ALLEGATO III

SCHEDA DEL TRATTAMENTO

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

Art. 28 Reg. UE 2018/679 ('**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,

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	*ClickWrap*
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, estrazione, utilizzo, comunicazione, cancellazione o distruzione.
FINALITÀ DEL TRATTAMENTO	Conclusione del Contratto ed esecuzione delle prestazioni oggetto del Contratto.
MODALITÀ DI EROGAZIONE	*Cloud* SaaS

CATEGORIE DI SOGGETTI INTERESSATI	• Clienti finali; • Utilizzatori del servizio; • Dipendenti.
CATEGORIE DI DATI PERSONALI TRATTATI	I Dati Personali trattati dal Responsabile per conto del Titolare appartengono alle seguenti categorie. **DATI COMUNI**: • **Dati anagrafici** (nome, cognome); • **Dati di navigazione** (indirizzo IP, file di log);
LUOGO DI CONSERVAZIONE DEI DATI	I dati sono conservati presso i *server* del Responsabile e/o dei Sub-Responsabili situati all'interno dell'Unione Europea/SEE.
DURATA DEL TRATTAMENTO DEI DATI PERSONALI	Il Trattamento dei Dati Personali ai fini della fornitura dei Servizi avrà la seguente durata: l'intera durata del Contratto con il Titolare; l'intera durata dell'Accordo con il Titolare se, per qualsiasi motivo, più lunga della durata del Contratto. Dopo la scadenza dei periodi sopra menzionati, al Responsabile è consentita un'ulteriore conservazione dei Dati Personali nella misura in cui costituisca conformità a specifici obblighi di legge o ordini delle Autorità competenti. La conservazione dei Dati Personali è inoltre consentita esclusivamente nella misura in cui tali Dati Personali siano necessari al Responsabile per dimostrare, far valere o difendere un proprio diritto, per un periodo massimo di 10 anni.
MISURE DI SICUREZZA	Rif. **Allegato III A** - MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE
SUB-RESPONSABILI	Il Responsabile si avvale, al fine di effettuare le operazioni di trattamento correlate all'erogazione del Servizio di altre società del Gruppo Namirial e di soggetti terzi selezionati che offrono garanzie di riservatezza dei dati. Alcuni di questi soggetti terzi potrebbero operare anche al di fuori dello Spazio Economico Europeo (SEE), inclusi gli Stati Uniti. 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. 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. 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 Fornitore del Servizio di cui al Contratto.

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	La soluzione consente di archiviare in modo sicuro i pacchetti di dati grazie all'utilizzo di una *blockchain permissioned*, basata sul meccanismo di consenso *Proof of Stake (PoS)*, che garantisce immutabilità e incorruttibilità. I dati in chiaro archiviati nei server AWS di ClickWrap vengono crittografati mediante il sistema Amazon S3 prima della memorizzazione. La piattaforma è accessibile solo tramite autenticazione dell'utente con ID e password, protetta da autenticazione a due fattori (2FA) tramite OTP inviato all'indirizzo e-mail del Cliente. Le API necessarie per la comunicazione con il provider di storage AWS sono protette mediante autenticazione API.
Misure per assicurare la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico	La *blockchain* non memorizza direttamente dati personali, ma solo un *hash* del file JSON, consentendo di verificare l'integrità dei dati senza comprometterne la sicurezza. Un file JSON in chiaro viene inviato ai server AWS di ClickWrap, per consentire successivamente di confrontare l'*hash* del file memorizzato con quello scritto nella *blockchain*. Il sistema è progettato per garantire l'alta disponibilità, evitando congestioni e problemi di *denial of service* grazie all'uso di ATP Server . (*Available-To-Promise-Server*).
Misure di protezione dei dati durante la conservazione	I dati archiviati nei server AWS vengono crittografati prima della memorizzazione e decrittografati solo al momento del *download*. La piattaforma utilizza database relazionali SQL, protetti da difese perimetrali, ATP Server, *Web Application Firewall* (WAF) e crittografia con il sistema Amazon S3. Il sistema utilizza WORM (*Write Once, Read Many*) per garantire l'integrità dei dati e prevenire modifiche illecite. Un WAF aiuta a proteggere le applicazioni web filtrando e monitorando il traffico HTTP tra un'applicazione *web* e *Internet*, al fine di proteggere le applicazioni *web* da attacchi come *cross-site forgery*, *cross-site-scripting* (XSS), inclusione di file e SQL *injection*, tra gli altri. Un WAF è una difesa di livello 7 del protocollo (nel modello OSI) e non è progettato per difendere il sistema da tutti i tipi di attacchi. Utilizzando un WAF a protezione di un'applicazione *web*, si pone uno scudo tra l'applicazione *web* e *Internet*.

