ACCORDO PRINCIPALE SUL TRATTAMENTO DEI DATI PERSONALI

Art. 28 Reg. UE 2018/679 ('**GDPR**')

Tra

Il **Cliente**, così come identificato del Contratto, nella persona del legale rappresentante munito dei necessari poteri, in qualità di,

Titolare del Trattamento

e

Namirial S.p.A., con sede in Senigallia (AN), Via Caduti sul Lavoro, 4, 60019 – C.F. e iscriz. al Reg. Impr. Ancona N. 02046570426**,** telefono 071/63494, e-mail/PEC amm.namirial@sicurezzapostale.it ('**Responsabile**' o '**Fornitore**'), nella persona del legale rappresentante munito dei necessari poteri, in qualità di

Responsabile del Trattamento

Inoltre, Titolare e Responsabile potranno essere di seguito indicati congiuntamente come '**Parti**' e, ciascuno individualmente, '**Parte**'.

PREMESSO CHE

I. le Parti hanno sottoscritto uno o più contratti ('**Contratto**') avente o aventi ad oggetto la fornitura di Servizi ('**Servizi**');
II. il Contratto comporta il trattamento di informazioni che la legge definisce come dati personali e le Parti, di conseguenza, intendono regolare, all'interno del presente Accordo Principale sul Trattamento dei Dati Personali ("**Accordo**"), i termini e le modalità per il trattamento dei dati personali eseguito dal Responsabile nell'ambito della fornitura dei Servizi di cui al Contratto;
III. i dettagli e le caratteristiche specifiche o condizioni particolari del trattamento dei dati personali sono contenuti all'interno delle cd. "**Schede di Trattamento**" relative ad uno o più Servizi attivati dal Cliente, le quali saranno, di volta in volta, allegate al presente Accordo.
IV. Tali Schede di Trattamento dettaglieranno le modalità operative del trattamento in relazione al Servizio specifico, indicando, ove applicabile, l'elenco dei Sub-Responsabili e le misure di sicurezza supplementari eventualmente applicate. Le Schede di Trattamento, previa sottoscrizione, saranno inserite come Allegati ulteriori al presente Accordo e ne costituiranno parte integrante e sostanziale;
V. prima di affidare al Responsabile lo svolgimento dei Servizi, il Titolare ne ha verificato esperienza, capacità e affidabilità, e ha valutato che il Responsabile offre garanzie sufficienti per mettere in atto misure tecniche e organizzative appropriate e per assicurare un'adeguata protezione dei dati trattati e dei diritti dei soggetti interessati;
VI. il Responsabile deve svolgere le operazioni di Trattamento in conformità alle istruzioni fornite per iscritto dal Titolare attraverso un contratto o altro atto giuridico vincolante che specifichi la durata, la natura e le finalità del Trattamento, le categorie di dati personali trattati e di soggetti interessati dal Trattamento, nonché gli obblighi e i diritti del Responsabile con riguardo al Trattamento;
VII. con il presente accordo ('**Accordo**'), il Titolare intende nominare il Responsabile indicato in epigrafe quale responsabile del Trattamento e fornirgli tutte le necessarie istruzioni per il Trattamento dei dati personali sotteso alla fornitura dei Servizi;
VIII. il Titolare autorizza il Responsabile, nonché le persone autorizzate da quest'ultimo, ad accedere ai soli dati personali strettamente necessari ai fini dell'esecuzione del Contratto ('**Dati Personali**' e, singolarmente, '**Dato Personale**');
IX. il presente Accordo non comporta alcun diritto del Responsabile a specifici compensi e/o indennità e/o rimborsi, diversi da quelli già eventualmente previsti nel Contratto, salvo ulteriori implementazioni specificamente richieste e concordate tra le Parti in un diverso accordo scritto;

X. nel caso in cui il Cliente agisca quale Responsabile del Trattamento per conto di un altro titolare (il "Cliente Finale"), il Cliente stesso assumerà, in relazione a tale specifico trattamento, gli obblighi e le responsabilità di un responsabile del Trattamento nei confronti di Namirial, che in tale contesto assumerà il ruolo di Sub-Responsabile del Trattamento. In tale situazione, le disposizioni relative al trattamento dei dati e gli obblighi del Responsabile di cui al presente Accordo saranno applicabili, ma con il Cliente che agirà come Responsabile per conto del Cliente Finale e Namirial che agirà come Sub-Responsabile per conto del Cliente;

XI. in ogni caso in cui il Cliente agisca come Titolare o responsabile del Trattamento per conto del Cliente Finale, Namirial accetta di svolgere il ruolo di Responsabile e/o Sub-Responsabile e, pertanto, si impegna a trattare i Dati Personali in conformità con le istruzioni ricevute dal Cliente e in modo da garantire la protezione dei Dati Personali stessi, secondo le misure di sicurezza stabilite nel presente Accordo e nelle Schede di Trattamento ad esso allegate.

Tutto ciò premesso, le Parti

CONVENGONO E STIPULANO QUANTO SEGUE

1. VALIDITÀ DELLE PREMESSE E DEGLI ALLEGATI. DEFINIZIONI

1.1. Le premesse e gli Allegati costituiscono parte integrante e sostanziale del presente Accordo.

1.2. Salvo ove diversamente stabilito nel presente Accordo, tutti i termini in maiuscolo utilizzati nel presente Accordo e negli Allegati avranno il significato a essi attribuito nel Contratto e si intendono espressi sia al singolare, sia al plurale. In conformità alle definizioni contenute nella legge applicabile, sono utilizzati i termini e le definizioni di cui all'**Allegato I – *Definizioni*** al presente Accordo, cui si rimanda.

