verifica del funzionamento, nel tempo, del sistema di conservazione e del Servizio CCT di TeamSystem. TeamSystem mette a disposizione di tutti i Titolari dei Documenti il proprio Manuale della Conservazione nell'apposita sezione della Piattaforma Agyo e sul sito internet di AgID, soggetto a variazioni sulla base delle esigenze tecniche e dell'evoluzione normativa. Sulla base di quanto espressamente previsto nelle Schede Servizio e nell'Atto di Delega, il Manuale della Conservazione di TeamSystem potrà essere oggetto di eventuale personalizzazione, a cura e sotto l'esclusiva responsabilità del Titolare dei Documenti, allo scopo di creare il Manuale della Conservazione del Cliente e/o del Terzo Beneficiario;
- **MDPA:** indica l'Accordo Principale per il Trattamento dei Dati Personali e il documento DPA – Condizioni Speciali applicabile, allegati alle presenti Condizioni Generali;
- **Modalità Automatica** e **Modalità Semiautomatica**: hanno il significato di cui al paragrafo 1.8.2;
- **Modello Organizzativo**: significa il modello di organizzazione, gestione e controllo adottato da TeamSystem ai sensi del d.lgs. 231/2001 e consultabile al sito *teamsystem.com*;
- **Nexi**: significa la società Nexi Payments S.p.A. (C.F. e P.IVA n. 04107060966), con sede legale in Milano, Corso Sempione 55 che, per quanto qui rileva, è autorizzata dal Consorzio CBI all'erogazione del Servizio CBI;
- **Norme CBI**: significa il "Testo coordinato della normativa CBI", elaborato dal Consorzio CBI e recante la disciplina regolamentare del Servizio CBI;
- **Offerta Integrata**: significa un'offerta commerciale proveniente da TeamSystem o da una società appartenente al gruppo del quale TeamSystem è parte o da un soggetto appartenente alla Rete Vendite TS e comprendente, oltre all'attivazione di uno o più Servizi Agyo, anche la concessione in licenza di ulteriori prodotti software e/o la prestazione di ulteriori servizi.
- **Ordine**: significa il modulo o coupon, in formato elettronico o cartaceo, compilato e accettato (anche on-line) dal Cliente e contenente alcuni termini e condizioni specificamente applicabili ai Servizi Agyo indicati nell'Ordine medesimo. Resta inteso che in caso di discordanza tra i termini e le condizioni indicate nell'Ordine e le disposizioni delle Condizioni Generali, prevarranno le disposizioni dell'Ordine;
- **PA**: significa la pubblica amministrazione;
- **Parti**: significa TeamSystem e il Cliente;
- **Partner**: significa il/i soggetto/i individuato/i da TeamSystem e che collabora/no con quest'ultima per la prestazione dei Servizi Hub, ivi inclusa, ma non limitatamente a, AliasLab quale soggetto che realizza le soluzioni di FEA oggetto del presente Contratto;
- **PEC**: significa posta elettronica certificata;
- **People App**: significa l'app per dispositivi mobili Android e iOS, utilizzando la quale i dipendenti del Cliente possono usufruire delle funzionalità del Servizio People App a loro dedicate, come individuate nella relativa Scheda Servizio;
- **Piattaforma Agyo**: significa la piattaforma *online* denominata "Agyo", di titolarità di TeamSystem, che costituisce il sistema centrale di gestione dei Servizi Agyo erogati da TeamSystem;

- **Produttore:** significa, nel Servizio CCT, il soggetto responsabile del trasferimento dei Documenti nel Data Center, secondo le modalità previste dal Manuale della Conservazione, dalla Scheda Servizio CCT e dal Regolamento Conservazione;

- **Proprietà Intellettuale**: significa ogni diritto di proprietà intellettuale e/o industriale, registrato o non registrato, in tutto o in parte, ovunque nel mondo, di titolarità di TeamSystem o di società appartenenti al medesimo gruppo o comunque collegate a TeamSystem ai sensi dell'articolo 2359 del codice civile, quali - a titolo esemplificativo e non esaustivo - marchi, brevetti, modelli di utilità, disegni e modelli, nomi a dominio, know-how, opere coperte dal diritto d'autore, database e software (ivi inclusi, ma non limitatamente a, le sue derivazioni, il codice sorgente, il codice oggetto e le interfacce);

- **Regolamento Conservazione**: significa il D.C.P.M. del 3 dicembre 2013, "Regole tecniche in materia di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter. Comma 4, 43, commi 1 e 3, 44, 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005";

- **Regolamento eIDAS**: significa il Regolamento (UE) n. 910/2014 del Parlamento Europeo e del Consiglio del 23 luglio 2014, in materia di identificazione elettronica e sevizi fiduciari per le transazioni elettroniche nel mercato interno che abroga la direttiva 1999/93/CE;

- **Reporting**: significa la generazione, da parte della Piattaforma Agyo, di un *report* contenente lo stato delle Fatture Elettroniche riferite al Cliente e/o al Terzo Beneficiario nella Piattaforma Agyo e lo stato di caricamento dei Documenti;

- **Responsabile della Conservazione**: significa, nel Servizio CCT, la persona fisica a tale scopo designata che opera presso il Titolare dei Documenti, la quale assume la responsabilità della gestione del sistema di conservazione ai sensi del Regolamento Conservazione;

- **Rete Vendite TS**: significa la rete di vendita di TeamSystem comprensiva di tutti i relativi canali di distribuzione, presenti e futuri, che TeamSystem utilizza per la commercializzazione di prodotti software (ivi inclusi, a titolo di esempio, la rete commerciale, l'e-commerce, gli agenti, i distributori e le società del gruppo TeamSystem);

- **Schede Servizio**: significa i documenti contenenti le specifiche normative tecniche, funzionali e procedurali di ciascun Servizio Agyo, pubblicati all'indirizzo www.agyo.io/it/schedeservizio, che il Cliente dichiara espressamente di aver visionato;

- **SDI**: significa il sistema di interscambio di cui all'articolo 1, comma 211 della L. 24 dicembre 2007, n. 244 e al Decreto Ministeriale 13 aprile 2013, n. 55;

- **Servizi Agyo**: significa, congiuntamente, il Servizio Fatturazione Elettronica, il Servizio CCT, il Servizio di Firma, il Servizio Telematici Fiscali, il Servizio Movimenti Bancari, il Servizio Privacy e il Servizio People App, nonché gli eventuali futuri e ulteriori servizi attivabili dal Cliente mediante la Piattaforma Agyo. Le presenti Condizioni Generali troveranno applicazione anche in relazione a ciascuno dei Servizi Agyo eventualmente attivati;

- **Servizio CBI**: significa, per quanto qui rileva, il servizio di cd. "*corporate banking interbancario*" erogato da Nexi, che consente di automatizzare l'interazione tra ciascun Cliente e le Banche aderenti al Consorzio CBI con cui il Cliente intrattenga rapporti di conto, rendendo possibile l'invio e la ricezione automatica dei Flussi Bancari nell'ambito e per il tramite del Servizio Movimenti Bancari;

- **Servizio CCT**: significa il servizio per la conservazione a norma dei Documenti ai sensi del CAD e del Regolamento Conservazione fornito da TeamSystem (in qualità di conservatore accreditato dall'AgID ai sensi dell'art. 44-bis del CAD e della circolare AgID n. 65 del 10 aprile 2014) attraverso la Piattaforma Agyo, attivabile dal Cliente tramite apposita funzionalità di attivazione e previa sottoscrizione, ove richiesto da TeamSystem, del relativo contratto;

- **Servizio di FEA**: significa il servizio attraverso il quale il Cliente può consentire a terzi di apporre una FEA Grafometrica o una FEA in Mobilità ad uno o più documenti informatici trattati nell'ambito dei rapporti giuridici intercorrenti tra il Cliente ed il terzo, in conformità alla relativa Scheda Servizio o alle successive istruzioni fornite da TeamSystem e previa sottoscrizione, da parte del terzo, della Documentazione FEA;

- **Servizio di Firma**: significa, congiuntamente, il Servizio di FEA e il Servizio di Firma Digitale;

- **Servizio di Firma Digitale**: significa il servizio attraverso il quale il Cliente (o il suo Dipendente e Collaboratore) può firmare digitalmente documenti informatici mediante l'apposizione di una Firma Digitale Remota o di una Firma Digitale Automatica e/o consentire a Terzi Beneficiari di firmare digitalmente documenti informatici mediante l'apposizione di una Firma Digitale Remota, in ogni caso previo rilascio di un certificato qualificato da parte del certificatore accreditato individuato ad esclusiva discrezione di TeamSystem, in conformità alla relativa Scheda Servizio;

- **Servizio Fatturazione Elettronica**: significa il servizio di (i) generazione di Fatture Elettroniche, (ii) invio e/o ricezione di Fatture Elettroniche nelle operazioni tra privati o con la PA e/o (iii) contabilizzazione di Fatture Elettroniche. Il Servizio Fatturazione Elettronicaè attivabile dal Cliente attraverso apposita funzionalità di attivazione della Piattaforma Hub, in conformità a quanto previsto dalla/e relativa/e Scheda/e Servizio;

- **Servizio Movimenti Bancari**: significa la messa a disposizione del Cliente, nell'ambito della Piattaforma Agyo, di uno specifico modulo software che consente l'interoperabilità e il dialogo tra i Flussi Bancari e determinati software compatibili;

- **Servizio People App**: significa il servizio a supporto della gestione delle risorse umane fornito da TeamSystem, utilizzando il quale il Cliente (attraverso la Piattaforma Agyo) e i dipendenti di quest'ultimo (attraverso la People App) possono controllare e gestire determinati aspetti inerenti al rapporto lavorativo tra loro in essere, in conformità alle e nei limiti delle funzionalità espressamente identificate e descritte nella relativa Scheda Servizio;

- **Servizio Privacy**: significa la messa a disposizione, nell'ambito della Piattaforma Agyo, di uno specifico modulo software idoneo a supportare il Cliente nella gestione degli Adempimenti GDPR e nella calendarizzazione delle attività di verifica connesse a questi ultimi;

- **Servizio Telematici Fiscali**: significa il servizio di invio all'Agenzia delle Entrate della "comunicazione liquidazioni periodiche IVA" e/o dei "dati delle fatture emesse e ricevute" del Cliente e/o del Terzo Beneficiario, in file formato XML sottoscritto dal Cliente con firma elettronica qualificata o digitale, nonché delle eventuali future comunicazioni o dichiarazioni indirizzabili in via telematica all'Agenzia delle Entrate alle quali TeamSystem potrà discrezionalmente estendere il servizio, attivabile dal Cliente attraverso apposita funzionalità di attivazione della Piattaforma Agyo, in conformità a quanto previsto dalla relativa Scheda Servizio;

- **TeamSystem**: significa la società TeamSystem Service s.r.l. (C.F. e P. IVA n. 01641790702), in persona del legale rappresentante pro tempore, con sede legale in Viale Giuseppe Ferro Snc, 86100 - Campobasso (CB);

- **Terzo Beneficiario**: significa, alternativamente, (a) la persona fisica o giuridica cliente del Cliente o (b) la società controllata dal Cliente ai sensi dell'art. 2359, 1° comma, n. 1 c.c., in favore della quale il Cliente richiede l'attivazione dei Servizi Agyo;

- **Titolare dei Documenti (o Soggetto Produttore)**: significa il Cliente o il Terzo Beneficiario titolare dei Documenti oggetto del Servizio CCT e tenuto, in base alla normativa vigente, alla conservazione dei Documenti medesimi;

- **Titolare di Firma**: significa il soggetto Cliente o Terzo Beneficiario, in proprio, ove consentito dalla legge applicabile, e/o Dipendente o Collaboratore al quale è attribuita la Firma Digitale per il relativo utilizzo;

- **Utenze Secondarie**: significa le utenze secondarie create e assegnate dal Cliente, allo scopo di consentire (i) agli uffici di fatturazione facenti parte della struttura aziendale del Cliente medesimo o (ii) a persone fisiche o giuridiche clienti del Cliente o (iii) a società controllate dal cliente ai sensi dell'art. 2359, 1° comma, n. 1 c.c. di usufruire, ove previsto, di specifiche e limitate funzionalità di determinati Servizi Agyo attivati, stabilite a discrezione di TeamSystem e con livelli di privilegio di volta in volta determinati dal Cliente medesimo. A titolo esemplificativo, il Cliente avrà la facoltà di autorizzare le Utenze Secondarie all'inserimento, nel Servizio Fatturazione Elettronica, dei dati relativi alle Fatture Elettroniche del Cliente, nel limite di cinquanta Fatture Elettroniche.

Art. 1 – Servizi Agyo

1.1 ***Servizio Fatturazione Elettronica***

1.1.1 Con l'attivazione da parte del Cliente del Servizio Fatturazione Elettronica (avente ad oggetto la generazione, la ricezione, l'invio e la contabilizzazione di Fatture Elettroniche), TeamSystem:

(a) a fronte del pagamento dei Corrispettivi, concede al Cliente, che accetta, una licenza d'uso, non esclusiva, non cedibile e temporanea della Piattaforma Agyo, al solo scopo di consentire al Cliente e di fruire del Servizio Fatturazione Elettronica, ai termini e alle condizioni indicate nel Contratto e, in particolare, in conformità a quanto previsto nella/e relativa/e Scheda/e Servizio;

(b) si impegna a concedere ai Terzi Beneficiari, su richiesta del Cliente, l'utilizzo del Servizio Fatturazione Elettronica.

