Bodivine — Accordo sul trattamento dei dati (DPA) per professionisti

> **BOZZA CONTRATTUALE INTERNA NON EFFICACE — 6 novembre 2026, revisione 2.** Il testo e gli Allegati A–D costituiscono una proposta sostanziale ai sensi dell'art. 28 GDPR, **non** un contratto già stipulato, una certificazione o una garanzia che le misure siano attive. Non pubblicare come DPA accettabile, non attribuire una versione contrattuale definitiva e non impostare `PROFESSIONAL_DPA_VERSION`, `PROFESSIONAL_DPA_URL` o `PROFESSIONAL_DPA_SHA256` prima della chiusura dei punti aperti nell'Allegato D. L'eventuale messa online di questa bozza non autorizza il trattamento dei dati dei clienti.

1. Parti, ruoli, ambito e precedenza

Titolare del trattamento dei dati dei propri clienti: il singolo professionista maggiorenne che crea o utilizza un account professionale Bodivine, i cui identificativi e dati contrattuali devono essere acquisiti e associati alla relativa accettazione; per persona giuridica occorre accertare poteri di rappresentanza e identità della parte.
Responsabile del trattamento: Cristian Montanari, persona fisica operante in Italia con il nome Bodivine, contatto `privacy@bodivine.fit`. L'indirizzo/recapito giuridicamente idoneo del responsabile non è ancora definito: **blocco prima della sottoscrizione**. Non viene dichiarata l'esistenza di una società, P.IVA o sede professionale.

Il DPA riguarda solo i dati personali dei clienti che il Professionista tratta come titolare e affida a Bodivine quale responsabile. Per registrazione/account degli utenti, autenticazione, sicurezza del servizio, richieste rivolte direttamente a Bodivine e gestione del rapporto con l'account, Bodivine può agire come **titolare autonomo** secondo la propria informativa, da distinguere caso per caso. L'utilizzo di una stessa infrastruttura non rende automaticamente tutte le operazioni trattamenti per conto del Professionista. Eventuali contitolarità richiederebbero un accordo distinto ex art. 26.

Il presente DPA, con tutti gli allegati completati, è parte dei Termini del Servizio per le attività descritte nell'Allegato A e prevale sui Termini in caso di contrasto sulla protezione dei dati affidati. Restano inderogabili il GDPR e gli obblighi di legge applicabili.

2. Oggetto, durata, categorie e istruzioni documentate — art. 28(3)

Oggetto, durata, natura, finalità, interessati, dati e operazioni sono specificati nell'**Allegato A**. Il periodo ordinario di trattamento è quello di accesso al servizio professionale, con successiva restituzione/cancellazione disciplinata dall'art. 12 e dall'Allegato D; i tempi tecnici residui devono essere stabiliti **prima dell'attivazione**.

Il Professionista impartisce istruzioni documentate mediante questo DPA, le funzionalità autorizzate (creare/assegnare/modificare/visualizzare/esportare/cancellare record, inviare inviti e comunicare) e successivi ordini verificabili inviati al contatto designato. Bodivine non può utilizzare dati cliente per pubblicità propria, addestramento di modelli, vendita a terzi, profilazione autonoma o scopi estranei alle istruzioni. Trasferimenti a paesi terzi sono anch'essi soggetti a istruzioni documentate e alle condizioni del capo V GDPR.

In caso di obbligo di legge dell'Unione o dello Stato membro applicabile che richieda un trattamento diverso, Bodivine informa il Professionista **prima** di procedere salvo divieto legale per rilevanti ragioni di interesse pubblico. Comunica **immediatamente** se, a suo parere, un'istruzione viola il GDPR o la normativa UE/nazionale applicabile; ove appropriato sospende la specifica istruzione illecita mentre se ne chiarisce la legittimità.

3. Obblighi e diritti del Professionista titolare

Il Professionista determina e documenta finalità, necessità, minimizzazione, accuratezza, termini di conservazione e destinatari; fornisce l'informativa ex artt. 12–14, individua una base giuridica ex art. 6 e, **se tratta categorie particolari come dati sanitari**, una distinta condizione applicabile ex art. 9(2), incluso il consenso esplicito **quando richiesto dalla legge**. Verifica la maggiore età dei clienti e non carica dati di minorenni (regola del servizio 18+); distingue l'autorizzazione a gestire un cliente dal consenso della persona interessata. Gestisce le richieste dei clienti e decide le notifiche di violazione come titolare.

