Data Processing Agreement (DPA)

ex. art.28 Regolamento UE 2016/679 – GDPR

Accordo sul Trattamento dei Dati Personali per i Servizi di Assistenza Tecnica ICT

TRA

IL TITOLARE DEL TRATTAMENTO (DATA CONTROLLER)
Cliente committente del servizio di assistenza tecnica
(in seguito, anche «*Cliente*» o «il *Titolare*»)

E

IL RESPONSABILE DEL TRATTAMENTO – (DATA PROCESSOR)
PROTOPIA TEAM s.r.l.
con sede legale in Via Felice Goffi, 5 – 10051 Avigliana (TO)
P. IVA: IT 08421130017
(in seguito, anche «*PROTOPIA*» o «il *Responsabile*»)

PREMESSO CHE

- l'art. 4 co. 1 n. 7) del Regolamento (UE) 2016/679 definisce il "***Titolare del Trattamento***" *come la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del Trattamento di dati personali*;
- secondo quanto stabilito dal Regolamento Generale sulla Protezione dei Dati Personali (UE) 2016/679 (in seguito anche "**Regolamento**" o "**GDPR**"), in merito al Trattamento dei dati personali, **Cliente** in qualità di **Titolare del Trattamento** è tenuto ad individuare e disciplinare i rapporti di Responsabilità/Titolarità con i soggetti esterni alla propria organizzazione, attraverso appositi contratti o atti giuridici a norma del diritto dell'Unione o degli Stati membri;
- il **Titolare del Trattamento** (di seguito anche semplicemente "**Titolare**") intende affidare in esterno le attività di gestione e manutenzione dei sistemi informatici aziendali;
- l'art. 4, co. 1, n. 8) del Regolamento (UE 2016/679) definisce il "***Responsabile***" *come "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratti dati personali per conto del Titolare del Trattamento"*;
- l'art. 28 co. 1 dispone che: "q*ualora un Trattamento debba essere effettuato per conto del Titolare del Trattamento, quest'ultimo ricorre unicamente a responsabili del Trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il Trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato*";
- **PROTOPIA** è in possesso di adeguate competenze tecniche, organizzative e know-how e presenta adeguate garanzie, circa gli scopi che si intendono affidare e le conseguenti modalità di trattamento dei Dati Personali, delle misure di sicurezza da adottare al fine di garantirne la riservatezza, l'integrità e la disponibilità, nonché circa le norme che disciplinano la protezione dei Dati Personali;
- **PROTOPIA** svolgerà il suo mandato, trattando i dati per conto del Titolare del Trattamento, in qualità di Responsabile del Trattamento (di seguito anche "***Responsabile***") ai sensi dell'art.28 del Regolamento;
- il rapporto tra le "**Parti**" (ovvero Titolare del Trattamento e Responsabile del Trattamento) è regolarmente disciplinato in un contratto di servizio (in seguito anche «***Contratto Principale***») in cui il Titolare del Trattamento, affida alla **PROTOPIA** i servizi di assistenza tecnica, di gestione e manutenzione dei sistemi informatici aziendali e le relative funzioni di amministrazione di sistema.
- l'art. 28 prescrive che "*i trattamenti da parte di un Responsabile del Trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il Responsabile del Trattamento al Titolare del Trattamento e che stipuli la materia disciplinata e la durata del Trattamento, la natura e la finalità del Trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e diritti del Titolare del Trattamento*";
- il Responsabile del Trattamento procederà al trattamento dei dati personali nell'ambito della sua autonomia professionale ma secondo le istruzioni impartite dal Titolare anche in relazione alla durata del Trattamento, al tipo di dati personali e alle categorie di interessati, agli obblighi e ai diritti del Titolare del Trattamento;
- i termini usati nel presente contratto devono essere intesi in accordo con le loro rispettive definizioni ex art. 4 Regolamento (UE) 2016/679;
- se non diversamente specificato, il termine "articolo o art." è da intendersi riferito alle specifiche parti del presente documento.

Tutto ciò premesso, evidenziando che la premessa costituisce parte integrante e sostanziale del presente accordo,

SI CONVIENE E STIPULA QUANTO SEGUE

Art. 1. OGGETTO DEL CONTRATTO

Il contratto ha ad oggetto la disciplina ai sensi dell'art. 28 del Regolamento (UE) 2016/679 del trattamento dei dati personali conferiti dal **Cliente,** in qualità di Titolare del Trattamento, a **PROTOPIA -** Responsabile del trattamento - limitatamente alle funzioni attribuite dal Contratto Principale e con riferimento alle sole informazioni cui il Responsabile può venire

Art. 2. DURATA

2.1 Il presente Accordo sarà valido ed efficace per tutta la durata del Contratto Principale e si intenderà automaticamente risolto, senza necessità di ulteriori comunicazioni, con la risoluzione e/o scioglimento del Contratto Principale ovvero, a discrezione del Titolare, qualora sia integrata da parte del Responsabile la violazione di disposizioni obbligatorie in materia di protezione di dati personali ovvero di termini del presente accordo.

2.2 Alla cessazione del Contratto, per qualsivoglia causa, continueranno ad avere efficacia quelle clausole che per loro natura sopravvivono all'estinzione del rapporto giuridico. In particolare, la cessazione del Contratto Principale e del presente Accordo, non comporterà il venire meno degli obblighi di riservatezza in merito alle informazioni acquisite dalle parti e al rispetto della normativa vigente sul Trattamento dei dati personali eventualmente conservati.