1.1.2 Con l'attivazione del Servizio Fatturazione Elettronica, il Cliente:

(a) affida a TeamSystem l'Emissione per Conto Terzi delle proprie Fatture Elettroniche, ferma restando in ogni caso la piena assunzione di responsabilità del Cliente circa la correttezza, la completezza e la veridicità di tutti i dati e le informazioni contenuti nei *file* Fatture Elettroniche;

(b) conferisce a TeamSystem l'incarico di agire in qualità di intermediario verso il SDI per la gestione dei processi di trasmissione e/o ricezione delle Fatture Elettroniche del Cliente e del Terzo Beneficiario e delle relative notifiche.

1.1.3 Il Cliente potrà richiedere, in conformità alle modalità individuate ad esclusiva discrezione di TeamSystem, che quest'ultima effettui l'Emissione per Conto Terzi delle Fatture Elettroniche del Terzo Beneficiario. In tal caso, senza pregiudizio circa la piena assunzione di responsabilità del Cedente/Prestatore circa la correttezza, la completezza e la veridicità di tutti i dati e informazioni contenuti nei *file* Fatture Elettroniche trasferiti al Servizio Fatturazione Elettronica, il Cliente si impegna a fare sottoscrivere al Terzo Beneficiario l'Atto di Affidamento e a trasmetterlo prontamente a TeamSystem per mezzo dell'apposita funzione disponibile sulla Piattaforma Agyo.

1.1.4 Il Cliente dichiara e garantisce: (i) che la gestione delle Fatture Elettroniche di ciascun Terzo Beneficiario nell'ambito del Servizio Fatturazione Elettronica avverrà sulla base di un regolare incarico a tale scopo conferito dal Terzo Beneficiario al Cliente; (ii) di avere tutti i poteri necessari, essendo stato validamente incaricato a tal fine da ciascun Terzo Beneficiario, per il conferimento a TeamSystem dell'incarico di agire in qualità di intermediario verso il SDI per la gestione dei processi di trasmissione e/o ricezione delle Fatture Elettroniche del Terzo Beneficiario e delle relative notifiche e, più in generale, per la gestione delle Fatture Elettroniche del Terzo Beneficiario nell'ambito del Servizio Fatturazione Elettronica, ivi incluse, senza limitazione, la gestione dei processi di generazione ed emissione delle Fatture Elettroniche ovvero l'eventuale affidamento a TeamSystem dell'Emissione per Conto Terzi delle Fatture Elettroniche del Terzo Beneficiario. TeamSystem, al fine di verificare il rispetto di quanto previsto al presente paragrafo, si riserva il diritto di richiedere al Cliente in ogni momento prova scritta dell'esistenza e del contenuto dei poteri conferiti dal Terzo Beneficiario al Cliente, che quest'ultimo si impegna a fornire entro 5 (cinque) giorni dalla ricezione della relativa richiesta. Il Cliente terrà indenne e manlevata TeamSystem con riferimento a qualsivoglia conseguenza negativa, passività o danno derivante da, o anche solo connessa a: (i) l'inesistenza, l'inefficiacia o l'invalidità della delega conferita dal Terzo Beneficiario; e/o (ii) eventuali pretese o azioni del Terzo Beneficiario connesse alla gestione delle Fatture Elettroniche per il tramite del Servizio Fatturazione Elettronica e/o della relativa Emissione per Conto Terzi: (iii) l'erroneità, l'incompletezza e/o la non veridicità dei dati inseriti dal Cliente nelle Fatture Elettroniche del Terzo Beneficiario.

1.1.5 È sin d'ora espressamente esclusa qualsiasi responsabilità di TeamSystem in conseguenza di potenziali modifiche normative e/o regolamentari che abbiano l'effetto di modificare in qualunque modo, sotto il profilo soggettivo e/o temporale, l'obbligo di inviare, ricevere e/o contabilizzare Fatture Elettroniche attraverso il SDI.

1.2 ***Conservazione Cloud TeamSystem (Servizio CCT)***

1.2.1 Con l'attivazione da parte del Cliente del Servizio CCT, TeamSystem:

(a) a fronte del pagamento dei Corrispettivi, concede al Cliente, che accetta, una licenza d'uso non esclusiva, non cedibile e temporanea della Piattaforma Agyo, al solo scopo di consentire al Cliente e di fruire del Servizio CCT, ai termini e alle condizioni indicate nel Contratto e, in particolare, in conformità a quanto previsto nella relativa Scheda Servizio;

(b) si impegna a concedere ai Terzi Beneficiari, su richiesta del Cliente, l'utilizzo del Servizio CCT.

1.2.2 Con l'attivazione da parte del Cliente del Servizio CCT, il Cliente, in qualità di Titolare dei Documenti e/o Produttore:

(a) affida a TeamSystem, che accetta, l'incarico di conservatore delegato dei Documenti ai sensi dell'art. 6, comma 7 e dell'art. 5 comma 2 lett. b del Regolamento Conservazione, affinché TeamSystem provveda all'esecuzione del processo di conservazione dei Documenti ai termini e alle condizioni indicate nel Contratto e, in particolare, in conformità a quanto previsto nella relativa Scheda Servizio, nel Manuale della Conservazione e nel rispetto di quanto previsto dal CAD e dal Regolamento Conservazione. In ogni caso, resta inteso fra le Parti che la redazione, emissione, tenuta, generazione e copia dei Documenti prima del relativo caricamento nella Piattaforma Agyo per mezzo del Servizio CCT è e rimane di esclusiva responsabilità del Titolare dei Documenti;

(b) si impegna, anche ai sensi dell'art. 1381 c.c., a far sì che il Responsabile della Conservazione sottoscriva e trasmetta a TeamSystem, eventualmente per il tramite del Cliente medesimo, l'Atto di Delega.

1.3 ***Servizio di Firma***

1.3.1 *Servizio di Firma Digitale* - Con l'attivazione del Servizio di Firma Digitale, TeamSystem, a fronte del pagamento dei Corrispettivi, concede al Cliente, che accetta, una licenza d'uso, non esclusiva, non cedibile e temporanea della Piattaforma Agyo, ai temini e alle condizioni di cui al Contratto e in conformità alla relativa Scheda Servizio, allo scopo di consentire:

(a) al Cliente (in proprio, ove consentito dalla normativa applicabile) e/o ai Dipendenti e Collaboratori di fruire del Servizio di Firma Digitale al fine di sottoscrivere documenti informatici mediante l'apposizione di una Firma Digitale Remota o di una Firma Digitale Automatica, e/o

(b) ai Terzi Beneficiari di fruire del Servizio di Firma Digitale al fine di sottoscrivere documenti informatici mediante l'apposizione di una Firma Digitale Remota.

Il Cliente prende atto e accetta che l'utilizzo della Firma Digitale Automatica nell'ambito del Servizio di Firma Digitale è espressamente riservata al Cliente medesimo e/o ai propri Dipendenti e Collaboratori.

1.3.2 Il Cliente prende sin d'ora atto e accetta che il Servizio di Firma Digitale implica l'accettazione, da parte del Titolare di Firma, dei termini e delle condizioni predisposte dal certificatore accreditato che verrà comunicato da TeamSystem all'attivazione del Servizio di Firma Digitale (le "**Condizioni del Certificatore**").

1.3.3 Il Cliente, nel caso in cui sia il Titolare di Firma, acconsente sin d'ora all'adozione della procedura di apposizione della Firma Digitale Automatica in relazione ai documenti informatici sottoscritti, ai sensi e per gli effetti dell'art. 35, 3° comma del CAD.

1.3.4 Il Cliente prende atto e accetta che l'ottenimento della qualifica di Incaricato alla Registrazione è condizione necessaria per potere validamente richiedere al certificatore accreditato, comunicato da TeamSystem, l'emissione di certificati qualificati di Firma Digitale in favore suo o di uno o più Terzi Beneficiari e/o di Dipendenti e Collaboratori. Pertanto, in tal caso, il Cliente si impegna a seguire integralmente le procedure pubblicate da TeamSystem nell'apposita sezione della Piattaforma Agyo ai fini dell'ottenimento della qualifica di Incaricato alla Registrazione.

1.3.5 Il Cliente che abbia ottenuto la qualifica di Incaricato alla Registrazione in conformità al paragrafo che precede e che intenda consentire:

(a) ad un Terzo Beneficiario di divenire Titolare di Firma, si impegna a fare sì che quest'ultimo accetti le Condizioni del Certificatore;

(b) ad un Dipendente o Collaboratore di divenire Titolare di Firma, si impegna a fare sì, anche ai sensi dell'art. 1381 c.c., che il Dipendente o Collaboratore *(i)* accetti le Condizioni del Certificatore, e *(ii)* consenta all'adozione della procedura di apposizione della Firma Digitale Automatica in relazione ai documenti informatici da quest'ultimo sottoscritti, ai sensi dell'art. 35, 3° comma CAD.

1.3.6 *Servizio di FEA* - Con l'attivazione del Servizio di FEA, TeamSystem, a fronte del pagamento dei Corrispettivi, concede al Cliente, che accetta, una licenza d'uso, non esclusiva, non cedibile e temporanea della Piattaforma Agyo, ai termini e alle condizioni di cui al Contratto e in conformità alla relativa Scheda Servizio, allo scopo di consentire al Cliente di fruire del Servizio di FEA al fine di fare sottoscrivere a terzi i documenti informatici trattati nell'ambito dei rapporti giuridici intercorrenti tra il Cliente ed il terzo mediante l'apposizione di una FEA Grafometrica o di una FEA in Mobilità.

1.3.7 Il Cliente, prima di consentire al terzo di utilizzare il Servizio FEA per gli scopi di cui al paragrafo che precede, si impegna a ottenere il consenso scritto del terzo all'utilizzo del Servizio FEA per la sottoscrizione dei documenti informatici trattati nell'ambito dei rapporti giuridici intercorrenti tra il Cliente e il terzo, eventualmente avvalendosi della Documentazione FEA messa a disposizione da TeamSystem nell'apposita sezione della Piattaforma Agyo. Il Cliente, in qualità di soggetto che eroga una soluzione di FEA al fine di utilizzarla nei rapporti intrattenuti con il terzo per motivi istituzionali, societari, professionali o commerciali, avvalendosi della soluzione di FEA, è consapevole di essere tenuto al rispetto degli obblighi di cui all'art. 57 del DPCM 22 febbraio 2013, come espressamente identificati e descritti nella relativa Scheda Servizio.

1.3.8 Il Cliente prende atto e riconosce che l'individuazione e la gestione dei documenti informatici sottoscritti mediante il Servizio di Firma rimane di propria esclusiva competenza e responsabilità.

1.4 ***Servizio Telematici Fiscali***

1.4.1 Con l'attivazione da parte del Cliente del Servizio Telematici Fiscali, TeamSystem a fronte del pagamento dei Corrispettivi, concede al Cliente, che accetta, una licenza d'uso, non esclusiva, non cedibile e temporanea della Piattaforma Agyo, al solo scopo di consentire al Cliente e di fruire del Servizio Telematici Fiscali, ai termini e alle condizioni indicate nel Contratto e in conformità a quanto previsto nella relativa Scheda Servizio.

1.4.2 Ai fini della sottoscrizione dei documenti informatici in formato XML da trasmettere all'Agenzia delle Entrate, il Cliente ha la facoltà, ma non l'obbligo, di usufruire, a fronte del pagamento dei relativi Corrispettivi così come specificati nel listino prezzi pubblicato nell'apposita sezione della Piattaforma Agyo, del servizio di Firma Digitale Automatica fornito da TeamSystem nell'ambito del Servizio Telematici Fiscali, previa sottoscrizione dell'apposito contratto con il certificatore accreditato indicato da TeamSystem e ai termini e alle condizioni di cui al Contratto.

1.4.3 Nel caso in cui intenda usufruire della facoltà di cui al paragrafo 1.4.2, il Cliente consente espressamente all'apposizione della Firma Digitale Automatica sui documenti informatici trattati nell'ambito del Servizio Telematici Fiscali ai sensi dell'art. 35, 3° comma del CAD.

1.5 ***Servizio Movimenti Bancari***

1.5.1 Con l'attivazione da parte del Cliente del Servizio Movimenti Bancari, TeamSystem, a fronte del pagamento dei Corrispettivi, concede al Cliente, che accetta, una licenza d'uso non esclusiva, non cedibile e temporanea della Piattaforma Agyo, al solo scopo di consentire al Cliente e di fruire del Servizio Movimenti Bancari, ai termini e alle condizioni indicate nel Contratto.

1.5.2 Il Cliente potrà fruire del Servizio Movimenti Bancari, alternativamente:

(a) mediante interconnessione con il Servizio CBI, come disciplinato dalle Norme CBI ("**Modalità Automatica**"). Il Cliente è consapevole che la fruizione del Servizio Movimenti Bancari in Modalità Automatica è subordinata alla sottoscrizione, da parte del Cliente, del Contratto CBI;

(b) mediante caricamento manuale sulla Piattaforma Hub dei Flussi Informativi ottenuti autonomamente dal Cliente ("**Modalità Semiautomatica**").

1.5.3 Il Cliente prende atto e accetta che il Servizio Movimenti Bancari è finalizzato unicamente a rendere interoperabili i Flussi Bancari con determinati software compatibili di titolarità di TeamSystem o di altra società facente parte del gruppo TeamSystem e concessi in licenza al Cliente in virtù di separato e specifico accordo.