Il Professionista può richiedere a Bodivine informazioni, assistenza, verifica di subresponsabili, restituzione e cancellazione secondo questo accordo, senza che l'attestazione privacy professionale costituisca di per sé prova della base giuridica di **ogni** cliente. Non utilizzare il servizio per caricare dati che l'infrastruttura contrattuale effettivamente autorizzata non può trattare.

4. Persone autorizzate e riservatezza — art. 28(3)(b)

Bodivine limita l'accesso ai dati affidati alle persone che ne abbiano effettiva necessità per prestare assistenza, gestire incidenti o adempiere istruzioni; queste sono vincolate a obbligo contrattuale o legale di riservatezza, anche dopo la cessazione dell'accesso. Autorizzazioni, credenziali e privilegi vanno revocati senza ritardo quando non più necessari. **Non è attestata qui la presenza di personale, un registro accessi amministrativi o una revisione delle autorizzazioni già eseguita**: verifiche nell'Allegato B.

5. Sicurezza del trattamento — artt. 28(3)(c), 32

Bodivine deve adottare e mantenere misure tecniche e organizzative adeguate al rischio: riservatezza, integrità, disponibilità, capacità di ripristino, verifica periodica dell'efficacia, controllo accessi e privilegi, sicurezza della trasmissione e protezione contro perdita o divulgazione. I controlli **osservati nel sorgente** e quelli **ancora da provare operativamente** sono separati nell'Allegato B; nessun riferimento a crittografia a riposo, audit di sicurezza, backup funzionanti o certificazioni equivale ad attestare che siano effettivi.

Il Professionista adotta adeguate misure proprie (sicurezza del dispositivo, credenziali, legittima condivisione degli export, autorizzazioni dei collaboratori). Il rischio specifico dell'uso di dati sanitari richiede garanzie proporzionate e non può essere sanato dal solo consenso dell'utente o dal presente documento.

6. Subresponsabili e autorizzazioni — art. 28(2), (4)

L'autorizzazione generale scritta del Professionista può riguardare **soltanto il registro dei subresponsabili effettivamente completato e approvato** nell'Allegato C alla data dell'accordo; questa bozza non conferisce autorizzazione ad alcuna lista provvisoria. Bodivine mantiene il registro aggiornato e informa anticipatamente delle aggiunte/sostituzioni, comunicando servizi, località e trasferimenti. **Termine operativo approvato dal gestore per la versione finale: preavviso di almeno 30 giorni, con opposizione motivata da presentare entro 14 giorni dalla comunicazione**. Questo impegno dovrà essere reso effettivo con una procedura di notifica e gestione delle obiezioni prima di far entrare in vigore il DPA. Durante il periodo di opposizione non deve attivare il nuovo trattamento contestato; in mancanza di alternativa valida, le parti concordano la cessazione della sola funzione interessata e restituzione/cancellazione.

Bodivine impone contrattualmente a ogni subresponsabile obblighi di protezione sostanzialmente equivalenti per i trattamenti affidati e rimane responsabile verso il Professionista dell'adempimento di tali obblighi ai sensi dell'art. 28(4). Per i servizi oggi necessari ma privi di verifica contrattuale, **l'attivazione del trattamento interessato resta bloccata**, non presunta autorizzata.

7. Trasferimenti e accessi extra-SEE — capo V GDPR

Le posizioni fisiche dichiarate delle regioni server non dimostrano che non vi siano accessi amministrativi remoti, log, assistenza, CDN, backup o trasferimenti extra-SEE. Prima dell'uso, Bodivine documenta per ogni flusso origine, destinazione, categorie di dati, ruolo, base di trasferimento (decisione di adeguatezza o SCC 2021/914 **effettivamente applicabili**, se pertinenti), valutazione del contesto di trasferimento e misure supplementari quando richieste. **Non si dichiara completata alcuna TIA né sottoscritte SCC con tutti i fornitori**. Se mancano le garanzie, il flusso viene sospeso o riprogettato; il consenso dell'interessato non è una soluzione generale per trasferimenti ripetuti.

