Allegato C - Atto di nomina a responsabile del trattamento

Il presente atto di nomina a responsabile del trattamento (basato su Clausole Contrattuali Tipo della Commissione Europea tra titolari e responsabili del trattamento ex art. 28(7) del Regolamento Europeo 2016/679 - RGPD è parte integrante del Contratto sottoscritto tra le Parti, e riguarda il trattamento dei dati personali effettuato dal Licenziante per conto del Licenziatario nell'ambito dei Servizi oggetto del Contratto.

Se non diversamente specificato nel presente DPA, tutti i termini in maiuscolo avranno il significato loro attribuito nel Contratto.

SEZIONE I

Clausola 1 - Scopo e ambito di applicazione

(a) Scopo delle presenti clausole contrattuali tipo (di seguito "clausole") è garantire il rispetto dell'articolo 28, paragrafi 3 e 4, del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

(b) I titolari del trattamento e i responsabili del trattamento di cui all'allegato I hanno accettato le presenti clausole al fine di garantire il rispetto dell'articolo 28, paragrafi 3 e 4, del regolamento (UE) 2016/679.

(c) Le presenti clausole si applicano al trattamento dei dati personali specificato all'allegato II.

(d) Gli allegati da I a IV costituiscono parte integrante delle clausole.

(e) Le presenti clausole lasciano impregiudicati gli obblighi cui è soggetto il titolare del trattamento a norma del regolamento (UE) 2016/679.

(f) Le presenti clausole non garantiscono, di per sé, il rispetto degli obblighi connessi ai trasferimenti internazionali conformemente al capo V del regolamento (UE) 2016/679.

Clausola 2 - Invariabilità delle clausole

(a) Le parti si impegnano a non modificare le clausole se non per aggiungere o aggiornare informazioni negli allegati.

(b) Ciò non impedisce alle parti di includere le clausole contrattuali tipo stabilite nelle presenti clausole in un contratto più ampio o di aggiungere altre clausole o garanzie supplementari, purché queste non contraddicano, direttamente o indirettamente, le presenti clausole o ledano i diritti o le libertà fondamentali degli interessati.

Clausola 3 - Interpretazione

(a) Quando le presenti clausole utilizzano i termini definiti nel regolamento (UE) 2016/679, tali termini hanno lo stesso significato di cui al regolamento interessato.

(b) Le presenti clausole vanno lette e interpretate alla luce delle disposizioni del regolamento (UE) 2016/679.

(c) Le presenti clausole non devono essere interpretate in un senso che non sia conforme ai diritti e agli obblighi previsti dal regolamento (UE) 2016/679 o che pregiudichi i diritti o le libertà fondamentali degli interessati.

Clausola 4 - Gerarchia

In caso di contraddizione tra le presenti clausole e le disposizioni di accordi correlati, vigenti tra le parti al momento dell'accettazione delle presenti clausole, o conclusi successivamente, prevalgono le presenti clausole.

Clausola 5 - Clausola di adesione successiva

(a) Qualunque entità che non sia parte delle presenti clausole può, con l'accordo di tutte le parti, aderire alle presenti clausole in qualunque momento, in qualità di titolare del trattamento o di responsabile del trattamento, compilando gli allegati e firmando l'allegato I.

(b) Una volta compilati e firmati gli allegati di cui alla lettera a), l'entità aderente è considerata parte delle presenti clausole e ha i diritti e gli obblighi di un titolare del trattamento o di un responsabile del trattamento, conformemente alla sua designazione nell'allegato I.

(c) L'entità aderente non ha diritti od obblighi derivanti a norma delle presenti clausole per il periodo precedente all'adesione.

SEZIONE II - OBBLIGHI DELLE PARTI

Clausola 6 - Descrizione del trattamento

I dettagli dei trattamenti, in particolare le categorie di dati personali e le finalità del trattamento per le quali i dati personali sono trattati per conto del titolare del trattamento, sono specificati nell'allegato II.

Clausola 7 - Obblighi delle parti

7.1. Istruzioni

(a) Il responsabile del trattamento tratta i dati personali soltanto su istruzione documentata del titolare del trattamento, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento. In tal caso, il responsabile del trattamento informa il titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto lo vieti per rilevanti motivi di interesse pubblico. Il titolare del trattamento può anche impartire istruzioni successive per tutta la durata del trattamento dei dati personali. Tali istruzioni sono sempre documentate.

(b) Il responsabile del trattamento informa immediatamente il titolare del trattamento qualora, a suo parere, le istruzioni del titolare del trattamento violino il regolamento (UE) 2016/679 o le disposizioni applicabili, nazionali o dell'Unione, relative alla protezione dei dati.