1.5.4 Il Cliente, qualora intenda gestire in Modalità Automatica i Flussi Bancari relativi a un soggetto terzo, si impegna a far sì che il terzo fornisca regolare consenso (anche ai fini del trattamento dei dati personali) all'erogazione, da parte di Nexi, dei Flussi Bancari ad egli riferiti attraverso il Servizio Movimenti Bancari del Cliente, mediante sottoscrizione della modulistica predisposta all'uopo da Nexi. Resta in ogni caso inteso che la gestione dei Flussi Bancari relativi ad un soggetto terzo è limitata ai rapporti intercorrenti tra (i) società appartenenti al medesimo gruppo, o (ii) il commercialista e il proprio cliente.

1.5.5 Il Cliente prende atto e accetta che, in caso di fruizione in Modalità Automatica del Servizio Movimenti Bancari, qualora dovesse cessare, per qualsiasi motivo, l'efficacia del Contratto (anche solo parzialmente con riferimento al Servizio Movimenti Bancari) senza la cessazione dell'efficacia del Contratto Nexi, TeamSystem potrebbe continuare a ricevere da Nexi i Flussi Informativi relativi al Cliente e/o ai clienti di quest'ultimo, senza che il Cliente possa accedervi. È pertanto specifico onere del Cliente, in tal caso, richiedere a Nexi di cessare l'erogazione dei Flussi Informativi verso TeamSystem.

1.5.6 Il Cliente, in caso di cessazione dell'efficacia del Contratto Nexi, potrà continuare ad utilizzare il Servizio Movimenti Bancari esclusivamente in Modalità Semiautomatica fintanto che sarà efficace tra le Parti il Contratto con riferimento al Servizio Movimenti Bancari.

1.5.7 Il Cliente prende atto e riconosce che l'erogazione dei Flussi Bancari non costituisce in alcun modo un'obbligazione, nemmeno parziale, in capo a TeamSystem, in quanto:

(a) in caso di fruizione del Servizio Movimenti Bancari in Modalità Automatica, i Flussi Bancari saranno scambiati esclusivamente tra il Cliente e Nexi nell'ambito del Servizio CBI, limitandosi TeamSystem a mettere a disposizione del Cliente il modulo software che consente il dialogo tra i software compatibili, la Piattaforma Agyo e i sistemi informativi di Nexi;

(b) in caso di fruizione del Servizio Movimenti Bancari in Modalità Semiautomatica, i Flussi Informativi saranno forniti dal Cliente medesimo o dai terzi di cui al paragrafo 1.5.4.

In nessun caso, pertanto, il Cliente potrà vantare alcuna pretesta nei confronti di TeamSystem in relazione all'inesattezza, incompletezza, illegittima acquisizione e/o uso improprio dei Flussi Bancari.

1.6 ***Servizio Privacy***

1.6.1 Con l'attivazione da parte del Cliente del Servizio Privacy, TeamSystem, a fronte del pagamento dei Corrispettivi, concede al Cliente, che accetta, una licenza d'uso, non esclusiva, non cedibile e temporanea della Piattaforma Agyo, al solo scopo di consentire al Cliente e di fruire del Servizio Privacy, ai termini e alle condizioni di cui al Contratto e in conformità alla relativa Scheda Servizio.

1.6.2 Ai fini della sottoscrizione dei documenti informatici prodotti dal Cliente attraverso il Servizio Privacy, il Cliente ha la facoltà di usufruire del Servizio di Firma Digitale fornito da TeamSystem nell'ambito della Piattaforma Agyo, in ogni caso previa corretta attivazione del Servizio di Firma Digitale.

1.6.3 Ai fini della conservazione a norma dei documenti informatici prodotti dal Cliente attraverso il Servizio Privacy, il Cliente ha la facoltà di usufruire del Servizio CCT fornito da TeamSystem nell'ambito della Piattaforma Agyo, in ogni caso previa corretta attivazione del Servizio CCT.

1.6.4 TeamSystem, nell'ambito del Servizio Privacy, avrà la facoltà, ma non l'obbligo, di mettere a disposizione del Cliente, a mero titolo informativo, un elenco di professionisti, studi associati e/o società di consulenza attivi nel settore della *data protection* ("**Consulenti**"), cui il Cliente potrà decidere di rivolgersi a propria esclusiva discrezione. Il Cliente prende atto e riconosce che in nessun caso i Consulenti potranno essere considerati Partner ai sensi del successivo articolo 12 e che TeamSystem rimarrà estranea a qualsiasi rapporto eventualmente instaurato tra il Cliente e ciascun Consulente. In nessun caso, pertanto, il Cliente potrà vantare alcuna pretesa nei confronti di TeamSystem in relazione ad eventuali danni, spese, costi e/o oneri, di qualunque natura, che dovessero derivare al Cliente e/o a terzi in conseguenza dell'attività prestata dai Consulenti.

1.7 ***Servizio People App***

1.7.1 Con l'attivazione da parte del Cliente del Servizio People App, TeamSystem, a fronte del pagamento dei Corrispettivi, concede al Cliente, che accetta, una licenza d'uso non esclusiva, non cedibile e temporanea della Piattaforma Agyo e di People App, al solo scopo di consentire al Cliente e ai dipendenti di quest'ultimo di fruire del Servizio People App attraverso, rispettivamente, la Piattaforma Agyo e di People App.

1.7.2 Fermo restando quanto previsto al paragrafo 13.1, il Cliente prende atto e accetta che l'utilizzo della People App da parte dei propri dipendenti avviene sotto l'esclusiva responsabilità del Cliente medesimo e che tale utilizzo è sottoposto al rispetto dei limiti, dei termini e delle condizioni di cui al Contratto.

1.7.3 A fronte del pagamento dei Corrispettivi previsti, TeamSystem potrà personalizzare la People App con il segno distintivo individuato ad esclusiva discrezione e responsabilità del Cliente. Il Cliente prende atto e accetta che quanto previsto al presente paragrafo costituisce l'unica possibilità di personalizzazione della People App e, in generale, del Servizio People App, restando espressamente esclusa qualsiasi ulteriore personalizzazione di carattere tecnico, funzionale e/o grafico. Fermo restando quanto previsto all'articolo 13, il Cliente garantisce la liceità dell'utilizzo del segno distintivo oggetto della personalizzazione della People App, restando espressamente esclusa qualsiasi responsabilità di TeamSystem in tal senso.

1.7.4 Ove espressamente consentito da TeamSystem successivamente all'attivazione del Servizio People App, il Cliente e i dipendenti di quest'ultimo avranno la facoltà, ma non l'obbligo, di usufruire del Servizio di Firma per la sottoscrizione dei documenti informatici trattati nell'ambito del Servizio People App, in ogni caso previa attivazione del Servizio di Firma e in conformità alle modalità, ai termini e alle condizioni di cui al Contratto.

1.7.5 Ove espressamente consentito da TeamSystem successivamente all'attivazione del Servizio People App, il Cliente avrà la facoltà di usufruire del Servizio CCT fornito da TeamSystem nell'ambito della Piattaforma Agyo ai fini della conservazione a norma dei documenti informatici prodotti dal Cliente e/o dai suoi dipendenti attraverso il Servizio People App, in ogni caso previa corretta attivazione del Servizio CCT e in conformità alle modalità, ai termini e alle condizioni di cui al Contratto.

1.7.6 Il Cliente è consapevole e accetta che TeamSystem, con esclusivo riferimento al trattamento di dati personali dei dipendenti del Cliente per le finalità di fruizione del Servizio People App attraverso l'uso della People App, fornirà a ciascun dipendente un'informativa corrispondente a quella reperibile all'indirizzo https://tc.teamsystem.com/InformativaPeopleApp.pdf, il cui contenuto il Cliente dichiara di condividere integralmente. Tale informativa verrà resa a ciascun dipendente per conto del Cliente (titolare del trattamento) mediante pubblicazione nella sezione dedicata al download della People App negli app store di riferimento. Il Cliente, quale condizione necessaria per l'attivazione del Servizio People App, si impegna a fornire a TeamSystem le informazioni e i dati necessari al completamento della predetta informativa quali, a titolo esemplificativo, i dati di contatto per l'esercizio dei diritti da parte degli interessati, nonché le generalità e i dati di contatto dell'eventuale DPO. Resta inteso che tutti gli adempimenti richiesti dalla normativa applicabile e connessi a trattamenti dei dati personali dei dipendenti nell'ambito del Servizio People App per finalità non comprese nell'ambito della predetta informativa saranno di esclusiva responsabilità del Cliente.

1.7.7 Fermo restando quanto previsto ai successivi paragrafi 13.2 e 15.3, il Cliente prende atto e accetta di essere l'unico ed esclusivo responsabile del puntuale rispetto di tutte le normative applicabili al rapporto di lavoro con i propri dipendenti anche in relazione agli aspetti gestiti attraverso il Servizio People App, ivi inclusi, senza limitazione, la L. 300/1970 (Statuto dei Lavoratori) e i contratti collettivi.

Art. 2 – Licenza della Piattaforma Agyo

2.1 Con il Contratto, TeamSystem concede al Cliente, che accetta, una licenza d'uso gratuita, non esclusiva, non cedibile e temporanea della Piattaforma Agyo, al fine di permettere al Cliente di fruire dei Servizi Agyo da quest'ultimo attivati.

Art. 3 – Obblighi di TeamSystem in relazione alla Piattaforma Agyo

3.1 Con il Contratto, TeamSystem si impegna a:

(a) erogare i Servizi Agyo attivati dal Cliente in conformità al Contratto, fermo restando che alcuni Servizi Hub, al momento della sottoscrizione del Contratto, potrebbero non essere immediatamente disponibili per motivi tecnici. In tal caso, i Servizi Agyo non immediatamente disponibili saranno contrassegnati nella Piattaforma Agyo dalla dicitura "in arrivo" o da diversa espressione di significato analogo;

(b) adeguare la Piattaforma Agyo e i Servizi Agyo attivati ad eventuali intervenute esigenze di carattere tecnico e/o normativo, apportando le necessarie modifiche e gli eventuali correttivi;

(c) nell'eventualità in cui ciò sia necessario, effettuare interventi di manutenzione ordinaria e/o straordinaria, al fine di assicurare l'accesso e l'uso della Piattaforma Agyo e dei Servizi Agyo. Tali interventi saranno effettuati, salvo particolari casi di urgenza e/o forza maggiore, in tempi e con modalità tali da arrecare il minor disagio possibile all'operatività del Cliente;

(d) organizzare e amministrare il Data Center nel rispetto delle norme legislative e regolamentari applicabili in relazione alle misure di sicurezza, nonché a dotarlo di appositi sistemi di protezione logica e fisica volti a impedire accessi non autorizzati;

(e) permettere al Cliente di creare ed assegnare Utenze Secondarie. Resta in ogni caso inteso fra le Parti che, anche in caso di creazione e assegnazione di Utenze Secondarie, il Cliente conserverà in ogni caso la facoltà di utilizzare i Servizi Agyo anche in nome e per conto di ciascuna delle Utenze Secondarie;

(f) fornire al Cliente, dietro il versamento dei relativi Corrispettivi, il codice di integrazione necessario al fine di collegare il *software* gestionale del Cliente alla Piattaforma Agyo e usufruire dei Servizi Hub attivati attraverso il gestionale medesimo;

(g) consentire l'accesso dei Terzi Beneficiari al Digital Box, a fronte del pagamento dei relativi Corrispettivi da parte del Cliente e, in generale, consentire al Cliente, sotto l'esclusiva responsabilità di quest'ultimo, di condividere dati e documenti con altri Clienti nell'ambito della Piattaforma Agyo, in ogni caso nei limiti delle funzionalità di quest'ultima.

Art. 4 – Obblighi del Cliente

4.1 Con il Contratto, il Cliente si impegna a:

(a) pagare a TeamSystem o al soggetto appartenente alla Rete Vendite TS i Corrispettivi dovuti ai sensi dell'articolo 6;

(b) dotarsi autonomamente di materiale *hardware* e *software*, nonché, tramite un operatore di telecomunicazioni di sua esclusiva e libera scelta, di una Connettività adeguata al fine di poter accedere al Data Center e poter utilizzare la Piattaforma Agyo e i Servizi Agyo attivati;

(c) adeguare le caratteristiche dei propri sistemi informatici e della Connettività alle modifiche e ai correttivi eventualmente apportati da TeamSystem alla Piattaforma Agyo e ai Servizi Agyo successivamente alla conclusione del Contratto;

(d) fornire a TeamSystem tutte le informazioni necessarie per la piena fruibilità della Piattaforma Agyo e dei Servizi Agyo attivati, nonché a comunicare immediatamente le eventuali successive variazioni, ivi inclusa qualsiasi variazione relativa alle Utenze Secondarie;

(e) verificare l'esito delle attività di Reporting generate dalla Piattaforma Agyo su richiesta del Cliente medesimo.

Art. 5 – Durata

5.1 Fatto salvo quanto eventualmente e diversamente previsto nell'Ordine o nell'apposita sezione della Piattaforma Agyo, il Contratto rimarrà efficace tra le Parti fino al 31 dicembre dell'anno di sottoscrizione e si intenderà automaticamente rinnovato alla scadenza per successivi periodi di un anno ciascuno, salvo disdetta da inviarsi con le modalità tecniche tempo per tempo indicate da TeamSystem oppure, in mancanza di diversa indicazione, a mezzo raccomandata A/R e/o PEC, almeno 6 (sei) mesi prima della scadenza. Fermo restando quanto precede, nel caso in cui i Servizi Agyo vengano forniti nell'ambito di un'Offerta Integrata, la durata del Contratto sarà la medesima di quella prevista nell'Offerta Integrata e, in caso di cessazione del rapporto contrattuale complessivo relativo all'Offerta Integrata, per qualsiasi ragione intervenuta, si intenderà cessato automaticamente anche il presente Contratto. A parziale deroga di quanto precede, le Fatture Elettroniche conservate nell'ambito del Servizio CCT verranno conservate per l'intero periodo indicato nel Modulo d'Ordine anche in caso di cessazione dell'efficacia del Contratto.