8. Diritti degli interessati — art. 28(3)(e)

Bodivine assiste il Professionista, considerando natura del trattamento e informazioni disponibili, per accesso, rettifica, cancellazione, limitazione, portabilità, opposizione e altre richieste applicabili. Quando riceve direttamente una richiesta relativa a un cliente gestito dal Professionista, non ne valuta autonomamente il merito, ma la inoltra al referente del Professionista **senza ritardo ingiustificato**, limitando i dati condivisi e assistendo nell'esecuzione delle istruzioni dopo verifica dell'identità e dei poteri del richiedente. I diritti dei clienti senza account richiedono una procedura manuale effettiva; non promettere un portale self-service non presente.

La risposta agli interessati resta responsabilità del Professionista titolare nei termini del GDPR. Bodivine non cancella indiscriminatamente dati di altri titolari; documenta l'istruzione, l'esito, eventuali restrizioni legali e le copie residue.

9. Violazioni di dati personali — art. 33(2)

Dopo aver appreso di una violazione dei dati affidati, Bodivine avvisa il Professionista **senza ingiustificato ritardo**, tramite il contatto di sicurezza convenuto. Il primo avviso indica, per quanto noto, natura e momento dell'incidente, categorie e quantità approssimative di persone e record coinvolti, sistemi interessati, possibili conseguenze, misure adottate/proposte e referente; informazioni mancanti vengono integrate progressivamente. Bodivine conserva evidenze proporzionate, contiene l'incidente, coopera alle analisi e informa delle correzioni.

La valutazione e l'eventuale notifica all'autorità **entro 72 ore dalla conoscenza, ove obbligatoria**, e agli interessati spettano al Professionista, con assistenza di Bodivine. L'eventuale SLA operativo di avviso/risposta e i canali di emergenza, incluso un recapito per professionista, **non sono ancora verificati e devono essere formalizzati** nell'Allegato D; non si presume un monitoraggio 24/7.

10. Assistenza per artt. 32–36 e richieste delle autorità — art. 28(3)(f)

Bodivine mette a disposizione le informazioni tecniche pertinenti e assiste il Professionista nelle verifiche di sicurezza, nella gestione delle violazioni, nella valutazione d'impatto e nell'eventuale consultazione preventiva con il Garante, nei limiti della natura del trattamento e delle informazioni disponibili. Comunica, quando legalmente consentito, richieste vincolanti di dati da parte delle autorità che riguardino dati affidati e ne limita la consegna al perimetro richiesto. L'obbligo del Professionista di svolgere una propria DPIA non è sostituito dalla DPIA della piattaforma.

11. Documentazione, audit e ispezioni — art. 28(3)(h)

Bodivine rende disponibili le informazioni necessarie a dimostrare l'osservanza dell'art. 28 e **consente e contribuisce** a audit e ispezioni del Professionista o di un revisore da esso designato, anche oltre l'esame documentale quando necessario. Le parti concordano tempi ragionevoli, riservatezza, sicurezza degli altri clienti e perimetro, senza eliminare il diritto sostanziale di verifica né i poteri del Garante. Incidenti gravi o fondati indizi di

violazione possono rendere necessarie verifiche più tempestive. Certificazioni, penetration test e report di conformità **non disponibili** non vengono dichiarati esistenti.

12. Fine servizio: scelta tra restituzione e cancellazione — art. 28(3)(g)

Alla cessazione del servizio per il Professionista, Bodivine, **a scelta documentata del titolare**, restituisce in formato utilizzabile i dati trattati per suo conto oppure li cancella e provvede alla cancellazione delle copie, salvo specifici obblighi legali UE/di Stato membro che ne impongano la conservazione. Fino all'esecuzione mantiene i dati segregati e non li riutilizza. Fornisce riscontro dell'esecuzione e delle eccezioni documentate.

L'export completo, l'eliminazione del workspace professionale, i tempi massimi, la sorte dei client account condivisi e la scadenza delle copie nei backup non sono stati provati end-to-end. L'account professionale richiede attualmente assistenza per la cancellazione, non un pulsante automatico; prima dell'attivazione occorrono procedura concreta, tempi approvati e verifica in QA (Allegato D). Il termine di conservazione delle email di supporto di Bodivine come titolare autonomo non determina la conservazione dei dati cliente affidati.