7.2. Limitazione delle finalità

Il responsabile del trattamento tratta i dati personali soltanto per le finalità specifiche del trattamento di cui all'allegato II, salvo ulteriori istruzioni del titolare del trattamento.

7.3. Durata del trattamento dei dati personali

Il responsabile del trattamento tratta i dati personali soltanto per la durata specificata nell'allegato II.

7.4. Sicurezza del trattamento

(a) Il responsabile del trattamento mette in atto almeno le misure tecniche e organizzative specificate nell'allegato III per garantire la sicurezza dei dati personali. Ciò include la protezione da ogni violazione di sicurezza che comporti accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati (violazione dei dati personali). Nel valutare l'adeguato livello di sicurezza, le parti tengono debitamente conto dello stato dell'arte, dei costi di attuazione, nonché della natura,

dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi per gli interessati.

(b) Il responsabile del trattamento concede l'accesso ai dati personali oggetto di trattamento ai membri del suo personale soltanto nella misura strettamente necessaria per l'attuazione, la gestione e il controllo del contratto. Il responsabile del trattamento garantisce che le persone autorizzate al trattamento dei dati personali ricevuti si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza.

7.5. Dati sensibili

Se il trattamento riguarda dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, dati genetici o dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona, o dati relativi a condanne penali e a reati ("dati sensibili"), il responsabile del trattamento applica limitazioni specifiche e/o garanzie supplementari.

7.6. Documentazione e rispetto

(a) Le parti devono essere in grado di dimostrare il rispetto delle presenti clausole.

(b) Il responsabile del trattamento risponde prontamente e adeguatamente alle richieste di informazioni del titolare del trattamento relative al trattamento dei dati conformemente alle presenti clausole.

(c) Il responsabile del trattamento mette a disposizione del titolare del trattamento tutte le informazioni necessarie a dimostrare il rispetto degli obblighi stabiliti nelle presenti clausole e che derivano direttamente dal regolamento (UE) 2016/679 . Su richiesta del titolare del trattamento, il responsabile del trattamento consente e contribuisce alle attività di revisione delle attività di trattamento di cui alle presenti clausole, a intervalli ragionevoli o se vi sono indicazioni di inosservanza. Nel decidere in merito a un riesame o a un'attività di revisione, il titolare del trattamento può tenere conto delle pertinenti certificazioni in possesso del responsabile del trattamento.

(d) Il titolare del trattamento può scegliere di condurre l'attività di revisione autonomamente o incaricare un revisore indipendente. Le attività di revisione possono comprendere anche ispezioni nei locali o nelle strutture fisiche del responsabile del trattamento e, se del caso, sono effettuate con un preavviso ragionevole.

(e) Su richiesta, le parti mettono a disposizione della o delle autorità di controllo competenti le informazioni di cui alla presente clausola, compresi i risultati di eventuali attività di revisione.

7.7. Ricorso a sub-responsabili del trattamento

(a) Il Responsabile del trattamento ha l'autorizzazione generale del titolare del trattamento per ricorrere a sub-responsabili del trattamento sulla base di un elenco concordato. Il Responsabile del trattamento informa specificamente per iscritto il titolare del trattamento di eventuali modifiche previste di tale elenco riguardanti l'aggiunta o la sostituzione di sub-responsabili del trattamento con un anticipo di almeno 30 giorni, dando così al titolare del trattamento tempo sufficiente per poter opporsi a tali modifiche prima del ricorso al o ai sub-responsabili del trattamento. Il responsabile del trattamento fornisce al titolare del trattamento le informazioni necessarie per consentirgli di esercitare il diritto di opposizione.

(b) Qualora il responsabile del trattamento ricorra a un sub-responsabile del trattamento per l'esecuzione di specifiche attività di trattamento (per conto del responsabile del trattamento), stipula un contratto che impone al sub-responsabile del trattamento, nella sostanza, gli stessi obblighi in materia di protezione dei dati imposti al responsabile del trattamento conformemente alle presenti clausole. Il responsabile del trattamento si assicura che il sub-

responsabile del trattamento rispetti gli obblighi cui il responsabile del trattamento è soggetto a norma delle presenti clausole e del regolamento (UE) 2016/679.

(c) Su richiesta del titolare del trattamento, il responsabile del trattamento gli fornisce copia del contratto stipulato con il sub-responsabile del trattamento e di ogni successiva modifica. Nella misura necessaria a proteggere segreti aziendali o altre informazioni riservate, compresi i dati personali, il responsabile del trattamento può espungere informazioni dal contratto prima di trasmetterne una copia.

