Bodivine — Data Processing Agreement (DPA) for professional users

INTERNAL NON-EXECUTED CONTRACT DRAFT — 6 November 2026, revision 2. This text and Annexes A–D provide substantive proposed terms under GDPR Article 28, **not** an executed agreement, compliance certification or representation that safeguards have been deployed. Do not publish as an agreement available for acceptance, assign a final contractual version or set `PROFESSIONAL_DPA_VERSION`, `PROFESSIONAL_DPA_URL` or `PROFESSIONAL_DPA_SHA256` before the open items in Annex D have been resolved. Making this draft publicly accessible does not authorise client-data processing.

1. Parties, roles, scope and priority

Controller of their clients' personal data: each adult professional holding or creating a Bodivine professional account, with identity and contracting details to be captured and linked to the corresponding acceptance; corporate professionals require confirmation of the contracting entity and the accepting representative's authority. **Processor:** Cristian Montanari, an individual operating in Italy under the name Bodivine, contact `privacy@bodivine.fit`. An appropriate legal/contact address for the processor has not been established: **a blocker before execution**. No incorporated company, VAT number or business address is asserted.

This DPA applies only where the Professional determines the purposes and essential means of their clients' processing and Bodivine processes those data on the Professional's behalf. For user accounts, authentication, service security, requests made directly to Bodivine and administration of its own account relationships, Bodivine may be an **independent controller**, as described in its Privacy Notice, depending on the particular processing. Shared infrastructure alone does not make every activity processing on behalf of the Professional. Any joint controllership would require a separate Article 26 arrangement.

Once completed and executed, this DPA, including all annexes, forms part of the Terms of Service for the activities in Annex A and prevails where the Terms conflict regarding entrusted client data. Mandatory data-protection rules remain unaffected.

2. Subject matter, duration, categories and documented instructions — Article 28(3)

The subject matter, duration, nature, purposes, data subjects, personal data and operations are specified in **Annex A**. Ordinary processing runs for the duration of the Professional's use of client-management services, followed by return or deletion under Section 12 and Annex D; technical post-termination limits must be agreed **before activation**.

The Professional issues documented instructions through this DPA, authorised product features (creating, assigning, updating, viewing, exporting and deleting client records, sending invitations and communicating), and subsequent verifiable instructions sent through the agreed contact channel. Bodivine must not use entrusted client data for its own advertising, model training, sale to third parties, independent profiling or purposes unrelated to the instructions. International transfers are also subject to documented instructions and GDPR Chapter V.

Where processing otherwise than on instructions is required by applicable Union or Member State law, Bodivine informs the Professional **before** processing unless legally prohibited for important public-interest reasons. Bodivine **immediately** informs the Professional if, in its opinion, an instruction infringes the GDPR or other applicable EU/Member State data protection law; where appropriate it suspends the specific unlawful instruction while the issue is resolved.

3. Professional controller's responsibilities and rights

The Professional defines and documents purposes, necessity, minimisation, accuracy, retention and recipients; provides privacy information under Articles 12–14; establishes an Article 6 lawful basis; and, **where special-category data such as health data are processed**, a separate applicable condition under Article 9(2), including explicit consent **when required by law**. The Professional verifies that clients are adults and must not upload minors' data (the Service's 18+ rule). Authority to manage a client and that client's consent are separate matters. The Professional handles clients' rights requests and decides controller-level breach notifications.

The Professional may request information, assistance, subprocessor review, return and erasure under this DPA. The separate professional privacy attestation is not, by itself, evidence of the lawful basis for **each individual client**. The Professional must not upload data that the actually authorised infrastructure is contractually prohibited from processing.

4. Authorised persons and confidentiality — Article 28(3)(b)

Bodivine limits access to entrusted data to persons who need it to provide support, handle incidents or carry out instructions. Such persons are bound by contractual or statutory confidentiality duties continuing after access ends. Permissions, credentials and privileges must be revoked promptly when no longer needed. **This draft does not claim that staff exist, that administrator access logs have been audited or that access reviews have already occurred**; see Annex B.

5. Security — Articles 28(3)(c) and 32

Bodivine must implement and maintain technical and organisational safeguards appropriate to risk: confidentiality, integrity, availability, resilience and restorability; periodic testing; access and privilege controls; protection in transit; and prevention of loss and unauthorised disclosure. Controls **identified in source code** are distinguished from controls **not yet operationally evidenced** in Annex B. References to at-rest encryption, security audits, functioning backups or certifications do not assert that any such measures are presently implemented.

The Professional is responsible for safeguards within their own control (devices, credentials, sharing exported files and authorising collaborators). Processing health data demands proportionate safeguards and is not rendered lawful merely by user consent or this document.