13. Durata, modifica, gerarchia e cessazione

Il DPA efficace decorre solo da accettazione esplicita e registrata di una **versione finale stabile su HTTPS** (documento, data, metodo, professionista/utente accettante e SHA-256 del documento pubblicato). La separata dichiarazione del professionista sulla propria responsabilità privacy non sostituisce il DPA. Una modifica sostanziale richiede una nuova versione e nuova accettazione quando necessaria; non modificare retroattivamente gli hash o le accettazioni storiche. A cessazione, sopravvivono riservatezza, cancellazione/restituzione, assistenza e responsabilità nella misura necessaria.

La violazione grave degli obblighi del presente DPA può giustificare sospensione del trattamento interessato e risoluzione secondo legge e Termini; nessuna previsione esclude responsabilità inderogabili ex artt. 82–83 GDPR né le facoltà delle autorità. Per controversie e legge applicabile si applicano le disposizioni lecite dei Termini, fermo restando il carattere imperativo della normativa privacy.

Allegato A — Descrizione concreta del trattamento (art. 28(3))

Elemento	Trattamento per conto del Professionista
Finalità	Gestire rapporti professionali con clienti maggiorenni, piani, attività, misure/progressi, comunicazioni e appuntamenti su istruzione
Natura/operazioni	Raccolta mediante professionista o account collegato, creazione, lettura, modifica, associazione, conservazione, ricerca, condivisione autorizzata, esportazione PDF, inviti, cancellazione
Interessati	Clienti **18+** del professionista con o senza account Bodivine; professionista stesso se compare in messaggi e inviti
Dati identificativi	Nome, cognome/display name, email, data di nascita, paese, relazione cliente-professionista e stato invito/attestazione
Dati di attività	Piani nutrizionali, pasti/macronutrienti, schede di allenamento, cronologia workout e set, attività cardio, peso, circonferenze, composizione corporea, date e appuntamenti
Categorie particolari	Campi patologie e intolleranze, note libere, peso/misure e informazioni che **nel contesto** rivelino dati relativi alla salute ex art. 9 GDPR
Comunicazioni	Chat professionista-cliente e relativi metadati, inviti via email; evitare referti e informazioni mediche nei messaggi email esterni

Elemento	Trattamento per conto del Professionista
Frequenza	Su azione dell'utente/professionista e durante consultazioni, sincronizzazioni di interfaccia e richieste server
Luoghi tecnici dichiarati	Vercel Functions `fra1` (esecuzione applicativa) e Neon PostgreSQL `eu-central-1` (persistenza), sulla base della configurazione dichiarata; verificare console, fornitori a monte, log e accessi remoti
Durata	Per il rapporto attivo, con termini definiti dal titolare e procedura di fine servizio da approvare ai sensi dell'art. 12
Confine dei ruoli	Account/auth, assistenza, sicurezza applicativa e altri trattamenti propri di Bodivine **non sono automaticamente** trattamenti per conto di questo Professionista

I PDF sono generati tramite funzionalità server e scaricati dal browser; non si assume che esista un archivio permanente di PDF distinto dai record di origine senza ulteriori verifiche. Importazione da Open Food Facts riguarda informazioni su prodotti alimentari: eventuali dati o metadati trasmessi all'esterno richiedono un controllo separato, senza equiparare automaticamente quel fornitore a un subresponsabile di dati sanitari.

Allegato B — Misure tecnico-organizzative (stato reale, lacune e prove necessarie)

Legenda: `CODICE` = meccanismo individuato nel repository, non collaudo in produzione; `DICHIARATO` = informazione fornita dal titolare, non audit indipendente; `APERTO` = non verificato/da realizzare. Il testo non rende una misura operativa per il solo fatto di elencarla.

