Data Processing Agreement (DPA) – Marivida AS

Version 1.0 – February 2026

This Data Processing Agreement ("Agreement" or "DPA") forms part of, and is incorporated into, the SaaS or other master agreement between the Controller and Marivida AS ("Processor") governing the provision of the MariCare / MariFlow services (the "Services").

1. Definitions

For the purposes of this DPA:

- **"Applicable Data Protection Law"** means the GDPR (Regulation (EU) 2016/679) and any applicable national data protection laws.
- **"Controller"** means the entity that determines the purposes and means of the Processing of Personal Data.
- **"Processor"** means Marivida AS, which Processes Personal Data on behalf of the Controller.
- **"Personal Data"** means any information relating to an identified or identifiable natural person as defined in the GDPR.
- **"Processing" / "Process"** means any operation or set of operations performed on Personal Data, whether automated or not.
- **"Subprocessor"** means any third party engaged by the Processor to Process Personal Data as part of the Services.
- **"Personal Data Breach"** means a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data.
- **"Main Agreement"** means the SaaS agreement or other contract referencing and including this DPA.

2. Purpose and Scope of Processing

The Processor shall Process Personal Data solely to deliver, operate, maintain, and secure the Services, and only in accordance with the Controller's documented instructions and Applicable Data Protection Law.
The Processing includes typical user account data, authentication data, system logs, and operational data required for service delivery.

3. Term

This DPA remains in effect for the duration of the Main Agreement and continues thereafter as needed for data return or deletion under Section 11.

4. Roles and Responsibilities

The Controller determines purposes and means of Processing and ensures a valid legal basis.
The Processor shall Process Personal Data only per documented instructions.
If the Processor considers an instruction unlawful, it shall notify the Controller without undue delay.
The Controller manages data entered into free-text fields and access/role configurations.

5. Confidentiality

All persons authorized to Process Personal Data are bound by confidentiality obligations and receive appropriate data protection training.

6. Technical and Organizational Measures

The Processor shall maintain measures appropriate to the risk per GDPR Article 32, including encryption, MFA, RBAC, secure logging, monitoring, backup routines, firewalling, and EU/EEA data residency.
A detailed list of security controls is provided in **Appendix C**.

7. Subprocessors

The Controller provides general authorization for Subprocessors listed in **Appendix B**.
Changes will be communicated via updates on Marivida's website.
The Processor imposes equivalent data protection obligations on all Subprocessors. The Processor shall maintain a current list of Subprocessors and ensure transparency on geographic locations and transfer mechanisms.

8. International Data Transfers

Personal Data is primarily stored and Processed within the EU/EEA. Where Processing involves a transfer to a third country, such transfer shall be made only in compliance with Chapter V GDPR, including the use of appropriate safeguards such as the European Commission's Standard Contractual Clauses and, if applicable, reliance on an adequacy decision (e.g., EU–US Data Privacy Framework) together with supplementary measures where required.

9. Assistance to the Controller

The Processor provides reasonable assistance regarding data subject requests, DPIAs, security assessments, and regulatory consultations relevant to the Services.

10. Personal Data Breaches

The Processor shall notify the Controller **without undue delay and preferably within 24 hours** of becoming aware of a breach.
Documentation and corrective actions shall be provided.

11. Return and Deletion of Data

Upon termination, the Processor shall return or delete Personal Data per the Controller's choice.
Unless otherwise instructed, deletion occurs within 30 days; backups follow retention rules in **Appendix C**.

12. Audits

Audits may be conducted once per 12 months (or upon material incident) with 10 days' notice. Audits must not disrupt operations or compromise other customers. If an audit reveals no material non-compliance, the Controller covers its own audit costs

13. Unlawful or Non-Compliant Instructions

If an instruction conflicts with law, the Processor may suspend execution until the Controller confirms or modifies it.

14. Publication and Updates

Appendices may be updated on Marivida's website. Material changes will be communicated when legally required.

Appendices

Appendix A – Overview of Processing
Appendix B – Subprocessors
Appendix C – Technical and Organizational Security Measures

Appendix A – Overview of Processing

This Appendix provides a structured overview of Personal Data and business-critical (non-personal) data Processed within the Marivida platform (MariCare/MariFlow/>future application>). Authentication uses Keycloak (OIDC/OAuth2) brokering Microsoft Entra ID. The following OAuth scopes are requested: openid, profile, email. The ID token claims received and stored are as follows:

Field	Source (Entra/JWT claim)	Stored in Keycloak	Stored in app DB
Email address	email	Yes	Yes
First name	given_name	Yes (firstName)	Yes
Last name	family_name	Yes (lastName)	Yes
Full name	name	Yes	Yes
Username (UPN)	preferred_username	Yes	No
Object ID (OID)	oid	Part of username	Yes (keycloakId)
Group membership	groups	Yes (attribute)	Yes
Roles	roles / resource_access	Yes (external_roles)	Yes
Tenant affiliation	tenant_id / tenant_slug	Yes	Yes

Note: No passwords are stored for SSO users—authentication is fully delegated to Entra ID. Tenant-specific attributes (tenant_id, tenant_code, tenant_name) are hardcoded per IdP and are not Personal Data. The access token issued to the application (MariCare /MariFlow) contains: sub, email, name, tenant_id, tenant_code, tenant_name, tenant_slug, tenant_groups, roles, realm_roles, aud.

A.1 Other Personal Data Processed

User model (application database): In addition to SSO claims, the following are stored: id (internal DB ID); keycloakId (link to Keycloak user); email, firstName, lastName, fullname (contact data); hprNumber (optional health professional registry number); status, roles, companies, locations (access and organizational affiliation); createdAt, updatedAt (timestamps).

