xatla AG Software aziendale
Dorfmattweg 8a | 3110 Münsingen
+41 31 331 01 01 | info@xatla.ch

Accordo sul trattamento dei dati

1 Oggetto

Il presente contratto disciplina i diritti e gli obblighi di xatla AG in qualità di incaricata e del committente, un cliente di xatla AG (di seguito denominati congiuntamente le «Parti») in relazione al trattamento dei dati in conformità con la normativa sulla protezione dei dati o al trattamento dei dati su incarico (di seguito denominati collettivamente «trattamento su incarico») di dati personali (di seguito denominati collettivamente «dati personali»).

Con il presente contratto, la contraente consente al committente di ottemperare ai requisiti applicabili in materia di protezione dei dati per il trattamento per conto di terzi.

Il presente contratto si applica a tutte le attività in cui il contraente tratta o fa trattare, in tutto o in parte, dati personali per conto del committente (di seguito denominato in modo univoco «trattamento»).

Il contraente è soggetto alla legislazione svizzera in materia di protezione dei dati, in particolare alla legge federale sulla protezione dei dati (LPD). Con decisione del 26 luglio 2000, la Commissione europea ha stabilito che la legislazione svizzera in materia di protezione dei dati garantisce un livello adeguato di protezione dei dati personali. Tale constatazione è considerata una decisione di adeguatezza ai sensi dell'art. 45 cpv. 1 del Regolamento generale sulla protezione dei dati (RGPD).

2 Natura, oggetto e finalità del trattamento per conto di terzi

Il trattamento su incarico avviene in conformità agli accordi contrattuali esistenti o da stipulare tra le parti, in particolare alle Condizioni Generali di Contratto (CGC). Le disposizioni del presente contratto prevalgono in caso di contraddizione tra le disposizioni del presente contratto e altri accordi contrattuali tra le parti.

Il trattamento su commissione comprende qualsiasi trattamento di dati personali, indipendentemente dai mezzi e dalle procedure utilizzati, in particolare la consultazione, il confronto, l'adeguamento, l'archiviazione, la conservazione, la lettura, la comunicazione, l'acquisizione, la limitazione, la registrazione, la raccolta, la cancellazione, la divulgazione, l'ordinamento, l'organizzazione, la memorizzazione, la modifica, il collegamento, la distruzione e l'utilizzo di dati personali. I dati personali sono tutte le informazioni che si riferiscono a una persona fisica identificata o identificabile, i cui dati vengono trattati.

Il trattamento su incarico comprende le categorie di dati personali di cui **all'allegato 1**.

Il trattamento su incarico comprende le categorie di persone interessate i cui dati personali vengono trattati, conformemente **all'allegato 2**.

3 Obblighi delle parti

3.1 Istruzioni e limitazione delle finalità

Il contraente tratta i dati personali esclusivamente per lo scopo o gli scopi previsti dagli accordi contrattuali tra le parti o secondo le istruzioni documentate del committente, a meno che il contraente non sia obbligato per legge o per regolamento a un determinato trattamento. Il committente può impartire ulteriori istruzioni documentate durante l'intera durata del trattamento su incarico.

Il contraente informa il committente qualora non sia in grado di eseguire, in tutto o in parte, un'istruzione impartita. Il contraente informa il committente qualora ritenga che gli accordi contrattuali o le istruzioni impartite violino i requisiti applicabili in materia di protezione dei dati.

3.2 Sicurezza

Il contraente adotta almeno le misure tecniche e organizzative (TOM) appropriate di cui **all'allegato 3** per garantire una sicurezza adeguata al rischio dei dati personali trattati (di seguito «sicurezza dei dati»). Tali misure comprendono in particolare la protezione dei dati personali trattati, compresi, se del caso, i dati personali particolarmente sensibili, da una violazione della sicurezza dei dati.

12 Il contraente concede ai propri ausiliari l'accesso ai dati personali del committente solo nella misura in cui tale accesso sia necessario per l'esecuzione, la sorveglianza e la gestione del presente contratto. Il contraente garantisce che le persone autorizzate al trattamento dei dati si siano impegnate a mantenere il segreto o siano soggette a un adeguato obbligo legale di riservatezza.