1.3. Le Schede di Trattamento relative ai Servizi utilizzati dal Cliente potranno accedere al presente Accordo, anche in un momento successivo, in caso di integrazione del Contratto per l'attivazione attivazione di nuovi Servizi. In tale ultimo caso, gli Allegati, sottoscritti dalle Parti unitamente all'addendum contrattuale, accedono al presente Accordo.

2. DIRITTI E OBBLIGHI DEL TITOLARE

2.1. Il Titolare affida al Responsabile tutte – ed esclusivamente – le operazioni di Trattamento dei Dati Personali necessarie alla piena esecuzione del Contratto.

2.2. Il Titolare dichiara di adempiere a tutti gli obblighi previsti dalla Legge Applicabile di sua competenza in relazione al Trattamento dei Dati Personali ai sensi del presente Accordo. In particolare, il Titolare:

2.2.1. ha il diritto e l'obbligo di prendere decisioni in merito alle finalità e ai mezzi del Trattamento, compresa l'individuazione della corretta base giuridica del Trattamento;

2.2.2. dichiara che i Dati Personali sono pertinenti e non eccessivi rispetto alle finalità per le quali sono stati raccolti e successivamente trattati, e sono trasmessi in conformità a ogni requisito previsto dalla Legge Applicabile;

2.2.3. predispone e – ove necessario – mette a disposizione del Responsabile informative sul Trattamento dei Dati Personali adeguate e complete ai sensi dell'art. 13 e/o dell'art. 14 del GDPR.

2.3. Il Titolare si impegna a notificare ufficialmente al Responsabile qualsiasi modifica che si renda necessaria con riguardo alle operazioni di Trattamento dei Dati Personali. Il Responsabile e le sue Persone Autorizzate non effettueranno operazioni di Trattamento dei Dati Personali diverse da quelle indicate dal Titolare ai sensi del presente articolo.

2.4. Il Titolare garantisce che le infrastrutture e i sistemi eventualmente messi a disposizione dal Titolare e/o da terzi da quest'ultimo incaricati, sui quali il Responsabile sarà chiamato a svolgere il Trattamento ('Sistemi del Titolare'), siano adeguati e conformi agli standard e alle normative di settore di riferimento e siano in grado di consentire la regolare erogazione dei Servizi nel rispetto del presente Accordo. Il Titolare si impegna pertanto a manlevare e tenere indenne il Responsabile da ogni disservizio, danno o interruzione nell'esecuzione del Trattamento che dovesse derivare dall'inadeguatezza, dalle anomalie e/o dagli eventuali malfunzionamenti dei Sistemi del Titolare sui quali il Responsabile è chiamato a operare.

3. OBBLIGHI DEL RESPONSABILE

3.1. Entro i limiti delle proprie competenze in virtù del Contratto e del presente Accordo, il Responsabile sarà tenuto, per sé e per le proprie Persone Autorizzate, a rispettare le disposizioni della Legge Applicabile, con

particolare riguardo alle disposizioni del GDPR, del Codice Privacy, nonché i provvedimenti applicabili delle competenti Autorità di Controllo che impongano specifici obblighi in capo ai responsabili del trattamento;

3.2. In particolare, il Responsabile procederà alle operazioni di Trattamento a egli assegnate in conformità alle istruzioni impartite dal Titolare contenute nel presente Accordo, nonché a quelle successive che il Titolare potrà notificare per iscritto con congruo preavviso.

3.3. Il Responsabile svolgerà le operazioni di Trattamento funzionali ai compiti a egli assegnati in conformità al presente Accordo e alle finalità per cui i Dati Personali sono raccolti e trattati. Ove si renda necessario un trattamento dei Dati Personali diverso ed eccezionale rispetto a quello oggetto del presente Accordo, il Responsabile si impegna a informare preventivamente e tempestivamente il Titolare, che potrà opporvisi.

3.4. Il Responsabile è tenuto a gestire la documentazione relativa al Trattamento affidatogli mediante idonee procedure, secondo criteri di efficienza e garantendo la custodia, la non alterazione e la facile reperibilità di ogni documento rilevante ai fini del rispetto dei requisiti imposti dal GDPR.

3.5. Il Responsabile mette a disposizione del Titolare tutte le informazioni e i documenti necessari a dimostrare il rispetto degli obblighi previsti all'art. 28 del GDPR; consente e contribuisce alle attività di audit, comprese le ispezioni notificate con congruo preavviso, svolte dal Titolare o da soggetto terzo da questi incaricato.

3.6. Il Responsabile informa immediatamente il Titolare qualora, a suo giudizio, un'istruzione violi il GDPR o altre disposizioni della Legge Applicabile. Inoltre, il Responsabile assiste il Titolare, su richiesta di quest'ultimo, nei procedimenti dinanzi alla competente Autorità di Controllo, ovvero all'Autorità giudiziaria, in relazione alle attività di Trattamento di sua competenza, in particolare mettendo a disposizione ogni informazione e documento utili ai fini di dimostrare il rispetto degli obblighi di cui alla Legge Applicabile con riguardo al Trattamento dei Dati Personali.

3.7. Il Responsabile comunica tempestivamente al Titolare eventuali richieste degli Interessati, le opposizioni, ispezioni o richieste delle Autorità di Controllo e giudiziarie, nonché ogni altra informazione rilevante in relazione al Trattamento dei Dati Personali.

