Data Processing Agreement (DPA)

Template based on Article 28 GDPR. Last updated: 23 May 2026.

This Data Processing Agreement ("DPA") forms part of the agreement between the customer ("Controller") and EquiDuty ("Processor") for the EquiDuty SaaS service. It is provided as a template for B2B customers who require a written DPA under Article 28 GDPR. Sign the executed copy and email it to info@equiduty.se.

1. Parties and roles

Controller: the customer organisation that subscribes to EquiDuty. Processor: EquiDuty, Stockholm, Sweden, info@equiduty.se. The Controller determines the purposes and means of processing; the Processor processes personal data on behalf of the Controller in accordance with documented instructions (the EquiDuty service agreement, the Terms of Service and this DPA).

2. Subject matter, duration, nature and purpose of processing

Subject matter: providing the EquiDuty stable-management SaaS (scheduling, horse data, messaging, billing). Duration: for as long as the Controller's EquiDuty subscription is active, plus the retention periods set out in the EquiDuty Privacy Policy. Nature and purpose: hosting, storing and processing personal data so the Controller and its users can operate stable activities.

3. Types of personal data and categories of data subjects

Types of personal data processed:

- Contact data (name, email, phone, organisation, address).
- Account data (user IDs, authentication tokens, preferences, device IDs).
- Activity data (schedules, tasks, routines, notes, photos, messages).
- Financial data (subscription state, invoices, payment metadata - card data is processed by Stripe).
- Audit/log data (IP addresses, user actions, timestamps).

Categories of data subjects:

- Stable owners and administrators.
- Stable members, staff and guests invited by the Controller.
- Service professionals (vets, farriers, trainers) invited by the Controller.

4. Obligations of the Processor

- Process personal data only on documented instructions from the Controller.
- Ensure persons authorised to process the data are bound by confidentiality.
- Implement appropriate technical and organisational measures (see Annex A).
- Assist the Controller, taking into account the nature of the processing, in fulfilling its obligations to respond to data subject requests under Chapter III GDPR.
- Assist the Controller in ensuring compliance with Articles 32 to 36 GDPR (security, breach notification, DPIA).
- At the choice of the Controller, delete or return all personal data after the end of the provision of services, subject to legal retention requirements (e.g. Swedish Bookkeeping Act, 7 years for financial records).
- Make available to the Controller all information necessary to demonstrate compliance with Article 28 GDPR.

5. Sub-processors

The Controller gives the Processor general written authorisation to engage sub-processors for the provision of the service. The current sub-processors are listed in the EquiDuty Privacy Policy and include Google Cloud Platform (Firebase, Firestore, Cloud Run, Cloud Functions), Stripe (payments), send.one.com (email), Firebase Cloud Messaging (push notifications) and, optionally, Telegram and Twilio. The Processor will keep the public sub-processor list in the Privacy Policy up to date. If the Controller objects to a specific sub-processor it must notify the Processor in writing; the parties will discuss in good faith and the Controller may terminate the affected service if no agreement is reached.

6. International transfers

Personal data is primarily stored in the EU (Google Cloud europe-west1, Belgium). Where a sub-processor transfers data outside the EU/EEA (currently: Stripe in the USA), the transfer is covered by the EU Standard Contractual Clauses and supplementary measures where required.

7. Security (Annex A summary)

- Encryption in transit (TLS) and at rest (AES-256).
- Identity and access management via Firebase Authentication with JWTs.
- Role-based access control with field-level permissions.
- Logging and audit trails for sensitive operations.
- Daily automated backups with point-in-time recovery.
- Access to production data restricted to authorised personnel on a need-to-know basis.

8. Personal data breach notification

The Processor will notify the Controller without undue delay, and no later than 72 hours, after becoming aware of a personal data breach affecting the Controller's data. The notice will describe the nature of the breach, likely consequences, measures taken and contact details for further information.

9. Audit rights

The Processor will make available to the Controller, on reasonable written request and no more than once per calendar year, written information necessary to demonstrate compliance with this DPA, including the most recent SOC 2 / ISO 27001 attestations of its sub-processors where available. Given that the Processor is a small organisation operating on managed cloud infrastructure, on-site audits and detailed third-party penetration tests are not offered as part of this DPA.

10. Termination and return / deletion of data

On termination of the service the Controller may, within 30 days, request a structured export of its personal data in machine-readable format (JSON). After this period, or on earlier written instruction from the Controller, the Processor will delete all personal data, subject to legal retention requirements.

11. Liability and governing law

Liability under this DPA is subject to the limitations in the EquiDuty Terms of Service. This DPA is governed by Swedish law and disputes are resolved in the Stockholm District Court, without prejudice to the data subject's right to lodge a complaint with a supervisory authority.

12. Signatures

Controller: _____ Date: _____ Name / title: _____

Processor (EquiDuty): _____ Date: _____ Name / title: _____