6. Subprocessors and authorisation — Article 28(2), (4)

General written authorisation by the Professional may apply **only to the final, approved register of actual subprocessors** in Annex C as of the effective date; this draft gives **no authorisation** for a provisional list. Bodivine maintains that register and provides advance notice of planned additions or replacements, identifying the services, locations and transfers. **Operational terms approved by the operator for the final agreement: at least 30 days' advance notice, with 14 days from notification to raise a reasoned objection**. A working notice and objection-handling procedure must be in place before this DPA takes effect. During the objection period Bodivine must not activate the challenged new processing; absent a lawful alternative, the parties arrange termination of the affected functionality and return/deletion.

Bodivine must impose substantially equivalent data-protection duties on each subprocessor through a binding contract and remains responsible to the Professional for that subprocessor's performance under Article 28(4). Where a required current service has not been contractually verified, **the relevant processing must remain disabled** rather than be deemed authorised.

7. International transfers and access outside the EEA — GDPR Chapter V

Declared server regions alone do not rule out remote administrative access, logs, support activity, CDN use, backups or transfers outside the EEA. Before processing, Bodivine documents for each flow its origin, destination, data categories, roles, transfer mechanism (adequacy decision or **actually applicable** 2021/914 SCCs where appropriate), transfer-context assessment and supplementary measures where required. **This document does not claim a completed TIA or executed SCCs with every provider.** Without adequate safeguards, the relevant flow must be suspended or redesigned. Individual consent is not a general fix for repeated transfers.

8. Data subject rights — Article 28(3)(e)

Taking into account processing's nature and the information available, Bodivine assists the Professional with access, rectification, erasure, restriction, portability, objection and other applicable rights requests. If Bodivine directly receives a request regarding a client managed by the Professional, it does not decide the merits but refers it to the Professional's agreed contact **without undue delay**, sharing only what is necessary and assisting with verified lawful instructions. Requests from clients without accounts need an effective manual process; no absent self-service portal is promised.

The Professional remains responsible for responding to data subjects within GDPR deadlines. Bodivine must not indiscriminately delete data belonging to different controllers; it records the instruction, action taken, applicable legal restrictions and any outstanding copies.

9. Personal data breaches — Article 33(2)

After becoming aware of a personal data breach affecting entrusted data, Bodivine notifies the Professional **without undue delay** through the agreed security contact. The initial notice includes, insofar as available, incident nature and timing, approximate categories and numbers of affected persons and records, impacted systems, likely consequences, measures taken or proposed and a contact person; missing details are supplied progressively. Bodivine preserves proportionate evidence, contains the incident, cooperates in investigation and reports remediation.

The Professional as controller determines whether to notify the supervisory authority **within 72 hours of awareness where required**, and whether to inform affected individuals, with Bodivine's assistance. Operational notice/response service levels and emergency contact details, including a contact for each Professional, **have not been validated and must be agreed** in Annex D; no 24/7 incident monitoring is asserted.

10. Assistance under Articles 32–36 and authority requests — Article 28(3)(f)

Bodivine makes relevant technical information available and assists the Professional with security reviews, breaches, data protection impact assessments and prior consultation with the supervisory authority, accounting for the processing's nature and the information available. Where legally permitted, it informs the Professional of binding authority requests concerning entrusted data and limits disclosure to what is lawfully required. The Professional's obligation to perform its own DPIA is not displaced by Bodivine's platform DPIA.

11. Evidence, audits and inspections — Article 28(3)(h)

Bodivine makes available all information necessary to demonstrate compliance with Article 28 and **allows and contributes to audits and inspections** by the Professional or an appointed auditor, beyond document review where necessary. Parties arrange reasonable timing, confidentiality, protection of other customers and scope without negating meaningful audit rights or supervisory authority powers. Serious incidents or credible suspected

breaches may justify more urgent examination. Certifications, penetration tests and compliance reports **not available** are not claimed to exist.

12. End of services: choice of return or erasure — Article 28(3)(g)

At the end of the Professional's service, Bodivine, **at the controller's documented choice**, returns entrusted personal data in a usable format or erases them and existing copies, unless specific Union or Member State law requires retention. Pending completion, remaining data are protected and not repurposed. Bodivine provides a record of execution and any documented legal exceptions.

Complete export, deletion of a professional workspace, maximum execution times, treatment of shared client accounts and backup erasure schedules have not been tested end-to-end. Currently professional account deletion requires support; it is not an automatic self-service action. Concrete procedures, agreed deadlines and QA evidence are required **before activation** (Annex D). Bodivine's own support-email retention as an independent controller does not determine retention of client data entrusted by the Professional.