3.3 Documentazione e possibilità di verifica

Le parti devono essere in grado di dimostrare il rispetto del presente contratto.

Il contraente elabora in modo adeguato e il più tempestivamente possibile le richieste del committente relative al trattamento dei dati ai sensi del presente contratto.

Su richiesta, il contraente mette a disposizione del committente tutte le informazioni disponibili necessarie per dimostrare il rispetto dei requisiti stabiliti nel presente contratto e derivanti direttamente dalle disposizioni applicabili in materia di protezione dei dati.

Su richiesta, il contraente consente al committente di verificare il trattamento dei dati ai sensi del presente contratto a intervalli adeguati o in presenza di indizi documentati di inadempienza.

Il committente può effettuare tale verifica autonomamente o farla eseguire da un revisore indipendente. Tali verifiche sono limitate a un giorno per anno solare. Una verifica può comprendere anche ispezioni presso le strutture fisiche o i locali del contraente, a condizione che tali ispezioni siano necessarie, si svolgano durante il normale orario di lavoro senza interferire con il regolare svolgimento delle attività e che la notifica avvenga con un preavviso adeguato. Tali ispezioni sono inoltre ammesse solo se e nella misura in cui la verifica non possa essere effettuata mediante prove adeguate, quali ad esempio conferme, documentazione e certificati o attestazioni, in particolare nel caso dei centri di calcolo.

Il committente si fa carico dei costi sostenuti dal contraente per tali verifiche.

Le parti mettono a disposizione di un'autorità di vigilanza competente, o delle autorità di vigilanza competenti, le informazioni di cui sopra, compresi i risultati delle verifiche, su richiesta, a meno che la messa a disposizione non sia vietata per motivi legali.

4 Trattamento in subappalto

Il committente concede al contraente l'autorizzazione generale a incaricare i subappaltatori elencati **nell'allegato 4**.

Il contraente informa il committente con almeno 30 giorni di anticipo, in forma elettronica o scritta, di tutte le modifiche previste a tale elenco mediante la sostituzione o l'aggiunta di subappaltatori. Il contraente concede così al committente tempo sufficiente per poter sollevare eventuali obiezioni alle modifiche previste prima dell'incarico.

In assenza di opposizione entro il termine previsto, le modifiche previste si considerano approvate. Qualora, in caso di opposizione, non sia possibile raggiungere un accordo tra le parti in merito alle modifiche previste e il Committente non sia disposto a rinunciare alla propria opposizione, le parti hanno il diritto di recedere dal presente contratto in via straordinaria con effetto dalla data delle modifiche previste.

Il contraente deve imporre contrattualmente ai subappaltatori incaricati dell'esecuzione del trattamento del commissionario sostanzialmente gli stessi obblighi che si applicano al contraente ai sensi del presente contratto. Il contraente garantisce che ogni subappaltatore adempia agli obblighi a cui il contraente è soggetto ai sensi del presente contratto e dei requisiti applicabili in materia di protezione dei dati.

5 Esportazione di dati personali

Qualsiasi esportazione di dati personali verso un Paese al di fuori della Svizzera e degli Stati membri dello Spazio economico europeo (SEE) o verso un'organizzazione internazionale avviene esclusivamente secondo quanto concordato contrattualmente o in conformità alle istruzioni documentate del committente, a meno che il contraente non sia tenuto per legge a effettuare una determinata esportazione di dati. In tal caso, il contraente informa il committente di tale obbligo legale, a meno che tale informazione non sia vietata per motivi di legge.

Ogni esportazione di dati personali in un paese al di fuori della Svizzera e degli Stati membri del SEE avviene in linea di principio esclusivamente se la legislazione sulla protezione dei dati nel paese in questione garantisce, secondo l'Incaricato federale della protezione dei dati e della trasparenza (IFPDT) o il Consiglio federale svizzero, un livello adeguato di protezione dei dati personali.

