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 RAMSOFT INFORMATICA s.r.l., con sede legale in Via Covignano 215 – 47921 Rimini (RN), P.iva 04196450409;

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 https://www.iridecloud.app/condizioni-duso/ (di seguito "DPA - Condizioni Speciali") le quali costituiscono parte integrante ed essenziale del presente Accordo.

Tutto quanto sopra premesso le 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 riportato 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;

"**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/fornire al Fornitore, dietro sua semplice richiesta scritta, la documentazione attestante quanto sopra.
2.3. Ciascuna delle Parti si impegna a conformarsi, nel trattamento dei Dati Personali, ai rispettivi obblighi derivanti dalla Legislazione in materia di Protezione dei Dati Personali applicabile.

3. **TRATTAMENTO DEI DATI PERSONALI**
3.1. Con la stipulazione del presente Accordo (inclusivo di 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 https://www.iridecloud.app/condizioni-duso/
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 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, strumentali all'adempimento dell'oggetto del Contratto, siano affidate dal Fornitore a soggetti terzi come indicato nei DPA – Condizioni Speciali. L'elenco completo dei sub-responsabili ed eventuali informazioni aggiuntive, quali gli specifici trattamenti loro affidati e la loro ubicazione, saranno resi disponibili, al Cliente, dietro espressa richiesta al Fornitore.

5.1.2. Su tale altro Responsabile del trattamento sono imposti, mediante un contratto o un altro atto giuridico, a norma del diritto dell'Unione o degli Stati membri, gli stessi obblighi in materia di protezione dei dati contenuti nel presente accordo.

5.1.3. Qualora l'altro Responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Fornitore, Responsabile iniziale, conserva nei confronti del Titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi dell'altro Responsabile.

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 ad 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.

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 dalla Commissione Europea nella decisione 2021/914 UE del 4 giugno 2021. 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.

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. 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 si riserva, a suo insindacabile giudizio, di sottoporre 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 del 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 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 E-mail 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 Servizi.

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 CANCELLAZIONE DEI 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;

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 ed 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.

Allegato 1

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:

MISURE TECNICHE ED ORGANIZZATIVE
Politica di sicurezza e procedure per la protezione dei dati personali **Obiettivo: Fornire gli indirizzi ed il supporto della direzione per la sicurezza delle informazioni in accordo con i requisiti di business, con le leggi e con i regolamenti pertinenti** e' presente una policy di sicurezza dedicata separata per quanto riguarda il trattamento dei dati personali; la policy viene approvata dal management competente e comunicata a tutti i dipendenti, persone autorizzate al trattamento ed alle parti esterne interessate; la policy di sicurezza si riferisce ai seguenti aspetti: i ruoli e le responsabilità del personale, le misure tecniche e organizzative di base adottate per la sicurezza dei dati personali, i responsabili del trattamento dei dati o altre terze parti coinvolte nel trattamento dei dati personali; viene mantenuto un inventario di policy / procedure specifiche relative alla sicurezza dei dati personali, basato sulla policy generale di sicurezza.
Ruoli e responsabilità della sicurezza delle informazioni **Obiettivo: Stabilire un quadro di riferimento gestionale per intraprendere e controllare l'attuazione e l'esercizio della sicurezza delle informazioni all'interno dell'organizzazione** in caso di riorganizzazioni interne o di dismissione di personale o assegnazione ad altro ruolo, l'organizzazione prevede una procedura chiaramente definita per la revoca dei diritti, delle responsabilità e dei profili di autorizzazione e la conseguente riconsegna di materiali e mezzi del trattamento; viene effettuata una chiara nomina delle persone incaricate di compiti specifici di sicurezza, compresa la nomina di un responsabile della sicurezza.
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.

Gestione degli incidenti / Violazione dei dati personali (Personal data breaches)
Obiettivo: Assicurare un approccio coerente ed efficace per la gestione degli incidenti relativi alla sicurezza delle informazioni, incluse le comunicazioni relative agli eventi di sicurezza ed ai punti di debolezza

il piano di risposta degli incidenti (incident response plan) viene documentato, compreso un elenco di possibili azioni di mitigazione e una chiara assegnazione dei ruoli;
le violazioni dei dati personali vengono segnalate immediatamente al management competente secondo l'organizzazione interna. sono in atto procedure di notifica per la segnalazione delle violazioni alle autorità competenti ed agli interessati.

Business continuity
Obiettivo: La continuità della sicurezza delle informazioni deve essere integrata nei sistemi per la gestione della continuità operativa dell'organizzazione

nell'organizzazione esistono procedure e controlli da eseguire al fine di garantire il necessario livello di continuità e disponibilità del sistema it mediante le quali si procede al trattamento dei dati personali (in caso di incidente / violazione di dati personali);
viene predisposto, dettagliato e documentato un business continuity plan (seguendo la politica generale di sicurezza) che include azioni chiare e assegnazione di ruoli;
viene definito nel business continuity plan, un livello di qualità del servizio garantito per i processi aziendali fondamentali che attengono alla sicurezza dei dati personali.