Area art. 32	Evidenza e stato al 06/11/2026	Condizione per la versione finale
Identificazione/autenticazione	`CODICE`: Better Auth, hash password bcrypt, verifica email, sessioni e supporto OAuth Google opzionale	QA reale session fixation/scadenze/revoca, sicurezza del segreto, configurazione cookie e MFA amministrativa
Autorizzazione e segregazione	`CODICE`: `lib/authz.ts`, gate DPA, controlli proprietario/cliente su route e query	Test multi-professionista, IDOR, query, inviti, revoche, race/concorrenza, chat, PDF, endpoint legacy
Consensi e responsabilità	`CODICE`: consenso salute dell'account; dichiarazione privacy e DPA separati/versionati nel branch	QA persistenza reale delle prove, condizioni art. 9 applicabili per cliente, revoca ed export
CSRF e abuso	`CODICE`: token CSRF e limitazione richieste	Test browser, proxy trusted IP, limiti per rotta, contromisure abuso e falsi positivi
Comunicazioni sicure	`CODICE`: API server e PDF in risposta autenticata	TLS effettivo per ogni hop, cache-control/download, assenza di payload salute nei log/email/URL
Dati a riposo e segreti	`APERTO`: cifratura, backup, key management, ruoli database, rotazione segreti e accessi provider non ispezionati	Evidenze contrattuali e tecniche dei provider, minimi privilegi, segreti non esposti, restore test
Logging e sicurezza operativa	`CODICE`: logger per request e alcuni eventi di sicurezza	Inventario di campi log, durata, redazione dati salute, alert, audit accessi amministrativi, incident response
Resilienza/disponibilità	`APERTO`: replica, PITR, backup, RPO/RTO, recupero e piano disaster recovery non collaudati	Prova di restore isolata, test perdita dati, runbook accessibile, tempi approvati
Diritto alla cancellazione	`CODICE`: cancellazione autonomo; professionista assistita; alcune rotte di cancellazione record	Workflow completo, backup/retention, conflitti su account collegati, registro richieste, prove cancellazione

Area art. 32	Evidenza e stato al 06/11/2026	Condizione per la versione finale
Fornitori e trasferimenti	`DICHIARATO`: regioni `fra1`/`eu-central-1`; email `privacy@bodivine.fit` inoltrata via Cloudflare Email Routing a Gmail con MFA attivata secondo titolare	Contratti per categorie particolari, località di ogni trattamento, accessi extra-SEE, DPA/SCC/TIA se necessari

Per le funzioni che trattano dati di salute il profilo **Vercel Hobby** segnalato nel registro di rilascio richiede un accordo idoneo o una migrazione reale del trattamento: le attuali condizioni DPA Vercel pubblicate vietano categorie particolari nei *Customer Data*. Non si afferma che il cambio di piano elimini il vincolo. Cloudflare Workers è un'ipotesi **non implementata**.

Allegato C — Registro dei fornitori/subresponsabili da confermare

La tabella non costituisce lista autorizzata né prova di contratti sottoscritti. `DA VERIFICARE` significa che non è possibile attivare il relativo trattamento professionale sulla sola base del presente documento. Separare il trattamento per conto del professionista dai dati che Bodivine tratta per finalità proprie.

Fornitore/servizio osservato	Possibile ruolo e dati pertinenti	Località/trasferimenti	Stato autorizzazione e verifica
Vercel, hosting Functions, SSR, API e PDF	**Subresponsabile candidato essenziale**: payload di record cliente e possibili dati salute transitano nelle funzioni; log e metadati da analizzare	`fra1` Francoforte **dichiarato**; rete/assistenza/accesso extra-SEE ignoti	**BLOCCANTE**: Hobby e divieto dati sensibili nel DPA pubblicato; richiede soluzione contrattuale/architetturale verificata, non una semplice URL
Neon, PostgreSQL	**Subresponsabile candidato essenziale**: archivio dei record cliente e categorie particolari	Regione `eu-central-1` Francoforte **dichiarata**; backup, personale, accessi e subfornitori da verificare	DPA applicabile, controparte giuridica, condizioni per dati salute, subfornitori, regioni/trasferimenti **DA VERIFICARE**
Resend, email transazionali	**Candidato limitato** agli inviti cliente (email, nome, link/token se inclusi) e comunicazioni autorizzate; parte delle email di account è trattamento proprio Bodivine	Destinazioni e accessi **DA VERIFICARE**; i termini pubblici non provano che l'account sia coperto	Validare DPA e lista subfornitori, payload email e assenza di dati salute; non presumere che tutti i contenuti delle chat vi transitino
Cloudflare Email Routing e **Google/Gmail**, ricezione `privacy@`/`support@`	Di regola **trattamento proprio di Bodivine** per richieste assistenza/privacy; se vi giungono dati affidati al professionista, verificare la catena concreta	Instradamento, archiviazione e accessi remoti **non verificati**	Non autorizzati automaticamente come subresponsabili del workspace; minimizzare/rimuovere dati sanitari inviati per errore; contratti/trasferimenti da classificare
Google OAuth, accesso account	Di norma account/autenticazione come trattamento proprio, non gestione diretta di patologie/clienti	Secondo effettiva configurazione provider	Verificare abilitazione, scope, ruoli e informativa; non includere senza nesso con dati per conto professionista
Vercel Analytics / Speed Insights	Analisi tecniche del sito: possibile trattamento proprio; **non deve** ricevere contenuti sanitari	Infrastruttura e condizioni da verificare	Controllare richieste di rete reali, identificatori, IP e assenza di contenuti clinici; non dichiararlo subresponsabile salute senza evidenza