L'esportazione di dati personali in un paese al di fuori della Svizzera e degli Stati membri del SEE, la cui legislazione in materia di protezione dei dati non garantisca un livello adeguato di protezione dei dati personali, può avvenire in via eccezionale se, per altri motivi, è garantito un livello di protezione adeguato secondo i requisiti applicabili in materia di protezione dei dati, in particolare in base ad accordi interstatali o sulla base delle clausole contrattuali standard vigenti emanate dalla Commissione europea. Il contraente è autorizzato ad adattare e integrare tali clausole contrattuali standard europee secondo le raccomandazioni dell'IFPDT, in modo che le clausole contrattuali standard corrispondano anche ai requisiti applicabili in materia di protezione dei dati in Svizzera e siano quindi idonee a garantire un livello adeguato di protezione dei dati in caso di esportazione di dati dalla Svizzera.

L'incarico conferito a Nylas Inc., USA, in qualità di subappaltatore del trattamento dei dati avviene in applicazione delle clausole standard di protezione dei dati della Commissione Europea, conformemente alle raccomandazioni dell'Incaricato federale della protezione dei dati e della trasparenza (IFPDT). Una copia delle garanzie vigenti può essere messa a disposizione su richiesta.

6 Assistenza al committente

Il contraente informa immediatamente il committente di ogni richiesta in materia di protezione dei dati che ha ricevuto da un interessato e che riguarda il trattamento per conto di terzi. Il contraente ha il diritto di confermare all'interessato la ricezione della richiesta, ma non risponde direttamente alla stessa, a meno che non sia stato incaricato dal committente.

Il contraente assiste il committente, tenendo conto della natura del trattamento per conto di terzi, nell'adempimento del suo obbligo di rispondere alle richieste in materia di protezione dei dati presentate dagli interessati.

Il contraente assiste inoltre il committente, tenendo conto della natura del trattamento dei dati e delle informazioni disponibili, nell'adempimento dei seguenti obblighi:

- tenuta di un eventuale registro delle attività di trattamento;
- effettuazione di una valutazione d'impatto sulla protezione dei dati, qualora un trattamento previsto di dati personali da parte del committente possa presumibilmente comportare un rischio elevato per i diritti fondamentali o la personalità degli interessati;
- consultazione dell'autorità o delle autorità di controllo competenti prima del trattamento dei dati personali, qualora una valutazione d'impatto sulla protezione dei dati indichi che il trattamento previsto comporta un rischio elevato per i diritti fondamentali o la personalità degli interessati, nonostante le misure previste.

Il committente si fa carico dei costi sostenuti dal contraente per tale assistenza.

7 Segnalazione di violazioni della sicurezza dei dati

In caso di violazione della sicurezza dei dati, la contraente collabora con la committente. Il contraente assiste il committente nell'adempimento dei suoi obblighi di notifica delle violazioni della sicurezza dei dati all'autorità o alle autorità di controllo competenti o di informazione delle persone interessate dalle violazioni della sicurezza dei dati, tenendo conto della natura del trattamento per conto di terzi e delle informazioni a sua disposizione.

Il committente si fa carico dei costi sostenuti dal contraente per tale assistenza.

8 Sospensione del trattamento dei dati

Nel caso in cui il contraente non adempia ai propri obblighi ai sensi del presente contratto, il committente può ordinare al contraente di sospendere il trattamento dei dati fino a quando il contraente non si conformi al presente contratto o fino alla risoluzione del presente contratto. Il contraente informa immediatamente il committente qualora, per qualsiasi motivo, non sia in grado di rispettare il presente contratto.

9 Responsabilità

La responsabilità è regolata da un'eventuale clausola di responsabilità ai sensi degli accordi contrattuali tra le parti.

10 Durata e risoluzione

Il contraente tratta i dati personali a tempo indeterminato fino alla risoluzione dell'ultimo accordo contrattuale tra le parti relativo al trattamento dei dati.

