

Informativa sulla Privacy

Versione 1.6 del 17.10.2026 - LAIO Sagl. Documento consegnato insieme al fascicolo contrattuale.

1. Titolare del trattamento

Per la gestione degli account, del rapporto commerciale e della sicurezza, il titolare è:

LAIO Sagl Via Verdabbio 21, 6537 Grono (GR), Svizzera UID: CHE-105.723.141 Contatto: support@laio.ch. Incidenti urgenti: +41 79 571 80 78; inviare anche una segnalazione scritta a support@laio.ch con oggetto INCIDENTE SICUREZZA.

Per i dati di clienti, fornitori e dipendenti inseriti nei gestionali, il titolare è l'organizzazione che usa il workspace; LAIO opera per suo conto come responsabile. Le istruzioni e gli obblighi sono descritti nell'accordo sul trattamento dati. Il referente di LAIO è Claudio Esposito.

2. Finalità del trattamento

Le finalità e i motivi del trattamento sono descritti di seguito. Per i dati del workspace, il cliente determina e documenta la liceità del trattamento secondo la normativa applicabile:

Erogazione del servizio - creazione e gestione dell'account, autenticazione, gestione dei workspace/gestionali, creazione di preventivi e fatture, funzionalità operative dell'applicazione. Motivo del trattamento: esecuzione del contratto d'uso con l'utente/il gestionale.

Adempimenti contabili e fiscali - emissione e conservazione di fatture e documenti contabili. Motivo del trattamento: obbligo legale (art. 958f CO).

Sicurezza e prevenzione abusi - registrazione di accessi e operazioni (audit log), verifica anti-bot (Cloudflare Turnstile) sui flussi di autenticazione. Motivo del trattamento: interesse legittimo alla sicurezza del sistema e dei dati degli utenti.

Comunicazioni transazionali - invio di email relative a preventivi, fatture, inviti, notifiche di sistema. Motivo del trattamento: esecuzione del contratto/richiesta dell'utente.

Gestione del rapporto di lavoro (per i workspace che utilizzano il modulo timbrature) - registrazione di presenze/timbrature dei dipendenti. Motivo del trattamento: esecuzione del rapporto di lavoro tra il gestionale (datore di lavoro) e il dipendente.

Notifiche push facoltative - avvisi di assegnazione dei turni ai dispositivi abilitati, su richiesta dell'utente e nel perimetro autorizzato dal cliente. Il permesso del sistema operativo riguarda la ricezione degli avvisi e non è un consenso generale ad altri trattamenti. Il rifiuto non impedisce di consultare i turni nell'app.

3. Categorie di dati trattati

Dati identificativi di utenti/dipendenti dei gestionali: nome, cognome, indirizzo email.

Dati aziendali e clienti inseriti dai gestionali: anagrafiche clienti, preventivi, fatture, dati bancari (IBAN) inseriti nelle impostazioni del gestionale per la generazione dei bollettini QR svizzeri.

Log di sicurezza (registro audit): indirizzo IP, user agent, tipo di azione effettuata, timestamp.



Dati di presenza/timbrature dei dipendenti (per i gestionali che attivano il modulo dedicato): orari di inizio/fine lavoro e pausa, note.

Spese, attività e turni: dati dei fornitori, giustificativi, rimborsi, attività lavorative, turni e assenze. Inserire solo i dati necessari. Certificati medici, diagnosi e altri documenti sanitari sono esclusi; le assenze si registrano con causali non diagnostiche.

Scansione AI facoltativa: documento caricato, riferimenti dei fornitori e categorie usati per proporre la compilazione; risultati e consumo del servizio.

Diagnostica: errori applicativi, identificativi di richieste, account e workspace; accesso Google con dati del profilo autorizzati.

Notifiche mobili: token del dispositivo e piattaforma iOS/Android, identificativi di utente, gestionale e notifica, data del turno e stato tecnico di invio. Fotocamera: acquisizione del giustificativo soltanto quando richiesta; il documento è caricato nel gestionale e trasmesso al fornitore AI solo se viene richiesta la scansione autorizzata.