5.2 Il rinnovo tacito non si applica nel caso in cui il Cliente sia una Pubblica Amministrazione.

Art. 6 – Corrispettivi

6.1 A fronte della prestazione da parte di TeamSystem dei Servizi Agyo attivati dal Cliente, quest'ultimo si impegna a corrispondere puntualmente a TeamSystem o al soggetto appartenente alla Rete Vendite TS i Corrispettivi indicati nell'Ordine o nel listino prezzi pubblicato nell'apposita sezione della Piattaforma Agyo, secondo le modalità previste.

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

6.3 Il Cliente prende atto che la Piattaforma Agyo e i Servizi Agyo sono soggetti, per loro natura, ad una costante evoluzione tecnologica e normativa che richiede continue e onerose attività di aggiornamento e sviluppo necessarie al fine di garantire la funzionalità della Piattaforma Agyo e la corretta e completa erogazione dei Servizi Agyo. In ragione di quanto precede, TeamSystem avrà il diritto di modificare i Corrispettivi anche in misura superiore all'indice ISTAT con le modalità previste dall'articolo 16 che segue.

6.4 Fermo restando quanto previsto al paragrafo 6.3 che precede, qualora, durante l'esecuzione del Contratto, dovessero verificarsi circostanze imprevedibili tali da rendere maggiormente onerosa l'esecuzione delle prestazioni da parte di TeamSystem, quest'ultima avrà diritto di percepire un equo compenso *una tantum* ovvero di modificare unilateralmente i Corrispettivi.

6.5 In caso di mancato o ritardato pagamento di una qualsiasi somma dovuta ai sensi del Contratto, il Cliente decadrà automaticamente dal beneficio del termine e TeamSystem avrà facoltà di applicare sulle somme ad essa dovute interessi di mora nella misura prevista dal d.lgs. 231/2002.

6.6 Il Cliente rinuncia a proporre eccezioni senza avere preventivamente adempiuto alle proprie obbligazioni di pagamento ai sensi del presente articolo 6.

Art. 7 – Credenziali di Accesso

7.1 Il Cliente potrà accedere alla Piattaforma Agyo e usufruire dei Servizi Agyo attivati mediante le Credenziali di Accesso.

7.2 Il Cliente è consapevole del fatto che la conoscenza delle Credenziali di Accesso da parte di soggetti terzi consentirebbe a questi ultimi l'accesso alla Piattaforma Agyo, ai dati e ai documenti ivi memorizzati, ivi incluse le Fatture Elettroniche, e ai Servizi Agyo.

7.3 Il Cliente è pertanto tenuto a custodire e a far sì che i propri dipendenti, collaboratori o consulenti incaricati custodiscano le Credenziali di Accesso con la massima riservatezza e con la massima diligenza, obbligandosi a non cederle né a consentirne l'uso a terzi non espressamente autorizzati.

7.4 TeamSystem non potrà in alcun caso essere ritenuta responsabile di qualsiasi danno, diretto e/o indiretto, che dovesse derivare al Cliente o a terzi in conseguenza della mancata osservanza da parte del Cliente e/o dei propri dipendenti, collaboratori o consulenti incaricati delle previsioni di cui al presente paragrafo.

Art. 8 – Riservatezza

8.1 È tassativamente vietata alle Parti ogni forma di comunicazione e/o divulgazione o comunque di utilizzazione, anche per interposta persona e/o ente, di qualsiasi notizia, informazione e documentazione comunque appresa e ottenuta in occasione dell'esecuzione del Contratto, da intendersi sin d'ora incondizionatamente riservata, anche ove non si tratti di veri e propri segreti industriali, tanto se attinente alle Parti, quanto se riguardante imprese loro clienti e/o fornitrici, salvo:

(a) quanto strettamente richiesto dall'esecuzione del Contratto;

(b) espressa autorizzazione per iscritto dell'altra Parte;

(c) quando le Parti siano a ciò obbligate per legge e/o per provvedimento dell'autorità amministrativa e/o giudiziaria.

8.2 Il divieto di cui al precedente paragrafo resterà incondizionatamente fermo anche dopo la cessazione, per qualsiasi causa intervenuta, del Contratto per il successivo periodo di 5 (cinque) anni, ritenuto congruo da entrambe le Parti, fatta salva la caduta in pubblico dominio dell'informazione che non sia imputabile alle Parti.

Art. 9 – Nomina del responsabile del trattamento

9.1 Il Cliente, quale titolare del trattamento dei dati, nomina TeamSystem quale responsabile del trattamento dei propri dati personali ai sensi dell'art. 28 del GDPR (il "**Responsabile**"), in relazione ai trattamenti di dati personali eseguiti per finalità connesse all'esecuzione del presente Contratto. Qualora titolare del trattamento dei dati fosse il Terzo Beneficiario, quest'ultimo autorizza sin dalla sottoscrizione dell'Atto di Affidamento (All. 1) la nomina da parte del Cliente di TeamSystem quale sub-responsabile del trattamento dei dati ai sensi dell'art. 29 GDPR.

9.2 Le Parti convengono che TeamSystem potrà procedere all'elaborazione e utilizzo di informazioni puramente statistiche, su base aggregata e previa anonimizzazione, raccolte in relazione all'utilizzo dei Servizi Agyo da parte del Cliente e del Terzo Beneficiario, ivi incluse informazioni relative ai meta-dati associati ai Documenti, a fini di studio e statistici, concedendo a tal fine a TeamSystem una licenza non esclusiva, perpetua, irrevocabile, valida in tutto il mondo e a titolo gratuito, ad utilizzare tali informazioni per dette finalità.

Art. 10 – Trattamento dei dati personali

10.1 Le Parti riconoscono e si danno reciprocamente atto che l'esecuzione dei Servizi Agyo può comportare il trattamento da parte di TeamSystem di dati personali di soggetti terzi di cui il Cliente o il Terzo Beneficiario sono titolari ai sensi della normativa in materia di protezione dei dati personali (i "**Dati Personali di Terzi**"). Con riguardo ai Dati Personali di Terzi trattati da TeamSystem in qualità di Responsabile, le Parti accettano di conformarsi a quanto previso nel MDPA allegato al presente Contratto (Allegato 2). Il Cliente e il Terzo Beneficiario dichiarano e riconoscono di essere responsabili dell'adempimento nei confronti degli interessati di tutti gli obblighi previsti dalla Legislazione in materia di protezione dei Dati Personali, salvi i compiti affidati a TeamSystem in virtù del MPDA. Pertanto, a titolo esemplificativo e non esaustivo, il Cliente si obbliga ad assicurare (ed a far sì che il Terzo Beneficiario assicuri): i) che gli interessati abbiano ricevuto un'adeguata informativa e abbiano prestato, ove necessario, idoneo consenso al loro trattamento anche attraverso i Servizi Agyo; ii) che siano adottate tutte le misure di sicurezza idonee alla tutela dei Dati Personali di Terzi, fatte salve le misure delegate a TeamSystem in qualità di Responsabile del trattamento dei dati personali nei limiti di quanto previsto dal MDPA.

10.2 Resta inteso che TeamSystem non assume alcuna responsabilità in merito alle conseguenze derivanti dall'inosservanza da parte del Cliente e/o del Terzo Beneficiario degli obblighi sui medesimi gravanti in qualità di titolari del trattamento ai sensi del precedente articolo 10.1. Il Cliente dovrà manlevare e tenere indenne TeamSystem da qualunque pregiudizio, onere, sanzione o pretesa che TeamSystem dovesse subire o ricevere in ragione della violazione da parte del Cliente e/o del Terzo Beneficiario di tali obblighi.

10.3 I dati personali del Cliente e del Terzo Beneficiario, salvo il caso di persone giuridiche, saranno trattati da TeamSystem secondo quanto riportato nell'informativa che sarà resa all'interessato ai sensi dell'art. 13 e 14 del GDPR.

Art. 11 – Memorizzazione

11.1 Le Fatture Elettroniche, i Documenti e, in generale, i dati immessi si intendono definitivamente acquisiti dalla Piattaforma Agyo e dai relativi Servizi Agyo nel momento in cui questi vengono compiutamente memorizzati ed accettati dalla Piattaforma Agyo.

11.2 È specifico onere del Cliente e/o di ciascun Terzo Beneficiario, attraverso le apposite funzionalità fornite dalla Piattaforma Agyo (ivi inclusa la funzionalità di Reporting)**,** verificare autonomamente la corretta acquisizione da parte della Piattaforma Agyo dei Documenti e delle Fatture Elettroniche, nonché, con riferimento al Servizio Fatturazione Elettronica, verificare il corretto andamento del procedimento di fatturazione elettronica.

11.3 In caso di attivazione del Servizio CCT, è specifico onere del Cliente o del Terzo Beneficiario, per il tramite del Produttore, verificare il buon esito del versamento tramite la presa visione del rapporto di versamento generato dal Servizio CCT medesimo.

11.4 Salvo i casi di dolo o colpa grave, TeamSystem non assume alcuna responsabilità per l'eventuale sottrazione, perdita, distruzione o smarrimento dei Documenti, delle Fatture Elettroniche e, più in generale, delle informazioni relative al Cliente prima che essi vengano definitivamente acquisiti e memorizzati dalla Piattaforma Agyo.

Art. 12 – Partner

12.1 TeamSystem, nell'adempiere alle proprie obbligazioni di cui al Contratto, potrà avvalersi, a propria insindacabile discrezione, della cooperazione tecnica, organizzativa e commerciale di Partner, ai quali potrà affidare la prestazione di alcune attività elencate nelle presenti Condizioni Generali.

12.2 A tal fine, TeamSystem s'impegna ad avvalersi di fornitori qualificati e diligenti, i quali dovranno a loro volta obbligarsi ad operare in accordo alle disposizioni delle presenti Condizioni Generali.

Art. 13 – Responsabilità del Cliente

13.1 Il Cliente si impegna a far sì che le disposizioni del Contratto siano rispettate da ciascun Terzo Beneficiario, da ciascun utilizzatore delle Utenze Secondarie e dai propri dipendenti, collaboratori, consulenti ed altri possibili aventi causa del Cliente stesso.

13.2 Il Cliente è, inoltre, esclusivo responsabile della correttezza, completezza, aggiornamento e veridicità dei dati immessi nella Piattaforma Agyo da ciascun utilizzatore anche delle Utenze Secondarie, da ogni Terzo

Beneficiario nonché dai propri dipendenti, collaboratori e consulenti, garantendo altresì il rispetto di tutte le normative applicabili, ivi incluse quelle in materia fiscale e civile.

13.3 Anche ai sensi e per gli effetti di cui all'art. 1381 c.c., il Cliente è esclusivo responsabile dell'operato dei propri dipendenti, collaboratori o consulenti e degli Utenti Secondari, nonché dell'autorizzazione a quest'ultimi concessa per utilizzare la Piattaforma Agyo e i Servizi Agyo in nome e per conto del Cliente.

13.4 È fatto divieto di utilizzare la Piattaforma Agyo e i Servizi Agyo al fine di depositare, conservare, inviare, pubblicare, trasmettere e/o condividere dati, applicazioni o documenti informatici che:

(a) siano in contrasto o violino la Proprietà Intellettuale e/o i diritti di proprietà industriale e/o intellettuale di titolarità di terzi;

(b) abbiano contenuti diffamatori, calunniosi o minacciosi;

(c) contengano materiale pornografico, osceno o comunque contrario alla pubblica morale;

(d) contengano virus, *worm*, *trojan horse* o, comunque, altre caratteristiche di contaminazione o distruttive;

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

(f) siano in contrasto con la Legislazione in materia di protezione dei dati personali;

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

13.5 TeamSystem si riserva il diritto di sospendere l'accesso al Cliente e, se del caso, a ciascun Terzo Beneficiario alla Piattaforma Agyo e ai Servizi Agyo, ovvero di impedire l'accesso ai dati e ai documenti ivi memorizzati, qualora venga a conoscenza di una violazione di quanto previsto nel presente articolo e/o venga avanzata espressa richiesta in tal senso da un organo giurisdizionale o amministrativo in base alle norme vigenti.

13.6 Nelle ipotesi di cui al comma precedente, TeamSystem provvederà a comunicare a mezzo PEC al Cliente le motivazioni dell'adozione della sospensione e/o interdizione all'accesso, salva la facoltà di risolvere il Contratto ai sensi del successivo articolo 18.

Art. 14 – Manleva

14.1 Il Cliente si impegna a manlevare e tenere indenne TeamSystem da qualsiasi danno, pretesa, responsabilità e/o onere, diretti o indiretti e comprese le ragionevoli spese legali, che TeamSystem dovesse subire o sopportare in conseguenza dell'inadempimento da parte del Cliente e/o di ciascun Terzo Beneficiario di ciascuno degli obblighi previsti dal Contratto e, in particolare, di quanto previsto dagli articoli 1.1.3, 4, 7.2, 7.3, 10.1,11.2, 11.3, 13 e 20.