3.8. Il Responsabile individua, nell'ambito della propria struttura aziendale, le Persone Autorizzate a compiere operazioni di Trattamento dei Dati Personali. Contestualmente alla nomina, il Responsabile fornisce alle Persone Autorizzate adeguate istruzioni scritte sulle modalità del Trattamento, nel rispetto di quanto previsto dall'art. 29 del GDPR e dal presente Accordo. A titolo meramente esemplificativo e non esaustivo, il Responsabile, nel designare per iscritto le Persone Autorizzate, prescrive che esse abbiano accesso ai soli Dati Personali la cui conoscenza è strettamente necessaria per lo svolgimento dei compiti loro assegnati (criterio del *need-to-know*). Il Responsabile deve altresì verificare che le Persone Autorizzate applichino tutte le misure di sicurezza relative alla custodia delle credenziali di accesso in caso di Trattamento svolto attraverso mezzi elettronici. Il Responsabile verifica, inoltre, che le Persone Autorizzate custodiscano in sicurezza i supporti non informatici contenenti qualsiasi copia dei Dati Personali, in particolare se appartenenti a Particolari Categorie. Sarà infine cura del Responsabile vincolare le Persone Autorizzate a efficaci obblighi di riservatezza, anche per il periodo successivo alla cessazione del rapporto di lavoro con il Responsabile, in relazione alle operazioni di Trattamento dei Dati Personali da questi effettuate.

3.9. In caso di danni derivanti dal Trattamento, il Responsabile manleverà e terrà indenne il Titolare da ogni danno qualora il Responsabile non abbia ottemperato agli obblighi del GDPR specificamente rivolti ai responsabili del trattamento, o abbia agito in modo difforme o contrario alle legittime istruzioni del Titolare, ai sensi degli artt. 83 e ss. del GDPR.

3.10. Ove applicabile e relativamente al Trattamento effettuato, ai fini dell'esecuzione del Contratto, dalle Persone Autorizzate con mansioni di 'Amministratore di Sistema', il Responsabile è altresì tenuto al rispetto delle disposizioni contenute nel Provvedimento del Garante Privacy del 27 novembre 2008, come modificato in base al Provvedimento del 25 giugno 2009. A tal fine, in particolare, il Responsabile conserva direttamente e specificatamente i dati identificativi delle Persone Autorizzate nominate Amministratori di Sistema e li fornisce al Titolare su richiesta di quest'ultimo.

3.11. Ai sensi dell'art. 28, par. 3, lett. a) GDPR, il Titolare inserisce tra le istruzioni al Responsabile l'effettuazione di trattamenti strettamente necessari alle seguenti attività di miglioramento dei Servizi oggetto del Contratto: test, misurazione e ottimizzazione delle prestazioni, taratura e validazione di modelli/algoritmi, miglioramento di accuratezza/affidabilità/usabilità, sicurezza e prevenzione frodi, correzione di bug e anomalie, in quanto funzionali alla migliore erogazione dei Servizi al Titolare. È escluso qualsiasi uso per finalità autonome del Responsabile o dei Sub-Responsabili, inclusi marketing, profilazione o sviluppo di prodotti/servizi non correlati.

3.12. Le attività di miglioramento di cui al comma precedente si svolgono solo secondo quanto strettamente necessario all'erogazione, manutenzione e sicurezza oppure su dati anonimizzati/aggregati, salvo istruzioni e

basi giuridiche prescelte del Titolare. Il Responsabile può avvalersi di Sub-Responsabili, imponendo divieto di riuso e di addestramento di modelli generali e l'obbligo di cancellazione dei dati al termine delle attività.

4. SICUREZZA DEL TRATTAMENTO

4.1. Nei limiti della sua competenza in virtù del Contratto e del presente Accordo, il Responsabile è tenuto, per sé e per le Persone Autorizzate, ad attuare le Misure di Sicurezza previste dalla Legge Applicabile, nonché quelle indicate dal Titolare, assistendo quest'ultimo nel garantire il rispetto dell'art. 32 del GDPR.

4.2. Nell'ambito delle attività di trattamento dei Dati Personali connesse alla fornitura dei Servizi, il Fornitore si impegna ad adottare misure tecniche e organizzative idonee a prevenire trattamenti illeciti o non autorizzati, nonché a proteggere i Dati Personali da distruzione, alterazione, perdita, accesso o divulgazione non autorizzata, come dettagliato nell'**Allegato II – Misure di Sicurezza Tecniche ed Organizzative** del presente Accordo.

4.3. L'**Allegato II** descrive le misure adottate dal Fornitore per garantire la riservatezza, integrità, disponibilità e resilienza dei sistemi e dei Servizi, nonché le procedure per il ripristino tempestivo dell'accesso ai Dati Personali in caso di incidente di sicurezza. Le misure implementate ("**Misure di Sicurezza**") sono definite in relazione al livello di rischio associato ai Dati Personali trattati, considerando lo stato dell'arte, i costi di implementazione e la natura, il contesto e le finalità del trattamento. Il Cliente riconosce e accetta che tali misure sono adeguate a garantire un livello di sicurezza conforme ai requisiti normativi applicabili.

4.4. Il Fornitore si riserva il diritto di aggiornare o modificare le Misure di Sicurezza per garantire un costante adeguamento agli sviluppi tecnologici e normativi, a condizione che tali modifiche non riducano il livello complessivo di protezione dei Servizi.

4.5. Qualora il Cliente richieda l'adozione di specifiche misure di sicurezza ulteriori rispetto a quelle previste, il Fornitore valuterà la fattibilità tecnica e operativa di tali richieste, riservandosi la possibilità di applicare costi aggiuntivi per eventuali implementazioni.

4.6. Nel caso di prodotti installati presso il Cliente o presso soggetti da esso incaricati (ad esempio, soluzioni *on-premises*), le Misure di Sicurezza adottate dal Fornitore si applicheranno esclusivamente ai Servizi che prevedono un trattamento dei Dati Personali da parte del Fornitore o dei suoi sub-responsabili (ad esempio, attività di supporto e assistenza da remoto o servizi di migrazione).

4.7. Nel caso in cui i Servizi consentano l'integrazione con software o applicativi di terze parti, il Fornitore non sarà responsabile delle Misure di Sicurezza applicate da tali soggetti o di eventuali vulnerabilità derivanti dall'integrazione effettuata direttamente dal Cliente o dai fornitori terzi.