I dati provengono dall'utente, dall'organizzazione che lo invita e inserisce i dati di lavoro, dai documenti caricati e dai log tecnici generati dal servizio. I dati di autenticazione necessari sono indispensabili per accedere; appunti, scansione AI, notifiche push e accesso Google sono facoltativi. LAIO OS non adotta decisioni sul personale o sui rimborsi basate unicamente sulla scansione AI: i risultati richiedono verifica umana.

4. Sub-processor e destinatari dei dati

I fornitori e i rispettivi ruoli sono descritti di seguito. Le configurazioni di Supabase e Vercel sono state rilevate il 16.10.2026; quella di Anthropic è stata verificata il 24.09.2026, senza nuova verifica dell'account al 16.10.2026; gli elenchi dei subfornitori sono acquisiti con la data della rispettiva versione; i flussi dei servizi di accesso e di avviso sono verificati sul codice dell'applicazione. Gli elenchi geografici non vengono ampliati oltre quanto documentato.

Supabase Pte. Ltd. - database, autenticazione e file. Sub-responsabile per i dati del gestionale. Progetto in Germania (eu-central-1) e piano Pro verificati presso il fornitore il 16.10.2026. Il DPA pubblico, versione 1 del 01.08.2026, è incorporato nei Terms of Service (§7.b); non richiede un nuovo PDF firmato separatamente. Un accordo separato ancora vigente prevale secondo §1.d dei termini. Le garanzie includono le clausole contrattuali tipo e gli adattamenti svizzeri. Elenco ufficiale dei subfornitori del 12.10.2026 acquisito: 21 subfornitori per hosting, supporto, monitoraggio e comunicazione, di cui 19 negli Stati Uniti, uno a Singapore e uno in Ungheria. I dati del gestionale restano in Germania; la regione del progetto non limita da sola supporto e accessi remoti. LAIO Sagl è la parte del rapporto con il fornitore.



Vercel Inc. - hosting, API e log. Progetto di produzione, team e dominio verificati presso il fornitore il 16.10.2026; funzioni eseguite in Germania (Francoforte, fra1) secondo la configurazione versionata dell'applicazione, mentre CDN, supporto e diagnostica possono coinvolgere altri Stati. Il DPA del 17.03.2026, efficace dal 31.03.2026, è incorporato nei Terms of Service (§10.1) e si applica ai piani Pro ed Enterprise; Schedule 3 e Schedule 4 §3 disciplinano le garanzie pertinenti, incluse quelle svizzere. Il Trust Center consultato il 15.10.2026 elenca subfornitori negli Stati Uniti, in Spagna e nel Regno Unito: è un elenco dell'intera piattaforma, non la prova che ogni servizio riceva i dati LAIO. I nuovi subfornitori sono comunicati con aggiornamento dell'elenco e, su iscrizione all'indirizzo privacy del fornitore, con 5 giorni di calendario per l'opposizione. Il servizio è sul piano Pro e LAIO Sagl è la parte del rapporto con il fornitore.

Resend / Plus Five Five, Inc. - email transazionali. Sub-responsabile: destinatari, messaggi e allegati negli Stati Uniti. DPA acquisito, versione 31.12.2025, con clausole contrattuali tipo e adattamenti svizzeri (§6.5). La regione europea di invio non modifica la conservazione negli USA. Termini dichiarati: email e log 30 giorni, backup 7 giorni, residui entro 90 giorni dalla chiusura dell'account. Questi termini sono distinti dallo storico conservato da LAIO OS.

Cloudflare, Inc. - verifica anti-bot Turnstile. Responsabile per la protezione del sito e titolare autonomo per il miglioramento del rilevamento dei bot. Riceve segnali tecnici di browser, dispositivo e rete all'apertura della pagina di accesso, come verificato sul codice dell'applicazione il 16.10.2026. Attivo nella verifica del 06.10.2026; nessun cookie sul dominio rilevato in quel controllo. Elenco dei subfornitori consultato il 16.10.2026, con aggiornamento dichiarato al 01.10.2025: per questo servizio non è indicato alcun subfornitore terzo, mentre supporto e altri prodotti coinvolgono fornitori in Stati Uniti, SEE, Regno Unito, Giappone, Australia, Canada, India e Singapore, oltre a sedici società del gruppo. Il servizio opera su rete globale, con DPA e clausole svizzere.