2.3 Le parti si impegnano, in ogni caso, a modificare ovvero integrare il contenuto del presente Contratto a fronte di sopravvenienze normative ovvero a fronte di carenze/insufficienze di disciplina risultanti dall'applicazione pratica del presente accordo. Il rifiuto opposto alle predette modifiche/integrazioni costituirà causa di risoluzione del presente contratto nonché di quello principale (art. 1456 Cod. civ)

Art. 3. ATTIVITA' DI TRATTAMENTO

3.1 I dati affidati, nell'ambito delle attività demandate al Responsabile attraverso il Contratto Principale, potranno essere trattati, anche in virtù dell'autonomia professionale riconosciuta dal Titolare, esclusivamente per le finalità riportate all'art. **17** del presente accordo.

Art. 4. MODALITA' DEL TRATTAMENTO

4.1 Nello svolgimento del proprio incarico, il Responsabile del Trattamento, si impegna ad usare la diligenza richiesta dalla natura della prestazione, dal carattere fiduciario, dall'interesse esclusivo del committente e ad effettuare i trattamenti previsti, nel rispetto delle Leggi applicabili in materia di trattamento dei dati personali, secondo le modalità previste nel presente accordo.

4.2 Il Titolare del Trattamento riconosce, al Responsabile del Trattamento, nei limiti del presente accordo e anche alla luce del principio di responsabilizzazione introdotto dal Regolamento, autonomia di azione e decisione in merito all'esecuzione dei trattamenti assegnati, alla scelta delle modalità e delle tecnologie ritenute più opportune, così come alla scelta di soggetti Autorizzati e dei collaboratori a cui affidare il Trattamento.

4.3 Le parti si impegnano ad adottare, misure tecniche ed organizzative idonee ad evitare la perdita, la cancellazione, la distruzione anche accidentale dei dati personali ed ogni altro rischio connesso al trattamento di dati personali al fine di garantire sempre una adeguata tutela dei diritti e le libertà dei soggetti interessati;

4.4 I dati personali potranno essere trattati dal Responsabile su qualunque supporto cartaceo o digitale idoneo, in base alle attività svolte, a patto che gli strumenti siano opportunamente individuati, inventariati e dotati di adeguate misure di sicurezza
ed il loro utilizzo da parte dei soggetti autorizzati, sia opportunamente disciplinato.

Art. 5. AFFIDABILITA' DEGLI AUTORIZZATI E NON DIVULGAZIONE

5.1 Il Responsabile adotterà misure ragionevoli per garantire l'affidabilità di qualsiasi dipendente o collaboratore che possa avere accesso ai dati personali affidati dal Titolare, assicurando in ogni caso che il loro accesso sia strettamente limitato alle persone che ne necessitano la conoscenza per svolgere le mansioni affidate.

5.2 Il Responsabile deve garantire che tutte le persone che hanno il compito di trattare i dati personali del Titolare:

1. siano informate della natura confidenziale dei Dati personali del Titolare e siano a conoscenza degli obblighi del Responsabile ai sensi del presente accordo e del Contratto Principale;
2. siano in possesso di formazione / certificazioni appropriate in relazione alle mansioni svolte e alle leggi applicabili sulla protezione dei dati o qualsiasi altra formazione / certificazione richiesta dal Titolare;
3. siano soggetti a impegni di riservatezza o obblighi professionali o normativi di riservatezza;
4. siano soggetti all'autenticazione dell'utente e a specifiche procedure di accesso quando accedono ai Dati personali del Titolare in conformità alle leggi applicabili in materia di protezione dei dati;
5. abbiano ricevuto adeguate istruzioni in merito alle operazioni corrette e sicure del trattamento e siano stati informati in merito ai controlli applicati.

Art. 6. OBBLIGHI DELLE PARTI

6.1 In relazione ai termini stabiliti dal presente accordo, il Responsabile:

1. conferma di essere a conoscenza delle disposizioni legali applicabili in materia di protezione dei dati e si impegna ad osservare i principi della corretta elaborazione dei dati trattati per conto del Titolare con particolare riguardo a quanto stabilito dal contratto principale
2. garantisce che i dati personali saranno trattati in modo lecito, raccolti, registrati e trattati per gli scopi espliciti e legittimi determinati dal Titolare nel Contratto Principale ed utilizzati con finalità e modalità conformi a quelle per le quali sono stati raccolti;
3. collabora con il Titolare ai fini dell'esatta applicazione della legge;
4. **agisce autonomamente** nell'ambito e nei limiti della propria attività ma sempre seguendo le direttive stabilite dal Titolare nel presente accordo;
5. in caso di necessità di ulteriore trattamento, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo diversa disposizione di legge, il Responsabile è tenuto all'obbligo di informare il Titolare sulla specifica necessità e ad attenersi alle sue specifiche istruzioni e autorizzazioni. Sul punto si precisa che, fatto salvo quanto autorizzato all'art.**16**, non è ammesso alcun trasferimento dei dati personali verso paesi non facenti parte dell'unione economica europea senza esplicito consenso del Titolare;
6. anche in virtù di quanto stabilito all' art. **5**, incarica e autorizza per iscritto eventuali soggetti che agiscono sotto la sua autorità in merito al Trattamento dei dati personali, impartendo agli stessi le istruzioni relative e verificandone la loro puntuale applicazione;
7. mantiene la massima riservatezza nel trattamento dei dati e in ottemperanza a quanto stabilito all' art. **5.2.3**, garantisce al Titolare del Trattamento che le persone autorizzate al trattamento (es. dipendenti e/o collaboratori) si siano impegnate per iscritto alla riservatezza o abbiano un adeguato obbligo legale di riservatezza ai sensi dell'art. 28 paragrafo 3 lettera b) del Regolamento;
8. garantisce, anche ai sensi di quanto stabilito negli artt. **5.2.1** e **5.2.2**, che i soggetti da lui utilizzati per elaborare i dati, siano stati autorizzati per iscritto e informati delle disposizioni pertinenti sulla protezione dei dati e del presente contratto, prima di iniziare a elaborare i dati. Le corrispondenti misure di formazione e sensibilizzazione sono eseguite in modo appropriato su base regolare. Il responsabile del trattamento garantisce che le persone incaricate del trattamento dei dati siano adeguatamente istruite e

controllate su base continuativa in termini di conformità ai requisiti di protezione dei dati:

9. si impegna a recepire e adottare le eventuali misure di sicurezza tecniche e organizzative concordate nel Contratto Principale o nel presente accordo. Sul punto si precisa che il Titolare del Trattamento, potrà inviare una notifica scritta al Responsabile del Trattamento se, a suo ragionevole giudizio, le misure tecniche e organizzative già concordate dovessero essere modificate per conformarsi a nuove prescrizioni imposte dalle Leggi in materia di protezione dei dati. Tale notifica scritta includerà una descrizione, il più possibile dettagliata, dei cambiamenti imposti dalle leggi e delle modifiche necessarie;
10. si impegna ad adottare, qualora contestualmente al contratto o successivamente **non fossero impartite** specifiche misure di sicurezza da parte del Titolare, tutte le misure tecniche ed organizzative (ex art. 32 del GDPR) ritenute adeguate per garantire un livello di sicurezza proporzionato al rischio, che tenga conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del Trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche. Tali misure devono essere attuate in modo da ridurre al minimo i rischi di distruzione o perdita anche accidentale dei dati stessi, di accesso non autorizzato o di Trattamento non consentito o non conforme alle finalità della raccolta. Sul punto si precisa che, su richiesta del Titolare, il Responsabile è tenuto a rendere disponibile una descrizione delle misure tecniche ed organizzative adottate e degli eventuali risultati delle attività di autovalutazione effettuate per verificarne l'efficacia;
11. si impegna per l'intera durata dell'incarico a rafforzare, integrare e ottimizzare le misure di sicurezza di cui al punto precedente, allo scopo di mantenere la conformità alle Leggi in materia di protezione dei dati personali e a quanto stabilito nel presente accordo;
12. informa il Titolare del Trattamento della necessità di ricorrere ad ulteriore Responsabile del Trattamento. Fatto salvo quanto stabilito nel Contratto Principale e nell'art **16** del presente accordo, e la facoltà per il Titolare di rifiutare la nomina di altro Responsabile, è necessario il previo espresso consenso scritto del Titolare del Trattamento per la nomina di ulteriori Responsabili;
13. assicura il Titolare del Trattamento nel soddisfare gli obblighi di legge ovvero qualora sia necessario: dare seguito alle richieste per l'esercizio dei diritti dell'interessato, assicurare la risposta, nei termini di legge, alle istanze presentate al Titolare dalle autorità di controllo, collaborare attivamente con lo stesso nel caso di richiesta di informazioni o nel caso di controlli. Sul punto si precisa che se il Responsabile del trattamento è soggetto all'ispezione delle autorità di controllo o di altri organismi o se le persone interessate esercitano diritti sul Responsabile del trattamento, questi è tenuto a supportare il Titolare nella misura richiesta, se i dati vengono elaborati per conto del Titolare;
14. deve cancellare o restituire tempestivamente, su richiesta del Titolare del Trattamento, tutti i dati personali e le copie esistenti di cui è in possesso senza poterne conservare copia alcuna, salvo espresso diverso accordo o previsione di legge. In ogni caso, eliminare e/o distruggere i dati personali quando siano state raggiunte le finalità per le quali i dati sono stati raccolti e trattati in mancanza di un obbligo di legge o della necessità di ulteriore conservazione.

6.2 Il Titolare conferma di essere a conoscenza delle disposizioni legali applicabili in materia di protezione dei dati e si impegna ad osservare quanto stabilito dal Regolamento UE 2016/679 ed i principi della corretta elaborazione dei dati trattati, con particolare riguardo ai trattamenti oggetto del contratto principale e si impegna a mettere a disposizione del Responsabile ogni informazione necessaria e richiesta per consentire il raggiungimento degli obiettivi del presente accordo, garantendo sempre la qualità e la sicurezza delle informazioni trasmesse.

Art. 7. TRATTAMENTO SECONDARIO

7.1 Con la stipula del presente contratto, il Titolare conferisce altresì autorizzazione generale al Responsabile del Trattamento (ai sensi dell'art. 28 paragrafo 2 del Regolamento), di coinvolgere gli eventuali ulteriori Responsabili del Trattamento («*sub-responsabili*») elencati nel Contratto Principale e/o negli articoli **16** e **19** del presente accordo.

7.2 In relazione a quanto stabilito all'art. **6.1.12**, per ciascun Sub-Responsabile del Trattamento, il Responsabile s'impegna a:

a) incaricare i Sub-Responsabili solo su base individuale con il consenso scritto del Titolare. Sul punto si precisa che il consenso è possibile solo se il subappalto è soggetto da contratto agli obblighi di protezione dei dati, che sono paragonabili a quelli stipulati nel presente accordo.
b) fornire al Titolare i dettagli completi del Trattamento che debba essere affidato in subappalto a ciascun Sub-Responsabile;
c) includere nel contratto tra il Responsabile e ciascun Sub-Responsabile del Trattamento, le stesse condizioni specificate nel presente accordo, e supervisionarne la conformità. Su richiesta, il Responsabile s'impegna a fornire al Titolare una copia dei contratti stipulati con i Sub-Responsabili del Trattamento, affinché il Titolare del Trattamento possa verificare l'adeguatezza del servizio e delle garanzie di sicurezza;
d) nei limiti entro i quali il subappalto comporti il trasferimento di Dati Personali al di fuori dell'Unione economica europea, incorporare clausole contrattuali o qualsivoglia altro meccanismo richiesto dal Regolamento per garantire il trasferimento a norma di legge e l'adeguata protezione dei Dati Personali;