Formazione
Obiettivo: assicurare che il personale e I collaboratori siano a conoscenza delle loro responsabilità per la sicurezza delle informazioni e vi adempiano

l'organizzazione garantisce che tutti i dipendenti, lavoratori e persone autorizzate al trattamento siano adeguatamente formati e informati sui controlli di sicurezza del sistema informatico relativi al loro lavoro quotidiano.si effettuano regolari campagne di sensibilizzazione o iniziative di formazione specifica per i dipendenti coinvolti nel trattamento dei dati personali.

Controllo degli accessi e autenticazione
Obiettivo: Assicurare l'accesso agli utenti autorizzati e prevenire accessi non autorizzati a sistemi e servizi

non esistono account utente comuni (con credenziali di accesso condivise tra più utenti);
viene definita e documentata una policy specifica per la password.

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.

Generazione di file di log e monitoraggio
Obiettivo: Registrare eventi e generare evidenze

i sistemi generano file di log che includono tutti i tipi di accesso ai dati (visualizzazione, modifica, cancellazione); gli stessi vengono contrassegnati con data e ora e adeguatamente protetti da manomissioni e accessi non autorizzati;
gli orologi sono sincronizzati con un'unica fonte temporale di riferimento.

Sicurezza delle Postazioni di lavoro

Obiettivo: Assicurare che la sicurezza delle informazioni sia parte integrante di tutto il ciclo di vita dei sistemi informativi. Questo include anche i requisiti specifici per i sistemi informativi che forniscono servizi attraverso reti pubbliche

il personale non è in grado di disattivare o bypassare le impostazioni di sicurezza;
le applicazioni antivirus e le firme di rilevamento vengono configurate su base giornaliera;
il sistema attiva il timeout di sessione quando l'utente non è attivo per un certo lasso di tempo;
gli aggiornamenti critici di sicurezza rilasciati dallo sviluppatore del sistema operativo sono installati regolarmente.

Sicurezza della Rete e delle Infrastrutture di comunicazione elettronica

Obiettivo: Assicurare la protezione delle informazioni nelle reti e nelle strutture per l'elaborazione delle informazioni a loro supporto

l'accesso wireless al sistema it viene consentito solo a utenti e per processi specifici;
viene protetto da meccanismi di crittografia;
in generale, quando avviene l'accesso da remoto al sistema it, lo stesso viene eseguito solo sotto il controllo e il monitoraggio di una persona specifica dall'organizzazione (ad esempio amministratore it / responsabile della sicurezza) attraverso dispositivi predefiniti;
il traffico da e verso il sistema it viene monitorato e controllato tramite firewall e sistemi di rilevamento delle intrusioni.

Backups

Obiettivo: Proteggere dalla perdita di dati

le procedure di backup e ripristino dei dati vengono definite, documentate e chiaramente collegate a ruoli e responsabilità;
ai backups vengono assegnati un livello adeguato di protezione fisica e ambientale coerente con gli standard applicati sui dati di origine;
i backups completi vengono eseguiti regolarmente;
i supporti di backup vengono testati regolarmente per assicurarsi che possano essere utilizzati per l'uso in caso di emergenza;
le copie del backup vengono conservate in modo sicuro in luoghi diversi;
se viene utilizzato un servizio di terze parti per l'archiviazione di backup, la copia viene crittografata prima di essere trasmessa dal titolare del trattamento.

Dispositivi mobili / portatili

Obiettivo: Assicurare la sicurezza del telelavoro e nell'uso di dispositivi portatili

i dispositivi mobili ai quali è consentito accedere al sistema informativo vengono pre-registrati e preautorizzati;
i dispositivi mobili sono soggetti agli stessi livelli delle procedure di controllo degli accessi (al sistema di elaborazione dei dati) delle altre apparecchiature terminali;
l'organizzazione è in grado di cancellare da remoto i dati personali (relativi a propri trattamenti) su un dispositivo mobile che è stato compromesso;
i dispositivi mobili supportano la separazione dell'uso privato e aziendale del dispositivo attraverso contenitori software sicuri.

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 indicati 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

Per i servizi di Data Center erogati da OVH:

https://www.ovh.it/protezione-dati-personali/sicurezza.xml

Cancellazione / eliminazione dei dati

Obiettivo: Prevenire la perdita, il danneggiamento, il furto o la compromissione di asset e l’interruzione delle attività operative dell’organizzazione oltre che prevenire la divulgazione non autorizzata, la modifica, la rimozione o la distruzione delle informazioni archiviate sui supporti

viene eseguita la triturazione della carta e dei supporti portatili utilizzati per memorizzare i dati personali;
vengono eseguiti più passaggi di sovrascrittura basata su software su tutti i supporti prima di essere smaltiti.

Sicurezza fisica

Obiettivo: Prevenire l’accesso fisico non autorizzato, danni e disturbi alle informazioni dell’organizzazione e alle strutture di elaborazione delle informazioni

il perimetro fisico dell'infrastruttura del sistema it non è accessibile da personale non autorizzato;
sono installati sistemi di rilevamento anti-intrusione in tutte le zone di sicurezza;
se del caso, esistono barriere fisiche per impedire l'accesso fisico non autorizzato;
il personale di servizio di supporto esterno ha un accesso limitato alle aree protette.