

Dispendo — Informativa privacy dell'app

privacy-2026-10-app-review-draft-1 · 2026-10-07 · IT

BOZZA • REVISIONE LEGALE PENDENTE

Dati legali/fiscali e verifiche contrattuali restano da completare. Questo documento non certifica la conformità del servizio.

Indice

Ambito e stato del documento

1. Titolare e contatti

2. Dati trattati e provenienza

3. Perché trattiamo i dati e base giuridica

4. Categorizzazione, AI e ricerca esercente

5. Destinatari e fornitori

6. Trasferimenti internazionali

7. Conservazione e cancellazione

8. Cookie, tracciamento e autorizzazioni del dispositivo

9. Sicurezza

10. Diritti

11. Eliminazione account e abbonamento

12. Minori

13. Modifiche

14. Provider AIS e flusso bancario

Ambito e stato del documento

BOZZA PER REVISIONE PROFESSIONALE — NON È L'INFORMATIVA FINALE DEL LANCIO
PUBBLICO Versione: privacy-2026-10-app-review-draft-1 Revisione: 7 ottobre 2026

Questa informativa riguarda l'app Dispendo, il backend e l'assistenza relativa all'app, inclusa la beta privata. La sola navigazione sul sito è descritta nell'informativa del sito, distinta da questa. La lingua segue quella selezionata nell'app. La presa visione non è un consenso generale: Termini, autorizzazione bancaria, preferenze AI e permessi del dispositivo sono controlli distinti.

1. Titolare e contatti

Il titolare del trattamento è Alberto Schianni, persona fisica, con indirizzo [INDIRIZZO PUBBLICO COMPLETO], codice fiscale [CODICE FISCALE] e, se attribuita prima del lancio, partita IVA [PARTITA IVA E DENOMINAZIONE ESATTA REGISTRATA].

- Privacy e diritti: privacy@dispendo.app
- Assistenza: support@dispendo.app

La necessità di nominare un DPO e gli eventuali contatti sono da verificare prima del lancio. Questa bozza non dichiara una nomina non avvenuta.

2. Dati trattati e provenienza

Dati forniti dall'utente

- email, nome visualizzato, lingua, preferenze e foto profilo facoltativa;
- credenziali gestite dal sistema di autenticazione; non possiamo leggere la password in chiaro;
- movimenti inseriti o importati, importi, valuta, date, descrizioni, categorie, note, budget, ricorrenze e dati dei portafogli condivisi;
- file CSV/XLSX/JSON selezionati per l'importazione: vengono analizzati dall'app e il file sorgente non viene conservato come allegato sui nostri server;
- richieste, feedback e informazioni che scegli di inviare all'assistenza. Non inviare password, codici monouso, credenziali bancarie o esportazioni complete se non richieste mediante un canale espressamente concordato.

Dati ricevuti da banche e open banking

Se colleghi volontariamente un conto tramite Enable Banking e la tua banca, possiamo ricevere dati del conto e dell'istituto, saldo se disponibile, movimenti, descrizioni, importi, valute, date, identificativi e informazioni di controparte (per esempio nome o IBAN), codici operazione/MCC e metadati del consenso/sincronizzazione. L'esatta disponibilità dipende dalla banca. La password bancaria viene inserita nel flusso della banca/provider e non deve essere comunicata a Dispendo.

Le descrizioni delle transazioni possono incidentalmente rivelare informazioni molto delicate e, in alcuni casi, categorie particolari di dati (per esempio salute, convinzioni religiose o politiche). Le proteggiamo con un livello elevato di riservatezza e ne limitiamo l'uso alle funzioni richieste; la base e le garanzie per eventuali trattamenti di categorie particolari devono essere confermate nella revisione legale finale.