7.3 La nomina di eventuali sub-responsabili, che devono trattare dati per conto del Titolare, che non sono ubicati e non operano esclusivamente all'interno dell'UE o della CEE, è possibile solo nel rispetto delle condizioni stabilite dal Regolamento (UE) 2016/679. In particolare, ciò è consentito solo se il sub-responsabile fornisce adeguate misure di protezione dei trattamenti. Il Responsabile del trattamento deve informare il Titolare delle garanzie specifiche sulla protezione dei dati fornite dal sub-responsabile e su come ottenerne evidenza.

7.4 Qualora il sub-responsabile non adempia ai propri obblighi di protezione dei dati, il Responsabile del trattamento sarà sempre e comunque responsabile nei confronti del Titolare.

7.5 Qualsiasi subappalto aggiuntivo eseguito dagli eventuali sub-responsabile non è consentito.

7.6 Ai fini del presente accordo, i sopra elencati termini, si riferiscono solo a quei servizi che sono direttamente associati all'espletamento del servizio primario da parte del Responsabile (sub-appalto totale o anche parziale). Non si applicano a servizi aggiuntivi, accessori o funzionali come il trasporto, la manutenzione e la pulizia, nonché all'utilizzo di servizi di telecomunicazione, servizi informatici o di sicurezza informatica anche in Cloud erogati come «*Infrastructure as a service» (IaaS)*, «*Platform as a service» (PaaS*) o «*Software as a service» (SaaS).* **L'obbligo del Responsabile di garantire al Titolare del trattamento che la protezione dei dati e la sicurezza dei trattamenti siano garantiti in questi casi, rimane inalterato e in ogni caso sotto la sua diretta responsabilità.** Sul punto si precisa che il Responsabile del Trattamento si assume tutte le responsabilità dei danni diretti e/o indiretti causati al Titolare, agli Interessati o a terzi, dall'utilizzo di qualunque servizio, compresi quelli accessori e non associabili all'espletamento dell'incarico assegnato dal titolare (esempio: software gestionali, connettività, servizi di sicurezza, di backup, EndPoint security, firewall e continuità operativa).

7.7 Ai fini del presente accordo, il Titolare del Trattamento si dichiara consapevole che quanto stabilito dall'art. 7.6 non si applica ai servizi Cloud gestiti dal Responsabile per conto del Titolare stesso, ovvero a tutti i servizi informatici di qualunque genere e per qualunque ragione attivati dal Titolare e affidati in gestione al Responsabile del trattamento.

Art. 8. ADESIONE A CODICI DI CONDOTTA O MECCANISMI DI CERTIFICAZIONE

8.1 Il Responsabile è invitato a prendere in considerazione l'adesione a codici di condotta (ex art. 40 GDPR) o a meccanismi di certificazione (ex art. 42 GDPR) onde dimostrare le garanzie sufficienti ai sensi dell'art 28 paragrafo 1 del GDPR, dandone tempestiva comunicazione al Titolare in caso di adesione.

Art. 9. DIRITTI DEL SOGGETTO INTERESSATO

9.1 Con riferimento a quanto stabilito all'art **6.1.13**, il Responsabile si impegna a notificare al Titolare del Trattamento, senza ingiustificato ritardo e comunque entro **cinque (5)** giorni lavorativi, l'eventuale ricezione di una richiesta proveniente da un soggetto interessato ai sensi di qualsivoglia Legge in materia, comprese le richieste per l'esercizio dei diritti di cui al Capo III del Regolamento, fornendo altresì i dettagli completi riguardanti tale richiesta.

9.2 Il Responsabile s'impegna a collaborare con il Titolare del Trattamento al fine di permettere allo stesso di adempiere ai propri doveri nei confronti dei soggetti interessati, delle autorità di controllo e di qualsiasi altro soggetto. In particolare, il Responsabile s'impegna a:

a. fornire tutte le informazioni richieste dal Titolare entro i tempi ragionevoli specificati in ciascun caso dal Titolare, compresi i dettagli completi e le copie del reclamo, della comunicazione o della richiesta e gli eventuali Dati Personali in suo possesso in relazione al soggetto interessato;
b. ove applicabile, fornire l'assistenza ragionevolmente richiesta dal Titolare per consentirgli di adempiere alla relativa richiesta entro i tempi prescritti dalle Leggi in materia di Protezione dei Dati;
c. implementare le eventuali misure tecniche e organizzative aggiuntive che dovessero essere ragionevolmente richieste dal Titolare del Trattamento per consentirgli di rispondere efficacemente ai relativi reclami, comunicazioni o richieste.

9.3 Il Titolare si impegna ad informare i soggetti interessati ai sensi degli artt. 12, 13 e 14 del GDPR e ad acquisire il consenso dell'interessato ai sensi degli art. 6 e 7 del GDPR, nei casi in cui il consenso risulti essere la corretta base giuridica del Trattamento.