Misure per garantire la registrazione degli eventi	La soluzione garantisce la registrazione e tracciabilità delle operazioni mediante la *blockchain*, che registra un *hash* immutabile del file JSON associato al consenso. L'hash del file JSON consente di dimostrare l'autenticità del consenso dato dall'utente, verificando che non sia stato modificato nel tempo. I *log* di accesso ai *database* e alle API sono protetti e monitorati per individuare eventuali attività sospette.
Misure per garantire la configurazione del sistema, compresa la configurazione per impostazione predefinita	Il lato applicativo della piattaforma è *cloud native* e utilizza microservizi progettati per essere attivati solo su richiesta e poi eliminati automaticamente, riducendo il rischio di esposizione a codice malevolo. La piattaforma adotta un modello di sicurezza basato su *least privilege*, limitando l'accesso solo alle risorse necessarie. Tutti i sistemi sono monitorati e aggiornati per prevenire vulnerabilità di configurazione.
Misure di informatica interna e di gestione e governance della sicurezza informatica	La *blockchain* utilizzata è *permissioned*, il che significa che l'accesso è limitato solo agli utenti autorizzati, i quali devono identificarsi tramite certificati digitali o altri strumenti di autenticazione. I validatori della *blockchain* vengono selezionati attentamente dopo un'attenta valutazione della loro architettura informatica e di alcuni ulteriori elementi per valutare un adeguato livello di sicurezza. Questo tipo di soluzione è raccomandata dalle autorità per la protezione dei dati, in quanto è in grado di offrire un livello di *privacy* più elevato. Il sistema è protetto da *Web Application Firewall* (WAF) per filtrare e monitorare il traffico HTTP e prevenire attacchi come *cross-site forgery*, XSS, SQL *injection* e inclusione di file.
Misure per garantire la conservazione limitata dei dati	Nella *blockchain* non vengono memorizzati dati personali in chiaro, ma solo un *hash* del file JSON, che non consente di ricostruire direttamente i dati originali. L'*hash* archiviato nella *blockchain* è deterministico, quindi il medesimo *input* produrrà sempre lo stesso *output*, garantendo la verifica dell'integrità dei dati senza necessità di conservarli. Le regole di conservazione sono configurate in modo da garantire la minimizzazione dei dati in conformità con il principio di *Data Protection by Design* e *by Default*.
Misure per garantire la responsabilità	L'accesso alla piattaforma è regolato da un sistema di autenticazione forte e da meccanismi di tracciabilità che permettono di identificare ogni operazione effettuata. La *blockchain* fornisce una prova crittografica inalterabile dell'operazione eseguita, garantendo la non ripudiabilità del consenso espresso dall'utente. I validatori della blockchain sono soggetti a controlli e verifiche per assicurare la loro compliance ai requisiti di sicurezza.
Misure per consentire la portabilità dei dati e garantire la cancellazione	La soluzione consente di esportare i dati in formato JSON, garantendo la loro portabilità e interoperabilità con altri sistemi. L'*hash* registrato nella *blockchain* può essere verificato in qualsiasi momento, garantendo trasparenza e accessibilità ai dati memorizzati.

	I dati in chiaro possono essere cancellati su richiesta, mantenendo l'*hash* nella *blockchain* per finalità di *audit*, senza che ciò comporti la conservazione di dati personali riconducibili all'utente.

2. MISURE DI SICUREZZA ORGANIZZATIVE

TIPO DI MISURA	DESCRIZIONE
Procedure per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento	Il sistema di *blockchain* e crittografia viene testato periodicamente per verificare l'integrità della registrazione degli *hash* e l'affidabilità della piattaforma. Sono previsti test di sicurezza sulle API e sulle infrastrutture cloud per garantire l'affidabilità dei controlli di accesso. La piattaforma viene sottoposta a verifiche di conformità con gli standard di sicurezza e *privacy*, in linea con le raccomandazioni delle autorità di protezione dei dati.

ALLEGATO III - B

SUB-RESPONSABILI DEL TRATTAMENTO

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.

RAGIONE SOCIALE	INDIRIZZO	LUOGO DEL TRATTAMENTO	AMBITO DI ATTIVITÀ
AWS EMEA SARL	Luxembourg, 38 Avenue John F. Kennedy L-1855	EEA	Servizi *Cloud*
Atlassian B.V.	Amsterdam, Singel 236 1016 AB Amsterdam, Netherlands	EEA/USA	Piattaforma di *Ticketing*
Zendesk Inc.	989 Market St, San Francisco, CA 94103	EEA	Piattaforma di *Ticketing*
Exalate NV	Roderveldlaan 2 bus 3, 2600 Berchem, Belgium	EEA	Sincronizzazione dei ticket di supporto
Yarix S.r.l.	Montebelluna (TV), Vicolo Boccacavalla n. 12, 31044	EEA	SOC (*Security Operation Center*) e MOC (*Monitoring Operation Center*)