Dati ricevuti da Apple, Google e dal dispositivo

In base alle scelte dell'utente e alle funzioni attive possiamo ricevere:

- identificativo, email/nome e metadati di autenticazione da Apple o Google;
- token di notifica e stato delle autorizzazioni del dispositivo;
- prodotto di abbonamento, identificativi tecnici della transazione, stato, scadenza, rinnovo, rimborso o revoca da Apple. Non riceviamo il numero della carta usata nell'App Store;
- versione app/sistema, data/ora, identificatori di richiesta/sessione, errori, IP e dati tecnici generati dai sistemi e dai fornitori per sicurezza e affidabilità.

Dati di altre persone

Per un accesso social non serve necessariamente una password. Dispendo: accesso e recupero possono dipendere da Apple o Google. Non chiediamo la posizione GPS per gestire le spese. Una città già contenuta in una causale bancaria non è geolocalizzazione del dispositivo.

Nei gruppi i membri autorizzati vedono dati del gruppo e attribuzione delle spese. “Aggiungi anche al gruppo” crea una copia dei dettagli previsti, a tuo nome, senza condividere l'intero conto né rimuovere la fonte personale. La copia è distinta: modifiche successive non si devono presumere sincronizzate. Verifica destinatari e dettagli prima della condivisione; altri membri possono averne conservato copie o esportazioni.

Una causale, una controparte o un portafoglio condiviso può contenere dati di un'altra persona. Usa solo dati che hai diritto di trattare, limita note e descrizioni allo stretto necessario e informa le altre persone quando richiesto. Dispendo minimizza l'uso di questi dati e rende pubblica questa informativa; il trattamento e le eventuali deroghe all'informazione individuale devono essere validati per il caso d'uso finale.

3. Perché trattiamo i dati e base giuridica

Finalità: Creare, autenticare, proteggere e recuperare l'account · Dati principali: contatto, provider identity, sessione, sicurezza · Base proposta e scelta: esecuzione del contratto; interesse legittimo per sicurezza e prevenzione abusi [LIA/LEGAL REVIEW]

Finalità: Fornire registro, import/export, budget, grafici, ricorrenze e condivisione · Dati principali: dati finanziari e configurazione · Base proposta e scelta: esecuzione del contratto

Finalità: Collegare conti e sincronizzare i movimenti richiesti · Dati principali: dati bancari, consenso e connessione · Base proposta e scelta: esecuzione del contratto; il consenso PSD2 presso banca/provider è distinto dal consenso GDPR [ROLE/BASIS REVIEW]

Finalità: Categorizzare con regole interne e rilevare rimborsi/giroconti · Dati principali: segnali transazione, categorie, correzioni · Base proposta e scelta: esecuzione del contratto

Finalità: Arricchimento esterno Anthropic di casi non riconosciuti · Dati principali: campi minimizzati descritti sotto · Base proposta e scelta: decisione aperta; raccomandazione di lancio: consenso separato, specifico e revocabile, funzione disattivata per impostazione predefinita

Finalità: Notifiche di servizio, sicurezza e budget · Dati principali: token, evento minimizzato, preferenza · Base proposta e scelta: esecuzione del contratto/interesse legittimo secondo il messaggio; autorizzazione OS revocabile [LEGAL REVIEW]

Finalità: Gestire abbonamento e diritto di accesso · Dati principali: prodotto, transazione, stato/rinnovo · Base proposta e scelta: esecuzione del contratto e obblighi di legge

Finalità: Sicurezza, limiti, diagnosi e incidenti · Dati principali: log e metadati tecnici minimizzati · Base proposta e scelta: interesse legittimo e, quando applicabile, obbligo legale [LIA]

Finalità: Provare versione dei Termini/Privacy mostrata e accettata · Dati principali: versioni, hash, lingua, fonte, timestamp · Base proposta e scelta: esecuzione del contratto/interesse legittimo di accountability [LEGAL REVIEW]

Finalità: Rispondere a diritti, reclami e obblighi · Dati principali: richiesta e verifica minima · Base proposta e scelta: obbligo legale

Se il trattamento è necessario al contratto e non fornisci il dato indispensabile, la relativa funzione non può essere erogata. Il collegamento bancario, le notifiche, la foto, i login sociali e l'arricchimento esterno sono facoltativi e devono poter essere gestiti separatamente.