Il committente ha il diritto di recedere dal presente contratto in via straordinaria e senza preavviso qualora:

- il committente ha sospeso il trattamento dei dati per conto di terzi e il rispetto del presente contratto non è stato ripristinato entro un termine ragionevole, in ogni caso non oltre un mese dalla sospensione;
- il contraente violi in misura significativa o in modo continuativo il presente contratto o non soddisfi i requisiti applicabili in materia di protezione dei dati;
- il contraente non ottemperi alla decisione vincolante di un'autorità di controllo competente o di un tribunale competente, avente per oggetto gli obblighi del contraente ai sensi dei requisiti applicabili in materia di protezione dei dati.

Il contraente ha il diritto di recedere dal presente contratto in via straordinaria e senza preavviso qualora il committente insista sull'adempimento di un accordo contrattuale o di una direttiva dopo essere stato informato dal contraente che l'accordo contrattuale o la direttiva violano i requisiti applicabili in materia di protezione dei dati.

Alla cessazione del presente contratto, il contraente cancella tutti i dati personali trattati per conto del committente, a meno che il contraente non sia autorizzato o obbligato per legge o per regolamento a conservare i dati personali. Fino alla cancellazione dei dati personali, il contraente garantisce il rispetto del presente contratto.

11 Disposizioni finali

Il presente contratto può essere stipulato in forma elettronica o scritta. Le modifiche al presente contratto possono essere apportate in forma elettronica.

Le parti si informano reciprocamente in merito a un eventuale consulente per la protezione dei dati o a un eventuale responsabile della protezione dei dati, conformemente ai requisiti applicabili in materia di protezione dei dati.

Le parti sono tenute a trattare in modo riservato e a lungo termine tutte le informazioni relative ai segreti commerciali dell'altra parte e ai dati personali acquisite nell'ambito del presente contratto, anche dopo la sua cessazione, a meno che una parte non sia tenuta per legge a una determinata divulgazione. In tal caso, la parte obbligata informa l'altra parte di tale obbligo legale, a condizione che, fintantoché e nella misura in cui tale informazione non sia vietata per motivi legali. Qualora una parte nutra dubbi sul fatto che un'informazione sia soggetta a tale obbligo di riservatezza, l'informazione deve essere trattata in modo riservato fino all'esplicita autorizzazione da parte dell'altra parte.

Qualora singole disposizioni del presente contratto risultassero inapplicabili, invalide o inefficaci, ciò non pregiudica l'applicabilità, la validità o l'efficacia delle restanti disposizioni e le parti sostituiranno la singola disposizione con una disposizione applicabile, valida o efficace che si avvicini il più possibile al risultato auspicato in materia di protezione dei dati della singola disposizione.

Il presente contratto è regolato esclusivamente dal diritto svizzero. Sono escluse le norme di conflitto di leggi e la Convenzione delle Nazioni Unite sui contratti di vendita internazionale di beni mobili. Il foro competente esclusivo è quello della sede del contraente.

Allegato 1 – Categorie di dati personali trattati

Il committente determina e controlla, a propria discrezione e sotto la propria responsabilità, quali categorie di dati personali vengono trattate. Il trattamento su incarico può comprendere in particolare le seguenti categorie di dati personali:

- Dati relativi all'assunzione
- Dati relativi al trattamento
- Metadati delle e-mail (ad es. mittente, destinatario, oggetto, data e ora, ecc.)
- Dati relativi alla sfera privata
- Dati relativi alla situazione previdenziale
- Dati relativi alla diagnosi
- Dati sanitari
- Dati relativi ai contenuti
- Dati relativi al calendario (ad es. ora, luogo, titolo e partecipanti agli appuntamenti, ecc.)
- Dati relativi alla comunicazione (ad es. contenuti delle e-mail, registrazioni delle chat, ecc.)
- Dati di contatto
- Dati sui farmaci
- Dati di utilizzo
- Dati relativi alle reazioni
- Dati anagrafici
- Dati relativi alla descrizione dei sintomi
- Dati relativi agli appuntamenti
- Dati relativi alle prescrizioni
- Dati assicurativi
- Dati contrattuali
- Dati relativi ai pagamenti
- Dati di accesso a sistemi collegati (ad es. token API, dati di autenticazione, ecc.)