13. Term, changes, hierarchy and termination

This DPA can become effective only through express, recorded acceptance of a **stable final version published over HTTPS** (document, date, method, Professional/accepting user and SHA-256 of the actually published document). The separate statement acknowledging professional privacy responsibility is not a substitute. Material changes require a new version and renewed acceptance where required, without altering historical hashes or acceptance evidence. Confidentiality, return/erasure, assistance and responsibility survive termination as necessary.

Serious non-compliance may justify suspension of the relevant processing and termination as allowed by law and Terms. No provision excludes mandatory liability under GDPR Articles 82–83 or supervisory authority powers. Law and disputes follow lawful Terms provisions, subject always to mandatory data protection law.

Annex A — Actual processing description (Article 28(3))

Element	Processing on behalf of the Professional
Purpose	Manage professional relationships with adult clients, plans, activities, measurements/progress, communications and appointments on instruction
Nature/operations	Collection through the Professional or linked account, creation, access, updates, linkage, storage, search, authorised sharing, PDF exports, invitations, deletion
Data subjects	Professional's **18+** clients with or without Bodivine accounts; the Professional where their details appear in communications and invitations
Identifiers	Name, surname/display name, email, date of birth, country, client–Professional relationship and invitation/attestation status
Activity data	Nutrition programmes, meals/macronutrients, workout plans, exercise and set logs, cardio, weight, measurements, body composition, dates and appointments
Special categories	Medical conditions, intolerances, free-text notes, weight/measurements and information which **in context** reveal health information under GDPR Article 9
Communications	Professional–client chat and related metadata, email invitations; avoid medical reports and health information in external emails
Frequency	On Professional/user actions and during interface requests and server-side data retrieval

Element	Processing on behalf of the Professional
Declared technical regions	Vercel Functions `fra1` (application processing) and Neon PostgreSQL `eu-central-1` (persistent storage), based on declared settings; verify provider consoles, underlying services, logs and remote access
Duration	During the active professional relationship, subject to controller-defined retention and the approved end-of-service process under Section 12
Role boundary	Accounts/authentication, support, application security and other Bodivine purposes are **not automatically** processing on behalf of that Professional

The application generates PDF exports using server-side features and returns them to browsers; no independent permanent PDF archive is asserted without further checks. Open Food Facts integration concerns food product information: any externally transmitted information or metadata require separate analysis, without automatically treating that provider as a subprocessor for health data.

Annex B — Technical and organisational measures (actual status, gaps and required evidence)

Key: `CODE` = mechanism identified in repository, **not** production audit; `DECLARED` = controller/operator statement, not independent assurance; `OPEN` = not verified or not implemented. Listing a measure does not make it operational.

Article 32 area	Evidence and status as of 6 Nov 2026	Condition before finalisation
Identification/authentication	`CODE`: Better Auth, bcrypt password hashing, email verification, sessions and optional Google OAuth	Test session fixation/expiry/revocation, secret safety, cookie settings and administrator MFA
Authorisation/tenant isolation	`CODE`: `lib/authz.ts`, DPA access gate, owner/client checks in routes and queries	Cross-professional, IDOR, query, invitation, revocation, race, chat, PDF and legacy endpoint QA
Consent/accountability	`CODE`: account health consent and separate versioned professional privacy declaration/DPA in branch	Real persistence tests, applicable client-level Article 9 conditions, withdrawal and exports
CSRF/abuse	`CODE`: CSRF tokens and request rate limiting	Browser tests, trusted-proxy IP configuration, route limits and abuse resistance
Secure communications	`CODE`: server API and authenticated PDF responses	Verify TLS on each hop, download/cache controls and absence of health payloads in logs, email and URLs
At-rest data/secrets	`OPEN`: encryption, backups, key management, DB roles, secret rotation and provider access not inspected	Provider technical/contract evidence, least privilege, no secret exposure, restoration testing
Logging/operations	`CODE`: request and selected security event logging	Inventory log fields, retention, health-data redaction, alerting, admin access audit and incident runbook
Availability/recovery	`OPEN`: replication, point-in-time restore, backup, RPO/RTO and disaster recovery untested	Isolated restore exercise, loss-of-data tests, available runbook and approved targets
Deletion	`CODE`: autonomous deletion, support-assisted professional deletion and selected client-record deletes	End-to-end process, backups/retention, linked-account conflicts, rights register and erasure evidence
Providers/transfers	`DECLARED`: `fra1`/`eu-central-1`; support email forwarded from `privacy@bodivine.fit` via Cloudflare Email Routing to Gmail with MFA reportedly enabled	Contracts allowing special categories, all processing/access locations, non-EEA access and DPA/SCC/TIA where necessary

For functions processing health data, the existing **Vercel Hobby** setup identified in the release gate requires an appropriate written arrangement or an actually completed architectural migration: Vercel's published DPA terms prohibit special-category *Customer Data*. No assumption is made that switching tiers alone removes that restriction. Cloudflare Workers is **not yet** the application host.