Art. 15 – Responsabilità di TeamSystem

15.1 Il Cliente prende atto e accetta che TeamSystem non si assume alcuna responsabilità ai fini degli adempimenti fiscali richiesti dalla normativa vigente ed eventuali successive modifiche.

15.2 TeamSystem, inoltre, non rilascia dichiarazioni e garanzie espresse o implicite sul fatto che i software che costituiscono la Piattaforma Agyo e i Servizi Agyo siano adatti a soddisfare le esigenze del Cliente, che siano esenti da errori o che abbiano funzionalità non previste nelle specifiche tecniche e nella documentazione relativa.

15.3 TeamSystem, salvo il caso di dolo o colpa grave, non potrà essere ritenuta responsabile per danni diretti o indiretti, di qualsiasi natura ed entità, che dovessero derivare al Cliente e/o a terzi, ivi inclusi gli eventuali Terzi Beneficiari, in conseguenza dell'uso (o del mancato uso) della Piattaforma Agyo e/o dei Servizi Agyo in maniera non conforme a quanto previsto dal Contratto e/o dalle leggi vigenti.

15.4 TeamSystem, inoltre, salvo il caso di dolo o colpa grave, non potrà essere ritenuta responsabile in relazione a danni diretti o indiretti, di qualsiasi natura ed entità, che il Cliente e/o terzi dovessero subire per manomissioni della Piattaforma Agyo e/o dei Servizi Agyo o per interventi sulle apparecchiature effettuati dal Cliente o da terzi non autorizzati da TeamSystem.

15.5 TeamSystem, salvo il caso in cui il Cliente abbia attivato il Servizio CCT e salvi gli inderogabili limiti di legge, non assume alcun obbligo di conservazione dei messaggi PEC, email, delle Fatture Elettroniche e in generale dei dati immessi nella Piattaforma Agyo, restando tale conservazione di esclusiva responsabilità del Cliente.

15.6 TeamSystem non sarà in alcun modo responsabile, direttamente o indirettamente, per eventuali malfunzionamenti e/o per la mancata fruizione della Piattaforma Agyo e dei Servizi Agyo che derivino da una Connettività inadeguata rispetto alle relative caratteristiche tecniche.

15.7 TeamSystem non potrà essere ritenuta responsabile per eventuali danni da lucro cessante, mancato guadagno o danni indiretti, perdita o danneggiamento di dati, fermo fabbrica, perdita di opportunità commerciali o di benefici

di altro genere, pagamento di penali, ritardi o altre responsabilità del Cliente e/o del Terzo Beneficiario verso terzi che dovessero derivare, in tutto o in parte dall'uso o dal mancato uso della Piattaforma Agyo e dei Servizi Agyo.

15.8 In ogni caso, salvo il caso di dolo o colpa grave, la responsabilità di TeamSystem non potrà mai eccedere l'ammontare del corrispettivo annuale pagato dal Cliente ai sensi del presente Contratto.

Art. 16 – Modifiche Unilaterali

16.1 Il Contratto potrà essere modificato da TeamSystem in qualsiasi momento, dandone semplice comunicazione scritta (anche via e-mail o con l'ausilio di programmi informatici) al Cliente.

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

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

Art. 17 – Recesso

17.1 TeamSystem si riserva il diritto di recedere dal presente Contratto in ogni momento, con comunicazione a mezzo PEC da inviarsi al Cliente con almeno 2 (due) mesi di preavviso.

17.2 Nel caso in cui TeamSystem esercitasse il proprio diritto di recesso per motivi diversi rispetto a quelli di cui al paragrafo che segue, il Cliente avrà diritto alla restituzione della quota di corrispettivo per il periodo di mancato utilizzo della Piattaforma Agyo e/o dei Servizi Agyo, qualora essa sia già stata versata.

17.3 TeamSystem si riserva altresì il diritto di recedere dal Contratto anche nell'ipotesi in cui il Cliente sia gravemente inadempiente con riferimento ad uno qualsiasi degli eventuali contratti conclusi tra il medesimo Cliente e (i) TeamSystem S.p.A., con sede legale in Pesaro (PU), via Gagarin 205, codice fiscale, partita IVA e iscrizione al registro delle Imprese di Pesaro e Urbino n. 01035310414, o (ii) una delle società controllate, direttamente o indirettamente, ai sensi dell'art. 2359, primo comma, c.c., da TeamSystem S.p.A.

17.4 Resta in ogni caso inteso fra le Parti che la facoltà del Cliente di procedere alla mera disattivazione della propria utenza sulla Piattaforma Agyo, mediante la funzione a tale scopo preposta, non può in nessun caso essere considerata come concessione al Cliente di un diritto di recesso dal presente Contratto.

Art. 18 – Clausola risolutiva espressa e interdizione dalla Piattaforma Agyo

18.1 Fatto salvo il risarcimento del danno, TeamSystem si riserva il diritto di risolvere il Contratto ai sensi dell'art. 1456 c.c. a seguito di invio di semplice comunicazione scritta a mezzo PEC ovvero lettera raccomandata A/R in caso di mancato adempimento da parte del Cliente e/o del Terzo Beneficiario anche di una sola delle previsioni contenute nei seguenti articoli:

(a) 4 (Obblighi del Cliente);

(b) 6 (Corrispettivi);

(c) 7 (Credenziali di Accesso);

(d) 13 (Responsabilità del Cliente);

(e) 20 (Codice di Condotta Anti-Corruzione e Modello Organizzativo).

18.2 La risoluzione opererà di diritto al semplice ricevimento da parte del Cliente di una comunicazione scritta a mezzo PEC contenente la contestazione dell'inadempimento e l'intenzione di avvalersi della presente clausola risolutiva.

18.3 Fermo restando l'obbligo per il Cliente di versare a TeamSystem i Corrispettivi di cui all'articolo 6, TeamSystem, in caso di inadempimento del Cliente e/o di ciascun Terzo Beneficiario ad una delle obbligazioni di cui al primo comma del presente articolo, si riserva altresì la facoltà di interdire in ogni momento al Cliente l'accesso alla Piattaforma Agyo e ai Servizi Agyo. In tale ipotesi, TeamSystem comunicherà al Cliente l'intenzione di interdire l'accesso alla Piattaforma Agyo e ai Servizi Agyo, invitando, ove possibile, il Cliente a porre rimedio all'inadempimento entro un determinato termine. Il Cliente rimane in ogni caso obbligato a versare quanto dovuto anche in caso di interdizione dalla Piattaforma Agyo.

Art. 19 – Effetti della cessazione del Contratto e restituzione

19.1 In ogni caso di cessazione del Contratto, per qualsiasi causa intervenuta, TeamSystem interdirà definitivamente al Cliente e a ciascun Terzo Beneficiario l'accesso alla Piattaforma Agyo e ai Servizi Agyo, fatta salva la possibilità per il Cliente e per ciascun Terzo Beneficiario di effettuare il download delle Fatture Elettroniche, dei Documenti

e, in generale, dei dati da esso caricati sulla Piattaforma Agyo entro il termine di 60 (sessanta) giorni dalla data di cessazione del Contratto.

19.2 In alternativa, la restituzione delle Fatture Elettroniche, dei Documenti e dei dati di cui al comma che precede potrà essere richiesta dal Cliente tramite modalità di consegna automatizzata da concordare ovvero su appositi supporti ottici a fronte del pagamento dei corrispettivi specificamente previsti.

19.3 Fatto salvo quanto diversamente previsto dalle Parti e gli inderogabili limiti di legge, laddove il Cliente e/o ciascun Terzo Beneficiario non abbia scaricato o richiesto la restituzione delle Fatture Elettroniche, dei Documenti e dei dati di cui al primo comma, TeamSystem avrà la facoltà di cancellarli.

19.4 Resta in ogni caso inteso che gli articoli 6 (Corrispettivi), 8 (Riservatezza), 11.4 (Memorizzazione), 13 (Responsabilità del Cliente), 14 (Manleva), 15 (Responsabilità di TeamSystem), 20 (Codice di Condotta Anti-Corruzione e Modello Organizzativo), 21 (Comunicazioni), 22 (Legge applicabile e foro esclusivo), 25 (Tolleranza) e 26 (Invalidità e inefficacia parziale) sopravvivranno alla cessazione del Contratto, per qualsiasi ragione intervenuta.

Art. 20 – Codice di Condotta Anti-Corruzione e Modello Organizzativo

20.1 Il Cliente dichiara di avere preso visione e di conoscere il contenuto del Codice di Condotta Anti-Corruzione e del Modello Organizzativo e si obbliga – anche ai sensi dell'art. 1381 c.c. per i propri eventuali dipendenti e collaboratori – a conformarsi alle regole ed alle procedure contenute nel Codice di Condotta Anti-Corruzione e nel Modello Organizzativo (laddove applicabili al Cliente) e ad informare tempestivamente TeamSystem di qualsiasi atto, fatto o comportamento di cui venga a conoscenza che possa integrare la violazione di uno dei principi previsti dal Codice di Condotta Anti-Corruzione e/o dal Modello Organizzativo.

Art. 21 – Comunicazioni

21.1 Tutte le comunicazioni al Cliente inerenti lo svolgimento del rapporto potranno essere effettuate all'indirizzo *email* comunicato dal Cliente medesimo in sede di certificazione. Le comunicazioni a TeamSystem andranno invece inviate via *email* al seguente indirizzo info@agyo.io. Resta inteso che sarà cura e responsabilità del Cliente comunicare ogni variazione in relazione all'indirizzo email identificato dal Cliente per tutte le comunicazioni.

Art. 22 – Legge applicabile e foro esclusivo

22.1 Il presente contratto è regolato e deve essere interpretato in conformità alla legge italiana.

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

Art. 23 – Divieto di cessione

23.1 Salva preventiva autorizzazione scritta dell'altra parte, è fatto divieto alle Parti di cedere in tutto o in parte il Contratto.

23.2 Il Cliente acconsente sin da ora, ai sensi e per gli effetti dell'art. 1407 c.c., alla cessione, dal soggetto appartenente alla Rete Vendite TS a TeamSystem, del contratto avente ad oggetto i Servizi Agyo intercorrente tra il Cliente e il soggetto appartenente alla Rete Vendite TS che abbia cessato, per qualsivoglia motivo, di rivestire tale qualifica.

Art. 24 – Effetto novativo

24.1 E' escluso qualsiasi rilievo di eventuali precedenti accordi individuali tra le Parti, che s'intendono assorbiti ed esaustivamente superati dalla disciplina del Contratto.

Art. 25 – Tolleranza

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

Art. 26 – Invalidità ed inefficacia parziale

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

ALLEGATO 1

ATTO DI AFFIDAMENTO

NOTA: il presente Atto di Affidamento è da compilarsi a cura del Terzo Beneficiario ed esclusivamente nel caso in cui quest'ultimo abbia: **(a)** conferito mandato al Cliente per attivare e utilizzare il Servizio Fatturazione Elettronica in suo nome e per suo conto e ove il Cliente abbia concordato con TeamSystem che quest'ultima effettui l'Emissione per Conto Terzi delle Fatture Elettroniche del Terzo Beneficiario, e/o **(b)** conferito mandato al Cliente per attivare e utilizzare il Servizio CCT in suo nome e per suo conto.

Premesso che:

(A) la società TeamSystem Service s.r.l. (C.F. e P. IVA n. 01641790702), con sede legale in Viale Giuseppe Ferro Snc, 86100 - Campobasso (CB) ("**TeamSystem**") e

Nome e Cognome/Denominazione Sociale:
C.F. e P. IVA:
Residenza/Sede:
("**Cliente**")

hanno sottoscritto un contratto relativo all'erogazione di determinati servizi ("**Servizi Agyo**") da parte di TeamSystem, attraverso una piattaforma *online* di titolarità di quest'ultima ("**Contratto**"). Ove non diversamente indicato, i termini e le espressioni contenute nel presente atto di affidamento ("**Atto di Affidamento**"), qualora riportate con le iniziali maiuscole, devono intendersi con il significato ad essi attribuiti nel Contratto e, in particolare, nelle relative Condizioni Generali;

(B) in conformità a quanto previsto nel Contratto, il Cliente, su espressa richiesta del soggetto di seguito indicato come Terzo Beneficiario, intende attivare e utilizzare determinati Servizi Agyo in favore di

Nome e Cognome/Denominazione Sociale:
C.F. e P. IVA:
Residenza/Sede:
("**Terzo Beneficiario**")

(C) il Terzo Beneficiario dichiara di avere conferito mandato al Cliente per attivare e utilizzare determinati Servizi Agyo in suo nome e per suo conto;

(D) la prestazione dei Servizi Agyo richiede il trattamento, da parte di TeamSystem, di dati di cui il Terzo Beneficiario è titolare ai sensi della Legislazione in materia di trattamento dei dati personali; il Contratto tra TeamSystem e il Cliente contiene, al riguardo uno specifico "Accordo Principale per il Trattamento di Dati Personali – Master Data Processing Agreement" ("**MDPA**") volto a disciplinare il trattamento e la protezione dei dati oggetto dei Servizi Agyo in conformità con il Regolamento generale per la protezione dei dati personali n. 679/2016 ("**GDPR**") e con cui TeamSystem è stata nominata Responsabile del Trattamento ai sensi dell'art. 28 GDPR;

(E) le premesse formano parte integrante del presente Atto di Affidamento e sono da considerarsi da esso inscindibili.