Anthropic Ireland, Limited - scansione AI facoltativa. Sub-responsabile per l'estrazione assistita da documenti ordinari; riceve il documento e il contesto necessario di fornitori e categorie. Termini commerciali e DPA incorporato con clausole contrattuali tipo e adattamenti svizzeri. Configurazione verificata il 24.09.2026: organizzazione LAIO Sagl, workspace negli Stati Uniti, inferenza con instradamento globale, conservazione standard 30 giorni, feedback disattivato e nessun accordo di conservazione zero. Addestramento: i termini commerciali Anthropic (§B), consultati il 17.10.2026, escludono l'addestramento sui contenuti del cliente inviati tramite API. Il Privacy Center precisa che materiali inviati volontariamente come feedback o tramite adesione esplicita possono essere usati per addestrare i modelli. LAIO non autorizza tali invii o adesioni per i dati del cliente. Fonti: <https://www.anthropic.com/legal/commercial-terms>; <https://privacy.claude.com/en/articles/7996868-is-my-data-used-for-model-training>. Nei casi di segnalazione di abuso il fornitore indica termini più lunghi: fino a 2 anni per input e output e 7 anni per le classificazioni di sicurezza. Il perimetro geografico dell'inferenza globale non è pubblicato Paese per Paese dal fornitore: il limite è documentato nella valutazione dei trasferimenti. L'uso richiede la scelta del cliente nell'allegato C; le istruzioni AI sono nell'allegato C bis. Non è autorizzato l'invio di dati sanitari o di altri dati degni di particolare protezione.



Google - accesso facoltativo con account Google. Il componente Google Identity Services viene caricato solo dopo la scelta «Attiva accesso Google» nella pagina di accesso. Da quel momento Google riceve dati tecnici, incluso l'indirizzo IP, e può usare il cookie g_state. Se completi l'accesso, LAIO riceve i dati del profilo autorizzati. Google opera come titolare autonomo per i propri trattamenti, secondo <https://policies.google.com/privacy>; il servizio può comportare trasferimenti negli Stati Uniti e negli altri Stati della sua infrastruttura indicati nella sua informativa. Il semplice accesso alla pagina, senza attivare Google, non carica questo componente. Il link via email resta disponibile.

Telegram - avvisi tecnici al referente LAIO. Riceve soltanto un testo fisso generico: la verifica sul codice dell'applicazione del 16.10.2026 mostra un'unica costante di avviso, senza dati dei clienti, identificativi, percorsi o dettagli degli errori. La diagnostica resta nel registro errori del gestionale. Non trattando dati dei clienti del gestionale, non opera come sub-responsabile di tali dati; tratta i dati dell'account destinatario e i metadati di consegna secondo la propria informativa.

Expo / 650 Industries, Inc. - inoltro delle notifiche push facoltative. Riceve token del dispositivo, testo dell'avviso e dati di instradamento: identificativi di notifica, utente e gestionale e data del turno. Apple/APNs per iOS e Google/Firebase Cloud Messaging per Android effettuano la consegna; Expo li elenca come subfornitori negli Stati Uniti. Non sono inviati allegati, importi, diagnosi o descrizioni dei turni. Il contenuto può apparire sulla schermata bloccata secondo le impostazioni del telefono.

Expo opera come responsabile per l'erogazione del servizio e descrive trattamenti propri nella sua informativa. I termini, §3.2, richiamano clausole contrattuali tipo quando si applica il GDPR; l'informativa dichiara adesione anche allo Swiss-U.S. Data Privacy Framework. Questa dichiarazione non attesta da sola la copertura di LAIO Sagl, dei dati dei lavoratori o del rapporto di sub-responsabilità: le notifiche push sono abilitate per un cliente solo dopo che tali presupposti e il perimetro dei trasferimenti sono documentati. Apple e Google svolgono inoltre i trattamenti propri delle rispettive piattaforme.

