Data Processing Agreement (DPA)

Between:

Dombestein Data ("Processor")

and

Client ("Controller")

Version: 1.0
Effective Date: 01.12.2025

1. **Introduction**
   This Data Processing Agreement ("Agreement" or "DPA") governs the processing of personal data performed by **Dombestein Data** on behalf of the **Client** in connection with software development, hosting, operations, maintenance, and associated digital services.

   This DPA forms an integral part of any service agreement, collaboration or project in which Dombestein Data processes personal data for the Client.

   This Agreement is intended to fulfill the requirements of Article 28 of the GDPR. The Controller determines the purposes and legal basis of all Processing activities. The Processor shall process Personal Data only on documented instructions from the Controller, unless required to do so by Union or Member State law.

2. **Definitions**
   Terms used in this DPA shall have the meaning given in Article 4 of the GDPR, including:
   - **"Personal Data"** – any information relating to an identifiable natural person.
   - **"Processing"** – any operations performed on Personal Data.
   - **"Controller" –** the entity which determines the purposes and means of processing Personal Data.
   - **"Processor" –** The entity which processes Personal Data on behalf of the Controller.
   - **"Sub-Processor" –** Any third party engaged by the processor to assist in processing activities
   - **"Data Subject" –** identified or identifiable natural person

- **“Supervisory Authority” –** the national authority responsible for enforcing GDPR

3. **Roles**
   Controller: The Client
   Processor: Dombestein Data (Isak Dombestein, sole proprietor)

   The Controller retains full control over the Personal Data and determines the purpose and legal basis for processing.

   The Processor acts solely on documented instructions from the Controller. Documented instructions from the Controller include configuration changes made through the system dashboard, written instructions sent by email, or instructions set out in contractual agreements between the Parties. Any instructions requiring material changes to the Processing must be confirmed in writing by both Parties.

   The processor shall immediately inform the controller if, in its opinion, an instruction from the Controller infringes the GDPR or other applicable data protection laws.

4. **Subject Matter and Purpose of Processing**
   The Processor may process Personal Data for the following purposes:
   - Hosting and maintenance of web services
   - Backend / API operations
   - Database hosting and management
   - Email delivery on behalf of the Client
   - Logging, monitoring, and support activities
   - Debugging and ensuring system stability
   - Import / Export of booking or operational data upon request

   The processor shall not use Personal Data for any other purposes.

5. **Duration**
   This DPA remains in effect for the duration of the service relationship and remains binding until all Personal Data has been returned or deleted in accordance with this Agreement.

6. **Type of Personal Data and Categories of Data Subjects**
   Depending on the Client's use of the system, the Processor may process:

   Types of Personal Data

   - Names
   - Email addresses
   - Contact details
   - Technical metadata (timestamps, logs, IP addresses if provided by upstream services)

   Technical logs generated by the platform or its Sub-processors may include IP addresses, timestamps, device identifiers and system-level metadata. Such logs are retained only as necessary for security monitoring, debugging, and ensuring system integrity.

   Categories of Data Subjects

   - Individuals submitting booking requests
   - Employees or volunteers of the Client
   - Website visitors (Limited to provided data)

   The processor does not intentionally process sensitive personal data (GDPR Art. 9).

   The Processor does not sell, rent, disclose, or otherwise commercialize Personal Data.

7. **Obligations of the Processor**
   The Processor shall:

   7.1 Process only under documented instructions

   Process Personal Data solely for:

   - Tasks explicitly agreed to,
   - Tasks clearly inherent to the system's operations, or
   - Tasks required to comply with law

7.2 Confidentiality

Ensure all persons with access to Personal Data:

- Are bound by confidentiality,
- Understand their obligations
- Only access data when necessary.

7.3 Security Measures

Implement appropriate technical and organizational security measures such as:

- Encrypted storage (PostgreSQL, Supabase)
- TLS / HTTPS encryption in transit
- Access control with MFA where available
- Secrets stored using secure environment variables
- Role-based access
- Daily / continuous backups (via Supabase)
- Logging and monitoring of system operations
- Zero direct access to email content unless strictly required for debugging

Full TOM documentation is attached in **Appendix A**.