Art. 10. VIOLAZIONE DEI DATI PERSONALI E GESTIONE DEGLI INCIDENTI

10.1 Il Responsabile, con rifermento ai trattamenti effettuati per conto del Titolare deve:

a) notificare senza ritardo al Titolare, comunque entro ventiquattro **(24) ore** dal momento in cui si è percepita la violazione (o la sospetta violazione) di dati (c.d. "**Data Breach**"), fornendo sufficienti informazioni che consentano di adempiere agli obblighi di segnalazione al Garante; tale notifica dovrà:
   a. descrivere la natura della violazione dei dati, le categorie e i numeri di soggetti interessati nonché le categorie e i numeri delle Registrazioni di Dati Personali in oggetto;
   b. comunicare il nominativo e i contatti del Responsabile della protezione dati del Responsabile del Trattamento (se nominato) o altri relativi contatti dai quali sarà possibile ottenere maggiori dettagli;
   c. descrivere le probabili conseguenze derivanti dalla violazione dei dati;
   d. descrivere le misure adottate o proposte per affrontare il Data Breach.
b) collaborare in buona fede con il Titolare all'indagine, alla mitigazione e alla correzione di ciascuna violazione dei dati, al fine di soddisfare qualsivoglia requisito previsto dalle Leggi in materia di Protezione dei Dati;
c) coordinarsi con il Titolare al fine di predisporre i contenuti di eventuali dichiarazioni pubbliche in materia di Data Breach, o le eventuali notifiche richieste per le persone coinvolte;
d) evitare di dare comunicazione a soggetti terzi dell'evento, senza espresso consenso preventivo scritto del Titolare, salve le ipotesi di notifica obbligatoria prevista dalle leggi dell'Unione europea o di uno Stato membro. In tal caso, il Responsabile s'impegna a informare il Titolare del Trattamento del suddetto obbligo, a fornire una copia della notifica proposta e a tenere conto di eventuali commenti fatti dal Titolare.

Art. 11. VALUTAZIONE D'IMPATTO E CONSULTAZIONE PREVENTIVA

11.1 Qualora fosse necessario e limitatamente ai trattamenti oggetto del presente accordo, il Responsabile del Trattamento s'impegna a fornire ragionevoli livelli di assistenza al Titolare in relazione alle eventuali valutazioni d'impatto sulla protezione dei dati richieste ai sensi dell'Art. 35 del GDPR e ad eventuali consultazioni preventive richieste ai sensi dell'Art. 36 del GDPR.

11.2 Il Responsabile del Trattamento effettua una valutazione di impatto sui trattamenti di dati personali effettuati per suo conto, da ulteriori responsabili del Trattamento, se:
a) il Trattamento riguarda categorie particolari di dati trattati con strumenti elettronici;
b) i dati sono interessati da trasferimenti transfrontalieri o extra UE;
c) i dati sono trasferiti ad organizzazioni internazionali.

Il Responsabile mette a disposizione del Titolare del Trattamento i risultati dalla Valutazione d'Impatto e non effettua il trasferimento/Trattamento senza consultazione preventiva del Titolare, qualora la valutazione rivelasse un rischio residuo non trascurabile.

Art. 12. CONSERVAZIONE, CANCELLAZIONE O RESTITUZIONE DEI DATI

12.1 Il Responsabile assicura su base permanente, che i dati personali saranno conservati per il periodo di tempo strettamente necessario all'esecuzione delle attività/servizi oggetto di Contratto, e comunque non oltre i termini di legge o quelli di volta in volta indicati o concordati con il Titolare.

12.2 Fatte salve le conservazioni di dati personali effettuate per adempiere a specifici obblighi di legge, subordinatamente a quanto stabilito all' art. **6.1.14**, il Responsabile del Trattamento, in base alla richiesta del Titolare, sollecitamente e comunque, qualora non fosse specificato un tempo diverso, entro **UN MESE** dal decorrere dal primo verificarsi della cessazione del Trattamento dei Dati Personali da parte del Responsabile del Trattamento o della risoluzione del presente accordo o del Contratto Principale, s'impegna a:

a) restituire una copia completa di tutti i Dati Personali al Titolare mediante trasferimento sicuro di file nel formato indicato dal Titolare tra gli standard disponibili del Responsabile e cancellare in modo sicuro tutte le altre copie;
b) cancellare in modo sicuro tutte le copie dei Dati Personali;

Il Responsabile fornirà in ogni caso, adeguata documentazione scritta al Titolare del Trattamento a dimostrazione dell'esatto adempimento alle disposizioni **a)** o **b)** della presente sezione.

Art. 13. DIRITTO DI VERIFICA

13.1 Il Responsabile del Trattamento s'impegna inoltre a:
a) mettere a disposizione del Titolare del Trattamento, ai sensi dell'art. 28 paragrafo 3 lettera h) del Regolamento, tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di legge e contribuisce alle attività di revisione, comprese le ispezioni (Audit), realizzate dal titolare del trattamento o da un altro soggetto da questi incaricato.
b) compiere attività di autovalutazione rispetto alle misure di sicurezza adottate ai sensi degli artt. **6.1.9** e **6.1.10** del presente accordo**,** fornendone, a richiesta, documentazione scritta al Titolare del Trattamento

13.2 In riferimento a quanto stabilito al punto a) della presente sezione, le parti concordano che in caso di ispezione del Titolare del Trattamento o di un altro soggetto da questi incaricato, presso le strutture operative o tecniche del Responsabile del Trattamento, il Responsabile ha il diritto di addebitare al Titolare del trattamento tutti i costi sostenuti per far fronte all'ispezione.

Art. 14. TRASFERIMENTI INTERNAZIONALI DI DATI PERSONALI

14.1 Fatto salvo quanto stabilito dall'art **7.6**, il Responsabile del Trattamento s'impegna a non trattare (permanentemente o temporaneamente) i Dati Personali e parimenti a non consentire a qualsivoglia ulteriore Responsabile del Trattamento di trattare i Dati Personali in un paese al di fuori dello Spazio Economico Europeo (SEE) senza un'autorizzazione scritta e preventiva del Titolare del Trattamento. In ogni caso il trattamento dovrà avvenire nel rispetto della normativa vigente.

