Data Processing Agreement (DPA)

Template — Article 28 GDPR / Personopplysningsloven

Version 1.1 · Effective from execution by both parties

Parties

Processor: Zelirotech AS, Norway. Contact: aleksander@zelirotech.dev.

Controller: _____ (the Customer identified in the Zelirotech subscription / order).

1. Subject matter and duration

This DPA governs the Processor's processing of personal data on behalf of the Controller under the Zelirotech subscription agreement (the “Service Agreement”). It runs for as long as the Processor processes personal data on behalf of the Controller, and survives termination to the extent required for return or deletion of data.

2. Nature, purpose and categories

Nature and purpose: hosting, operating and maintaining the Controller's web and mobile application as described in the Service Agreement.

Categories of data subjects: the Controller's end users, employees, customers and any individuals whose personal data the Controller chooses to store in the Service.

Categories of personal data: identifiers (name, email, phone, account ID), authentication data, profile and preference data, transaction and billing metadata, content submitted by data subjects, technical data (IP, device, timestamps).

Special categories: none expected; the Controller shall not submit Art. 9 / Art. 10 data without prior written notice and a documented lawful basis.

3. Processor obligations

The Processor shall: (a) process personal data only on documented instructions from the Controller, including the Service Agreement and this DPA; (b) ensure persons authorised to process the data are bound by confidentiality; (c) implement the technical and organisational measures listed in Annex II; (d) assist the Controller with data subject requests and Art. 32–36 obligations; (e) make available all information necessary to demonstrate compliance and allow for audits (one per year, on 30 days' notice, at Controller cost).

4. Sub-processors

The Controller grants general written authorisation for the Processor to engage the sub-processors listed in Annex I. The Processor will notify the Controller of any intended changes at least 30 days in advance, giving the Controller the opportunity to object on reasonable data-protection grounds.

5. International transfers

Primary processing takes place in the EU/EEA on Supabase-managed infrastructure within the EU region. Where a sub-processor processes data outside the EEA, the Processor relies on the EU Standard Contractual Clauses (2021/914) and supplementary measures as required by Schrems II.

6. Security

The Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, in line with Art. 32 GDPR. See Annex II.

7. Personal data breach

The Processor shall notify the Controller without undue delay and at the latest within 72 hours of becoming aware of a personal data breach affecting the Controller's data, with the information required by Art. 33(3).

8. Data subject rights

Taking into account the nature of the processing, the Processor shall assist the Controller by appropriate technical and organisational measures, insofar as possible, in fulfilling the Controller's obligation to respond to requests under Chapter III GDPR.

9. Return or deletion of data

On termination of the Service Agreement the Processor shall, at the Controller's choice, return or delete all personal data, save where Union or Member State law requires storage. A 30-day handover window is provided in which the Controller may export the data via the dashboard or by signed pg_dump on request. After 30 days, customer workspaces are permanently deleted; backups age out within a further 60 days.

10. Liability and governing law

Liability for breach of this DPA follows the limitation regime of the Service Agreement. This DPA is governed by Norwegian law, with venue in Oslo District Court.

Annex I — Sub-processors

Supabase — Managed Postgres, authentication, file storage. Location: EU region.

Cloudflare — Static frontend hosting and CDN (no customer data). Location: Global edge.

Stripe — Subscription billing and payment processing. Location: EU + US (SCCs).

Resend — Transactional email delivery. Location: EU + US (SCCs).

Annex II — Technical and organisational measures

• Encryption in transit (TLS 1.2+) and at rest (AES-256 on Supabase managed Postgres and storage).

• Per-customer workspace isolation enforced by Postgres row-level security policies.

• Least-privilege access controls; the service-role key is restricted to server-side functions only.

• Multi-factor authentication required on all Zelirotech admin accounts.

• Daily automated backups, retained 30 days, with documented restore procedure.

• Centralised application and database logs; alerting on anomalous access.

• Documented incident-response runbook with 72-hour breach notification target.

• Annual review of sub-processors and their security posture.

Signatures

For the Controller:

Name: _____ Title: _____

Signature: _____ Date: _____

For the Processor (Zelirotech AS):

Name: Aleksander Stenseth Title: Founder

Signature: _____ Date: _____

This is a template. The executed version, once signed by both parties, prevails. Email aleksander@zelirotech.dev to request a counter-signed copy.