7.4 Sub-processors

The Processor may use the following Sub-processors:

Sub-Processor	**Purpose**	**Location**	**Safeguards**
Supabase	Database, auth, storage	EU region	GDPR DPA + SCCs
Cloudflare	Edge Hosting, DNS, CDN	EU / Global	GDPR DPA + SCCs
Resend	Transactional Email	US	GDPR DPA + SCCs
GitHub	Code Hosting	US / EU	SCCs

The processor shall:

- Notify the Controller of material changes to sub-processors,
- Ensure sub-processors are GDPR compliant,
- Ensure they only process data necessary for their function.

The Controller may object to the engagement of a new Sub-processor on reasonable ground relating to data protection. In such a case, the Parties shall

discuss in good faith to reach a commercially reasonable solution. If the Controller objects to a new Sub-processor and no agreement can be reached, either party may terminate the affected services without penalty.

7.5 Assistance

Assist the Controller in fulfilling GDPR obligations, including:

- Responding to data subject requests,
- Providing relevant information for impact assessments,
- Implementing appropriate security measures.

7.6 Breach Notification

Notify the Controller **without undue delay** and **no later than 24 hours** after becoming aware of a Personal Data Breach.

Notification must include:

- Description of the breach,
- Type of data affected,
- Number and categories of data subjects,
- Mitigation steps taken.

7.7 Return or deletion of data

Upon termination of service, the Processor shall:

- Return all Personal Data upon request, and
- Permanently delete all Personal Data within **60 days**, except where retention is required by law.

Deletion is logged and verifiable.

Backups maintained automatically by Sub-processors (e.g., Supabase) may retain encrypted copies of data for their standard retention period. Such backups expire automatically and are not actively accessible.

8. **Obligations of the Controller**

   The Controller shall:

   - Ensure personal data is processed lawfully,
   - Provide clear instructions to the Processor,
   - Maintain an appropriate legal basis for all data sent to the Processor,
   - Inform the Processor of any inaccuracies requiring correction,
   - Ensure Data Subjects are properly informed.

9. **International Transfers**

   If data is transferred outside the EEA by a Sub-processor:

   - This shall occur only with GDPR-approved safeguards, such as **Standard Contractual Clauses (SCCs).**
   - The Processor ensures sub-processors maintain compliance.

   The Processor does not perform international transfers of Personal Data except through approved Sub-processors listed in this document.

10. **Audits**

    The Controller may request documentation or evidence of compliance. Formal audits may be performed with reasonable notice and at reasonable cost, unless mandated by law.

11. **Liability**

    Each party is liable for GDPR violations to the extent they are responsible under applicable law. Processor shall not be liable for actions taken under the Controller's explicit instructions.

12. **Governing Law and Jurisdiction**

    This Agreement shall be governed by the laws of Norway. Disputes shall be resolved by Norwegian courts, with **Bergen Tingrett** as agreed legal venue.

13. **Contact Information**

Controller Contact	**Processor Contact (Dombestein Data)**
To be specified in the applicable service agreement or order form.	Isak Dombestein isak@dombesteindata.net

14. Amendments

This DPA may be updated to maintain GDPR compliance. Material changes require written approval by both parties.

For the Controller (Client):

Name: _____
Role: _____
Date: _____

Sign: _____

For the Processor (Dombestein Data):

Name: _____
Role: _____
Date: _____

Sign: _____

Appendix A – Technical & Organizational Measures (TOMs)

Access Control

- Limited access based on role and necessity
- MFA enabled where supported
- Secure credential storage
- Least privilege principles

Encryption

- HTTPS / TLS for all communication
- Encrypted database connections
- Passwords stored using Supabase Auth hashing (bcrypt / scrypt depending on config)

System Monitoring

- Application logs
- Error tracking
- Monitoring of failed login attempts
- No collection of unnecessary user metadata

Backup & Recovery

- Managed by Supabase with automatic recovery points
- Regular system health checks

Data Separation

- Tenant-level logical segregation
- Dedicated database tables for client data

Secure Development Practices

- Version Control through GitHub
- Code reviews for security-critical changes
- Dependency updates and vulnerability scanning