La coda LAIO è soggetta a pulizia dei record più vecchi di 7 giorni; il messaggio richiede una validità di consegna di 24 ore. Expo dichiara conservazione del contenuto in memoria e in coda per il tempo necessario all'inoltro, senza archivio permanente del contenuto. Non si estende questo termine ai metadati dei fornitori. Il token è revocato tramite l'app al logout o quando viene rilevata la revoca del permesso; la sola disinstallazione non ne prova la cancellazione dal server.

Fonti consultate il 16.10.2026: <https://expo.dev/terms>; <https://expo.dev/privacy>; <https://expo.dev/privacy/subprocessors> (15.09.2026); <https://docs.expo.dev/push-notifications/faq/>; <https://www.apple.com/legal/privacy/>; <https://firebase.google.com/support/privacy>. L'elenco Expo riguarda tutta la piattaforma: non significa che ogni suo subfornitore riceva le notifiche LAIO.

Per i trasferimenti all'estero LAIO verifica i presupposti applicabili, documenta Stati, destinatari e garanzie e aggiorna le informazioni pertinenti. La firma del cliente non sostituisce queste verifiche né autorizza trasferimenti privi dei presupposti richiesti dagli artt. 16-17 LPD.

5. Tempi di conservazione

Documenti contabili (fatture, note di credito e documentazione correlata): 10 anni, come previsto dall'art. 958f del Codice delle obbligazioni (CO).



Per i datori soggetti alla legge svizzera sul lavoro, le registrazioni necessarie alla sua esecuzione sono conservate almeno 5 anni dopo la scadenza della loro validità (art. 73 OLL 1). Per gli altri dati del personale il datore determina i termini in base a finalità, obblighi e pretese applicabili, senza conservarli indefinitamente; termini diversi sono documentati nell'allegato C.

Account e dati operativi: conservati secondo necessità del servizio e istruzioni del titolare. La cancellazione dell'account non cancella automaticamente dati e documenti del workspace.

Email presso Resend: il fornitore dichiara 30 giorni per email e log sui piani standard, 7 giorni per i backup e cancellazione dei dati residui entro 90 giorni dalla chiusura dell'account Resend. Questi termini non cancellano lo storico email conservato da LAIO OS.

Termini adottati da LAIO il 06.10.2026: diagnostica interna 30 giorni; audit di sicurezza e storico delle email operative non contabili 12 mesi; copie di sicurezza operative massimo 30 giorni; evidenze minime di richieste privacy e incidenti 3 anni dalla chiusura. Proroghe soltanto per motivi documentati, incidenti o obblighi applicabili. Le email con valore contabile seguono i documenti cui si riferiscono. L'archiviazione di un workspace non ne elimina i dati. I termini sono impegni di gestione, non un'attestazione che ogni cancellazione sia automatica; le procedure sono eseguite e verificate da LAIO.

Alla cessazione, anche per mancato pagamento, LAIO rende disponibile un export standard entro 30 giorni dalla cessazione o dalla precedente richiesta: dati tabellari in formato aperto e allegati originali, su canale protetto al referente verificato. L'export standard non è subordinato al saldo. Per 30 giorni dalla cessazione è previsto accesso in sola lettura; se impedito da ragioni di sicurezza, LAIO consegna l'export su canale alternativo. Il cliente verifica la consegna entro 15 giorni e segnala eventuali omissioni, che LAIO corregge prima della cancellazione. Le copie operative sono cancellate entro 30 giorni dalla conferma della consegna completa. In assenza di richiesta o conferma, LAIO rende comunque disponibile l'export e cancella entro 90 giorni dalla cessazione, previo avviso di almeno 15 giorni con data di cancellazione e modalità di ritiro. Il silenzio non è una conferma della completezza: LAIO verifica e documenta la consegnabilità dell'export. Obblighi di legge, contestazioni tempestive sulla completezza o istruzioni scritte di proroga motivata sospendono la cancellazione dei soli dati interessati, con accessi limitati e data di riesame. La copia di consegna segue gli stessi termini; i backup scadono entro il successivo ciclo massimo di 30 giorni.

