DATA PROCESSING AGREEMENT

This Data Processing Agreement (hereinafter the "Agreement") is entered into between the following parties:

Mydata ApS

Trindsovej 6, 1

8000 Aarhus C

CVR: 31068258

(hereinafter "MD / the Supplier")

and

Name:

Address:

CVR:

(hereinafter "the Customer")

The following applies to the Agreement, which furthermore constitutes an appendix to the Terms and Conditions for the provision of data protection services (hereinafter the "Main Agreement").

The Main Agreement will always be available at www.mydata.security

1. General

1.1 The Agreement concerns the Supplier's obligations to comply with the security requirements set out in Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.

1.2 On 25 May 2018, the Danish Act on Processing of Personal Data was replaced by Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (hereinafter the "General Data Protection Regulation" or "GDPR").

1.3 The Agreement incorporates the requirements imposed on data processing agreements under the GDPR.

1.4 The Supplier shall process personal data in accordance with good data processing practice and in compliance with the applicable rules and regulations governing the processing of personal data at any given time.

2. Purpose

Pursuant to the Main Agreement with the Customer, the Supplier processes personal data on behalf of the Customer.

This concerns general data necessary to provide our services, such as name, address, e-mail address, telephone number, IP address, order data, and other information that the Customer may enter into the system or submit when using it.

3. Rights and Obligations of the Supplier

3.1 The Customer is the data controller for the personal data that the Customer instructs the Supplier to process.

The Customer is responsible for ensuring that the personal data which the Customer instructs the Supplier to process may lawfully be processed by the Supplier, including that such processing is necessary and legitimate in relation to the Customer's performance of its tasks.

3.2 The Customer has the rights and obligations assigned to a data controller under applicable legislation.

4. Obligations of the Supplier

4.1 The Supplier acts as data processor for the personal data processed by the Supplier on behalf of the Customer.

As data processor, the Supplier is subject to the obligations imposed on data processors under applicable legislation.

4.2 The Supplier shall only process the entrusted personal data in accordance with instructions from the Customer and solely for the purpose of fulfilling the Main Agreement.

4.3 The Supplier shall safeguard personal data through appropriate technical and organisational security measures as described in the GDPR.

4.4 The Supplier shall disclose geographical processing locations and relevant certifications/statements (e.g. ISO/IEC 27001, ISAE 3000/3402) in an updated appendix or on an accessible URL. Changes shall be notified in writing.

5. Sub-processors

5.1 A sub-processor is defined as a sub-supplier to whom the Supplier has delegated all or part of the processing carried out on behalf of the Customer.

5.2 The Supplier may not, without the Customer's general prior written consent, engage sub-processors other than those listed in Appendix 1, including replacements.

Changes to Appendix will always be visible online through www.mddata.fi. The Customer may raise a justified objection within the notice period; the parties shall seek a solution. Failure to object constitutes approval.

5.3 If the Supplier delegates the processing of personal data for which the Customer is the data controller to a sub-processor, the Supplier shall enter into a written (sub-)data processing agreement with the sub-processor.

5.4 The sub-processor agreement shall impose on the sub-processor the same data protection obligations as those imposed on the Supplier under this Agreement.

5.5 Where the Supplier delegates processing to sub-processors, the Supplier remains liable towards the Customer for the sub-processors' compliance.

5.6 The Customer may at any time request documentation regarding sub-processor agreements.

5.7 All communication between the Customer and any sub-processor shall take place via the Supplier.

6. Instructions

6.1 The Supplier's processing of personal data on behalf of the Customer shall take place solely in accordance with the instructions contained in the Main Agreement.

6.2 The Supplier shall immediately notify the Customer if an instruction conflicts with applicable legislation.

7. Technical and Organisational Security Measures

7.1 The Supplier shall review its internal security policies at least once annually.

7.2 The Supplier and its employees are prohibited from obtaining any information that is not relevant.

7.3 The Supplier is obliged to instruct employees regarding confidentiality.

7.4 The Supplier shall immediately notify the Customer of any personal data breach.

7.5 The Supplier may not publicly communicate about breaches without prior agreement.

7.6 In the event of a personal data breach, the Supplier shall notify the Customer without undue delay and no later than 24 hours after becoming aware of the breach.

The notification shall at a minimum describe:

(i) the nature of the breach,

(ii) the likely consequences,

(iii) the measures taken or proposed to mitigate the breach.

8. Transfers to Third Countries

8.1 Any transfer of personal data to countries outside the EU shall take place in accordance with the Supplier's instructions.

