# ALLEGATO III

# SCHEDA DEL TRATTAMENTO

## Condizioni particolari di cui all'Accordo Generale sul Trattamento dei Dati Personali

Art. 28 Reg. UE 2016/679 ('**GDPR**')

Tra

Il **Titolare del Trattamento**, così come identificato nell'Accordo, nella persona del legale rappresentante munito dei necessari poteri,

e

Il **Responsabile del Trattamento**, così come identificato nell'Accordo, nella persona del legale rappresentante munito dei necessari poteri,

Inoltre, il Titolare e il Responsabile potranno essere congiuntamente indicati come '**Parti'** e singolarmente come '**Parte'**.

**PREMESSO CHE**

I. le Parti hanno sottoscritto l'Accordo Principale sul Trattamento dei Dati Personali ("Accordo"), che disciplina i termini e le modalità del trattamento dei dati personali eseguito dal Responsabile nell'ambito della fornitura dei Servizi oggetto del Contratto;
II. ai sensi del predetto Accordo, il trattamento dei dati personali connesso alla fornitura di specifici Servizi è disciplinato attraverso Schede di Trattamento che ne definiscono le caratteristiche operative, le categorie di dati trattati, le finalità, le misure di sicurezza applicate e l'eventuale coinvolgimento di Sub-Responsabili;
III. la presente Scheda di Trattamento specifica i dettagli del Servizio in conformità con l'Accordo. Essa integra e completa le disposizioni generali dell'Accordo, costituendone parte integrante e vincolante tra le Parti;
IV. in caso di conflitto tra le disposizioni della presente Scheda di Trattamento e quelle dell'Accordo, prevarranno le disposizioni dell'Accordo, salvo che la Scheda di Trattamento preveda espressamente deroghe concordate tra le Parti;
V. per quanto in esse non espressamente previsto, trovano applicazione le disposizioni e definizioni previste nell'Accordo e nel Contratto, che ivi si intendono integralmente richiamati.

Tutto ciò premesso, le Parti riportano, nella seguente tabella, le specifiche del trattamento dei dati personali relativo al Servizio, includendo informazioni su finalità, categorie di dati trattati, misure di sicurezza applicate e ogni altro dettaglio rilevante ai fini dell'Accordo.

| | **DESCRIZIONE** |
|---|---|
| **SERVIZIO** | ***Modulo "AI SpinOff" per funzionalità di estrazione automatica dei dati***<br>*Il Modulo "AI SpinOff" è un componente opzionale del software gestionale on-premise SpinOff di Namirial, dedicato all'estrazione automatica dei dati contenuti nei documenti o immagini. Il modulo utilizza modelli di intelligenza artificiale per identificare e strutturare le informazioni contenute nei documenti, restituendo un output in formato JSON validato.*<br>*Il trattamento è articolato nel seguente flusso operativo:*<br>*Acquisizione: il documento resta nell'infrastruttura del Titolare. Il Modulo effettua localmente le elaborazioni tecniche necessarie alla predisposizione del contenuto da trasmettere al Provider AI, secondo le modalità tempo per tempo supportate dal Modulo;* |