4.8. Fermi restando gli obblighi di sicurezza a carico del Fornitore, il Cliente è responsabile dell'adozione di tutte le misure necessarie per garantire la protezione dei Dati Personali trattati nell'ambito della fruizione dei Servizi da parte del proprio personale o di eventuali soggetti autorizzati.

4.9. Il Cliente si impegna a utilizzare i Servizi in modo conforme alle *best practice* di sicurezza e a garantire un livello di protezione adeguato rispetto ai rischi connessi al trattamento dei Dati Personali.

4.10. Il Cliente deve implementare tutte le misure idonee per proteggere le credenziali di autenticazione, i dispositivi e i sistemi utilizzati per accedere ai Servizi, nonché per effettuare regolari backup dei Dati Personali, in modo da garantirne il ripristino in conformità alle normative applicabili.

4.11. Il Fornitore non sarà responsabile della protezione dei Dati Personali che il Cliente o soggetti terzi trattano al di fuori dei sistemi del Fornitore e dei suoi sub-responsabili, inclusi dati conservati su supporti cartacei o su infrastrutture IT interne del Cliente (ad esempio, *data center* privati o *server on-premises*).

5. SUB-RESPONSABILI

5.1. Esclusivamente al fine di procedere alla fornitura dei Servizi oggetto del Contratto, e in conformità con le disposizioni del presente Accordo, i Dati Personali potranno essere trattati da Sub-Responsabili individuati dal Responsabile.

5.2. Il Responsabile si impegna a selezionare i propri Sub-Responsabili tra persone la cui esperienza, capacità e affidabilità forniscano garanzie sufficienti per implementare Misure di Sicurezza adeguate, in modo che il Trattamento soddisfi tutti i requisiti della Legge Applicabile e garantisca la tutela dei Diritti dell'Interessato. Per l'effetto, il Responsabile si impegna a stipulare specifici contratti o altri atti giuridici vincolanti con i Sub-Responsabili, mediante i quali il Responsabile descrive analiticamente i loro compiti e chiede loro di rispettare i medesimi obblighi imposti dal Titolare al Responsabile ai sensi della Legge Applicabile e del presente Accordo.

5.3. In qualunque caso in cui un Sub-Responsabile non rispetti i propri obblighi in materia di protezione dei dati personali, il Responsabile riconosce di mantenere la piena responsabilità nei confronti del Titolare con riguardo al comportamento di tale Sub-Responsabile. Per l'effetto, il Responsabile si impegna a manlevare e

tenere indenne il Titolare da qualsiasi danno, pretesa e richiesta di risarcimento che dovesse essere avanzata nei confronti del Titolare a seguito del mancato rispetto da parte del Sub-Responsabile degli obblighi su di esso gravanti e, più in generale, di qualsiasi violazione della Legge Applicabile ad opera del Sub-Responsabile e di qualsiasi suo subcontraente e/o persona autorizzata.

5.4. Le Schede di Trattamento individuano ed elencano i Sub-Responsabili nominati dal Responsabile e già approvati dal Titolare. Il Responsabile si impegna altresì a informare per iscritto il Titolare di eventuali modifiche o sostituzioni previste in merito ai Sub-Responsabili, dando così al Titolare la possibilità di opporsi a tali modifiche entro 30 (trenta) giorni dal ricevimento della relativa comunicazione.

5.5. La comunicazione di cui al comma che precede può essere assolta, alternativamente, anche con la pubblicazione dell'elenco aggiornato dei Sub-Responsabili nella sezione "Documentazione" sul sito *web* di Namirial (www.namirial.com).

6. TRASFERIMENTO DEI DATI PERSONALI

6.1. Il Responsabile dichiara che non trasferirà i Dati Personali al di fuori dello SEE, a meno che non sia preventivamente e specificatamente autorizzato per iscritto dal Titolare. In caso di autorizzazione, il Responsabile potrà trasferire i Dati Personali solo su istruzione documentata del Titolare e, in particolare, nel pieno rispetto degli artt. 44, 45, 46 e 49 del GDPR.

6.2. Nel caso di trasferimenti verso paesi terzi od organizzazioni internazionali che siano richiesti dalla legislazione dell'UE o di uno Stato membro cui è soggetto il Responsabile, e che non sono stati richiesti dal Titolare con un'istruzione specifica, il Responsabile è tenuto a informare il Titolare di tale obbligo prima del trasferimento, a meno che la legislazione stessa non vieti tale comunicazione per importanti motivi di interesse pubblico rilevante.

6.3. In ogni caso di trasferimento dei Dati Personali al di fuori dello SEE, nella misura in cui non vi sia una Decisione di adeguatezza della Commissione Europea per il paese di destinazione dei Dati Personali, il Responsabile è tenuto a firmare, e far firmare ai soggetti destinatari dei Dati Personali, le Clausole Contrattuali Tipo nella loro ultima versione adottata dalla Commissione Europea, assicurando che gli stessi obblighi ivi contenuti siano garantiti nei confronti di eventuali ulteriori destinatari dei Dati Personali in caso di c.d. *onward transfer*. Se e ove necessario, il Responsabile dovrà inoltre stipulare l'adozione di eventuali Misure di Sicurezza aggiuntive in conformità alle *Raccomandazioni 01/2020 relative alle misure che integrano gli strumenti di trasferimento al fine di garantire il rispetto del livello di protezione dei dati personali dell'UE e alle Raccomandazioni 2/2020 relative alle garanzie essenziali europee per le misure di sorveglianza* adottate dal Comitato Europeo per la Protezione dei Dati ('**EDPB**').