Stato attuale: la beta abilita l'AI esterna per impostazione predefinita, con possibilità di disattivazione. L'interruttore non è descritto come consenso preventivo. Prima del lancio vanno approvati base giuridica e flusso di scelta; l'eventuale opt-in richiede anche un cambiamento tecnico. La lettura di questa bozza non sana né sostituisce tale verifica.

4. Categorizzazione, AI e ricerca esercente

La maggior parte dei movimenti viene trattata nel backend Dispendo con regole deterministiche. Se l'opzione di categorizzazione avanzata è attiva, un movimento ancora non riconosciuto può essere inviato ad Anthropic (modelli Claude) per suggerire una categoria o identificare un esercente tramite ricerca web.

I campi sono limitati a quelli necessari, come esercente normalizzato, direzione, importo e valuta, giorno del mese, ricorrenza, MCC/codice operazione e causale ripulita. Per una ricerca pubblica dell'esercente si usano descrittore normalizzato e segnali contestuali limitati, non importo e data esatti. Prima dell'invio, i controlli rimuovono IBAN, numeri di carta, telefoni, email e codici fiscali e sostituiscono nomi che sembrano riferiti a persone fisiche. Non vengono inviati l'identificativo dell'utente, il suo IBAN o il saldo. La redazione è euristica e non garantisce il riconoscimento di ogni dato identificativo: parliamo di dati minimizzati e potenzialmente personali/pseudonimizzati, non di dati sicuramente anonimi.

Puoi disattivare l'opzione da Privacy: impedisce nuovi invii esterni, senza disattivare regole, correzioni e memoria privata. Non ritira richieste già ricevute dal provider. La revoca di un eventuale consenso non pregiudica i trattamenti precedentemente leciti.

Le condizioni Anthropic, le impostazioni di uso dei dati e la conservazione applicabile devono essere verificate per il contratto Dispendo: non promettiamo assenza assoluta di conservazione o addestramento senza questa verifica.

Google Places è attualmente una funzione sperimentale di sola osservazione e non deve essere attiva per utenti pubblici finché non è stata separatamente approvata, configurata e descritta. Il community learning è disattivato e non sarà attivato senza nuova valutazione, informativa e, quando necessario, scelta dell'utente.

Le categorie restano suggerimenti modificabili. Non assumiamo decisioni basate unicamente su un trattamento automatizzato che producano effetti giuridici o analogamente significativi ai sensi dell'art. 22 GDPR.

5. Destinatari e fornitori

Usiamo solo i servizi pertinenti alla funzione scelta. L'elenco tecnico attuale comprende:

- Supabase: autenticazione, database, storage, funzioni e operazioni backend;
- Enable Banking e la banca/ASPSP selezionata: connessione e dati open banking;
- Anthropic: categorizzazione/ricerca esterna soltanto quando attivata e applicabile;
- Google: login facoltativo, Firebase Cloud Messaging e, solo se successivamente approvato, Places;
- Apple: distribuzione, acquisti, login facoltativo e trasporto notifiche APNs;
- Resend: email transazionali e di sicurezza;
- Cloudflare: DNS/TLS e pagine di rientro dei link email;
- Netlify: pagine pubbliche e host separato della console amministrativa;
- servizio di instradamento email e casella del gestore: ricezione dell'assistenza;
- consulenti o autorità soltanto quando necessario e con una base giuridica.

[PRIMA DEL LANCIO: per ogni soggetto indicare entità contraente, ruolo, DPA/accordo, regioni, sub-responsabili, conservazione, cancellazione, contatto incidenti e trasferimenti. Non definire automaticamente ogni soggetto "responsabile" senza verifica.]

Non vendiamo dati personali e non li usiamo per pubblicità comportamentale. La versione attuale non integra SDK pubblicitari né analytics di terze parti identificati nell'audit del codice; ciò deve essere ricontrollato sul binario firmato finale.