| | |
|---|---|
| | *Elaborazione AI: il contenuto del documento, o una sua rappresentazione tecnica generata dal Modulo, viene trasmesso tramite canale cifrato al Provider AI, che restituisce dati strutturati in formato JSON. I dati trasmessi non sono utilizzati dal Provider AI per addestrare i propri modelli, secondo le condizioni contrattuali applicabili;*<br>*Validazione umana: il Modulo mette a disposizione dell'operatore del Titolare funzionalità di verifica, controllo ed eventuale approvazione o modifica dell'output prima della registrazione nel gestionale SpinOff, secondo le configurazioni applicabili;*<br>*Registrazione: i dati validati vengono registrati nel database locale SpinOff del Titolare.* |
| **SOGGETTO EROGATORE** | **Namirial S.p.A.**<br>Laddove il Soggetto Erogatore non coincida con il Fornitore identificato nella Proposta Commerciale, agisce quale Sub-Responsabile Infragruppo per conto del Fornitore, operando in forza di accordi infragruppo preesistenti tra le società del Gruppo Namirial, conformi all'Articolo 28 GDPR. |
| **NATURA DEL TRATTAMENTO** | Il Responsabile può trattare i Dati Personali del Cliente nel contesto della fornitura del Servizio, nei limiti di quanto strettamente necessario all'esecuzione delle prestazioni di cui al Contratto, in termini di: raccolta, registrazione, organizzazione o strutturazione, consultazione, elaborazione, selezione, estrazione, raffronto, utilizzo, comunicazione, cancellazione o distruzione, nonché attività di analisi automatizzata dei contenuti dei documenti mediante modelli di intelligenza artificiale (AI). Il trattamento avviene esclusivamente su iniziativa e sotto il controllo del Titolare, il quale rimane responsabile della correttezza e completezza dei dati immessi nel gestionale. |
| **FINALITÀ DEL TRATTAMENTO** | Esecuzione del Contratto di fornitura del Modulo "AI integrata in SpinOff", comprendente:<br>• calcolo e comunicazione all'operatore del Confidence Score per ogni estrazione, al fine di supportare la validazione umana;<br>• pre-compilazione dei campi del gestionale SpinOff per ridurre l'inserimento manuale e gli errori di digitazione;<br>• miglioramento dell'efficienza dei processi. |
| **MODALITÀ DI EROGAZIONE** | *On-premise. Il Modulo è installato direttamente sull'infrastruttura del Titolare (server locali o rete aziendale). I documenti sono trattati localmente dal Modulo e il contenuto necessario all'elaborazione AI, o una sua rappresentazione tecnica, viene trasmesso in forma transitoria e cifrata al Provider AI per l'inferenza. Non è previsto alcuno storage persistente dei dati personali presso il Provider AI.* |
| **CATEGORIE DI SOGGETTI INTERESSATI** | • Dipendenti/collaboratori del Titolare;<br>• Operatori del Titolare incaricati della validazione degli output AI e della registrazione nel gestionale SpinOff;<br>• Soggetti terzi i cui dati identificativi possono essere presenti nei documenti (es. committenti, destinatari finali della merce). |

## SCHEDA DEL TRATTAMENTO

| | |
|---|---|
| **CATEGORIE DI DATI PERSONALI TRATTATI** | I Dati Personali trattati per conto del Titolare sono quelli contenuti nei documenti sottoposti al Modulo AI e appartengono alle seguenti categorie.<br>**DATI COMUNI:**<br>• I dati contenuti nei documenti sottoposti al Modulo AI e possono includere, a titolo esemplificativo e non esaustivo: dati identificativi, dati di contatto, dati fiscali, dati commerciali, dati logistici, dati amministrativi;<br>• Dati tecnici di elaborazione: Confidence Score dell'estrazione, timestamp di elaborazione, token API consumati, tempi di risposta.<br>**DATI PARTICOLARI (art. 9 GDPR):**<br>• Non sono previsti trattamenti sistematici di categorie particolari di dati. Non è tuttavia escludibile che, in casi specifici, contenuti dei documenti possano includere informazioni riconducibili a categorie particolari (es. dati sanitari in forniture medicali). Il Titolare è responsabile di valutare e limitare il conferimento di tali dati al Modulo AI. |
| **LUOGO DI CONSERVAZIONE DEI DATI** | Sede del Titolare (on-premise): i documenti originali, i log tecnici e i dati registrati nel gestionale SpinOff sono conservati esclusivamente presso i server del Titolare del trattamento. Namirial non ha accesso remoto ai dati conservati, salvo interventi di supporto tecnico espressamente autorizzati dal Titolare.<br>Provider AI (per elaborazione transitoria): le informazioni estratte dal documento sono trasmesse all'API del Provider AI esclusivamente per l'inferenza AI in tempo reale. Il Provider AI non memorizza i dati inviati in modo persistente. Il trasferimento verso gli USA, se necessario, è effettuato ai sensi dell'art. 46 GDPR, mediante Clausole Contrattuali Standard (SCC) adottate dalla Commissione Europea con decisione di esecuzione 2021/914 del 4 giugno 2021.<br>Resta inteso che Namirial potrà trattare metriche tecniche e di consumo relative all'utilizzo del Modulo, quali numero di elaborazioni, pagine elaborate, timestamp, esiti tecnici, token o altri indicatori di consumo, ai fini di monitoraggio, rendicontazione e fatturazione del servizio, senza accesso al contenuto dei documenti trattati, salvo interventi di supporto tecnico espressamente autorizzati dal Titolare. |
| **DURATA DEL TRATTAMENTO DEI DATI PERSONALI** | I dati personali contenuti nei documenti caricati sono trattati esclusivamente per il tempo necessario all'inferenza (elaborazione in tempo reale, senza storage persistente). I risultati JSON dell'estrazione sono disponibili all'operatore del Titolare per la durata della sessione lavorativa.<br>I log tecnici locali sono conservati sul server del Titolare per un periodo massimo di 12 mesi, salvo diversa indicazione del Titolare medesimo o obblighi legali specifici.<br>I dati registrati nel gestionale SpinOff a seguito della validazione umana sono soggetti alle politiche di conservazione proprie del Titolare, definite in relazione agli obblighi fiscali e contabili applicabili (tipicamente 10 anni per i documenti fiscali). |