xatla AG Software aziendale
Dorfmattweg 8a | 3110 Münsingen
+41 31 331 01 01 | info@xatla.ch

Allegato 2 – Categorie di interessati i cui dati personali vengono trattati

Il committente determina e controlla, a propria discrezione e sotto la propria responsabilità, le categorie di interessati i cui dati personali vengono trattati. Il trattamento per conto di terzi può comprendere in particolare le seguenti categorie di dati personali:

- Referenti
- Referenti
- Fornitori di servizi
- Contatti esterni provenienti da piattaforme o servizi collegati
- Strutture sanitarie
- Partner commerciali
- Persone interessate
- Clienti
- Partner di comunicazione (ad es. contatti e-mail o calendario)
- Fornitori
- Collaboratori
- Utenti
- Pazienti

Allegato 3 – Misure tecniche e organizzative (TOM)

Le misure tecniche e organizzative (TOM) volte a garantire la protezione e la sicurezza dei dati personali trattati sono suddivise: il contraente, in qualità di produttore, mette a disposizione l'applicazione ed è responsabile della sicurezza del software e del database. L'infrastruttura di base e l'ambiente operativo sono forniti da ServerBase AG, Svizzera, in qualità di fornitore di servizi di hosting.

Il contraente, in qualità di PMI svizzera agile, è specializzato nello sviluppo di applicazioni e, pur non disponendo intenzionalmente di certificazioni ISO proprie e separate, garantisce un elevato livello di protezione dei dati grazie a un approccio professionale e alla selezione mirata di partner certificati. Esso garantisce che ServerBase AG rispetti tutte le misure necessarie in conformità con i requisiti vigenti in materia di protezione dei dati. Le misure più importanti comprendono:

1. **Sicurezza delle applicazioni e dei database (responsabilità del contraente)**
    1. **Pentest:** il framework software utilizzato dal contraente viene sottoposto a test di penetrazione (analisi delle vulnerabilità di sicurezza) da parte di specialisti esterni.
    2. **Aggiornamento continuo**: l'applicazione viene costantemente sottoposta a manutenzione dal contraente e dotata delle patch di sicurezza più recenti.
    3. **Monitoraggio proattivo:** monitoraggio continuo delle prestazioni dell'applicazione e del server SQL per individuare immediatamente anomalie o tentativi di accesso non autorizzati.
    4. **Separazione crittografica e crittografia (at rest):** i file memorizzati su disco e i campi di dati sensibili all'interno del database vengono salvati in modo crittografato di default. La decrittografia è strettamente limitata alla rispettiva chiave organizzativa. Questa chiave organizzativa è a sua volta crittografata con la chiave utente individuale. Un accesso diretto a livello di tabella è tecnicamente impossibile senza la sessione attiva dell'utente e i dati rimangono illeggibili.
2. **Protezione avanzata perimetrale e difesa informatica (Myra Security)**
   Myra è collegata direttamente a monte dell'applicazione come schermo di protezione specializzato a tre livelli (HTTP/S-Reverse-Proxy). Il filtraggio avviene secondo le linee guida del GDPR dell'UE. Ciò comprende:
    1. **Web Application Firewall (WAF) hyperscale:** filtraggio continuo del traffico a livello di contenuto per colmare le lacune di sicurezza e respingere gli attacchi secondo l'OWASP Top 10 (ad es. SQL injection, Cross-Site Scripting [XSS], Directory Traversal).
    2. **Protezione DDoS e bot:** filtraggio permanente e trasparente dei flussi di traffico dannosi (attacchi basati su volume, infrastruttura e applicazioni). Grazie all'utilizzo della piattaforma Myra, lo scudo protettivo è progettato in modo flessibile e altamente scalabile per respingere efficacemente anche attacchi di grandi volumi prima che raggiungano l'infrastruttura di hosting.
    3. **Multi Site Load Balancer:** distribuzione intelligente del carico del traffico in entrata sull'infrastruttura. Il rilevamento integrato dei guasti (*Dead Backend Detection / Site Fail Over*) assicura che i server temporaneamente non raggiungibili vengano automaticamente bypassati, al fine di garantire l'alta disponibilità (SLA di almeno il 99,9%).
    4. **Gestione automatizzata dei certificati:** trasmissione sicura dei dati grazie all'uso obbligatorio del protocollo HTTPS, alla Perfect Forward Secrecy (PFS) come standard, al supporto HSTS, nonché all'emissione completamente

automatizzata e al rinnovo tempestivo dei certificati TLS/SSL per evitare vulnerabilità di sicurezza.