6. Trasferimenti internazionali

Il progetto principale è configurato in una regione europea, ma alcuni fornitori o sub-fornitori possono trattare dati fuori dallo Spazio economico europeo. Prima del lancio pubblico indicheremo per ciascun flusso l'effettiva destinazione e la garanzia applicabile, per esempio decisione di adeguatezza, clausole contrattuali standard ed eventuali misure supplementari.

[BLOCCO: completare transfer assessment e contratti nel vendor register. Non pubblicare questa sezione come definitiva finché le informazioni non sono verificate.]

7. Conservazione e cancellazione

Applichiamo la durata più breve compatibile con la finalità, salvo obbligo documentato di conservazione:

Dato: account, profilo, preferenze e avatar · Regola prevista: fino alla cancellazione/sostituzione dell'account o del contenuto

Dato: movimenti manuali/importati e dati normalizzati bancari · Regola prevista: fino a cancellazione della riga, connessione o account, secondo il controllo scelto

Dato: file sorgente di import · Regola prevista: non conservato come allegato server; restano le righe importate e la provenienza necessaria

Dato: payload bancari grezzi · Regola prevista: massimo 12 mesi dal recupero o 90 giorni dopo che una connessione scaduta/revocata diventa inattiva, se precedente

Dato: tentativi OAuth conclusi/consumati/scaduti · Regola prevista: massimo 30 giorni oltre l'ultimo evento del ciclo di vita

Dato: token notifiche · Regola prevista: fino a logout, invalidazione, rimozione o cancellazione account

Dato: acquisti/diritti di accesso · Regola prevista: per il contratto, la riconciliazione e gli obblighi legali applicabili [PERIODO DA DEFINIRE]

Dato: accettazioni legali · Regola prevista: oggi fino alla cancellazione account; l'eventuale conservazione minima successiva richiede una nuova decisione documentata

Dato: log di sicurezza, email e fornitori · Regola prevista: [PERIODI MASSIMI DA VERIFICARE PER FORNITORE/PIANO]

Dato: audit di autorizzazione console · Regola prevista: 30 giorni, dati minimi dell'operatore, non contenuti finanziari

Dato: backup · Regola prevista: [PIANO SUPABASE, RPO, PERIODO E LAG MASSIMO DI CANCELLAZIONE DA INSERIRE]

Dato: richieste privacy, reclami e incidenti · Regola prevista: [PERIODO MINIMIZZATO DA DEFINIRE CON IL CONSULENTE]

“Cancellazione” indica l'eliminazione dal sistema live. Copie residue in backup protetti e log del fornitore non vengono riutilizzate nell'app e scadono secondo i periodi massimi verificati che saranno inseriti qui. Dopo un ripristino, le cancellazioni devono essere riapplicate per evitare che i dati tornino attivi.

Non è implementata una cancellazione automatica generalizzata dopo 24 mesi di inattività. La regione europea del database non garantisce da sola trattamento esclusivamente nel SEE.

8. Cookie, tracciamento e autorizzazioni del dispositivo

Al lancio, le pagine pubbliche informative non devono usare cookie pubblicitari o analytics non necessari. Le pagine tecniche di conferma/recupero possono usare soltanto memoria locale o dati strettamente necessari a completare e proteggere il flusso, senza profilazione. Se in futuro vengono aggiunti analytics, cookie o SDK, aggiorneremo valutazione, preferenze, informativa e consenso prima dell'attivazione.

Notifiche e altre autorizzazioni del dispositivo vengono richieste nel contesto della relativa funzione e possono essere revocate dalle impostazioni iOS; alcune funzioni potrebbero quindi non essere disponibili.

9. Sicurezza

Usiamo controlli quali TLS, separazione degli accessi per utente, autorizzazioni minime, storage privato per avatar, segreti lato server, logging minimizzato, revisione delle dipendenze, MFA degli operatori, job di conservazione e procedure di incidente/recupero. Nessun sistema è completamente sicuro: mantieni protetti dispositivo e account e scrivi a support@dispendo.app se sospetti un abuso. Non inviare dati bancari completi in email.