| | |
|---|---|
| **MISURE DI SICUREZZA** | Rif. **Allegato III A - MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE** |
| **SUB-RESPONSABILI** | Il Soggetto Erogatore del Servizio (identificato nella riga precedente) si avvale, per l'erogazione del Servizio, di altre società del Gruppo Namirial e di soggetti terzi selezionati che offrono garanzie di riservatezza dei dati.<br><br>L'elenco aggiornato è riportato nell'Allegato III B, suddiviso in **Tabella A** (società del Gruppo Namirial coinvolte nell'erogazione del servizio, operanti in forza di accordi infragruppo preesistenti conformi all'Articolo 28 GDPR e separati dal presente Accordo) e **Tabella B** (Sub-Responsabili terzi).<br><br>Alcuni di questi soggetti terzi potrebbero operare anche al di fuori dello Spazio Economico Europeo (SEE), inclusi gli Stati Uniti.<br><br>Per garantire la conformità con il GDPR (artt. 44-49) e la normativa sulla protezione dei dati personali, il Fornitore potrà avvalersi di meccanismi adeguati per il trasferimento dei dati.<br><br>Tali soggetti vengono selezionati in conformità con le disposizioni di cui all'Accordo, ricevono istruzioni precise sul trattamento dei dati e svolgono esclusivamente le attività necessarie nel rispetto delle direttive fornite.<br><br>L'elenco aggiornato di questi soggetti è riportato nell'Allegato III B del presente documento. |

## ALLEGATO III - A

## MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE

Le misure di sicurezza descritte nel presente Allegato si applicano in aggiunta a quelle previste dall'Accordo e costituiscono un livello di protezione supplementare per i trattamenti disciplinati dalla Scheda di Trattamento cui sono annesse. Esse sono applicate ed applicabili al Soggetto Erogatore del Servizio di cui al Contratto, che può coincidere o meno con il Responsabile.

### 1. MISURE DI SICUREZZA TECNICHE

| TIPO DI MISURA | DESCRIZIONE |
|---|---|
| **Misure per assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento** | Il Modulo AI opera su infrastruttura on-premise del Titolare, con accesso limitato agli operatori autorizzati mediante autenticazione applicativa gestita da SpinOff.<br>• Le comunicazioni tra il Modulo AI e l'API di del Provider AI sono protette da TLS e canali cifrati. I contenuti o le rappresentazioni tecniche trasmesse al Provider AI sono trattati in modo transitorio per il tempo necessario all'elaborazione e non persistono localmente dopo l'invio.<br>• Namirial mantiene la conformità ISO/IEC 27001 per i propri processi di sviluppo e distribuzione del software. Il contratto Enterprise con il Provider AI include impegni di sicurezza certificati (ISO 27001, SOC 2 Type II). |
| **Misure per assicurare la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico** | La continuità operativa del Modulo AI dipende dall'infrastruttura on-premise del Titolare (server locali, backup aziendali) e dalla disponibilità del servizio del Provider AI.<br>• Il Modulo è progettato per essere resiliente a errori transitori dell'API (retry automatici con backoff esponenziale). In caso di indisponibilità dell'API del Provider AI, il flusso di inserimento manuale nel gestionale SpinOff rimane pienamente operativo senza dipendenza dal Modulo AI.<br>• La Business Continuity dell'infrastruttura on-premise è responsabilità del Titolare del trattamento, in conformità con le proprie politiche interne. |
| **Misure di protezione dei dati durante la conservazione** | Il Modulo AI tratta localmente i documenti sull'infrastruttura del Titolare e, ove tecnicamente necessario ai fini dell'elaborazione AI, genera una rappresentazione tecnica del relativo contenuto. Ai soli fini dell'inferenza, tale contenuto o rappresentazione tecnica può essere trasmesso al Provider AI tramite canale cifrato, per il tempo strettamente necessario all'elaborazione.<br>**Il Provider AI garantisce che i dati inviati tramite API non siano utilizzati per addestrare o migliorare i modelli del Provider AI. I dati inviati non sono condivisi con terzi e non sono soggetti a storage persistente presso il Provider AI.**<br>• Ogni chiamata API è autenticata tramite credenziali tecniche dedicate, configurate nell'ambiente Namirial e associate al cliente o al servizio secondo le configurazioni applicabili. Le credenziali non sono esposte nell'interfaccia utente o nei log applicativi. |