(d) Il responsabile del trattamento rimane pienamente responsabile nei confronti del titolare del trattamento dell'adempimento degli obblighi del sub-responsabile del trattamento derivanti dal contratto che questi ha stipulato con il responsabile del trattamento. Il responsabile del trattamento notifica al titolare del trattamento qualunque inadempimento, da parte del sub-responsabile del trattamento, degli obblighi contrattuali.

(e) Il responsabile del trattamento concorda con il sub-responsabile del trattamento una clausola del terzo beneficiario secondo la quale, qualora il responsabile del trattamento sia scomparso di fatto, abbia giuridicamente cessato di esistere o sia divenuto insolvente, il titolare del trattamento ha diritto di risolvere il contratto con il sub-responsabile del trattamento e di imporre a quest'ultimo di cancellare o restituire i dati personali.

7.8. Trasferimenti internazionali

(a) Qualunque trasferimento di dati verso un paese terzo o un'organizzazione internazionale da parte del responsabile del trattamento è effettuato soltanto su istruzione documentata del titolare del trattamento o per adempiere a un requisito specifico a norma del diritto dell'Unione o degli Stati membri cui è soggetto il responsabile del trattamento, e nel rispetto del capo V del regolamento (UE) 2016/679.

(b) Il titolare del trattamento conviene che, qualora il responsabile del trattamento ricorra a un sub-responsabile del trattamento conformemente alla clausola 7.7 per l'esecuzione di specifiche attività di trattamento (per conto del titolare del trattamento) e tali attività di trattamento comportino il trasferimento di dati personali ai sensi del capo V del regolamento (UE) 2016/679, il responsabile del trattamento e il sub-responsabile del trattamento possono garantire il rispetto del capo V del regolamento (UE) 2016/679 utilizzando le clausole contrattuali tipo adottate dalla Commissione conformemente all'articolo 46, paragrafo 2, del regolamento (UE) 2016/679, purché le condizioni per l'uso di tali clausole contrattuali tipo siano soddisfatte.

Clausola 8 - Assistenza al titolare del trattamento

(a) Il responsabile del trattamento notifica prontamente al titolare del trattamento qualunque richiesta ricevuta dall'interessato. Non risponde egli stesso alla richiesta, a meno che sia stato autorizzato in tal senso dal titolare del trattamento.

(b) Il responsabile del trattamento assiste il titolare del trattamento nell'adempimento degli obblighi di rispondere alle richieste degli interessati per l'esercizio dei loro diritti, tenuto conto della natura del trattamento. Nell'adempiere agli obblighi di cui alle lettere a) e b), il responsabile del trattamento si attiene alle istruzioni del titolare del trattamento.

(c) Oltre all'obbligo di assistere il titolare del trattamento in conformità della clausola 8, lettera b), il responsabile del trattamento assiste il titolare del trattamento anche nel garantire il rispetto dei seguenti obblighi, tenuto conto della natura del trattamento dei dati e delle informazioni a disposizione del responsabile del trattamento:

(i) l'obbligo di effettuare una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali ("valutazione d'impatto sulla protezione dei dati") qualora un tipo di trattamento possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche;

(ii) l'obbligo, prima di procedere al trattamento, di consultare la o le autorità di controllo competenti qualora la valutazione d'impatto sulla protezione dei dati indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio;

(iii) l'obbligo di garantire che i dati personali siano esatti e aggiornati, informando senza indugio il titolare del trattamento qualora il responsabile del trattamento venga a conoscenza del fatto che i dati personali che sta trattando sono inesatti o obsoleti;

(iv) gli obblighi di cui all'articolo 32 regolamento (UE) 2016/679.

(d) Le parti stabiliscono nell'allegato III le misure tecniche e organizzative adeguate con cui il responsabile del trattamento è tenuto ad assistere il titolare del trattamento nell'applicazione della presente clausola, nonché l'ambito di applicazione e la portata dell'assistenza richiesta.

Clausola 9 - Notifica di una violazione dei dati personali

In caso di violazione dei dati personali, il responsabile del trattamento coopera con il titolare del trattamento e lo assiste nell'adempimento degli obblighi che incombono a quest'ultimo a norma degli articoli 33 e 34 del regolamento (UE) 2016/679, ove applicabile, tenuto conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento.