Art. 15. VARIE

15.1 In caso di discrepanze tra le disposizioni del presente Contratto e qualsivoglia altro contratto tra le parti, compreso, a mero titolo esemplificativo, il Contratto Principale, le disposizioni del presente Contratto prevarranno in relazione agli obblighi delle parti riferiti alla protezione dei Dati Personali.

15.2 La conformità da parte del Responsabile del Trattamento alle disposizioni del presente Contratto non comporterà costi aggiuntivi per il Titolare del Trattamento. Su tale punto si precisa che sono escluse le eventuali ulteriori misure di sicurezza eventualmente richieste dal Titolare qualora queste non fossero riconducibili ad un principio di ragionevole richiesta o comunque non in linea con gli standard di sicurezza adottati per i trattamenti effettuati nel settore di riferimento.

Art. 16. AUTORIZZAZIONI GENERALI ULTERIORI SOGGETTI RESPONSABILI

16.1 Fatto salvo quanto previsto dal Contratto Principale e quanto stabilito negli artt. **6** e **7** del presente accordo, il Titolare autorizza il Responsabile del Trattamento a servirsi delle seguenti categorie di ulteriori responsabili (c.d. sub-responsabili):

a) soggetti che trattano i dati per scopi accessori e funzionali ai Trattamenti affidati dal Titolare al Responsabile, quali servizi aggiuntivi come il trasporto, la manutenzione e la pulizia, nonché servizi di telecomunicazione, servizi informatici o di sicurezza informatica anche in cloud come *Infrastructure as a service (IaaS)*, *Platform as a service (PaaS)* o *Software as a service (SaaS).* A scopo esemplificativo ma non esaustivo:
   - soggetti che effettuano i servizi di assistenza ai sistemi informatici del Responsabile;
   - soggetti che gestiscono i servizi tecnologici in cloud del responsabile (es. software applicativi, posta elettronica, backup, ecc.);
   - operatori telefonici e fornitori di connettività Internet del Responsabile.

b) Consulenti e/o professionisti del Responsabile necessari e funzionali allo svolgimento delle attività affidate dal Titolare del Trattamento (es. consulenti tecnici, legali, amministrativi, sicurezza, ecc.)

16.2 Fatto salvo quanto stabilito dall' art. **14** del presente accordo, sono autorizzati i trasferimenti di dati verso sub-responsabili, delle sopraindicate categorie, in paesi terzi (extra UE), solamente per scopi tecnologici e funzionali a:
- servizi di comunicazione e applicazioni in cloud come ad esempio Google GSUITE e Microsoft OFFICE 365
- servizi di gestione e protezione Endpoint, Server anche con Sandbox a patto che le tecnologie di sicurezza adottate siano scelte tra le più efficaci presenti sul mercato (stato dell'arte)

Art. 17. SPECIFICHE E AUTORIZZAZIONI

17.1 **Finalità del Trattamento**
Nel rispetto e ad integrazione di quanto eventualmente stabilito nel Contratto Principale, se richiesto dal Titolare, il Responsabile potrà trattare i dati del Titolare per le seguenti finalità:

a) Configurazione, gestione e manutenzione di:
- Sistemi di Gestione degli Asset
- Sistemi di Gestione delle Vulnerabilità (Patch)
- Sistemi di gestione dei Log di accesso ai sistemi
- Sistemi di gestione delle credenziali di autenticazione e autorizzazione degli Utenti
- Sistemi di sicurezza perimetrale UTM (Firewall)
- Sistemi di sicurezza Endpoint (antivirus, anti-malware, anti-exploit, ecc.)
- Sistemi di Backup e Ripristino di dati e sistemi
- Servizi di Dominio Active Directory
- Server e storage di rete
- Postazioni di lavoro client (es. PC, Notebook, ecc.)
- Tablet, Smartphone e dispositivi di tipo mobile in genere
- Sistemi di acquisizione e stampa
- Dispositivi di storage mobile in genere
- Device IoT
- Sistemi di Infotainment/Gps autoveicoli aziendali
- Sistemi automatici integrati nei processi produttivi
- Servizi WEB
- Dispositivi di connessione e navigazione in internet
- Sistemi di videoconferenza
- Servizi e piattaforme Cloud
- Piattaforme social
- Sistemi e software di comunicazione (es. videoconferenza)
- Sistemi per collegamento remoti
- Motori di Database tecnici (correlati a specifiche applicazioni)
- Motori di Database generici (correlati a software applicativi)
- Reti Lan cablate e relativi appartai attivi di networking
- Reti Wi-Fi e apparati di gestione
- Servizi e centralini Voip
- Sistemi di videosorveglianza
- Sistemi di sicurezza fisica e ambientale (es. controllo sala dati)
- Sistemi di controllo accessi e presenza (es.timbrature)
- Servizi di assistenza tecnica e manutenzione sistemi sia on-site che attraverso accesso remoto

b) Coordinamento e/o supporto di:
- Staff IT del Titolare (se presente)
- Soggetti delegati dal Titolare all'amministrazione di sistemi o servizi specifici (se presenti)
- Soggetti esterni incaricati dal Titolare alla manutenzione e gestione di sw applicativi soggetti a specifico contratto di manutenzione
- Soggetti incaricati dal Titolare alla manutenzione di hardware soggetto a specifico contratto di manutenzione o noleggio (es. Sistemi di stampa multifunzione)
- Attività del Titolare che comportano l'intervento di più soggetti in ambiti specifici
- Attività che prevedono o possono comportare fermi di servizio da parte del Titolare
- Attività che prevedono interventi sull'infrastruttura IT del Titolare
- Attività che prevedono interventi a livello di sottoservizi del Titolare. (es. interventi elettrici, idraulici o edili nelle sale dati o nei locali sedi di trattamento dei dati)

c) Progettazione di:
- Privacy by design and by default (art. 25 Reg. UE 2016/679)
- Sistemi, e servizi
- Integrazioni e migrazioni

d) Attività di Analisi

- Analisi e valutazione del Rischio IT, valutazione degli impatti, studi di fattibilità e ricerca delle soluzioni