10. Diritti

Nei casi previsti, puoi chiedere accesso, rettifica, cancellazione, limitazione, portabilità e opporti al trattamento; puoi inoltre revocare un consenso senza pregiudicare il trattamento già avvenuto. I diritti non sono assoluti e una richiesta può richiedere verifica proporzionata dell'identità.

Nell'app puoi:

- modificare diversi dati e preferenze;
- esportare movimenti in CSV/Excel/JSON;
- scaricare un archivio JSON versionato dei dati dell'account;
- cancellare singoli dati e l'intero account.

L'archivio account esclude credenziali e payload grezzi dei provider ma include i dati finanziari normalizzati e le informazioni di proprietà dell'utente. Per altri diritti scrivi a privacy@dispendo.app. Risponderemo senza ingiustificato ritardo e normalmente entro un mese, salve proroghe e comunicazioni consentite dalla legge.

Una proroga per complessità può arrivare a ulteriori due mesi; motivo e durata sono comunicati entro il primo mese. Contattarci prima non è un requisito per proporre reclamo all'autorità.

Puoi proporre reclamo al Garante per la protezione dei dati personali: <https://www.garanteprivacy.it/>. Ti invitiamo, senza limitarne il diritto, a contattarci prima per permetterci di risolvere il problema.

11. Eliminazione account e abbonamento

“Elimina account” nel Profilo avvia una conferma esplicita e rimuove l'utente di autenticazione e i dati live di sua proprietà, inclusi gli oggetti avatar, salvo una conservazione obbligatoria documentata. Dati condivisi o riferiti ad altre persone vengono trattati secondo proprietà, ruoli e obblighi applicabili. Backup e log scadono secondo la sezione 7.

L'eliminazione dell'account non annulla un abbonamento Apple. L'app deve offrire prima un accesso diretto alla gestione dell'abbonamento, ma non può impedire l'eliminazione immediata. Consulta la pagina pubblica “Assistenza e cancellazione account” per dettagli.

12. Minori

Il servizio pubblico non è destinato a minori di 18 anni. Se veniamo a conoscenza di un account di un minore, valuteremo e applicheremo misure proporzionate, inclusa la cancellazione quando necessaria. Contattaci a privacy@dispendo.app.

13. Modifiche

Pubblicheremo data e versione di ogni aggiornamento. In caso di cambiamenti materiali alle finalità, ai fornitori, ai trasferimenti o ai diritti, forniremo un avviso adeguato e raccoglieremo un nuovo consenso o una nuova accettazione quando richiesta. Le versioni associate a prove di accettazione restano immutabili.

14. Provider AIS e flusso bancario

Usiamo Enable Banking Oy, Business ID 2988499-7, Otakaari 5, 02150 Espoo, Finlandia, registrato come prestatore AIS e vigilato da FIN-FSA. Nel modello basato sulla sua autorizzazione si applicano termini e informativa propri, distinti dai servizi Dispendo: <https://tilisy.enablebanking.com/terms>. Accordo effettivo e ruoli privacy devono ancora essere confermati. Non definiamo automaticamente ogni soggetto responsabile del trattamento.

Autorizzazione e rinnovo seguono il flusso banca/provider. Non promettiamo durata uniforme di 180 giorni o dati in tempo reale. Revoca/disconnessione interrompe nuovi recuperi secondo l'esito del flusso; la cancellazione dello storico è distinta. Consenso PSD2 e base GDPR non sono intercambiabili. Per dati di terzi o categorie particolari, minimizzazione e contratto non sostituiscono condizioni/valutazioni necessarie degli artt. 9 e 14.

Le statistiche operative/prodotto della console derivano da superfici curate e aggregate del servizio, con soppressioni per piccoli campioni. Non sono un'interfaccia di consultazione libera delle spese personali. Soglie e pseudonimizzazione non garantiscono da sole anonimato.