Prima dell'attivazione approvare una **scheda per ciascun subresponsabile effettivo**: denominazione legale e sede, finalità, categorie dati/operazioni, regione primaria/backup, personale con accesso, subfornitori ulteriori, termini DPA effettivi, meccanismo art. 44 ss., eventuale TIA e misure supplementari, data della prova, canale

preavviso e persona che ha approvato. **Non** inserire Cloudflare Workers come provider attuale finché il traffico non vi sia realmente migrato.

Allegato D — Piano operativo vincolante da completare prima dell'accettazione

Elemento operativo / evidenza	Responsabile da confermare	Stato e condizione di chiusura
Identità contrattuale completa e recapito idoneo di Bodivine e del Professionista	Bodivine / Professionista	**APERTO**: persona fisica identificata ma recapito non definito; poteri di rappresentanza dei titolari professionali da verificare
Lista C firmata/approvata, contratti a valle e trasferimenti	Bodivine	**APERTO**: verificare contratti, sub-responsabili e trasferimenti applicabili; predisporre notifiche con almeno 30 giorni di preavviso e 14 giorni per opposizioni, come approvato dal gestore
Procedura diritti per clienti con/senza account	Bodivine / Professionista	Il gestore si incarica personalmente delle richieste via `privacy@bodivine.fit` (esportazione, cancellazione, chiusura profili professionali), fermo il ruolo del Professionista titolare dei dati dei clienti. **APERTO**: formalizzare verifica identità/istruzioni, registro, tempi, prove QA e modalità di comunicazione
Restituzione/cancellazione fine servizio	Bodivine / Professionista	**APERTO**: formato export, tempi, backup, account condivisi, attestazione completamento, eccezioni legali
Incident response e contatti	Bodivine / Professionista	**APERTO**: recapito per escalation, cronologia, presidio, reperibilità realistica, esercitazione
Controlli tecnici e ripristino	Bodivine / provider	**APERTO**: audit API multi-tenant, segreti, backup/recovery, log, retention, cifratura e accessi reali
Test DPA e informativa pubblicata	Bodivine	**APERTO**: URL HTTPS immutabile, contenuto effettivo, hash SHA-256, versione non retroattiva, doppia accettazione verificata in QA, nessun bypass
Decisione legale e autorizzazione attivazione	Titolare di Bodivine + consulente competente	**NON EMESSA**; firma elettronica/accettazione soltanto dopo chiusura dei punti sopra

Fonti normative e riscontro tecnico: GDPR artt. 6, 9, 28, 32–36, 44 ss.; EDPB: Linee guida titolare/responsabile; DPA Vercel (testo pubblico, da confrontare con l'accordo effettivo); DPA Resend. Repository: `prisma/schema.prisma`, `lib/authz.ts`, `lib/legal.ts`, `lib/professional-legal.ts`, `lib/auth.ts`, rotte `app/api/` e note interne `legal/RELEASE-GATE-2026-11-06.md`. Le condizioni dei provider devono essere riverificate alla data di efficacia.