17.2 **Categorie di soggetti interessati**

Per le finalità sopra indicate, il Responsabile potrà trattare i dati per conto del Titolare del Trattamento delle seguenti categorie di soggetti interessati: **Clienti, Fornitori, Prospect** - **Dipendenti, Collaboratori, Candidati** - **Utenti**

17.3 **Tipologie di dati personali trattati**

Dati personali: Per le finalità di cui all' art. **17.1**, e relativamente ai soggetti interessati indicati all'art. **17.2**, il Responsabile, potrà trattare anche in forma aggregata, per conto del Titolare del Trattamento, le seguenti tipologie di informazioni contenenti dati potenzialmente personali:

- Informazioni relative alla configurazione Hardware e software del sistema utilizzato dall'utente
- Informazioni relative all' account utente e relativa cronologia degli accessi
- Informazioni relative al traffico di rete, e all'utilizzo dei servizi Web e Cloud (es. nome macchina, indirizzo IP, MAC Address, sistema operativo, applicazioni, data, ora, e tutte le altre informazioni implicite nel protocollo di comunicazione).
- Informazioni sui file e le applicazioni utilizzate dall'utente con i nomi dei file modificati e le marche temporali
- Informazioni sulla posizione geografica dell'utente collegato al sistema da remoto
- Informazioni contenute nei Log degli apparati e nei sistemi di LOG Management
- Informazioni raccolte dai sistemi di sicurezza relative all'attività degli utenti (data/ora degli eventi, percorso/nome del file/siti web/applicazioni/messaggi di posta oggetto del controllo ed azione intrapresa)
- Informazioni relative ad attività proprie delle applicazioni utilizzate dagli utenti (file temporanei, log di database etc.)
- Informazioni relative ai dispositivi mobili utilizzati (tipo IMEI, MAC. Address, n° di telefono, dati relativi alla posizione etc.)
- alle attività di rete ()
- informazioni relative ai lavori di stampa e scansione
- informazioni relative ai sistemi di localizzazione o altri strumenti in grado di tracciare la posizione
- informazioni contenute nei file e nelle cartelle di cui il Responsabile deve garantire la Riservatezza, l'Integrità e la Riservatezza per conto del Titolare del Trattamento.

Categorie Particolari di Dati personali: Per le finalità di cui all' art. **17.1**, e relativamente ai soggetti interessati indicati all'art. **17.2**, il Responsabile, potrà trattare, per conto del Titolare del Trattamento, le seguenti tipologie di informazioni potenzialmente contenenti Categorie Particolari di Dati (ex. art. 9 del Reg. UE 2016/679):

- informazioni contenute nei file e nelle cartelle di cui il Responsabile deve garantire la Riservatezza, l'Integrità e la Riservatezza per conto del Titolare del Trattamento
- informazioni rilevate dai sistemi di sicurezza per finalità di controllo di sicurezza.

17.4 **Impegno del Titolare del Trattamento**

Il Titolare del Trattamento si impegna a segnalare la presenza di categorie particolari di dati personali (ex. Art. 4 del Regolamento UE 2016/679) all'interno dei sistemi, archivi o servizi affidati in gestione al Responsabile. Sul punto si precisa che il Responsabile del trattamento non potrà garantire una adeguata sicurezza dei trattamenti senza conoscere la criticità delle informazioni trattate.

Art. 18. ACCESSO ALLE INFORMAZIONI CONTENUTE NEI FILE E NELLE BANCHE DATI DEL TITOLARE DEL TRATTAMENTO

18.1 Ai sensi dell'art. 615 ter del Codice penale, fatti salvi gli accessi previsti dal normale svolgimento delle mansioni affidate nel Contratto Principale, Il Responsabile non accederà ai sistemi e/o alle informazioni contenute all'interno dei File e/o delle banche dati del Titolare del Trattamento all'insaputa del Titolare o del referente aziendale assegnato dal Titolare al responsabile (art. **22**).

18.2 Responsabile è consapevole che il Titolare del Trattamento potrà effettuare controlli sugli accessi effettuati dal Responsabile al fine di verificare abusi o accessi non autorizzati ai sistemi e/o ai file, e/o alle banche dati.

Art. 19. INCARICO AD AMMINISTRATORE DI SISTEMA - AdS

Preso atto che il Provvedimento del Garante del 27 novembre 2008 definisce l'Amministratore di Sistema o AdS come *"una figura professionale dedicata alla gestione e alla manutenzione di impianti di elaborazione con cui vengano effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, i sistemi software complessi quali i sistemi ERP (Enterprise resource planning) utilizzati in grandi aziende e organizzazioni, le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati personali",*

in riferimento ai soli sistemi e servizi ICT oggetto del Contratto Principale, il Titolare del Trattamento, **INCARICA** il Responsabile del Trattamento a svolgere le funzioni di **Amministratore di Sistema**

19.1 Il Responsabile del trattamento comunicherà al Titolare del trattamento le generalità e i dati di contatto delle persone fisiche incaricate a svolgere le funzioni di AdS per proprio conto sulla struttura del Titolare.