Journaling and documentation: Journal entries record createdBy (full name and email), as well as signedById and signedAt (who created and signed a note, with timestamps).

Prescription module: Stores hprNumber for the prescribing aquatic health biologist, contactPersonName and contactPersonPhone for delivery, and helper (assistant).

Audit log (activity log): All CREATE/UPDATE/DELETE operations are logged with user ID, timestamp, before/after data (JSON snapshot), and tenant ID, providing a full trace history.

A.2 Logging and Monitoring (Infrastructure)

Log type	Content	Retention
Keycloak application logs	Login attempts (success/failure), admin actions, sessions, user ID, email, IP	Prod: 90 days / 7 years (immutable)
PostgreSQL database logs	Connections, disconnections, slow queries (>1s)	Staging: 60 days, Test: 30 days
Azure Key Vault audit	Retrieval, creation, deletion of secrets	Same retention as above
IP address	Logged only on authentication failures; rate limiting kept in memory	Not persisted (rate limiting)

No third-party analytics services (e.g., Google Analytics, Mixpanel) are used.

A.3 Database Backups

Environment	Backup retention	Geo-redundancy
Test	7 days	No
Staging	14 days	No
Production	30 days	Yes

A.4 Business-Critical Information (non-Personal Data)

Data category	Details / data model	Criticality
Fish health status and diagnoses	Disease diagnoses with species, verification status (CONFIRMED/SUSPECTED), activity status. Visit types (ROUTINE/EMERGENCY/EXTRA), health assessment, notifiable status.	High – regulatory
Sea-lice counts	Complete per-individual counts: attached, mobile, mature lice and Caligus (liceCount_persistentCount/movingCount/matureCount/caligusCount).	High – food safety authority
Welfare scores	Numeric scores per welfare indicator per individual inspection. Configurable indicators per company. Thresholds (3 levels) for scale loss, eye injuries, gill bleeding, gill scores (AGD, totalScore).	High – animal welfare
Mortality	Acute mortality thresholds level 1–3 (acuteMortalityLvl1/2/3). Diagnosis severity (HIGH/MEDIUM/LOW).	High – reporting duty
Treatment instructions	Treatment plans with procedure descriptions, starting settings, alert criteria, pause/stop criteria, follow-up criteria, assistants.	High – veterinary requirements
Safety assessments	Justification, expected effect, environmental and resistance assessments, health status, water quality assessment, risk rating (LOW/MEDIUM/HIGH/VERY HIGH), risk-reducing measures.	High – documentation duty
Starvation data	Post-mortem registration (hasFoodInStomach). Additional data may be logged via journal notes/free text.	High – animal welfare

Stock and biomass data	Population biometrics: total fish count, total weight (biomass), measurement time. Individual length/weight per fish. Population transfers (count, volume). Prescription dosing data.	High – commercially sensitive
Confinement time	Threshold values for confinement levels 1–3 (confinementLvl1/2/3) in threshold configuration.	High – animal welfare
Treatment settings	Treatment method, wellboat, procedures, starting settings, combination methods (treatmentComboMethod). Prescription: drug strength, dosing, pellet size, feeding %, number of fish.	High – equipment safety
Oxygen levels during treatment	Oxygen thresholds for healthy and sick fish under confinement (oxygenConfinementHealthy/Unhealthy, levels 1–3). Actual measurements may be logged via treatment log.	High – welfare/ safety
Unnecessary starvation	No dedicated front-end model; likely recorded via journal notes or treatment evaluation.	High – animal welfare requirements
Laboratory results	PCR, microbiology, histology, virology with CT values, analysis types and supplier information. Patolink integration shares email addresses with external lab partner.	High – diagnostics

Appendix B – Subprocessors

The following Subprocessors are engaged to deliver the Services:

Name	Service	Country/Region
Microsoft Corporation	Azure cloud platform and related services	EU
Microsoft Corporation	Entra ID authentication	EU
Avo Consulting AS	Operations, maintenance, technical support	Norway
Cipher Bergen AS	Technical support	Norway
Cloudflare, Inc.	Web application firewall (WAF) service	USA and EU
Better Stack, Inc. / Better Stack s.r.o.	Monitoring, logging, and incident management	EU

Appendix C – Technical and Organizational Security Measures

Measure	Description
Tenant isolation	All data is isolated per tenant via automated middleware; no cross-tenant data exposure.
Role-based access control (RBAC)	Company-scoped RBAC; roles synchronized from Keycloak at each login.
Encrypted session	Session cookie encrypted with JWE (AES-256-GCM) containing access token, refresh token, and ID token.
Network security	PostgreSQL accessible only via private endpoint; VNet-integrated architecture with NSG rules; TLS 1.2+ enforced.

Key management	Entra ID client secrets stored in Azure Key Vault; soft delete (90 days) and purge protection enabled; private network only.
Document storage	Documents stored in Azure Blob Storage with tenant namespacing.
Long-term log archiving	Production logs archived for 7 years using immutable storage.

GDPR Rights and Retention Notes

Right to erasure (Art. 17): User data can be deleted upon request from the Controller or the data subject. The system architecture supports identifying and removing relevant records.

Data portability (Art. 20): Data can be exported on request in a structured, commonly used and machine-readable format.

Data retention / purge: There is currently no automated data purge beyond backup retention. Given the limited amount of Personal Data, this is deemed proportionate; retention schedules are listed in Appendix A.3.