Data Processing Agreement (DPA)

Pursuant to Article 28 GDPR

Document ID: ENT-DPA
Version: 1.0.0
Effective Date: 15 June 2026
Last Updated: 15 June 2026
Status: Current

Between

Customer
(the "Controller")

and

Mahdi Ghorban Pour - Digitexia
Operator of the Entovist platform
(the "Processor")

Together referred to as the **"Parties"**.

Table of Contents

---

1. Purpose and Scope

This Data Processing Agreement ("DPA") governs the processing of personal data by the Processor on behalf of the Controller in connection with the Controller's use of the Entovist workforce scheduling platform and related services.

This DPA forms an integral part of the agreement governing the use of Entovist.

---

2. Subject Matter of Processing

The Processor provides software-as-a-service (SaaS) functionality for workforce management, employee scheduling, absence management, shift planning, reporting, and related business operations.

The Processor processes personal data solely to provide, secure, maintain, and support the Entovist services in accordance with the Controller's documented instructions.

---

3. Duration

This Agreement shall remain in force for the duration of the service relationship between the Parties.

Upon termination of the service relationship, the provisions concerning deletion, return of data, confidentiality, and liability shall continue to apply as required by law.

---

4. Nature and Purpose of Processing

Processing activities may include:

- Collection
- Recording
- Organization
- Structuring
- Storage
- Adaptation
- Retrieval
- Consultation
- Use
- Transmission
- Deletion

solely as necessary to provide, secure, maintain, and support the Entovist platform in accordance with the Controller's documented instructions.

---

5. Categories of Personal Data

Depending on the Controller's use of the service, the following categories of personal data may be processed:

Employee Data

- First name
- Last name
- Employee identifier
- Email address
- Phone number
- Employment-related information

Scheduling Data

- Shift assignments
- Availability information
- Team assignments
- Location assignments
- Work schedules

Absence Data

- Vacation records
- Sick leave records

- Other absence records

User Account Data

- Usernames
- Login records
- Audit logs
- User activity information

---

6. Categories of Data Subjects

Data subjects may include:

- Employees
- Managers
- Team leaders
- Schedulers
- Human resources personnel
- Administrators
- Other authorized users

---

7. Instructions of the Controller

The Processor shall process personal data only on documented instructions from the Controller, including with regard to transfers of personal data to a third country or international organization, unless required to do so by applicable law.

Where applicable law requires processing outside such instructions, the Processor shall inform the Controller before processing unless prohibited by law.

If the Processor considers an instruction to violate applicable data protection laws, the Processor shall inform the Controller without undue delay.

---

8. Confidentiality

The Processor shall ensure that all persons authorized to process personal data:

- Have committed themselves to confidentiality; or
- Are subject to an appropriate statutory obligation of confidentiality.

Such confidentiality obligations shall continue after termination of their activities.

---

9. Technical and Organizational Measures

The Processor shall implement and maintain appropriate technical and organizational measures designed to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access.

The current Technical and Organizational Measures are described in Annex 3.

The Processor may modify and improve such measures over time provided that the overall level of protection is not materially reduced.

---

10. Assistance to the Controller

Taking into account the nature of processing, the Processor shall assist the Controller through appropriate technical and organizational measures in fulfilling obligations relating to:

- Data subject access requests
- Rectification requests
- Erasure requests
- Restriction requests
- Data portability requests
- Objection requests

The Processor shall further assist the Controller in fulfilling obligations under Articles 32 to 36 GDPR, including:

- Security of processing
- Personal data breach notifications
- Data protection impact assessments (DPIA)
- Prior consultations with supervisory authorities

to the extent reasonably possible and appropriate.

---

11. Personal Data Breaches

The Processor shall notify the Controller without undue delay after becoming aware of a personal data breach affecting Customer Data.

Such notification shall include, where available:

- Description of the nature of the breach
- Categories of affected data
- Likely consequences
- Measures taken or proposed to address the breach

---

12. Sub-Processors

The Controller grants general authorization for the engagement of Sub-processors.

The Processor shall ensure that each Sub-processor is bound by written obligations providing a level of data protection substantially equivalent to this Agreement.

Current authorized Sub-processors are listed in Annex 4.

---

13. Changes to Sub-Processors

The Processor may engage additional Sub-processors or replace existing Sub-processors.