TUTTO CIÒ PREMESSO:

1. Il Terzo Beneficiario dichiara di avere letto, compreso ed accettato il contenuto del Contratto, in tutto e in ogni sua parte, ivi incluse le Condizioni Generali e il MDPA unitamente a ciascuna Scheda Servizio.

2. Il Terzo Beneficiario

2.1 nel caso in cui abbia conferito mandato al Cliente per attivare e utilizzare il Servizio Fatturazione Elettronica in suo nome e per suo conto e ove il Cliente abbia concordato con TeamSystem che quest'ultima effettui l'Emissione per Conto Terzi delle Fatture Elettroniche del Terzo Beneficiario:

(a) affida a TeamSystem, che accetta, l'incarico di Emissione per Conto Terzi delle Fatture Elettroniche per conto del Terzo Beneficiario, ferma restando la piena assunzione di responsabilità del Terzo Beneficiario circa la correttezza, la completezza e la veridicità di tutti i dati e informazioni contenuti nei file fattura trasferiti al Servizio SDI;

(b) conferisce a TeamSystem l'incarico di agire in qualità di intermediario verso il SDI per la gestione dei processi di generazione, emissione, trasmissione e/o ricezione delle Fatture Elettroniche e delle relative notifiche.

2.2 nel caso in cui abbia conferito mandato al Cliente per attivare e utilizzare il Servizio CCT in suo nome e per suo conto:

(a) affida a TeamSystem, che accetta, l'incarico di conservatore delegato dei Documenti ai sensi dell'art. 5 comma 2 lett. b e dell'art. 6, comma 7 del Regolamento Conservazione, affinché TeamSystem provveda all'esecuzione del processo di conservazione dei Documenti ai termini e alle condizioni indicate nel Contratto e, in particolare, in conformità a quanto previsto nella relativa Scheda Servizio, nel Manuale della Conservazione e nel rispetto di quanto previsto dal CAD e dal Regolamento Conservazione. In ogni caso, resta inteso che la redazione, emissione, tenuta, generazione e copia dei Documenti prima del relativo caricamento nella Piattaforma Agyo per mezzo del Servizio CCT è e rimane di esclusiva responsabilità del Titolare dei Documenti;

(b) si impegna, anche ai sensi dell'art. 1381 c.c., a far sì che il Responsabile della Conservazione sottoscriva e trasmetta a TeamSystem, eventualmente per il tramite del Cliente medesimo, l'Atto di Delega.

3. Salvo diversamente richiesto da TeamSystem, eventuali futuri affidamenti a TeamSystem da parte del Terzo Beneficiario necessari a permettere al Cliente di utilizzare eventuali ulteriori Servizi Agyo in nome e per conto del Terzo Beneficiario devono intendersi sin d'ora ricompresi nel presente Atto di Affidamento.

4. Il Terzo Beneficiario autorizza la nomina da parte del Cliente di TeamSystem quale sub-responsabile del trattamento dei dati ai sensi dell'art. 29 GDPR in relazione ai trattamenti di dati personali eseguiti per finalità connesse all'esecuzione dei Servizi Agyo sopra selezionati.

Luogo e data: _____

Nome, cognome e carica *del firmatario che si dichiara munito di tutti i necessari poteri per la sottoscrizione del presente Atto di Affidamento*:

_____

Firma leggibile: _____

****

Ai sensi e per gli effetti degli articoli 1341 e 1342 c.c., il Terzo Beneficiario dichiara di aver letto, esaminato e di approvare specificamente le seguenti clausole del Contratto:

3 (OBBLIGHI DI TEAMSYSTEM IN RELAZIONE ALLA PIATTAFORMA HUB), 4 (OBBLIGHI DEL CLIENTE), 5 (DURATA DEL CONTRATTO), 6.3, 6.4, 6.5, 6.6 (CORRISPETTIVI), 7.3, 7.4 (CREDENZIALI DI ACCESSO), 11.2, 11.3 (MEMORIZZAZIONE), 12 (PARTNER), 13 (RESPONSABILITÀ DEL CLIENTE), 14 (MANLEVA), 15 (RESPONSABILITÀ DI TEAMSYSTEM), 16 (MODIFICHE UNILATERALI), 17 (RECESSO), 18 (CLAUSOLA RISOLUTIVA ESPRESSA E INTERDIZIONE DALLA PIATTAFORMA AGYO), 19 (EFFETTI DELLA CESSAZIONE DEL CONTRATTO E RESTITUZIONE, 20 (CODICE DI CONDOTTA ANTI-CORRUZIONE), 22 (LEGGE APPLICABILE E FORO ESCLUSIVO), 23 (DIVIETO DI CESSIONE)

Luogo e data: _____

Firma leggibile: _____

****

Presa visione dell'informativa sul trattamento dei dati personali disponibile al seguente link: https://tc.teamsystem.com/InformativaPrivacy.pdf, Le chiediamo di fare qui le Sue scelte sui consensi che intende rilasciare a TeamSystem, titolare del trattamento dei dati:

□ desidero rimanere aggiornato su novità e offerte commerciali dei prodotti e servizi TeamSystem, tramite mezzi di comunicazioni automatizzati e tramite strumenti di comunicazione tradizionali;

□ desidero rimanere aggiornato sulle novità e offerte commerciali delle altre società del gruppo TeamSystem e dei relativi partner, a cui i miei dati saranno comunicati;

□ acconsento all'analisi delle mie preferenze, attività e abitudini di spesa al fine di ricevere offerte commerciali personalizzate.

Resta fermo che potremo utilizzare i Suoi dati personali per le finalità di interesse legittimo così come descritte nell'informativa. Potrà, in ogni caso, opporsi all'invio delle comunicazioni sopra indicate nonché all'invio di comunicazioni commerciali relative a prodotti e servizi simili a quelli utilizzati, inviando una comunicazione all'indirizzo privacy@teamsystem.com.

Luogo e data: _____

Firma leggibile:_____

ALLEGATO 2

MDPA

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

TRA

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

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

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

E

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

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

PREMESSO CHE

a) il Cliente ha sottoscritto uno o più contratti con il Fornitore (di seguito il "**Contratto**");

b) le Parti intendono disciplinare nel presente "*accordo principale per il trattamento dei dati personali – Master Data Processing Agreement*" (nel seguito "**MDPA**" o "**Accordo**") le condizioni e le modalità del trattamento dei dati personali eseguito dal Fornitore nell'ambito del Contratto e della prestazione dei Servizi e le responsabilità connesse al trattamento medesimo, ivi incluso l'impegno assunto dal Fornitore quale Responsabile del trattamento dei dati personali ai sensi dell'art. 28 del Regolamento generale europeo sulla protezione dei dati del 27 aprile 2016 n. 679 (nel seguito "**GDPR**");

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

Tutto quanto sopra premessole Parti convengono quanto segue:

1. DEFINIZIONI E INTERPRETAZIONE

1.1. Le premesse costituiscono parte integrante del presente Accordo. Nell'Accordo i seguenti termini ed espressioni avranno il significato associato ad essi qui di seguito:

"Data di Decorrenza dell'Accordo" indica la data in cui il Cliente sottoscrive o accetta il presente Accordo;

"Dati Personali" ha il significato di cui alla Legislazione in materia di Protezione dei Dati Personali e includerà, a titolo puramente esemplificativo, tutti i dati forniti, archiviati, inviati, ricevuti o altrimenti elaborati, o creati dal Cliente, o dall'Utente Finale in relazione alla fruizione dei Servizi, nella misura in cui siano oggetto di trattamento da parte del Fornitore, sulla base del Contratto. Un elenco delle categorie di Dati Personali è riportata nei DPA – Condizioni Speciali;

"Decisione di Adeguatezza" indica una decisione della Commissione Europea sulla base dell'Articolo 45(3) del GDPR in merito al fatto che le leggi di un certo paese garantiscano un adeguato livello di protezione, come previsto dalla Legislazione in materia di Protezione dei Dati Personali;

"Giorni Lavorativi" indica ciascun giorno di calendario, a eccezione del sabato, della domenica e dei giorni nei quali le banche di credito ordinarie non sono di regola aperte sulla piazza di Milano, per l'esercizio della loro attività;

"Email di notifica" si intende l'indirizzo (o gli indirizzi) email fornito/i dal Cliente, all'atto della sottoscrizione del Servizio o fornito tramite altro canale ufficiale al Fornitore, a cui il Cliente intende ricevere le notifiche da parte del Fornitore;

"Istruzioni" indica le istruzioni scritte impartite dal Titolare nel presente Accordo (inclusivo dei relativi DPA – Condizioni Speciali) e, eventualmente, nel Contratto;

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

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

"Richiesta" indica una richiesta di accesso di un Interessato, una richiesta di cancellazione o correzione dei Dati Personali, o una richiesta di esercizio di uno degli altri diritti previsti dal GDPR;

"Responsabile Ulteriore del Trattamento" indica qualunque subappaltatore cui il Fornitore abbia subappaltato uno qualsiasi degli obblighi assunti contrattualmente e che, nell'adempiere tali obblighi,

potrebbe dover raccogliere, accedere, ricevere, conservare o altrimenti trattare Dati Personali;
"Servizio/i" indica il servizio o i servizi oggetto dei Contratti sottoscritti tempo per tempo tra il Cliente e il Fornitore;
"**Utente Finale**" si intende l'eventuale fruitore finale del Servizio, Titolare del Trattamento; e
"**Violazione della Sicurezza dei Dati Personali**" indica la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai Dati Personali occorsa su sistemi gestiti dal Fornitore o comunque sui quali il Fornitore abbia un controllo.

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

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

2. RUOLO DELLE PARTI

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

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

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

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

3. TRATTAMENTO DEI DATI PERSONALI

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

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

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

4. LIMITAZIONI ALL'UTILIZZO DEI DATI PERSONALI

4.1. Nell'eseguire il trattamento dei Dati Personali ai fini della prestazione dei Servizi, il Fornitore si impegna a eseguire il trattamento dei Dati Personali:

4.1.1. soltanto nella misura e con le modalità necessarie per erogare i Servizi o per adempiere opportunamente i propri obblighi, previsti dal Contratto e dal presente Accordo ovvero imposti dalla legge o da un organo di vigilanza o controllo competente. In tale ultima circostanza il Fornitore ne informerà il Cliente (salvo il caso in cui ciò sia vietato dalla legge per ragioni di pubblico interesse) mediante comunicazione trasmessa all'Email di notifica;

4.1.2. in conformità alle Istruzioni del Cliente.

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

5. AFFIDAMENTO A TERZI

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

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

– Condizioni Speciali.

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

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

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

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

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

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

6. DISPOSIZIONI IN MATERIA DI SICUREZZA

6.1. *MISURE DI SICUREZZA DEL FORNITORE* – Nell'eseguire il trattamento dei Dati Personali ai fini della prestazione dei Servizi il Fornitore si impegna ad adottare misure tecnico-organizzative adeguate per evitare il trattamento illecito o non autorizzato, la distruzione accidentale o illecita, il danneggiamento, la perdita accidentale, l'alterazione e la divulgazione non autorizzata di, o l'accesso ai, Dati Personali, come descritte nell'Allegato 1 al presente Accordo ("**Misure di Sicurezza**").

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

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

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

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

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

6.1.4.2. conformandosi agli obblighi di cui al punto 6.3.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

7.2. Se, ai fini della conservazione o del trattamento dei Dati Personali da parte di un Responsabile Ulteriore del trattamento, è necessario effettuare il trasferimento dei Dati Personali fuori dallo SEE in un paese che non gode di una decisione di adeguatezza da parte della Commissione Europea ai sensi dell'art. 45 del GDPR, il Fornitore:

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

7.2.2. potrà proporre al Cliente altre modalità di trasferimento dei Dati Personali conformi a quanto previsto dalla Legislazione in materia di Protezione dei Dati Personali (es. Privacy Shield in caso di Responsabili Ulteriori del trattamento situati negli Stati Uniti e per cui sia verificabile l'aderenza tramite i canali e registri ufficiali, o trasferimenti infragruppo del Responsabile Ulteriore del Trattamento che sia parte di un gruppo societario che ha ottenuto l'approvazione delle BCR per i Responsabili del trattamento).

7.3. Nei casi di cui al precedente punto 7.2.1 con il presente Accordo il Cliente conferisce espressamente mandato al Fornitore a sottoscrivere le Clausole Contrattuali Tipo con i Responsabili Ulteriori del Trattamento riportati nei relativi DPA – Condizioni Particolari. Qualora Titolare del trattamento sia l'Utente Finale, il 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.

8. VERIFICHE E CONTROLLI

8.1. Il Fornitore sottopone ad audit periodici la sicurezza dei sistemi e degli ambienti di elaborazione dei Dati Personali dallo stesso utilizzati per l'erogazione dei Servizi e le sedi in cui avviene tale trattamento. Il

Fornitore avrà la facoltà di incaricare dei professionisti indipendenti selezionati dal Fornitore per lo svolgimento di audit secondo standard internazionali e/o *best practice*, i cui esiti saranno riportati in specifici report ("**Report**"). Tali Report, che costituiscono informazioni confidenziali del Fornitore, potranno essere resi disponibili al Cliente per consentirgli di verificare la conformità del Fornitore agli obblighi di sicurezza di cui al presente Accordo.