9.1 Violazione riguardante dati trattati dal titolare del trattamento

In caso di una violazione dei dati personali trattati dal titolare del trattamento, il responsabile del trattamento assiste il titolare del trattamento:

(a) nel notificare la violazione dei dati personali alla o alle autorità di controllo competenti, senza ingiustificato ritardo dopo che il titolare del trattamento ne è venuto a conoscenza, se del caso/(a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche);

(b) nell'ottenere le seguenti informazioni che, in conformità dell'articolo 33, paragrafo 3, del regolamento (UE) 2016/679, devono essere indicate nella notifica del titolare del trattamento e includere almeno:

(i) la natura 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 in questione;

(ii) le probabili conseguenze della violazione dei dati personali;

(iii) le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali, se del caso anche per attenuarne i possibili effetti negativi.
Qualora, e nella misura in cui, non sia possibile fornire tutte le informazioni contemporaneamente, la notifica iniziale contiene le informazioni disponibili in quel momento, e le altre informazioni sono fornite successivamente, non appena disponibili, senza ingiustificato ritardo.

(c) nell'adempiere, in conformità dell'articolo 34 del regolamento (UE) 2016/679 all'obbligo di comunicare senza ingiustificato ritardo la violazione dei dati personali all'interessato, qualora la violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

9.2 Violazione riguardante dati trattati dal responsabile del trattamento

In caso di una violazione dei dati personali trattati dal responsabile del trattamento, quest'ultimo ne dà notifica al titolare del trattamento senza ingiustificato ritardo dopo esserne venuto a conoscenza. La notifica contiene almeno:

(a) una descrizione della natura della violazione (compresi, ove possibile, le categorie e il numero approssimativo di interessati e di registrazioni dei dati in questione);

(b) i recapiti di un punto di contatto presso il quale possono essere ottenute maggiori informazioni sulla violazione dei dati personali;

(c) le probabili conseguenze della violazione dei dati personali e le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione, anche per attenuarne i possibili effetti negativi.

Qualora, e nella misura in cui, non sia possibile fornire tutte le informazioni contemporaneamente, la notifica iniziale contiene le informazioni disponibili in quel momento, e le altre informazioni sono fornite successivamente, non appena disponibili, senza ingiustificato ritardo.

Le parti stabiliscono nell'allegato III tutti gli altri elementi che il responsabile del trattamento è tenuto a fornire quando assiste il titolare del trattamento nell'adempimento degli obblighi che incombono al titolare del trattamento a norma degli articoli 33 e 34 del regolamento (UE) 2016/679.

SEZIONE III - DISPOSIZIONI FINALI

Clausola 10 - Inosservanza delle clausole e risoluzione

(a) Fatte salve le disposizioni del regolamento (UE) 2016/679, qualora il responsabile del trattamento violi gli obblighi che gli incombono a norma delle presenti clausole, il titolare del trattamento può dare istruzione al responsabile del trattamento di sospendere il trattamento dei dati personali fino a quando quest'ultimo non rispetti le presenti clausole o non sia risolto il contratto. Il responsabile del trattamento informa prontamente il titolare del trattamento qualora, per qualunque motivo, non sia in grado di rispettare le presenti clausole.

(b) Il titolare del trattamento ha diritto di risolvere il contratto per quanto riguarda il trattamento dei dati personali conformemente alle presenti clausole qualora:

(i) il trattamento dei dati personali da parte del responsabile del trattamento sia stato sospeso dal titolare del trattamento in conformità della lettera a) e il rispetto delle presenti clausole non sia ripristinato entro un termine ragionevole e in ogni caso entro un mese dalla sospensione;

(ii) il responsabile del trattamento violi in modo sostanziale o persistente le presenti clausole o gli obblighi che gli incombono a norma del regolamento (UE) 2016/679;

(iii) il responsabile del trattamento non rispetti una decisione vincolante di un organo giurisdizionale competente o della o delle autorità di controllo competenti per quanto riguarda i suoi obblighi in conformità delle presenti clausole o del regolamento (UE) 2016/679.

(c) Il responsabile del trattamento ha diritto di risolvere il contratto per quanto riguarda il trattamento dei dati personali a norma delle presenti clausole qualora, dopo aver informato il titolare del trattamento che le sue istruzioni violano i requisiti giuridici applicabili in conformità della clausola 7.1, lettera b), il titolare del trattamento insista sul rispetto delle istruzioni.

(d) Dopo la risoluzione del contratto il responsabile del trattamento, a scelta del titolare del trattamento, cancella tutti i dati personali trattati per conto del titolare del trattamento e certifica a quest'ultimo di averlo fatto, oppure restituisce al titolare del trattamento tutti i dati

personali e cancella le copie esistenti, a meno che il diritto dell'Unione o dello Stato membro non richieda la conservazione dei dati personali. Finché i dati non sono cancellati o restituiti, il responsabile del trattamento continua ad assicurare il rispetto delle presenti clausole.