| | |
|---|---|
| **Misure per garantire la registrazione degli eventi** | **Ogni operazione di estrazione documentale genera log applicativi locali contenenti:**<br>• identificativo univoco della richiesta e del documento elaborato;<br>• timestamp di inizio/fine elaborazione;<br>• Confidence Score calcolato e dettaglio per campo;<br>• numero di token API consumati e costo stimato (USD);<br>I log sono archiviati localmente sul server del Titolare e accessibili tramite endpoint API dedicati (/api/v1/metrics, /api/v1/metrics/dashboard). La conservazione è limitata a 12 mesi salva diversa configurazione del Titolare. |
| **Misure per garantire la configurazione del sistema, compresa la configurazione per impostazione predefinita** | Le configurazioni del Modulo sono impostate in modo da rendere disponibile all'operatore una funzionalità di verifica dell'output AI e un'indicazione del relativo livello di affidabilità o completezza, secondo le soglie e i parametri tempo per tempo configurati.<br>Il principio di "privacy by design e by default" (art. 25 GDPR) è implementato attraverso:<br>• trattamento locale dei documenti sull'infrastruttura del Titolare, salvo la trasmissione al Provider AI del contenuto o della rappresentazione tecnica strettamente necessaria all'elaborazione;<br>• trasmissione dei dati al Provider AI tramite canali cifrati e per il tempo strettamente necessario all'inferenza AI;<br>• configurazione del Modulo in modo da consentire all'operatore la verifica, la modifica, l'approvazione o il rifiuto dell'output AI prima del relativo utilizzo operativo, secondo le funzionalità disponibili;<br>• minimizzazione dell'output restituito dal Modulo ai dati e ai campi pertinenti rispetto alla specifica funzionalità utilizzata;<br>• messa a disposizione di avvisi informativi nell'interfaccia utente circa la natura automatizzata e probabilistica dell'output AI e la necessità di verificarne l'accuratezza prima dell'utilizzo operativo, ove previsto dalla configurazione del Modulo.<br>• disclaimer mostrato all'operatore nell'interfaccia utente circa la natura probabilistica dell'output AI. |
| **Misure di informatica interna e di gestione e governance della sicurezza informatica** | Il Modulo AI è sviluppato e distribuito nell'ambito del Sistema di Gestione della Sicurezza delle Informazioni di Namirial, certificato ISO/IEC 27001. Sono applicate policy interne per la gestione degli accessi, il controllo delle versioni software (release management), il change management e la valutazione periodica dei sub-responsabili.<br>La governance AI è progressivamente allineata ai principi della ISO/IEC 42001:2023, anche mediante documentazione delle attività di sviluppo, testing e manutenzione del Modulo AI e tracciamento delle versioni dei modelli utilizzati.<br>Il Titolare è responsabile della governance IT della propria infrastruttura on-premise (accessi fisici e logici ai server, aggiornamenti del sistema operativo, backup). |
| **Misure per garantire la conservazione limitata dei dati** | I contenuti o le rappresentazioni tecniche generate per l'elaborazione AI sono trattati per il tempo strettamente necessario all'elaborazione e non sono conservati dal Responsabile in forma persistente, salvo quanto |