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

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

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

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

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

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

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

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

9. ASSISTENZA A FINI DI CONFORMITÀ

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

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

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

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

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

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

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

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

10. OBBLIGHI DEL CLIENTE E LIMITAZIONI

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

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

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

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

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

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

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

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

11. DURATA

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

12. DISPOSIZIONI PER LA RESTITUZIONE O LA CANCELLAZIONEDEI DATI PERSONALI

12.1. Alla cessazione del Servizio, per qualunque causa intervenuta, il Fornitore cesserà ogni trattamento dei Dati Personali e

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

12.1.2. distruggerà eventuali Dati Personali conservati in formato cartaceo in suo possesso, tranne il caso in cui la conservazione dei dati da parte del Fornitore sia necessaria ai fini del rispetto di norme di legge italiane o europee; e

12.1.3. manterrà a disposizione del Cliente i Dati Personali per l'estrazione per il periodo di 12 (dodici) mesi successivi alla cessazione del Contratto. Durante tale periodo, il trattamento sarà limitato alla sola conservazione finalizzata a mantenere i Dati Personali a disposizione del Cliente per l'estrazione di cui al punto 12.2.

12.2. Fermo restando quanto altrimenti previsto nel presente Accordo, il Cliente riconosce di poter estrarre i Dati Personali, alla cessazione del Servizio, nei modi convenuti nel Contratto e conviene che è sua responsabilità provvedere all'estrazione totale o parziale dei soli Dati Personali che ritenga utile conservare e che tale estrazione dovrà essere effettuata prima della scadenza del termine di cui al punto 12.1.3.

12.3. Resta inteso che quanto previsto ai punti 12.1e 12.2 non si applica ai Contratti aventi ad oggetto prodotti installati presso il Cliente o presso fornitori del Cliente. In tali casi, è responsabilità del Cliente estrarre, entro e non oltre 30 (trenta) giorni dal termine della Durata del 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 nei rispettivi DPA – Condizioni Speciali.

13. RESPONSABILITA'

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

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

14. DISPOSIZIONI VARIE

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

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

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

Allegato1

Misure tecnico-organizzative

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

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

A – CLOUD SaaS

Misure di sicurezza organizzative	*Policy e Disciplinari utenti* – Il Fornitore applica dettagliate policy e disciplinari, ai quali tutta l'utenza con accesso ai sistemi informativi ha l'obbligo di conformarsi e che sono finalizzate a garantire comportamenti idonei ad assicurare il rispetto dei principi di riservatezza, disponibilità ed integrità dei dati nell'utilizzo delle risorse informatiche. *Autorizzazione accessi logici* – il Fornitore definisce i profili di accesso nel rispetto del *least privilege* necessari all'esecuzione delle mansioni assegnate. I profili di autorizzazione sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento. Tali profili sono oggetto di controlli periodici finalizzati alla verifica della sussistenza delle condizioni per la conservazione dei profili attribuiti. *Gestione interventi di assistenza* – Gli interventi di assistenza sono regolamentati allo scopo di garantire l'esecuzione delle sole attività previste contrattualmente e impedire il trattamento eccessivo di dati personali la cui titolarità è in capo al Cliente o all'Utente Finale. *Valutazione d'impatto sulla protezione dei dati (DPIA)* – In conformità agli artt. 35 e 36 del GDPR e sulla base del documento WP248 – Linee guida sulla valutazione d'impatto nella protezione dei dati adottate dal Gruppo di lavoro ex art. 29, il Fornitore ha predisposto una propria metodologia per l'analisi e la valutazione dei trattamenti che, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, presentino un rischio elevato per i diritti e le libertà delle persone fisiche allo scopo di procedere con la valutazione dell'impatto sulla protezione dei dati personali prima di iniziare il trattamento. *Incident Management* – Il Fornitore ha realizzato una specifica procedura di Incident Management allo scopo di garantire il ripristino delle normali operazioni di servizio nel più breve tempo possibile, garantendo il mantenimento dei livelli migliori di servizio. *Data Breach* – Il Fornitore ha implementato un'apposita procedura finalizzata alla gestione degli eventi e degli incidenti con un potenziale impatto sui dati personali che definisce ruoli e responsabilità, il processo di rilevazione (presunto o accertato), l'applicazione delle azioni di contrasto, la risposta e il contenimento dell'incidente / violazione nonché le modalità attraverso le quali effettuare le comunicazioni delle violazioni di dati personali al Cliente. *Formazione*: Il Fornitore eroga periodicamente ai propri dipendenti coinvolti nelle attività di trattamento corsi di formazione sulla corretta gestione dei dati personali
Misure di sicurezza tecniche	*Firewall, IDPS* - I dati personali sono protetti contro il rischio d'intrusione di cui all'art. 615-quinquies del codice penale mediante sistemi di Intrusion Detection & Prevention, mantenuti aggiornati in relazione alle migliori tecnologie disponibili. *Sicurezza linee di comunicazione*- Per quanto di propria competenza, sono adottati dal

	Fornitore protocolli di comunicazione sicuri e in linea con quanto la tecnologia rende disponibile. *Protection from malware*– I sistemi sono protetti contro il rischio di intrusione e dell'azione di programmi mediante l'attivazione di idonei strumenti elettronici aggiornati con cadenza periodica. Sono in uso strumenti antivirus mantenuti costantemente aggiornati. *Credenziali di autenticazione* – I sistemi sono configurati con modalità idonee a consentirne l'accesso unicamente a soggetti dotati di credenziali di autenticazione che ne consentono la loro univoca identificazione. Fra questi, codice associato a una parola chiave, riservata e conosciuta unicamente dallo stesso; dispositivo di autenticazione in possesso e uso esclusivo dell'utente, eventualmente associato a un codice identificativo o a una parola chiave. *Parola chiave* – Relativamente alle caratteristiche di base ovvero obbligo di modifica al primo accesso, lunghezza minima, assenza di elementi riconducibili agevolmente al soggetto, regole di complessità, scadenza, history, valutazione contestuale della robustezza, visualizzazione e archiviazione, la parola chiave è gestita conformemente alle best practice. Ai soggetti ai quali sono attribuite le credenziali sono fornite puntuali istruzioni in relazione alle modalità da adottare per assicurarne la segretezza. *Logging* – I sistemi sono configurabili con modalità che consentono il tracciamento degli accessi e, ove appropriato, delle attività svolte in capo alle diverse tipologie di utenze (Amministratore, Super Utente, etc.) protetti da adeguate misure di sicurezza che ne garantiscono l'integrità. *Backup & Restore* – Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati. Ove gli accordi contrattuali lo prevedono è posto in uso un piano di continuità operativa integrato, ove necessario, con il piano di disaster recovery; essi garantiscono la disponibilità e l'accesso ai sistemi anche nel caso di eventi negativi di portata rilevante che dovessero perdurare nel tempo. *Vulnerability Assessment & Penetration Test* – Il Fornitore effettua periodicamente attività di analisi delle vulnerabilità finalizzate a rilevare lo stato di esposizione alle vulnerabilità note, sia in relazione agli ambiti infrastrutturali sia a quelli applicativi, considerando i sistemi in esercizio o in fase di sviluppo. Ove ritenuto appropriato in relazione ai potenziali rischi identificati, tali verifiche sono integrate periodicamente con apposite tecniche di Penetration Test, mediante simulazioni di intrusione che utilizzano diversi scenari di attacco, con l'obiettivo di verificare il livello di sicurezza di applicazioni/sistemi/reti attraverso attività che mirano a sfruttare le vulnerabilità rilevate per eludere i meccanismi di sicurezza fisica/logica ed avere accesso agli stessi. I risultati delle verifiche sono puntualmente e dettagliatamente esaminati per identificare e porre in essere i punti di miglioramento necessari a garantire l'elevato livello di sicurezza richiesto. *Amministratori di Sistema* – Relativamente a tutti gli utenti che operano in qualità di Amministratori di Sistema, il cui elenco è mantenuto aggiornato e le cui funzioni attribuite sono opportunamente definite in appositi atti di nomina, è gestito un sistema di log management finalizzato al puntuale tracciamento delle attività svolte ed alla conservazione di tali dati con modalità inalterabili idonee a consentirne ex post il monitoraggio. L'operato degli Amministratori di Sistema è sottoposto ad attività di verifica in modo da controllarne la rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previsti dalle norme vigenti. *Data Center* – L'accesso fisico al Data Center è limitato ai soli soggetti autorizzati. Per il dettaglio delle misure di sicurezza adottate con riferimento ai servizi di data center erogati dai Responsabili Ulteriori del Trattamento, così come individuati nei DPA Condizioni Speciali, si fa rinvio alle misure di sicurezza indicate descritte dai medesimi Responsabili Ulteriori e rese disponibili nei relativi siti istituzionali ai seguenti indirizzi (o a quelli che saranno successivamente resi disponibili dai Responsabili Ulteriori):

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

B – Servizi Iaas

Misure di sicurezza organizzative	*Certificazioni* – il Fornitore ha ottenuto le seguenti certificazioni/attestazioni: • ISO/IEC 27001:2013: "Erogazione dei servizi di progettazione e gestione dell'infrastruttura ICT, di gestione delle applicazioni interne al Gruppo e di gestione dell'infrastruttura Cloud (IaaS)" • ISO/IEC 27018:2014 per la protezione dei dati personali nei servizi Public Cloud. *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. *Utenze* – Le utenze del servizio si scindono in utenze amministrative dell'infrastruttura di virtualizzazione e utenze amministrative della console di gestione dell'infrastruttura cloud TeamSystem. 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, sono adottati dal Fornitore protocolli di comunicazione sicuri e in linea con quanto la tecnologia rende disponibile in relazione al processo di autenticazione.

Misure di sicurezza tecniche	*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. *Formazione*: Il Fornitore eroga periodicamente ai propri dipendenti coinvolti nelle attività di trattamento corsi di formazione sulla corretta gestione dei dati personali. *Protection from malware* – Le VM sono protette contro il rischio di intrusione e dell'azione di programmi mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza periodica. Tutte le VM sono gestite tramite funzionalità antivirus (sia a livello hypervisor che infrastrutturale). *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 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. È comunque demandata al Titolare del trattamento la facoltà di eseguire autonomamente il backup dei propri dati per l'intera durata del contratto e per i 60 giorni successivi al termine dello stesso. *Logging* – 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. *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. *Incident Management*– 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, garantendo il mantenimento dei livelli migliori di servizio. *Alta affidabilità* – il Fornitore garantisce l'alta affidabilità nei seguenti termini: • L'architettura Server è 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. *Data center* – L'ambiente di virtualizzazione (inclusa la SAN – Storage Area network) è presente su server ospitati in un data center sito in Italia la cui gestione è demandata ad un fornitore certificato ISO 27001. In particolare le misure di sicurezza fisica poste a protezione del Data Center sono di seguito elencate: • Perimetro di sicurezza esterno:

	• Recinzione perimetrale che delimita il confine di proprietà composta da una protezione passiva anti scavalcamento con altezza minima di 3 m; • Le aree esterne sono monitorate da barriere infrarossi e/o sistemi di videoanalisi e sistemi di videosorveglianza con videoregistrazione; • Accesso pedonale selettivo/singolo; • Accesso veicolare selettivo; • Ronda armata; • Perimetro di sicurezza interno: • Presidio di vigilanza per controlli aree interne ed esterne, supervisione; • Allarmi, gestione visitatori con consegna badge in osservanza a disposizioni aziendali e specifiche per i Data Center; • Presidio di reception per la gestione degli accessi; • Tornelli a braccio triplice prospicienti al locale del presidio vigilanza e reception; • Perimetro di massima sicurezza interno: • Varco di accesso sala sistemi dotato di protezione passiva interbloccato; • Sistema di controllo accessi con gestione delle liste ABILITATI; • Sensori magnetici stato porta in grado di rilevare lo stato della porta; • Uscite d'emergenza dotate di sensori stato porta. Tutti gli allarmi sono remotizzati al presidio di vigilanza.