ALLEGATO I - ELENCO DELLE PARTI

Titolare del trattamento	Il Licenziatario, così come generalizzato nell'Accordo di Licenza Software.
Responsabile del Trattamento	Il Licenziante, così come generalizzato nell'Accordo di Licenza Software. Indirizzo privacy dedicato per le comunicazioni relative alla presente nomina: info@optimens.it

ALLEGATO II - DESCRIZIONE DEL TRATTAMENTO

II.1 - Finalità del trattamento, categorie di interessati e dati trattati da parte del Responsabile del trattamento per conto del Titolare del trattamento

La finalità del trattamento è la fornitura del nostro servizio e le funzionalità in essa contenute come descritte nei Termini e Condizioni in cui il presente DPA è allegato.

Finalità Erogazione del servizio Calliope

Attività

Registrazione account, Creazione profilo admin, Creazione profilo operatore, Creazione profilo utenti, Assegnazione dei test agli utenti finali, Analisi statistica

Categorie di interessati e dati trattati

Interessato	Categorie di dati personali	Categoria speciale di dati	Esempi di dati trattati
Calliope - Cliente (Azienda)	Identificativi - Informazioni Personali	No	Indirizzo email
			Nome e cognome del rappresentante legale
			Residenza/domicilio
	Indentificativi - Finanziari	No	Metodo e modalità di pagamento
Calliope - Operatore	Identificativi - Informazioni Personali	No	Cognome
			Mail
			Nome
			Telefono
Calliope - Utente	Dati comuni - Caratteristiche personali	No	Genere
	Identificativi - Informazioni Personali	No	Cognome
			Data di nascita
			Età

Interessato	Categorie di dati personali	Categoria speciale di dati	Esempi di dati trattati
			Indirizzo
			Nome
			Telefono
			Telefono secondario
	Dati relativi alla salute	Sì	Livello efficienza cognitiva
			Risposte alle domande dei questionari
			Trend e andamento cognitivo generale
	Dati Particolari - Altri	Sì	Note rilevanti

Il Responsabile del trattamento tratta i dati personali nella misura necessaria a fornire i propri Servizi.

II.2 Il trattamento dei dati personali da parte del Responsabile del trattamento per conto del Titolare ha la seguente durata e frequenza:

I trattamenti effettuati in qualità di Responsabile del trattamento avranno la stessa durata e frequenza del Contratto concluso tra le Parti.

II.3 Altre disposizioni in merito al trattamento dei dati personali degli Utenti e del Titolare del trattamento.

Il Responsabile del trattamento potrà trattare dati personali resi anonimi in modo tale da non consentire più l'identificazione, diretta o indiretta, degli interessati. Tali dati anonimizzati potranno essere utilizzati dal Responsabile esclusivamente per finalità di ricerca scientifica e statistica, nel rispetto dei principi di liceità, correttezza e trasparenza, nonché delle misure tecniche e organizzative adeguate atte a garantire l'irreversibilità del processo di anonimizzazione.

Il Responsabile si impegna a:

- non tentare in alcun modo di re-identificare gli interessati;
- adottare idonee misure di sicurezza volte a prevenire rischi di re-identificazione o accessi non autorizzati.

Poiché l'attività di de-identificazione richiede il trattamento di dati personali relativi a interessati identificabili, il Responsabile del trattamento, agendo per finalità proprie, opererà come Titolare del trattamento.

Il Responsabile del trattamento, insieme al Cliente provvederanno ad informare gli interessati utilizzando i mezzi più idonei.

ALLEGATO III - MISURE TECNICHE E ORGANIZZATIVE PER GARANTIRE LA SICUREZZA DEI DATI

[Company]

Organisational Security Measures

Documentazione

[Data Subject] Calliope - Cliente (Azienda)

L'azienda ha già reso disponibile un'informativa sulla privacy per il progetto per questo interessato.

Sicurezza fisica e ambientale

L'azienda adotta misure di sicurezza fisica e ambientale per proteggere le aree dove vengono trattati dati protetti o informazioni critiche.
L'azienda adotta misure di sicurezza fisica e ambientale per proteggere il luogo di lavoro da calamità naturali, attacchi dolosi o incidenti.
L'azienda conserva registri per documentare le riparazioni e le modifiche apportate ai componenti di sicurezza fisica della propria struttura.
L'azienda ha definito delle procedure di emergenza per i propri locali fisici.