The Processor shall provide notice of material changes to the Controller.

The Controller may object to such changes within thirty (30) days of notification where reasonable data protection concerns exist.

The Parties shall work in good faith to resolve such concerns.

---

14. International Data Transfers

Where personal data is transferred outside the European Economic Area (EEA), the Processor shall ensure that appropriate safeguards are implemented in accordance with applicable data protection laws.

Such safeguards may include:

- Adequacy decisions
- Standard Contractual Clauses (SCCs)
- Other legally recognized transfer mechanisms

---

15. Audit and Compliance

The Processor shall make available to the Controller information reasonably necessary to demonstrate compliance with this Agreement.

The Controller may conduct audits or inspections, directly or through an independent auditor, subject to:

- Reasonable prior notice
- Confidentiality obligations
- Normal business hours
- Avoidance of unreasonable disruption

The Processor may satisfy audit requests through documentation, security reports, certifications, questionnaires, or similar evidence where appropriate.

---

16. Return and Deletion of Data

Upon termination of services and upon request by the Controller, the Processor shall:

- Return Customer Data in a commonly used electronic format where technically feasible; and/or
- Delete Customer Data within a reasonable period unless retention is required by law.

Backup copies may remain until overwritten through normal backup retention procedures.

---

17. Liability

Each Party shall remain responsible for its obligations under applicable data protection laws.

Liability under this Agreement shall otherwise be governed by the primary service agreement and applicable law.

---

18. Governing Law

This Agreement shall be governed by the laws of the Federal Republic of Germany.

The competent courts of Germany shall have jurisdiction where permitted by law.

---

19. Contact Information

Processor

Mahdi Ghorban Pour - Digitexia
Operator of Entovist
Email: info@entovist.com

Website: https://entovist.com
W-IdNr: DE453465065

Controller

The customer organization using the Entovist platform.

Annex 1 – Description of Processing Activities

Purpose:

Provision of workforce scheduling and employee management services through the Entovist platform.

Activities include:

- Employee scheduling
- Shift planning
- Availability management
- Absence management
- Reporting
- User administration
- Audit logging
- Customer support

Annex 2 – Categories of Personal Data

Personal data may include:

- Employee names
- Contact details
- Employment information
- Scheduling information
- Shift assignments
- Availability information
- Absence information
- User account information
- Audit logs

Special categories of personal data under Article 9 GDPR are not intentionally processed and should not be uploaded unless separately agreed.

Annex 3 – Technical and Organizational Measures (TOMs)

The Processor maintains measures including:

Access Control

- Unique user accounts
- Role-based permissions
- Authentication controls

Data Transmission

- TLS/HTTPS encryption
- Secure communication channels

System Security

- Firewalls
- Security monitoring
- Vulnerability management
- Software updates and patching

Availability

- Backups
- Disaster recovery procedures
- Infrastructure monitoring

Organizational Measures

- Confidentiality obligations
- Restricted personnel access
- Security awareness practices

Annex 4 – Authorized Sub-Processors

The Controller grants general authorization for the following Sub-Processors engaged by the Processor for the provision and operation of the Entovist platform.

Provider	Location	Purpose
IONOS SE	Germany / European Union	Hosting infrastructure, virtual servers, databases, backups, storage, and operation of the Entovist platform

Provider	Location	Purpose
Cloudflare, Inc.	Global Services / EU Data Processing where applicable	DNS services, content delivery network (CDN), website security, web application firewall (WAF), bot protection, and DDoS mitigation
Stripe Payments Europe, Ltd.	Ireland / European Union	Subscription billing, payment processing, invoice management, and payment-related customer data
Mailjet SAS	France / European Union	Delivery of transactional emails, including account invitations, password reset emails, account notifications, and service-related communications
Google Ireland Limited (Google Analytics)	Ireland / European Union	Analytics and usage statistics for the public marketing website only; not used within the authenticated Entovist application
TrustSig	European Union	Anti-bot protection, abuse prevention, login protection, registration protection, and contact form security

The Processor shall ensure that all Sub-Processors are contractually bound to implement appropriate technical and organizational measures and to process personal data in accordance with applicable data protection laws.

The Processor may engage additional Sub-Processors or replace existing Sub-Processors in accordance with Section 13 of this Agreement.