Notifiche: pulizia della coda LAIO oltre 7 giorni dalla creazione; token sul server finché il dispositivo è abilitato, salvo revoca o rilevamento di token non valido. Gli impegni di cancellazione e i termini dei fornitori restano distinti, come descritto al punto 4.

6. Diritti dell'interessato

In qualità di interessato, hai diritto di accesso, rettifica, cancellazione e opposizione al trattamento dei tuoi dati personali, oltre al diritto alla portabilità dei dati, nei limiti previsti dalla nLPD.

Se sei già registrato, puoi gestire i tuoi dati personali dalla pagina /impostazioni/dati-personali per esportare profilo e appartenenze, fino a 500 eventi degli ultimi 360 giorni, o richiedere la cancellazione dell'account previa verifica dell'identità. Questo export non comprende tutti i dati di lavoro: per timbrature, note spese e altre informazioni rivolgiti al titolare del workspace o al contatto seguente.

In alternativa, o se non hai un account, puoi esercitare i tuoi diritti scrivendo a support@laio.ch.



Le richieste di accesso sono evase di regola gratuitamente entro 30 giorni secondo la LPD; eventuali limiti o differimenti sono motivati. Se si applica il GDPR, valgono il termine di un mese e le condizioni di proroga previste dall'art. 12. La verifica dell'identità è proporzionata e non richiede dati eccedenti il necessario.

Puoi segnalare possibili violazioni all'Incaricato federale della protezione dei dati e della trasparenza (IFPDT), <https://www.edoeb.admin.ch/it>, e far valere i tuoi diritti davanti al giudice competente. Quando si applica il GDPR, puoi inoltre chiedere la limitazione del trattamento, revocare un consenso senza pregiudicare il trattamento precedente e proporre reclamo all'autorità di controllo competente; i diritti e le relative condizioni sono quelli della normativa applicabile.

7. Sicurezza dei dati

Adottiamo misure tecniche e organizzative volte a proteggere i dati personali, tra cui:

Hosting dei dati in infrastruttura Supabase con regione dati UE (eu-central-1).

Cifratura delle comunicazioni in transito (HTTPS/TLS) e cifratura dei dati a riposo lato infrastruttura di hosting.

Backup aggiuntivi di database e allegati su SSD scritto da un Mac mini gestito da LAIO e custodito negli studi di LAIO, in Svizzera, in luogo chiuso e ad accesso riservato al referente tecnico: copia giornaliera sostitutiva e settimanale il lunedì, ultime due settimane conservate, con avviso in caso di errore. Il referente conferma il 16.10.2026 attuate la cifratura delle copie locali, la custodia separata delle chiavi, la protezione di una copia offline o immutabile e la prova di ripristino DB/allegati. Si tratta di una conferma del referente; dettagli tecnici e verbale non sono stati acquisiti nel dossier.

Isolamento dei dati tra gestionali tramite controllo degli accessi a livello di database (Row Level Security) e verifica dei permessi applicativi per ogni pagina/risorsa.

Registro delle operazioni sensibili protetto da modifiche degli utenti ordinari e consultabile dai soggetti autorizzati. Le operazioni di servizio privilegiate possono modificarlo.

Verifica anti-bot (Cloudflare Turnstile) sui flussi di autenticazione via link magico.

8. Cookie e memoria locale

Usiamo cookie di accesso e sicurezza, preferenze e appunti locali. La pagina di accesso carica Cloudflare per la sicurezza; Google viene caricato su scelta dell'utente. Finalità, durata e modalità di cancellazione sono descritte in <https://laioos.com/cookie>. Nel codice esaminato non risultano strumenti pubblicitari o analytics comportamentali.

9. Aggiornamenti e ambito dell'informativa

Questa informativa riguarda LAIO OS web e le app iOS e Android nel perimetro descritto. LAIO pubblica numero e data delle revisioni e informa delle modifiche sostanziali prima dei nuovi trattamenti. Le organizzazioni clienti forniscono ai propri lavoratori, clienti e fornitori le informazioni relative ai trattamenti di cui sono titolari; la consegna di questa informativa al firmatario non sostituisce tale obbligo.

Contatto: support@laio.ch. La consegna di questa informativa non richiede un consenso generale al trattamento.