Annex C — Provider/subprocessor register awaiting validation

This table is neither an authorised subprocessor list nor proof of signed agreements. `TO VERIFY` means professional processing cannot be activated solely on this document. Distinguish processing on behalf of the Professional from Bodivine's own controller activities.

Observed provider/service	Potential role and relevant data	Location/transfers	Authorisation and verification status
Vercel, Functions/SSR/API/PDF hosting	**Essential candidate subprocessor**: client-record requests and possible health data pass through server functions; logs/metadata require assessment	`fra1` Frankfurt **declared**; network, support and non-EEA access unknown	**BLOCKER**: Hobby and prohibition of special-category Customer Data in published DPA; verified contractual/architectural remedy required, not merely a URL
Neon, PostgreSQL	**Essential candidate subprocessor**: client records and special categories stored	`eu-central-1` Frankfurt **declared**; backups, personnel, remote access and downstream providers unverified	Applicable DPA, legal counterparty, health-data permissions, subproviders, regions/transfers **TO VERIFY**
Resend, transactional email	**Limited candidate** for client invites (address, name and link/token if included); some account emails are Bodivine's own processing	Destinations and remote access **TO VERIFY**; public terms do not establish acceptance by this account	Check actual DPA/subprovider list, email payloads and exclusion of health data; do not assume all chat messages are transmitted
Cloudflare Email Routing and **Google/Gmail** receiving `privacy@`/`support@`	Generally **Bodivine's own processing** of privacy/support mail; assess actual chain if entrusted client data arrive there	Routing, storage and remote access **not verified**	Not automatically authorised workspace subprocessors; minimise/remove inadvertently received health data; classify contracts and transfers
Google OAuth for account sign-in	Generally Bodivine account/authentication, not direct handling of client pathologies	Depends on configured provider settings	Verify whether enabled, scopes, roles and notice; do not include without evidence of entrusted-data access
Vercel Analytics / Speed Insights	Site telemetry potentially Bodivine's own processing; **must not** receive health content	Infrastructure and terms to verify	Inspect actual requests, identifiers/IP and absence of clinical content; not deemed health subprocessors without evidence

Before activation complete an **approved per-actual-subprocessor record**: legal entity/address, task, data categories and processing operations, primary/backup regions, personnel access, further processors, actually effective DPA, GDPR Articles 44 et seq. mechanism, any transfer impact assessment and supplementary measures, proof date, advance-notice route and approving person. Do **not** list Cloudflare Workers as current app hosting until traffic and processing have actually moved.

Annex D — Operational schedule requiring completion before acceptance

Operational item/evidence	Responsible party to confirm	Status and completion requirement
Complete contracting identity and valid contact of Bodivine and the Professional	Bodivine / Professional	**OPEN**: individual known, legal contact address unresolved; authority of Professional's corporate representative needs checking
Approved Annex C, downstream contracts and transfers	Bodivine	**OPEN**: verify applicable contracts, subprocessors and transfers; implement notices of at least 30 days and a 14-day objection window, as approved by the operator
Rights handling for clients with/without accounts	Bodivine / Professional	The operator will personally handle requests received at `privacy@bodivine.fit` (exports, erasure and professional account closure), while the Professional remains the controller for client records. **OPEN**: verify identity and instructions, document response records, deadlines, QA and communication steps
Return/erasure at end of services	Bodivine / Professional	**OPEN**: export format, deadlines, backups, shared accounts, completion record and legal exceptions
Incident response and contact routes	Bodivine / Professional	**OPEN**: escalation details, timeline, realistic coverage and exercise
Security checks and recovery	Bodivine / providers	**OPEN**: tenant isolation, secrets, backups/recovery, logs, retention, encryption and real access
Published DPA and acceptance tests	Bodivine	**OPEN**: immutable HTTPS content, real SHA-256, versioning without retroactive overwrite, dual acceptance tested in QA, no bypass
Legal sign-off and activation approval	Bodivine's accountable operator + qualified adviser	**NOT ISSUED**: electronic execution/acceptance only after the above are resolved

Legal sources and technical grounding: GDPR Articles 6, 9, 28, 32–36 and 44 et seq.; EDPB controller/processor guidelines; Vercel DPA (published text, compare with the actually effective agreement); Resend DPA. Repository: `prisma/schema.prisma`, `lib/authz.ts`, `lib/legal.ts`, `lib/professional-legal.ts`, `lib/auth.ts`, `app/api/` routes and `legal/RELEASE-GATE-2026-11-06.md`. Provider terms must be verified again at effective date.