C – BUSINESS PROCESS OUTSOURCING (BPO)

Misure di sicurezza organizzative	*Certificazioni* – Il Fornitore ha ottenuto le seguenti certificazioni/attestazioni: • ISO/IEC 27001:2013: "Erogazione dei servizi di progettazione e gestione dell'infrastruttura ICT, di gestione delle applicazioni interne al Gruppo e di gestione dell'infrastruttura Cloud (IaaS)". • ISO/IEC 27018:2014 per la protezione dei dati personali nei servizi Public Cloud. *Policy e Disciplinari utenti* – Sono in essere dettagliate policy e disciplinari, ai quali tutta l'utenza con accesso ai sistemi informativi ha l'obbligo di conformarsi, finalizzate a garantire comportamenti idonei ad assicurare il rispetto dei principi di riservatezza, disponibilità ed integrità dei dati nell'utilizzo delle risorse informatiche. *Autorizzazione accessi logici* – Il Fornitore definisce i profili di accesso nel rispetto del *least privilege* necessario all'esecuzione delle mansioni assegnate. I profili di autorizzazione sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento. Tali profili sono oggetto di controlli periodici finalizzati alla verifica della sussistenza delle condizioni per la conservazione dei profili attribuiti. *Gestione interventi di assistenza* – Il Fornitore regolamenta la gestione degli interventi di assistenza allo scopo di garantire l'esecuzione delle sole attività disciplinate contrattualmente e impedire il trattamento eccessivo di dati personali la cui titolarità è in capo al Cliente o all'Utente Finale. *Change Management* – Il Fornitore ha in essere una specifica procedura attraverso la quale regolamenta il processo di Change Management in considerazione dell'introduzione di eventuali innovazioni tecnologiche o cambiamenti della propria impostazione e della propria struttura organizzativa. *Valutazione d'impatto sulla protezione dei dati (DPIA)* – In conformità agli artt. 35 e 36 del GDPR e sulla base del documento WP248 – Linee guida sulla valutazione d'impatto nella protezione dei dati adottate dal Gruppo di lavoro ex art. 29, il Fornitore ha predisposto una propria metodologia per l'analisi e la valutazione dei trattamenti che, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, presentino un rischio elevato per i diritti e le libertà delle persone fisiche allo scopo di procedere con la valutazione dell'impatto sulla protezione dei dati personali prima di iniziare il trattamento. *Incident Management* – Il Fornitore ha realizzato una specifica procedura di Incident Management allo scopo di garantire il ripristino delle normali operazioni di servizio nel più breve tempo possibile, garantendo il mantenimento dei livelli migliori di servizio. *Data Breach* – Il Fornitore ha implementato un'apposita procedura finalizzata alla gestione degli eventi e degli incidenti con un potenziale impatto sui dati personali che definisce ruoli e responsabilità, il processo di rilevazione (presunto o accertato), l'applicazione delle azioni di contrasto, la risposta e il contenimento dell'incidente / violazione nonché le modalità attraverso le quali effettuare le comunicazioni delle violazioni di dati personali al Cliente. *Formazione*: Il Fornitore eroga periodicamente ai propri dipendenti coinvolti nelle attività di trattamento, corsi di formazione sulla corretta gestione dei dati personali.
Misure di sicurezza tecniche	*Alta affidabilità* – Il Fornitore garantisce l'alta affidabilità nei seguenti termini: • L'architettura Server è completamente basata sull'utilizzo della soluzione di virtualizzazione VMWare applicata mediante duplicazione fisica e virtuale dei singoli sistemi, al fine di garantire la tolleranza ai guasti e l'eliminazione dei single point of failure. In particolare in caso di failure di un sistema, il software di gestione dell'ambiente virtuale è in grado di ridistribuire le attività in corso verso gli altri sistemi (high availabilty e load balancing), riducendo al minimo i disservizi e garantendo la persistenza delle connessioni esistenti. • Ciascun Server è attestato su una SAN mediante connessione iSCSI ad alta velocità.

	• Tutte le componenti dell'infrastruttura, tra i quali server, apparati di rete e sicurezza, sistemi Storage ed infrastruttura SAN, sono completamente ridondate per eliminare ogni single point of failure. • L'architettura di rete è progettata per proteggere i sistemi di front-end da Internet e dalle reti interne mediante l'utilizzo di una DMZ protetta da due livelli di firewalling distinti (defense-in-depth): un firewall di frontiera connesso ad Internet ed un secondo firewall, che integra anche funzionalità di Intrusion Prevention e antimalware, di proprietà dell'organizzazione, è messo a protezione della DMZ e dei sistemi di backend. *Hardening* – Sono in essere apposite attività di hardening finalizzate a prevenire il verificarsi di incidenti di sicurezza minimizzando le debolezze architetturali dei sistemi operativi, delle applicazioni e degli apparati di rete considerando - in particolare - le diminuzione dei rischi connessi alle vulnerabilità di sistema, la diminuzione dei rischi connessi al contesto applicativo presente sui sistemi e l'aumento dei livelli di protezione dei servizi erogati dai sistemi stessi. *Firewall, IDS/IPS* – I sistemi anti-intrusione, quali Firewall e IDS/IPS, sono posizionati all'interno del segmento di rete che collega l'infrastruttura cloud con Internet, al fine di intercettare ogni eventuale azione malevola volta a degradare, parzialmente o totalmente, l'erogazione del servizio. Nello specifico gli apparati adottati sono del tipo UTM SourceFire (Cisco), che includono sia la componente Firewall sia la componente IDS/IPS. *Sicurezza linee di comunicazione* - Per quanto di propria competenza, sono adottati dal Fornitore protocolli di comunicazione sicuri e in linea con quanto la tecnologia rende disponibile. *Protection from malware* – Le VM sono protette contro il rischio di intrusione e dell'azione di programmi mediante l'attivazione di idonei strumenti elettronici aggiornati con cadenza periodica. Tutte le VM sono gestite tramite funzionalità antivirus (sia a livello hypervisor che infrastrutturale). *Credenziali di autenticazione* – I sistemi sono configurati con modalità idonee a consentirne l'accesso unicamente a soggetti dotati di credenziali di autenticazione che ne consentono la loro univoca identificazione. Fra questi, codice associato a una parola chiave, riservata e conosciuta unicamente dallo stesso; dispositivo di autenticazione in possesso e uso esclusivo dell'utente, eventualmente associato a un codice identificativo o a una parola chiave.. *Parola chiave* – Relativamente alle caratteristiche di base ovvero, obbligo di modifica al primo accesso, lunghezza minima, assenza di elementi riconducibili agevolmente al soggetto, regole di complessità, scadenza, history, valutazione contestuale della robustezza, visualizzazione e archiviazione, la parola chiave è gestita conformemente alle best practice. Ai soggetti ai quali sono attribuite le credenziali sono fornite puntuali istruzioni in relazione alle modalità da adottare per assicurarne la segretezza. *Logging* – I sistemi sono configurabili con modalità che consentono il tracciamento degli accessi e, ove appropriato, delle attività svolte in capo alle diverse tipologie di utenze (Amministratore, Super Utente, etc.) protetti da adeguate misure di sicurezza che ne garantiscono l'integrità. *Backup & Restore* – Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati. È comunque demandata al Titolare la facoltà di eseguire autonomamente il backup dei propri dati per l'intera durata del contratto e per i 60 giorni successivi al termine dello stesso. Ove gli accordi contrattuali lo prevedono è posto in uso un piano di continuità operativa integrato, ove necessario, con il piano di disaster recovery i quali garantiscono la disponibilità e l'accesso ai sistemi anche nel caso di eventi negativi di portata rilevante che dovessero perdurare nel tempo. *Vulnerability Assessment & Penetration Test* – Il Fornitore effettua periodicamente attività di analisi delle vulnerabilità finalizzata a rilevare lo stato di esposizione alle

	vulnerabilità note, sia in relazione agli ambiti infrastrutturali sia a quelli applicativi, considerando i sistemi in esercizio o in fase di sviluppo. Ove ritenuto appropriato in relazione ai potenziali rischi identificati, tali verifiche sono integrate periodicamente con apposite tecniche di Penetration Test, mediante simulazioni di intrusione che utilizzano diversi scenari di attacco, con l'obiettivo di verificare il livello di sicurezza di applicazioni / sistemi / reti attraverso attività che mirano a sfruttare le vulnerabilità rilevate per eludere i meccanismi di sicurezza fisica / logica ed avere accesso agli stessi. I risultati delle verifiche sono puntualmente e dettagliatamente esaminati per identificare e porre in essere i punti di miglioramento necessari a garantire l'elevato livello di sicurezza richiesto. *Amministratori di Sistema* – Relativamente a tutti gli utenti che operano in qualità di Amministratori di Sistema, il cui elenco è mantenuto aggiornato e le cui funzioni attribuite sono opportunamente definite in appositi atti di nomina, è gestito un sistema di log management finalizzato al puntuale tracciamento delle attività svolte ed alla conservazione di tali dati con modalità inalterabili idonee a consentirne ex post il monitoraggio. L'operato degli Amministratori di Sistema è sottoposto ad attività di verifica in modo da controllarne la rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previsti dalle norme vigenti. *Data Center* – L'ambiente di virtualizzazione (inclusa la SAN – Storage Area network) è presente su server ospitati in un data center sito in Italia la cui gestione è demandata ad un fornitore certificato ISO 27001. In particolare le misure di sicurezza fisica poste a protezione del Data Center sono di seguito elencate: • Perimetro di sicurezza esterno: ✓ recinzione perimetrale che delimita il confine di proprietà composta da una protezione passiva anti scavalcamento con altezza minima di 3 m; ✓ le aree esterne sono monitorate da barriere infrarossi e/o sistemi di videoanalisi e sistemi di videosorveglianza con videoregistrazione; ✓ accesso pedonale selettivo/singolo; ✓ accesso veicolare selettivo; ✓ ronda armata. • Perimetro di sicurezza interno: ✓ presidio di vigilanza per controlli aree interne ed esterne, supervisione; ✓ allarmi, gestione visitatori con consegna badge in osservanza a disposizioni aziendali e specifiche per i Data Center; ✓ presidio di reception per la gestione degli accessi; ✓ tornelli a braccio triplice prospicienti al locale del presidio vigilanza e reception. • Perimetro di massima sicurezza interno: ✓ varco di accesso sala sistemi dotato di protezione passiva interbloccato; ✓ sistema di controllo accessi con gestione delle liste ABILITATI; ✓ sensori magnetici stato porta in grado di rilevare lo stato della porta; ✓ uscite d'emergenza dotate di sensori stato porta. Tutti gli allarmi sono remotizzati al presidio di vigilanza.

D - BPI – BUSINESS PROCESS INSOURCING

Misure di sicurezza organizzative	*Policy e Disciplinari utenti* – Sono in essere dettagliate policy e disciplinari, ai quali tutta l'utenza con accesso ai sistemi informativi ha l'obbligo di conformarsi, finalizzate a garantire comportamenti idonei ad assicurare il rispetto dei principi di riservatezza, disponibilità ed integrità dei dati nell'utilizzo delle risorse informatiche. *Autorizzazione accessi logici* – Il Fornitore definisce i profili di accesso el rispetto del least privilege necessario all'esecuzione delle mansioni assegnate. I profili di autorizzazione sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento. Tali profili sono oggetto di controlli periodici finalizzati alla verifica della sussistenza delle condizioni per la conservazione dei profili attribuiti. *Data Breach* – Il Fornitore ha implementato un'apposita procedura finalizzata alla gestione degli eventi e degli incidenti con un potenziale impatto sui dati personali che

	definisce ruoli e responsabilità, il processo di rilevazione (presunto o accertato), l'applicazione delle azioni di contrasto, la risposta e il contenimento dell'incidente / violazione nonché le modalità attraverso le quali effettuare le comunicazioni delle violazioni di dati personali al Cliente. *Formazione*: Il Fornitore eroga periodicamente ai propri dipendenti coinvolti nelle attività di trattamento corsi di formazione sulla corretta gestione dei dati personali.
Misure di sicurezza tecniche	*Sicurezza linee di comunicazione* - Per quanto di propria competenza, sono adottati dal Fornitore protocolli di comunicazione sicuri e in linea con quanto la tecnologia rende disponibile in relazione al processo di autenticazione. *Backup & Restore* – Ove previsto dagli accordi contrattuali, sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati.

E – ON PREMISES

Misure di sicurezza organizzative	*Policy e Disciplinari utenti* – Sono in essere dettagliate policy e disciplinari, ai quali tutta l'utenza con accesso ai sistemi informativi ha l'obbligo di conformarsi, finalizzate a garantire comportamenti idonei ad assicurare, in fase di assistenza tecnica, il rispetto dei principi di riservatezza, disponibilità ed integrità dei dati nell'utilizzo delle risorse informatiche. *Autorizzazione accessi logici* – Il Fornitore definisce i profili di accesso nel rispetto del *least privilege* necessario all'esecuzione delle mansioni assegnate. I profili di autorizzazione sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento. Tali profili sono oggetto di controlli periodici finalizzati alla verifica della sussistenza delle condizioni per la conservazione dei profili attribuiti. *Gestione interventi di assistenza* – Il Fornitore regolamenta la gestione degli interventi di assistenza allo scopo di garantire l'esecuzione delle sole attività previste contrattualmente e impedire il trattamento eccessivo di dati personali la cui titolarità è rivestita dal Cliente. *Incident Management & Data Breach* – Il Fornitore ha implementato un'apposita procedura finalizzata alla gestione degli eventi e degli incidenti con un potenziale impatto sui dati personali che definisce ruoli e responsabilità, il processo di rilevazione (presunto o accertato), l'applicazione delle azioni di contrasto, la risposta e il contenimento dell'incidente / violazione nonché le modalità attraverso le quali effettuare le comunicazioni delle violazioni di dati personali al Cliente. *Formazione*: Il Fornitore eroga periodicamente ai propri dipendenti coinvolti nelle attività di trattamento corsi di formazione sulla corretta gestione dei dati personali
Misure di sicurezza tecniche	*Sicurezza linee di comunicazione*- Per quanto di propria competenza, in fase di gestione di interventi di assistenza, sono adottati dal Fornitore protocolli di comunicazione sicuri e in linea con quanto la tecnologia rende disponibile. *Protection from malware*– Le postazioni di lavoro adottate in fase di Assistenza tecnica, sono protette contro il rischio di intrusione e dell'azione di programmi mediante l'attivazione di idonei strumenti elettronici aggiornati con cadenza periodica. Tutte le VM sono gestite tramite funzionalità antivirus (sia a livello hypervisor che infrastrutturale). *Amministratori di Sistema* – Relativamente a tutti gli utenti che operano in qualità di Amministratori di Sistema, il cui elenco è mantenuto aggiornato e le cui funzioni attribuite sono opportunamente definite in appositi atti di nomina, è gestito un sistema di log management finalizzato al puntuale tracciamento delle attività svolte ed alla conservazione di tali dati con modalità inalterabili idonee a consentirne ex post il monitoraggio. L'operato degli Amministratori di Sistema è sottoposto ad attività di verifica in modo da controllarne la rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previsti dalle norme vigenti.