[Product] Calliope

Organisational Security Measures

Documentazione

Per le attività svolte in qualità di Titolare, l'azienda ha predisposto una sezione nel RoPA in cui vengono mappate le attività di trattamento relative al progetto analizzato.
Per le attività svolte in qualità di Responsabile del trattamento, l'azienda ha predisposto una sezione nel RoPA in cui sono elencate tutte le attività di trattamento svolte per conto dei Titolari del trattamento.
[Data Subject] Calliope - Operatore

L'azienda ha già reso disponibile un'informativa sulla privacy per il progetto per questo interessato.
[Data Subject] Calliope - Cliente (Azienda)

L'azienda ha già reso disponibile un'informativa sulla privacy per il progetto per questo interessato.

Technical Security Measures

Technological Controls

Crittografia di rete

Tutte le comunicazioni tra l'applicazione e il backend crittografate utilizzano almeno il TLS 1.3.
In caso di trasferimento di dati protetti a provider esterni, l'azienda ne garantisce la crittografia durante il transito.
L'azienda utilizza protcolli DNS sicuri su tutti gli endpoint e trasferimenti di dati.

Sicurezza degli endpoint

L'azienda garantisce che gli URL delle API non contengano mai informazioni sensibili, come chiavi API e token di sessione.

Controllo di sicurezza del sistema IT

L'autenticazione dell'applicazione è gestita nel backend.

Gestione dello sviluppo

Attualmente l'azienda sta verificando attivamente gli strumenti di sviluppo utilizzando l'elenco CVE.
L'azienda garantisce l'utilizzo di password complesse per l'accesso a tutti gli strumenti di sviluppo software e al codice base.

Ambiente di sviluppo

L'azienda applica la separazione degli ambienti tra test, staging e produzione.
L'azienda garantisce che tutte le password per gli accessi di provider terzi siano complesse.

Qualità del codice

L'azienda esamina regolarmente tutto il codice per individuare eventuali bug.

Controlli di sicurezza delle applicazioni

Il testo nelle caselle di inserimento di password viene oscurato usando asterischi o simili.
Il dominio esterno è fornito da una terza parte affidabile.
Il percorso locale dell'applicazione è nascosto.

Test dell'applicazione

L'azienda garantisce che vengano eseguiti test sufficienti su scenari di utilizzo reali e su estensioni e adattamenti sviluppati prima che questi vengano messi in produzione.

Controllo degli accessi alle infrastrutture

[Architectural Component] [A] Login Amministrativo Cloud

Gli accessi come superuser, root, con privilegi o admin sono limitati in modo specifico.
L'azienda assegna gli account con privilegi a individui specifici e identificabili.
L'azienda impedisce l'escalation dei ruoli su tutti i server e le workstation.

Gestione dell'autenticazione

[Architectural Component] [F] Autenticazione Utenti

L'Azienda impone l'autenticazione per tutti i dati non pubblici.
L'Azienda utilizza il framework di Supabase per l'autenticazione degli utenti.
Tutti i dati di autenticazione degli utenti vengono conservati in modo sicuro dal sistema crittografico di Supabase.
L'azienda testa i flussi di accesso, assicurandosi che l'autenticazione e l'autorizzazione vengano eseguite correttamente.

[Architectural Component] [A] Login Amministrativo Cloud

Tutti i dati di autenticazione degli utenti admin vengono conservati in modo sicuro.
L'azienda testa i flussi di accesso, assicurandosi che l'autenticazione e l'autorizzazione vengano eseguite correttamente.

Gestione della sessione

[Architectural Component] [F] Autenticazione Utenti

Il backend/endpoint API gestito da Bubble genera identificatori di sessione casuali con entropia sufficiente e tramite procedure stabilite.
Il token di sessione viene firmato utilizzando un algoritmo sicuro.
Quando un utente si disconnette, tutte le sessioni esistenti vengono terminate dall'endpoint.
È garantito che una sessione una volta invalidata non possa essere riattivata anche se sono noti i dati della singola sessione.
L'Azienda garantisce che l'utente possa uscire dalla sessione e invalidarla esplicitamente.

Diritti di accesso all'applicazione e login

[Architectural Component] [F] Autenticazione Utenti

L'Azienda garantisce che gli utenti dispongano di diritti di accesso e permessi in linea con le loro attività e ruoli, nel rispetto dei principi di "need-to-know" e di "minimo privilegio".
Ogni utente ha un identificativo di accesso univoco.