3. **Sedi dei centri di calcolo e certificazioni (hosting a cura di ServerBase AG)**
    1. **Conservazione** dei dati **in Svizzera:** i dati vengono memorizzati ed elaborati esclusivamente nei centri di calcolo svizzeri di ServerBase AG (Rümlang ZH e Lupfig AG).
    2. **Standard di conformità:** questa infrastruttura è interamente certificata secondo la norma ISO 27001 e soddisfa i requisiti della FINMA (FINMA RS 08/7) e della legge svizzera sulla protezione dei dati (LPD).
4. **Monitoraggio continuo della sicurezza (SOC / NOC)**
    1. **Monitoraggio 24/7:** l'infrastruttura di rete e server sottostante viene monitorata 24 ore su 24, 7 giorni su 7, 365 giorni all'anno dal Security Operations Center (SOC) dedicato e dal Network Operations Team (NOC) di Myra, al fine di rilevare in tempo reale gli incidenti di sicurezza IT e contrastarli mediante livelli di escalation definiti.
5. **Misure di sicurezza fisica (ServerBase AG)**
    1. **Controllo degli accessi:** servizio di sicurezza in loco 24 ore su 24, 7 giorni su 7, per la sorveglianza dei centri di calcolo e rigorosi controlli di accesso a più livelli (ad es. scansioni biometriche, controlli dei documenti d'identità) per impedire l'accesso non autorizzato.
    2. **Protezione dell'infrastruttura:** impianti automatizzati di estinzione a gas per la protezione antincendio, alimentazione elettrica ridondante (UPS/alimentazione di emergenza) e sistemi di climatizzazione all'avanguardia per il funzionamento ottimale dell'hardware.
6. **Backup e ripristino dei dati**
    1. **Backup geo-ridondanti in Svizzera (residenza dei dati garantita in Svizzera):** backup regolari e automatizzati di tutti i dati dei clienti per evitare efficacemente la perdita di dati. Trattandosi di dati altamente sensibili, questi rimangono in ogni momento interamente in Svizzera. I backup crittografati vengono conservati in luoghi separati esclusivamente nei due data center ServerBase svizzeri (Rümlang ZH e Lupfig AG).
    2. **Continuità operativa**: processi di ripristino collaudati per un rapido recupero dei dati in caso di guasti (*disaster recovery*) e manutenzione proattiva dell'infrastruttura IT.
7. **Assistenza clienti sicura e co-browsing (Fullview)**
    1. **Cobrowsing isolato:** per l'assistenza tecnica ai clienti viene utilizzata la tecnologia di **Fullview**. Durante le sessioni di assistenza, il team di supporto ha accesso esclusivamente alla scheda del browser isolata dell'applicazione web. L'accesso al resto del desktop o alle applicazioni di terze parti dell'utente è tecnicamente impossibile.
    2. **Mascheramento automatico dei dati (filtro per la protezione dei dati):** per proteggere i dati altamente sensibili (in particolare i dati dei pazienti) è attivo un filtro automatico per la protezione dei dati. I campi di immissione sensibili, i dati personali o le password vengono **automaticamente oscurati (mascherati)** in tempo reale per il personale di assistenza e non vengono affatto trasmessi.
    3. **Basato sul consenso:** una sessione di assistenza non può essere avviata in nessun momento senza che l'utente se ne accorga; richiede sempre l'approvazione esplicita e attiva da parte dell'utente finale.