8.2 The Supplier shall ensure a valid transfer mechanism in accordance with GDPR Chapter V.

9. Confidentiality

9.1 The Supplier shall ensure that all persons who process information are subject to confidentiality obligations.

10. Audits and Statements

10.1 The Supplier is obliged to provide the Customer with necessary information.

10.2 The Supplier shall continuously conduct independent audits.

11. Amendments to the Agreement

11.1 The Customer may at any time, with at least 14 days' prior notice, make amendments.

12. Deletion of Data

12.1 The Customer shall decide whether personal data shall be deleted or returned after processing has ceased.

12.2 Deletion or return shall take place to the extent permitted by law.

12.3 No later than 14 days prior to termination, the Customer shall notify the Supplier.

12.4 The Supplier shall provide documentation confirming deletion.

13. Breach of Contract etc.

13.1 Breach of contract and other disputes are governed by the Main Agreement.

In the event of any breach by the Customer of the Main Agreement, the Supplier may not withhold the Customer's data.

14. Liability

14.1 Liability matters are governed by the Main Agreement.

15. Entry into Force and Term

15.1 The Agreement enters into force upon signature by both parties and remains in effect until termination of the Main Agreement.

16. Formal Requirements

16.1 The Agreement shall be in writing, including electronically, and shall be held by both the Customer and the Supplier.

17. Signatures

This Agreement is executed in two original copies, one for each party.

The signatories confirm by their signatures that they are authorised signatories of the respective parties.

The Customer:

Date:

Name:

Signature:

MYDATA:

Date: 16/2 2026

Name: AUGUST MAHLER

Signature:

ANNEX 1 – SUB- PROCESSORS

NAME	DESCRIPTION
Microsoft Ireland Ltd.	Operation of software services
Zendesk Inc.	Support tickets
Trustbox A/S	Offered service
Panda Security SL	Offered service
WHMCS Limited	Backend
Digital Ocean Inc.	Server hosting
CPSMS	SMS sending/Customer care
Enreach	Call System
Hit	Call System
Defentry	Offered service
Facebook Inc.	Advertising
SendGrid	Email system
Google	Website statistics
Quickpay	Payment gateway
Telavox	PBX Service
Mollie	Payment gateway
Watchguard	Offered service
Elovade	Offered service
TEAM.BLUE DENMARK A/S	Hosting services
Scala Hosting	Hosting services
Team Viewer	Remote Support

ANNEX 2 - OPERATIONAL DATA PROCESSING ACTIVITIES

Controller: My Data ApS
Processor: MD Data Oy

1. Purpose of Processing

The Processor is authorized to process Personal Data strictly for the purpose of delivering the following services on behalf of the Controller:

- Sales and customer onboarding
- Customer relationship management (CRM)
- Invoicing and financial administration
- Customer support and technical assistance
- Remote IT-support and troubleshooting
- Monitoring and administration of IT systems, including backup and security platforms
- Delivery and maintenance of subscribed SaaS and IT services

---

2. Categories of Personal Data

Processing may include, but is not limited to:

- Name, email, phone number
- Company details (including VAT where applicable)
- User credentials (where required for support)
- Device identifiers, IP addresses
- Support tickets and communication history
- Billing and payment-related information

---

3. Categories of Data Subjects

- Customers (B2B contacts)
- End-users of services

- Prospects and leads
- Employees of customer companies

---

4. Nature of Processing Activities

The Processor is explicitly authorized to:

4.1 Sales & CRM

- Store and manage customer and lead data
- Contact customers via phone, email, and digital platforms
- Maintain CRM-systems

4.2 Invoicing & Administration

- Issue invoices on behalf of the Controller
- Process customer billing data
- Maintain financial records related to services

4.3 Customer Support

- Access customer accounts and service environments
- Respond to support requests
- Troubleshoot technical issues

4.4 Remote IT Support

- Access customer systems via remote tools
- View and interact with systems containing Personal Data
- Perform necessary technical actions to resolve issues

Such access may include temporary visibility of Personal Data where necessary for troubleshooting.

4.5 System Monitoring & Dashboards

- Access dashboards (backup, security, SaaS platforms)
- Monitor system status, logs, and alerts
- Perform administrative actions required for service delivery

5. Special Processing Conditions

The Processor shall:

- Only access Personal Data **when necessary**
- Avoid downloading or storing data locally unless required
- Not use Personal Data for its own purposesx
- Ensure all access is **logged where technically possible**
- Use secure, encrypted remote access tools

6. Confidentiality & Access Control

- Staff are bound by confidentiality agreements
- Access is limited to authorized personnel
- Role-based access control must be applied

7. Sub-processors

The Processor may use sub-processors (e.g. SaaS platforms, backup providers), provided that:

- They are bound by equivalent data protection obligations
- A list is maintained and available upon request

8. International Transfers

If data is accessed from outside the EU/EEA, the Processor shall ensure:

- Appropriate safeguards (SCCs or equivalent)
- Secure access environments