

Data Processing Addendum (DPA)

Between Nila Solutions Limited (Processor) and the Customer named in the Order Form (Controller).

Template. This is the standard form Nila Solutions Limited offers to Enterprise customers (250+ seats). It is intended as a starting point for legal review by your counsel. The executed DPA forms part of the Master Services Agreement (MSA). Square brackets [] indicate fields to be completed at signature.

1. Definitions

Capitalised terms not defined here have the meaning given in the MSA. "Applicable Data Protection Law" means PIPEDA (Canada), GDPR / UK GDPR, the California Consumer Privacy Act as amended by the CPRA, and any other privacy or data-protection law applicable to the Processing of Personal Data under this Addendum.

2. Roles of the Parties

Customer is the Controller of Personal Data of its employees who redeem a Nila membership. Nila Solutions Limited acts as Processor of seat-administration metadata (invite codes, redemption status, aggregate engagement) on behalf of Customer.

Member-generated content — symptoms, journal entries, mood patterns, community posts, conversations with Nila — is processed by Nila as an independent Controller in a direct relationship with the individual member, governed by the member-facing Privacy Policy. Customer has no rights of access to this data and Nila will not disclose it to Customer.

3. Scope and Purpose of Processing

- **Subject matter:** administration of menopause-support memberships purchased by Customer for its workforce.
- **Duration:** the term of the Order Form plus the retention periods set out below.
- **Nature and purpose:** issuing and tracking invite codes; producing aggregate, anonymized engagement reporting; processing billing.
- **Categories of data subjects:** Customer's employees and contractors who choose to redeem a seat.
- **Categories of Personal Data:** work email address (only if Customer chooses to distribute codes by email); redemption status; aggregate engagement metrics.
- **Special categories:** none processed on Customer's behalf. Member health data is processed by Nila as Controller in its direct relationship with the member.

4. Processor Obligations

Nila will: (a) Process Personal Data only on documented instructions from Customer, including with regard to transfers to third countries; (b) ensure persons authorised to Process Personal Data are bound by confidentiality; (c) implement the technical and organisational measures described in Annex A; (d) assist Customer with data-subject requests and DPIAs to the extent reasonably required; (e)

notify Customer without undue delay (and within 72 hours where feasible) of any Personal Data Breach affecting Customer Data; (f) make available information necessary to demonstrate compliance and allow for audits as set out in §8.

5. Sub-processors

Customer authorises Nila to engage the sub-processors listed in Annex B. Nila will give Customer at least 30 days' notice of any intended addition or replacement and will give Customer the opportunity to object on reasonable data-protection grounds.

6. International Transfers

Where Personal Data is transferred outside the country of collection, Nila will rely on an appropriate transfer mechanism, including (as applicable) the EU Standard Contractual Clauses, the UK International Data Transfer Addendum, and PIPEDA-compatible contractual safeguards. The current primary hosting region is the United States (AWS us-west-2, operated by Supabase, Inc.).

7. Security

Annex A describes the technical and organisational measures Nila maintains, including encryption in transit and at rest, role-based access, audit logging, principle-of-least-privilege for administrative access, and tested backup and incident-response procedures.

8. Audit

Customer may, no more than once per twelve (12) months and on at least 30 days' written notice, request a remote audit limited to information necessary to verify Nila's compliance with this Addendum. Nila will respond to a reasonable written security questionnaire in lieu of an on-site audit.

9. Return and Deletion

On termination Nila will, at Customer's choice, return or delete all Customer Data (seat administration data) within sixty (60) days, except where retention is required by law. Member-generated content is retained or deleted in accordance with the member-facing Privacy Policy and the member's own choices.

10. Liability and Order of Precedence

Liability under this Addendum is subject to the limitations in the MSA. In the event of conflict between this Addendum and the MSA on matters of Personal Data, this Addendum prevails.

Annex A — Technical and Organisational Measures

- TLS 1.2+ for all data in transit; AES-256 at rest.
- Role-based access; multi-factor authentication required for administrative access.
- Row-level security enforced on member data; service-role keys held in restricted secret stores.
- Audit logs retained for a minimum of 90 days.
- Documented incident-response procedure with defined severities and notification SLAs.
- Tested encrypted backups; defined RPO and RTO disclosed on request.

Annex B — Sub-processors (current)

- Supabase, Inc. — managed Postgres, auth, storage, edge functions. Region: US (AWS us-west-2).
- Stripe, Inc. — payment processing for seat purchases.
- Resend (or Customer-equivalent) — transactional email delivery for invite codes.
- Cloudflare, Inc. — edge delivery, DDoS protection.

The live sub-processor list is published at hellonila.com/data-privacy-institutional and updated on material change.

Signatures

Customer (Controller)

Name: _____ Title: _____

Signature: _____ Date: _____

Nila Solutions Limited (Processor)

Name: _____ Title: _____

Signature: _____ Date: _____