7. ASSISTENZA AL TITOLARE

7.1. Tenendo conto della natura del Trattamento e delle informazioni nella sua disponibilità, il Responsabile è tenuto a fornire supporto al Titolare affinché quest'ultimo possa adempiere agli obblighi che la Legge Applicabile impone ai titolari del trattamento, quali, a titolo meramente esemplificativo e non esaustivo, gli obblighi di:

7.1.1. effettuare, senza ingiustificato ritardo e, ove possibile, entro e non oltre 72 ore dal momento in cui ne è venuto a conoscenza, la notifica di una Violazione dei Dati Personali alla competente Autorità di Controllo, a meno che sia improbabile che tale Violazione comporti un rischio per i diritti e le libertà delle persone fisiche;

7.1.2. effettuare una valutazione di impatto sulla protezione dei dati ('**DPIA'**) relativa al Trattamento disciplinato dal presente Accordo, se tale Trattamento presenta le caratteristiche di cui all'art. 35 del GDPR;

7.1.3. consultare la competente Autorità di Controllo ai sensi dell'art. 36 del GDPR, se una DPIA indica che il Trattamento disciplinato dal presente Accordo comporterebbe un rischio elevato in assenza di misure adottate per attenuare il rischio;

7.1.4. rispondere alle richieste di esercizio dei Diritti degli Interessati, ai sensi del Capo III del GDPR. Laddove il Responsabile riceva direttamente tali richieste, il Responsabile dovrà (i) informare tempestivamente il Titolare per iscritto, allegando copia della richiesta; e (ii) tenendo conto della natura del Trattamento, assistere il Titolare con misure tecniche e organizzative adeguate di sua competenza al fine di soddisfare tali richieste.

7.2. Il Responsabile dovrà inoltre informare tempestivamente il Titolare, e comunque entro 48 (quarantotto) ore dal ricevimento, mediante comunicazione all'indirizzo E-mail di notifica, di qualsiasi contestazione, ispezione

o richiesta da parte dell'Autorità di Controllo e delle Autorità Giudiziarie, nonché di ogni altra informazione rilevante relativa al Trattamento dei Dati Personali oggetto del presente Accordo.

8. VIOLAZIONI DEI DATI PERSONALI

8.1. Nel caso in cui il Responsabile venga a conoscenza di una Violazione dei Dati Personali che coinvolga o possa coinvolgere, anche indirettamente, i sistemi e le operazioni di Trattamento impiegati per conto del Titolare, ovvero i Dati Personali oggetto del presente Accordo, il Responsabile si impegna a informare il Titolare tramite comunicazione formale inoltrata all'indirizzo E-mail di notifica, senza indebito ritardo e non oltre 48 (quarantotto) ore dal momento in cui viene a conoscenza della Violazione dei Dati Personali.

8.2. A seguito del rilevamento di un'anomalia o di una presunta Violazione dei Dati Personali oggetto del presente Accordo, il Responsabile è tenuto ad avviare un'analisi preliminare volta a raccogliere i dati relativi all'anomalia e, in ogni caso, tutte le informazioni necessarie per la classificazione e gestione della violazione, inclusi i dettagli relativi alla natura dell'incidente, ai dati coinvolti, alle misure adottate e alle tempistiche di intervento.

8.3. Il Responsabile si impegna a garantire il rispetto delle suddette tempistiche e a manlevare e tenere indenne il Titolare da eventuali danni, pretese e richieste che dovessero essere rivolte al Titolare a seguito del mancato rispetto, da parte del Responsabile e/o di una Persona Autorizzata e/o di un Sub-Responsabile e/o di eventuali ulteriori sub-contraenti, degli obblighi previsti dalla Legge Applicabile.

8.4. Nell'eventualità di una Violazione dei Dati Personali, il Responsabile si impegna a fornire, per quanto di propria competenza e spettanza ai sensi del Contratto, la massima collaborazione al Titolare e alle competenti Autorità di Controllo, al fine di adempiere a ogni obbligo di legge applicabile (ad esempio, obbligo di notifica all'Autorità di Controllo, eventuale comunicazione agli Interessati, applicazione di idonee misure volte a mitigare o prevenire rischi e danni). In tal senso, il Titolare si impegna a fornire, senza indugio, prova al Responsabile di qualsiasi comunicazione scambiata con le competenti Autorità di Controllo in cui il Responsabile sia in qualsiasi modo coinvolto o menzionato.

9. DURATA. CANCELLAZIONE E RESTITUZIONE DEI DATI PERSONALI

9.1. La nomina a Responsabile del Trattamento ai sensi del presente Accordo avrà la stessa durata del Contratto, salvo revoca anticipata, nel qual caso la nomina continuerà a essere efficace per quanto necessario al completamento delle operazioni di Trattamento necessarie per la cessazione del rapporto tra le Parti o per l'adempimento di obblighi di legge gravanti sulle stesse.

9.2. Alla cessazione delle operazioni di Trattamento affidate, nonché alla cessazione per qualsiasi motivo del rapporto contrattuale con il Responsabile, quest'ultimo, a discrezione del Titolare, sarà tenuto a (i) restituire al Titolare i Dati Personali oggetto del Trattamento, o (ii) provvedere alla completa distruzione dei Dati Personali e di ciascuna copia degli stessi, fatta eccezione per i casi in cui la conservazione dei dati sia richiesta dalla legge o persegua altri scopi legittimi (es. finalità contabili, fiscali, ecc.). In entrambi i casi, il Responsabile dovrà fornire al Titolare una dichiarazione scritta attestante che nessuna copia dei Dati Personali oggetto del presente Accordo è detenuta dal Responsabile.