| | |
|---|---|
| | necessario per log tecnici, metriche di servizio o attività di supporto autorizzate.<br><br>Gli output JSON dell'elaborazione sono conservati in memoria applicativa solo per il tempo necessario alla validazione umana e alla registrazione nel gestionale. Non sono conservati dal Responsabile in forma che consenta l'identificazione degli interessati.<br><br>I log tecnici sono conservati per un massimo di 12 mesi e successivamente eliminati automaticamente o su richiesta del Titolare. |
| **Misure per garantire la responsabilità** | Ogni ciclo di estrazione documentale è tracciato con identificativo univoco, versione del modello AI utilizzato e Confidence Score.<br><br>Il Modulo mette a disposizione funzionalità che consentono all'operatore del Titolare di verificare, validare, modificare o rifiutare l'output AI prima del relativo utilizzo operativo, secondo le configurazioni applicabili (conformità art. 22 GDPR - divieto di decisioni automatizzate con effetti giuridici significativi).<br><br>Namirial mantiene la documentazione tecnica del Modulo, il registro delle versioni e le registrazioni dei modelli AI utilizzati, conformemente ai requisiti dell'AI Act (Reg. UE 2024/1689) e alle proprie politiche interne. |
| **Misure per consentire la portabilità dei dati e garantire la cancellazione** | I dati elaborati dal Modulo AI sono registrati nel gestionale SpinOff del Titolare e sono quindi soggetti alle politiche di portabilità e cancellazione del Titolare stesso.<br><br>Il Responsabile non conserva copie dei dati personali trattati in esecuzione del Servizio e non è pertanto il soggetto da interpellare per le richieste di accesso, rettifica, portabilità o cancellazione degli interessati.<br><br>In caso di cessazione del Contratto, il Titolare potrà richiedere la disinstallazione del Modulo e la cancellazione di qualsiasi dato eventualmente conservato sul sistema del Responsabile (es. chiavi API, configurazioni tenant). La cancellazione sarà documentata e certificata. |

## ALLEGATO III - B

## SUB-RESPONSABILI

Il presente Allegato riporta l'elenco dei Sub-Responsabili del Trattamento approvati alla data di sottoscrizione della relativa Scheda di Trattamento, ai sensi dell'Accordo.

I soggetti elencati sono stati selezionati in base a criteri di esperienza, affidabilità e garanzie di conformità alle normative applicabili, in particolare alle disposizioni di cui all'art. 28 del Regolamento UE 2016/679.

Essi operano sotto l'autorità del Responsabile, attenendosi alle istruzioni ricevute e adottando misure di sicurezza adeguate alla protezione dei Dati Personali trattati.

L'elenco dei Sub-Responsabili potrà essere aggiornato nel tempo in conformità alle previsioni dell'Accordo.

**TABELLA A**

**SOCIETÀ DEL GRUPPO NAMIRIAL COINVOLTE NELL'EROGAZIONE DEL SERVIZIO**

| RAGIONE SOCIALE | INDIRIZZO | LUOGO DEL TRATTAMENTO | AMBITO DI ATTIVITÀ |
|---|---|---|---|
| **Namirial SPA** | Via Caduti sul Lavoro 4 – Senigallia (AN) Italia | EEA | Fornitore del servizio |

**TABELLA B**

**SUB-RESPONSABILI TERZI**

| RAGIONE SOCIALE | INDIRIZZO | LUOGO DEL TRATTAMENTO | AMBITO DI ATTIVITÀ |
|---|---|---|---|
| **OpenAI LLC** | 3180 18th Street San Francisco, CA 94110 USA | USA (extra-UE) Trasferimento ex art. 46 GDPR SCC Dec. CE 2021/914 | Inferenza AI per estrazione strutturata dei dati dai documenti. Elaborazione transitoria: nessuno storage persistente dei dati personali. |
| **Zendesk Inc.** | 989 Market St, San Francisco, CA 94103 | EEA | Gestione dei ticket di assistenza |
| **Atlassian B.V.** | Amsterdam, Singel 236 1016 AB, Netherlands | EEA | Gestione dei ticket di assistenza |
| **Exalate NV** | Roderveldlaan 2 bus 3, 2600 Berchem, Belgium | EEA | Sincronizzazione dei ticket di assistenza |