19.2 Qualora gli amministratori, nell'espletamento delle proprie mansioni, trattino dati personali dei lavoratori, questi ultimi hanno diritto di conoscere l'identità dei predetti. In tal caso, è fatto onere al Titolare di rendere noto ai lavoratori dipendenti detto loro diritto.

19.3 Gli amministratori di sistema si impegnano a svolgere gli interventi di assistenza per conto del Responsabile e a Redigere, gli appositi verbali riepilogativi dell'attività di assistenza;

19.4 In caso si rendano necessari interventi di assistenza straordinaria, l'amministratore di sistema, si impegna ad informare tempestivamente il titolare e a redigere verbale ad hoc contenente i nominativi delle persone autorizzate al trattamento intervenute, l'oggetto dell'intervento manutentivo, le modalità ed i tempi di risoluzione dello stesso, nonché le misure di sicurezza adottate in caso di necessità.

19.5 Fatto salvo quanto stabilito all'art. 18 e i controlli effettuati dal Titolare del Trattamento, l'operato degli amministratori di sistema dovrà essere oggetto di verifica da parte del Responsabile, con cadenza almeno annuale, per accertare che le attività svolte dall'amministratore per conto del Responsabile, siano effettivamente conformi alle mansioni attribuite dal Titolare nel contratto principale o nel presente accordo.

19.6 Il Responsabile del trattamento si impegna a far svolgere le attività concordate agli AdS e garantisce per la loro affidabilità e risponde del loro operato.

Art. 20. INFORMAZIONI DI CONTATTO E REFERENTI

20.1 In riferimento al presente accordo, il Titolare del Trattamento e il Responsabile del Trattamento si scambieranno i riferimenti di contatto dei reciproci referenti.

20.2 Le parti si impegnano a mantenere aggiornati i contatti e a comunicare senza ingiustificato ritardo ogni variazione.

Art. 21. MANLEVA E RESPONSABILITA' PER VIOLAZIONE DELLE DISPOSIZIONI

21.1 Il Responsabile con l'accettazione della presente accordo, si impegna a mantenere indenne il Titolare da qualsiasi responsabilità, danno, incluse le spese legali, o altro onere che possa derivare da pretese, azioni o procedimenti avanzate da terzi a seguito dell'eventuale illiceità delle operazioni di trattamento dei Dati Personali che sia imputabile a fatto, comportamento o omissione del Responsabile (o di suoi dipendenti e/o collaboratori).

21.2 Il Responsabile si impegna a comunicare prontamente al Titolare eventuali situazioni sopravvenute che, per il mutare delle conoscenze acquisite in base al progresso tecnico o per qualsiasi altra ragione, possano incidere sulla propria idoneità allo svolgimento dell'incarico.

21.3 Il Titolare ha il diritto di reclamare dal Responsabile la parte dell'eventuale risarcimento di cui dovesse essere chiamato a rispondere nei confronti di terzi per le violazioni commesse dal Responsabile ai sensi dell'art. 82, paragrafo 5, del GDPR.

21.4 Nel caso di mancata o ritarda comunicazione di Data Breach al Titolare da parte del Responsabile o del Sub-Responsabile da quest'ultimo individuato, il Titolare può richiedere il risarcimento dei danni equivalenti alla sanzione comminata dall'Autorità, quelli derivanti dal risarcimento danni degli interessati e dal danno reputazionale.

21.5 In caso di violazione da parte del Responsabile delle disposizioni contenute nel presente accordo relativamente alle finalità e modalità di trattamento dei dati, di azione contraria alle istruzioni ivi contenute o in caso di mancato adempimento agli obblighi specificatamente diretti al Responsabile dal Regolamento UE 2016/679, il Responsabile risponderà direttamente davanti alla legge e agli interessati in qualità di autonomo Titolare del Trattamento.

Art. 22. CLAUSOLA RISOLUTIVA ESPRESSA

22.1 L'inosservanza o il verificarsi di quanto previsto agli articoli 2, 3, 6,18 e 21.5 del presente Contratto costituisce grave inadempimento ai sensi dell'art. 1456 Cod. civ. a fronte del quale la parte non inadempiente si riserva la facoltà di risolvere di diritto il presente Contratto, nonché quello principale. Resta in ogni caso salvo il diritto al risarcimento del danno subito.

Art. 23. ACCETTAZIONE DELL'ACCORDO

23.1 Con la sottoscrizione del presente atto, stipulato ai sensi dell'art. 28 del Regolamento UE 2016/679, le parti accettano gli accordi sul trattamento, in relazione ai dati personali il cui trattamento risulta essere indispensabile per l'adempimento delle obbligazioni di cui al Contratto Principale.

23.2 I termini del presente accordo annullano e prevalgono su qualunque altro termine o accordo precedentemente stipulato tra le parti, in qualsivoglia forma, relativamente al Contratto Principale, in materia di trattamento dei dati personali.

23.3 Le parti dichiarano di essere a conoscenza degli obblighi previsti dal Regolamento UE 2016/679 e dal D.lgs. 196/2003 e dichiarano inoltre di attenersi alle previsioni ed ai compiti stabiliti nel presente Accordo.

23.4 Il presente Contratto è soggetto alle Leggi Italiane. Al fine di dirimere eventuali controversie derivanti da o riferite al presente accordo, il Foro competente è esclusivamente quello di Torino.

23.5 Per quanto non previsto esplicitamente nel presente contratto si rimanda alle norme di legge vigenti in materia.

Documento letto e sottoscritto dalle parti mediante firma digitale