10. AUDIT E ISPEZIONI

10.1. Il Responsabile mette a disposizione del Titolare tutte le informazioni necessarie per dimostrare la conformità ai propri obblighi ai sensi del presente Accordo e della Legge Applicabile, e consentirà e contribuirà alle attività di audit, comprese le ispezioni effettuate dal Titolare e/o da un soggetto terzo da questi individuato. A tale scopo, previo preavviso scritto di almeno 10 (dieci) giorni lavorativi, il Titolare e/o le persone da esso nominate avranno il diritto di accedere ai locali di pertinenza del Responsabile in cui avviene il Trattamento o in cui sono disponibili dati o documenti relativi al presente Accordo. In ogni caso, il Titolare si impegna, per sé e per i terzi da egli eventualmente nominati, a utilizzare le informazioni raccolte durante le operazioni di verifica solo per tali scopi, e a svolgere qualsiasi verifica ai sensi del presente articolo senza ragionevolmente pregiudicare il regolare svolgimento delle attività lavorative del Responsabile.

11. COMUNICAZIONI TRA LE PARTI

11.1. Ai fini del presente Accordo, il Responsabile dichiara di aver nominato un Responsabile della protezione dei dati (DPO) domiciliato presso la sede del Responsabile, che può essere contattato al seguente indirizzo dpo@namirial.com o al numero di telefono che segue: 071/63494.

11.2. Il Responsabile provvederà a contattare il Titolare, in tutti i casi previsti all'interno del presente Accordo, mediante comunicazione trasmessa all'indirizzo E-mail di notifica comunicata dal Titolare.

11.3. Le Parti si impegnano a notificarsi prontamente qualsiasi modifica dei loro indirizzi di contatto. In assenza di tale tempestiva notifica, le comunicazioni inoltrate all'indirizzo non aggiornato saranno ritenute valide ed efficaci.

Luogo e data	
IL TITOLARE (Cliente)	

Luogo e data	Senigallia,
IL RESPONSABILE (Fornitore)	

ALLEGATO I

DEFINIZIONI

a) **'Accordo'** significa il presente Accordo sul Trattamento dei Dati Personali, incluse le premesse gli Allegati;
b) **'Amministratori di Sistema'** significa le Persone Autorizzate incaricate della gestione e manutenzione di un impianto di elaborazione o di sue componenti, così come individuate dal Provvedimento del GPDP n. 300/2008, recante *Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema*, e ss.mm.ii.;
c) **'Autorità di Controllo'** significa qualsiasi Autorità di controllo indipendente ai sensi del Capo VI del GDPR, competente a vigilare e garantire l'applicazione delle disposizioni di legge in materia di protezione dei dati personali, con riferimento al Trattamento dei Dati Personali effettuato nell'esecuzione del Contratto (ivi inclusa l'Autorità Garante per la Protezione dei Dati Personali o '**GPDP**');
d) **'Categorie Particolari di Dati Personali'** significa i Dati Personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché il trattamento di dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o dati relativi alla vita sessuale o all'orientamento sessuale di una persona fisica, così come individuati all'art. 9 del GDPR;
e) **'Clausole Contrattuali Tipo'** significa le clausole adottate dalla Commissione Europea nella decisione 2021/914/UE del 4 giugno 2021 per il trasferimento di dati personali da un titolare del trattamento stabilito in Unione Europea ('**UE**') / Spazio Economico Europeo ('**SEE**') a un organismo non UE o non SEE che agisce in qualità di responsabile del trattamento;
f) **'Contratto'** significa il contratto firmato tra le Parti e avente ad oggetto la fornitura dei Servizi;
g) **'Dato Personale'** significa qualsiasi informazione relativa a una persona fisica identificata o – direttamente o indirettamente – identificabile ('**Interessato**') trattata dal Responsabile, per conto del Titolare, in relazione all'esecuzione del Contratto;
h) **'Diritti dell'Interessato'** significa i diritti riconosciuti all'Interessato dalla Legge Applicabile. Nei limiti di applicabilità del GDPR, per 'Diritti dell'Interessato' si intende, ad esempio, il diritto di richiedere al Titolare del trattamento l'accesso, la rettifica o la cancellazione dei Dati Personali, il diritto alla limitazione del Trattamento dei dati dell'Interessato o il diritto di opporsi al Trattamento, nonché il diritto alla portabilità dei dati;
i) **'E-mail di notifica'** si intende l'indirizzo (o gli indirizzi) email fornito/i dal Cliente, all'atto della sottoscrizione del Contratto o fornito tramite altro canale ufficiale al Responsabile, a cui il Cliente intende ricevere le notifiche da parte del Responsabile;
j) **'Legge Applicabile'** significa la normativa in materia di protezione dei dati personali applicabile al Trattamento dei Dati Personali sotteso al Contratto, quale il Regolamento UE 2016/679 *relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati* ('**GDPR**'), il Decreto Legislativo n. 196 del 30 giugno 2003 e ss.mm.ii., recante il *Codice in materia di protezione dei dati personali* ('**Codice Privacy**'), nonché ogni altra specifica normativa applicabile, ivi inclusi i provvedimenti, le linee guida e le indicazioni delle competenti Autorità di Controllo;
k) **'Misure di Sicurezza'** significa le misure tecniche e organizzative, di cui all'art. 32 del GDPR, idonee a garantire un adeguato livello di sicurezza dei Dati Personali, nonché tutte le misure necessarie per prevenire o almeno ridurre al minimo qualsiasi rischio ragionevolmente prevedibile di distruzione, perdita, alterazione, divulgazione non autorizzata o accesso, accidentale o illecito, ai Dati Personali trattati;
l) **'Persone Autorizzate'** significa le persone fisiche all'interno della struttura organizzativa del Responsabile specificatamente individuate per iscritto e autorizzate ad accedere ai Dati Personali e a trattarli nel contesto dell'esecuzione del Contratto, e che agiscono sotto il controllo e secondo le istruzioni del Responsabile;
m) **'Responsabile'** significa generalmente la persona fisica o giuridica, l'autorità pubblica, l'agenzia o altro organismo che tratta dati personali per conto di un titolare del trattamento;
n) **'Servizi'** significa i servizi forniti ai sensi del Contratto;
o) **'Sistemi del Titolare'** significa le infrastrutture e i sistemi eventualmente messi a disposizione dal Titolare e/o da terzi da quest'ultimo incaricati, sui quali il Responsabile è chiamato a svolgere il Trattamento;
p) **'Sub-Responsabile'** significa un organismo individuato dal Responsabile che effettua in tutto o in parte il Trattamento dei Dati Personali affidato al Responsabile, nel rispetto degli obblighi e delle istruzioni stabiliti dal Titolare, e che sia stato espressamente autorizzato da quest'ultimo;