Gestione delle password

[Architectural Component] [F] Autenticazione Utenti

L'applicazione impone l'uso di una password per accedervi.
L'Azienda ha messo in atto meccanismi aggiuntivi per rendere più difficile indovinare i parametri di accesso.
Viene garantito che le password non vengano mai trasmesse o memorizzate in chiaro.

[Architectural Component] [A] Login Amministrativo Cloud

L'applicazione impone l'uso di una password per accedervi.

Errori di accesso e avvisi

[Architectural Component] [F] Autenticazione Utenti

Tutti gli errori o malfunzionamenti del sistema di controllo degli accessi comportano il rifiuto dell'accesso.

[Architectural Component] [A] Login Amministrativo Cloud

Tutti gli errori o malfunzionamenti del sistema di controllo degli accessi comportano il rifiuto dell'accesso.

Minimizzazione dei dati

L'applicazione prevede fin dalla progettazione la minimizzazione dei dati personali.
L'Azienda si assicura di ridurre al minimo le duplicazioni inutili di dati all'interno dei sistemi.

Qualità e integrità dei dati

Viene garantito che tutti gli aggiornamenti dei dati vengano immediatamente propagati a tutti i sistemi che ne hanno bisogno.

3rd parties - Technical controls

Standard di sicurezza dichiarato

L'azienda ha scelto i fornitori terzi verificando che siano in grado di fornire un livello di servizio adeguato.
L'azienda verifica che i fornitori terzi offrano garanzie in merito ai trasferimenti di dati al di fuori dell'UE.

[Data recipient] Supabase, Inc.

L'azienda verifica che il fornitore dei servizi cloud implementi una protezione contro malware, DDoS e altre forme di traffico indesiderato.
L'azienda verifica che il fornitore di servizi cloud fornisca garanzie scritte riguardo alla protezione da accessi non autorizzati al data centre.
[Data recipient] Bubble Group, Inc.

L'azienda verifica che il fornitore di servizi cloud fornisca garanzie scritte riguardo alla protezione da accessi non autorizzati al data centre.

Livello di servizio

[Data recipient] Supabase, Inc.

L'azienda garantisce che i suoi fornitori terzi non imporranno limiti di servizio che possano influire negativamente sull'applicazione.
L'azienda ha testato la latenza massima per tutti i fornitori terzi e ha verificato che siano accettabili per i requisiti dell'applicazione.
I limiti di archiviazione dei dati sono stati verificati e sono risultati adeguati alle esigenze attuali e future dell'applicazione.
L'azienda verifica se gli SLA/MSA/BAA indicati nei contratti con i fornitori terzi soddisfano le sue esigenze operative.
I fornitori terzi garantiscono che i dati personali verranno eliminati definitivamente dagli stessi e dai loro sub-responsabili al momento della cessazione del servizio o su richiesta diretta.

[Data recipient] Bubble Group, Inc.

L'azienda ha testato la latenza massima per tutti i fornitori terzi e ha verificato che siano accettabili per i requisiti dell'applicazione.
I limiti di archiviazione dei dati sono stati verificati e sono risultati adeguati alle esigenze attuali e future dell'applicazione.
L'azienda verifica se gli SLA/MSA/BAA indicati nei contratti con i fornitori terzi soddisfano le sue esigenze operative.
I fornitori terzi garantiscono che i dati personali verranno eliminati definitivamente dagli stessi e dai loro sub-responsabili al momento della cessazione del servizio o su richiesta diretta.

Continuità aziendale di terze parti

[Data recipient] Supabase, Inc.

L'azienda ha accesso a una copia dei piani di Ripristino in caso di emergenza dei fornitori terzi utilizzati per la soluzione software.

ALLEGATO IV - ELENCO DEI SUB-RESPONSABILI DEL TRATTAMENTO

(Sub)re-sponsabili	Luoghi del trat-tamento	Attività	Interessato	Categoria di dati
Bubble Group, Inc.	EEA (Area Economica Europea)	Analisi stat-istica	Calliope - Utente	Dati comuni - Caratteristiche person-ali
				Identificativi - Informazioni Personali
				Dati relativi alla salute
	EEA (Area Economica Europea)	Asseg-nazione dei test agli utenti finali	Calliope - Utente	Identificativi - Informazioni Personali
				Dati relativi alla salute
				Dati Particolari - Altri
	EEA (Area Economica Europea)	Creazione profilo ad-min	Calliope - Operatore	Identificativi - Informazioni Personali
	EEA (Area Economica Europea)	Creazione profilo op-eratore	Calliope - Operatore	Identificativi - Informazioni Personali
	EEA (Area Economica Europea), Singapore, Stati Uniti d'America (senza Data Privacy Frame-work), Stati Uniti d'America (Data Privacy Framework)	Creazione profilo utenti	Calliope - Utente	Dati comuni - Caratteristiche person-ali
				Identificativi - Informazioni Personali
				Dati Particolari - Altri
Hetzner Online GmbH - Cloud	EEA (Area Economica Europea)	Analisi stat-istica	Calliope - Utente	Dati comuni - Caratteristiche person-ali
				Identificativi - Informazioni Personali