8. **Misure organizzative e prove**
    1. **Sicurezza interna del contraente:** assegnazione pragmatica ed efficace dei diritti (principio del «need-to-know» / principio di minimizzazione), uso sistematico dell'autenticazione a più fattori (MFA) per l'accesso al sistema e sensibilizzazione continua dei propri collaboratori in materia di protezione dei dati.
    2. **Documentazione:** su richiesta, è possibile fornire ai clienti prove relative all'infrastruttura (come le certificazioni ISO 27001 di ServerBase AG o i rapporti di sicurezza Myra).

Allegato 4 – Elenco dei sub-responsabili del trattamento

Il contraente incarica i seguenti subappaltatori in relazione al trattamento dei dati:

- **Myra Security GmbH**, Germania – Fornitura della rete di distribuzione dei contenuti (CDN), di servizi di sicurezza altamente sviluppati (Hyperscale Web Application Firewall) e della protezione dagli attacchi DDoS. Il trattamento dei dati avviene in piena conformità con i requisiti della LPD svizzera e del GDPR dell'UE esclusivamente su infrastrutture all'interno dell'Unione Europea (UE).
- **cloudscale.ch AG**, Svizzera – Fornitura di infrastrutture digitali (cloud hosting e servizi server).
- **Datadog, Inc**., USA – Fornitura di servizi di logging e monitoraggio (analisi e sorveglianza dei sistemi IT).
- **Health Info Net AG (HIN)**, Svizzera – Soluzioni IT e interconnessione per il settore sanitario svizzero (comunicazione sicura ed elaborazione dei dati).
- **Intercom Inc**., USA **/ Intercom R&D Unlimited Company**, Irlanda – Fornitura di servizi di assistenza e comunicazione (ad es. funzione di chat, richieste dei clienti, automazione). Il trattamento dei dati avviene sulla base di un Data Processing Addendum (DPA) stipulato con clausole contrattuali standard ai sensi dell'art. 16 cpv. 2 lett. d LPD.
- **LINK Mobility Austria GmbH**, Austria – Invio e gestione di messaggi SMS (servizi di comunicazione).
- **MediData AG**, Svizzera – Soluzioni IT per il settore sanitario svizzero (servizi di fatturazione elettronica e trasmissione dati).
- **Microsoft Corporation**, USA / **Microsoft Ireland Operations Ltd**. – Fornitura di servizi cloud e di piattaforma (ad es. SignalR, componenti Azure).
- **Nylas Inc**., USA – Fornitura di interfacce di programmazione (API) per l'accesso a dati relativi a e-mail, calendario e contatti nell'ambito di funzioni di comunicazione e gestione degli appuntamenti. Il trattamento dei dati avviene sulla base di un Data Processing Addendum (DPA) stipulato con clausole contrattuali standard ai sensi dell'art. 16 cpv. 2 lett. d LPD.
- **Pingen AG,** Svizzera – Invio di documenti di fatturazione in formato digitale e cartaceo (stampa, posta ibrida). Il trattamento avviene in Svizzera; in caso di trasferimento verso paesi terzi, viene garantita un'adeguata protezione dei dati.
- **ServerBase AG**, Svizzera – Hosting e fornitura di infrastrutture digitali (gestione dei server e servizi IT).
- **Infomaniak Network SA**, Svizzera – Fornitura di servizi di IA conformi alla protezione dei dati (modelli linguistici di IA/inferenza). Il trattamento e l'archiviazione dei dati avvengono esclusivamente nei centri di calcolo propri di Infomaniak in Svizzera, certificati ISO 27001 e ISO 50001. Il trasferimento di dati verso paesi terzi o fornitori terzi a fini di addestramento è escluso sia dal punto di vista tecnico che contrattuale.
- **Fullview ApS, Danimarca** – Fornitura di strumenti di supporto visivo (cobrowsing e infrastruttura di assistenza clienti). Il trattamento dei dati avviene in conformità al GDPR e alla DSG esclusivamente su server situati all'interno dell'Unione Europea (regione di Francoforte, Germania). I campi contenenti dati sensibili vengono resi irriconoscibili dal sistema prima della trasmissione (data masking).