q) **'Titolare'** significa generalmente la persona fisica o giuridica, l'autorità pubblica, l'agenzia o altro organismo che, da solo o congiuntamente ad altri, determina le finalità e i mezzi del trattamento dei dati personali;

r) **'Trattamento'** significa qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate ai Dati Personali o a insiemi di Dati Personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

ALLEGATO II

MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE

1. MISURE DI SICUREZZA ORGANIZZATIVE

TIPO DI MISURA	DESCRIZIONE
Policy e Regolamenti interni	Il Responsabile ha adottato un insieme di *policy*, procedure e regolamenti interni, vincolanti per tutto il personale autorizzato al trattamento dei dati personali. Tali *policy* e linee guida definiscono le regole per l'uso sicuro delle risorse informatiche e prevedono specifici disciplinari interni per la gestione delle informazioni, con l'obbligo di conformità da parte di tutti gli utenti. L'obiettivo è garantire il rispetto dei principi di riservatezza, integrità e disponibilità dei dati personali, minimizzando i rischi di accesso non autorizzato o uso improprio delle informazioni all'interno di tutte le società del gruppo.
Autorizzazione degli accessi e controlli logici	Il Responsabile definisce i profili di accesso nel rispetto dei 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 personali necessari per effettuare le operazioni di trattamento. Per le operazioni più sensibili, viene adottata l'autenticazione a due fattori (MFA) per rafforzare la sicurezza degli accessi. Tali profili sono oggetto di controlli periodici finalizzati alla verifica della sussistenza delle condizioni per la conservazione dei profili attribuiti
Monitoraggio degli accessi	Viene garantita la registrazione e il monitoraggio degli accessi ai sistemi che trattano dati personali, con analisi periodica dei log per individuare eventuali anomalie o attività sospette.
Change Management	Il Responsabile ha adottato una specifica procedura mediante 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.
Incident Management e Business Continuity	Il Responsabile ha posto 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. Gli incidenti vengono classificati per gravità e impatto sui dati personali. Il personale è addestrato a gestire eventi di sicurezza e a eseguire le procedure di contenimento. Sono previsti test periodici sulla reattività dell'organizzazione agli incidenti. È implementato un Piano di Continuità Operativa (*Business Continuity Plan*) per garantire la resilienza dei servizi anche in caso di emergenze.
Misure per garantire la conservazione limitata dei dati	Il Responsabile segue i principi di *Data Protection by Design* e *by Default*. **Misure tecniche**: • non vengono raccolti più dati personali di quelli necessari per il rispettivo scopo; • utilizzo di impostazioni predefinite rispettose della protezione dei dati. **Misure organizzative**:

	• politica di protezione dei dati secondo i principi "*privacy by design / by default*" inclusa nella SCS-P14 Group Privacy and Personal Data Protection Policy; • vengono eseguiti i controlli di sicurezza *OWASP Secure Mobile Development* (si eda, SCS-P08 Group Secure Coding Policy); Analisi del perimetro delle applicazioni *web*.
Data Breach	Il Responsabile 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 tempestivamente le comunicazioni delle violazioni di dati personali al Titolare. Per quanto di pertinenza del Responsabile tale procedura rileva almeno: • la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali coinvolti; • le probabili conseguenze della violazione dei dati personali; • le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.
Formazione	Per garantire un adeguato livello di consapevolezza, il Responsabile eroga formazione periodica sul corretto trattamento dei dati personali e sulla sicurezza delle informazioni. La formazione è obbligatoria per tutto il personale che accede ai dati personali. Sono previsti test e verifiche per valutare il livello di comprensione delle *policy* di sicurezza. Si organizzano campagne di simulazione di attacchi informatici (es. *phishing test*) per educare il personale sulle minacce più comuni. La formazione è aggiornata periodicamente per riflettere le evoluzioni normative e tecnologiche.
Gestione dei Sub-Responsabili	Quando il Responsabile si avvale di Sub-Responsabili, vengono attuati rigorosi controlli per verificare la conformità degli stessi alle misure di sicurezza richieste. • ogni Sub-Responsabile è tenuto a rispettare standard di sicurezza equivalenti a quelli del Responsabile. • sono previsti audit e ispezioni periodiche per verificare la compliance dei fornitori. • il Responsabile mantiene un registro aggiornato dei Sub-Responsabili.
Backup e Recupero dei dati	Per garantire la disponibilità dei dati e la resilienza ai guasti, il Responsabile implementa un sistema di *backup* e *disaster recovery* che prevede: • *backup* periodici con *policy* di conservazione definite; • protezione dei *backup* mediante cifratura e accesso controllato. • test periodici per garantire il ripristino rapido dei dati in caso di necessità. • replica dei dati in *data center* sicuri per prevenire la perdita di informazioni critiche.
Procedure per testare, verificare e valutare regolarmente l'efficacia	Le policy interne relative alle misure di sicurezza sono periodicamente riviste e confermate per l'adeguatezza e l'efficacia durante gli audit

delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento	interni in corso e annualmente da organismi di certificazione indipendenti, esterni e accreditati come parte degli audit di monitoraggio e ricertificazione ISO 9001 e ISO 27001.
Nomina del CISO	Al fine di garantire un adeguato livello di sicurezza delle informazioni e la conformità alle normative applicabili, il Responsabile ha designato un *Chief Information Security Officer* (**CISO**) con il compito principale di : • supervisionare l'attuazione e l'efficacia delle misure di sicurezza adottate per la protezione dei Dati Personali; • monitorare l'evoluzione delle minacce informatiche e promuovere l'aggiornamento continuo delle *policy* di sicurezza; • coordinare le attività di risposta agli incidenti di sicurezza; • definire strategie di miglioramento della sicurezza per la protezione degli *asset* aziendali. Il CISO opera in sinergia con le altre funzioni aziendali coinvolte nella gestione della sicurezza e della protezione dei dati.
Certificazioni di conformità	La lista completa delle certificazioni in possesso del Responsabile è disponibile al seguente indirizzo: https://www.namirial.com/it/company/certificazioni/

2. MISURE DI SICUREZZA TECNICHE

TIPO DI MISURA	DESCRIZIONE
***Capacity Planning* e Monitoraggio delle prestazioni**	Il Responsabile attua un processo continuo di analisi e ottimizzazione delle risorse IT per garantire performance adeguate alla fornitura dei Servizi e alla gestione dei Dati Personali. Il sistema prevede un monitoraggio proattivo della capacità di elaborazione, *storage* e banda di rete. Viene effettuata una proiezione delle esigenze future per garantire scalabilità e continuità operativa. Sono previsti test periodici di carico e resilienza per prevenire criticità dovute a sovraccarichi o picchi di utilizzo.
Sicurezza e *hardening* dei sistemi	Per minimizzare le vulnerabilità e migliorare la protezione delle infrastrutture IT, il Responsabile applica misure di *hardening* ai sistemi operativi, ai *software* applicativi e alle reti aziendali. I sistemi sono configurati seguendo le *best practice* di sicurezza per limitare esposizioni a rischi. Sono disabilitate funzionalità non necessarie e applicate restrizioni di accesso ai servizi di rete. Le configurazioni sono revisionate periodicamente e aggiornate secondo le evoluzioni delle minacce.
Patch Management e aggiornamenti di sicurezza	Il Responsabile mantiene un processo strutturato di gestione degli aggiornamenti per garantire la protezione contro vulnerabilità software. Gli aggiornamenti di sicurezza vengono applicati tempestivamente in base alla gravità delle vulnerabilità. Sono previste procedure di *testing* pre-rilascio per evitare impatti negativi sulla continuità del servizio. I sistemi critici sono soggetti a verifiche periodiche per individuare eventuali vulnerabilità non ancora risolte.

Protezione della rete e dei sistemi	I Dati Personali sono protetti da soluzioni avanzate di sicurezza perimetrale e intrusion detection, tra cui: • *Firewall* di nuova generazione per il filtraggio avanzato del traffico in entrata e uscita; • sistemi IDPS (*Intrusion Detection & Prevention System*) per identificare e bloccare attività sospette; • segmentazione della rete per limitare i rischi di propagazione in caso di attacco.
Protezione da *Malware* e minacce informatiche	Il Responsabile impiega strumenti di protezione avanzata per mitigare i rischi derivanti da malware e attacchi informatici: • *antivirus* e *anti-malware* aggiornati regolarmente per rilevare e bloccare minacce in tempo reale; • sistemi di *sandboxing* per analizzare e isolare file sospetti prima dell'esecuzione. • monitoraggio delle minacce per prevenire attacchi *zero-day*.
Sicurezza delle comunicazioni e protezione della trasmissione dei dati	Il Responsabile adotta protocolli di sicurezza avanzati per garantire l'integrità e la riservatezza delle comunicazioni: • cifratura *end-to-end* per proteggere i dati in transito; • autenticazione e certificati digitali per verificare l'integrità delle comunicazioni; • segmentazione VPN e reti private per ridurre i rischi di intercettazione.
Protezione fisica delle infrastrutture IT	L'accesso ai locali in cui sono conservati o trattati i Dati Personali è sottoposto a misure di sicurezza fisica rafforzate: accesso controllato con sistemi di *badge*, registrazione ingressi e autorizzazione preventiva. Videosorveglianza e allarmi anti-intrusione attivi 24/7. Misure di sicurezza ambientale, tra cui sistemi antincendio, ridondanza degli impianti elettrici e di climatizzazione, UPS e generatori di per garantire la continuità operativa. Procedure di emergenza e *disaster recovery*, con simulazioni periodiche per testare i piani di risposta agli incidenti.
Gestione delle credenziali e accesso ai sistemi	Per prevenire accessi non autorizzati, il Responsabile implementa un rigoroso sistema di autenticazione e gestione delle credenziali: • autenticazione Multi-Fattore per gli utenti con accesso a dati personali ed informazioni sensibili; • *password policy* avanzata con requisiti di lunghezza, complessità e scadenza periodica. • revoca immediata degli accessi in caso di cessazione del rapporto di lavoro o cambiamento di mansioni.
Gestione degli Amministratori di Sistema	Gli Amministratori di Sistema, in quanto soggetti con privilegi elevati, sono sottoposti a un rigoroso regime di controllo e monitoraggio. Il Responsabile mantiene un elenco aggiornato e documentato degli Amministratori di Sistema. Vengono tracciate e registrate le attività amministrative con *log* protetti e inalterabili. Vengono effettuati audit periodici per verificare l'operato degli amministratori e la corretta applicazione delle *policy* di sicurezza.