(Sub)re-sponsabili	Luoghi del trat-tamento	Attività	Interessato	Categoria di dati
				Dati relativi alla salute
	EEA (Area Economica Europea)	Asseg-nazione dei test agli utenti finali	Calliope - Utente	Identificativi - Informazioni Personali
				Dati relativi alla salute
				Dati Particolari - Altri
	EEA (Area Economica Europea)	Creazione profilo ad-min	Calliope - Operatore	Identificativi - Informazioni Personali
	EEA (Area Economica Europea)	Creazione profilo op-eratore	Calliope - Operatore	Identificativi - Informazioni Personali
	EEA (Area Economica Europea), Singapore, Stati Uniti d'America (senza Data Privacy Frame-work), Stati Uniti d'America (Data Privacy Framework)	Creazione profilo utenti	Calliope - Utente	Dati comuni - Caratteristiche person-ali
				Identificativi - Informazioni Personali
				Dati Particolari - Altri
	EEA (Area Economica Europea)	Regis-trazione ac-count	Calliope - Cliente (Azienda)	Identificativi - Informazioni Personali
				Indentificativi - Finanziari
			Calliope - Operatore	Identificativi - Informazioni Personali
n8n GmbH	EEA (Area Economica Europea)	Analisi stat-istica	Calliope - Utente	Dati comuni - Caratteristiche person-ali
				Identificativi - Informazioni Personali
				Dati relativi alla salute

(Sub)re-sponsabili	Luoghi del trat-tamento	Attività	Interessato	Categoria di dati
	EEA (Area Economica Europea)	Asseg-nazione dei test agli utenti finali	Calliope - Utente	Identificativi - Informazioni Personali
				Dati relativi alla salute
				Dati Particolari - Altri
	EEA (Area Economica Europea)	Creazione profilo ad-min	Calliope - Operatore	Identificativi - Informazioni Personali
	EEA (Area Economica Europea)	Creazione profilo op-eratore	Calliope - Operatore	Identificativi - Informazioni Personali
	EEA (Area Economica Europea), Singapore, Stati Uniti d'America (senza Data Privacy Frame-work), Stati Uniti d'America (Data Privacy Framework)	Creazione profilo utenti	Calliope - Utente	Dati comuni - Caratteristiche person-ali
				Identificativi - Informazioni Personali
				Dati Particolari - Altri
	EEA (Area Economica Europea)	Regis-trazione ac-count	Calliope - Cliente (Azienda)	Identificativi - Informazioni Personali
				Indentificativi - Finanziari
			Calliope - Operatore	Identificativi - Informazioni Personali
Supabase, Inc.	EEA (Area Economica Europea)	Analisi stat-istica	Calliope - Utente	Dati comuni - Caratteristiche person-ali
				Identificativi - Informazioni Personali
				Dati relativi alla salute
		Asseg-nazione dei	Calliope - Utente	Identificativi - Informazioni Personali

(Sub)re-sponsabili	Luoghi del trat-tamento	Attività	Interessato	Categoria di dati
	EEA (Area Economica Europea)	test agli utenti finali		
				Dati relativi alla salute
				Dati Particolari - Altri
	EEA (Area Economica Europea)	Creazione profilo ad-min	Calliope - Operatore	Identificativi - Informazioni Personali
	EEA (Area Economica Europea)	Creazione profilo op-eratore	Calliope - Operatore	Identificativi - Informazioni Personali
	EEA (Area Economica Europea), Singapore, Stati Uniti d'America (senza Data Privacy Frame-work), Stati Uniti d'America (Data Privacy Framework)	Creazione profilo utenti	Calliope - Utente	Dati comuni - Caratteristiche person-ali
				Identificativi - Informazioni Personali
				Dati Particolari - Altri
	EEA (Area Economica Europea)	Regis-trazione ac-count	Calliope - Cliente (Azienda)	Identificativi - Informazioni Personali
				Indentificativi - Finanziari
			Calliope - Operatore	Identificativi - Informazioni Personali