Data Processing Agreement — dealday GmbH.

This Data Processing Agreement (**"Agreement"**) forms part of the Contract for Services (**"Principal Agreement"**) between the customer (the **"Company"**) and **dealday GmbH**. (the **"Processor"**) (together as the **"Parties"**).

WHEREAS

(A) The Company acts as a Data Controller.

(B) The Company wishes to subcontract certain Services, which imply the processing of personal data, to the Processor.

(C) The Parties seek to implement a data processing agreement that complies with applicable Data Protection Laws (as defined below) (D) The Parties wish to lay down their rights and obligations.

IT IS AGREED AS FOLLOWS:

1. **Definitions and Interpretation**
   - 1.1. Unless otherwise defined herein, capitalized terms and expressions used in this Agreement shall have the following meaning:
     - 1.1.1. "Agreement" means this Data Processing Agreement and all Annexes;
     - 1.1.2. "Company Personal Data" means any Personal Data provided to or Processed by the Processor on behalf of the Company pursuant to or in connection with the Principal Agreement;
     - 1.1.3. "Data Protection Laws" means all applicable laws relating to Processing of Personal Data and privacy that may exist in any relevant jurisdiction, including European Data Protection Laws;
     - 1.1.4. "EEA" means the European Economic Area;
     - 1.1.5. "EU Personal Data" means the Processing of Personal Data to which (i) data protection legislation of the European Union, or of a Member State of the European Union or EEA, was applicable prior to the Processing by the Processor;
     - 1.1.6. "European Data Protection Laws" means the GDPR, UK Data Protection Act 2018, the UK GDPR, ePrivacy Directive 2002/58/EC, FADP, and any associated or additional legislation in force in the EU, EEA, Member States and the United Kingdom as amended, replaced or superceded from time to time;
     - 1.1.7. "FADP" means the Swiss Federal Act on Data Protection and its Ordinances, as amended from time to time;
     - 1.1.8. "FDPIC" means the Swiss Federal Data Protection and Information Commissioner;
     - 1.1.9. "GDPR" means General Data Protection Regulation EU2016/679;

1.1.10. "UK GDPR" means General Data Protection Regulation (EU) 2016/679 as applicable as part of UK domestic law by virtue of section 3 of the European Union (Withdrawal) Act 2018 and as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (as amended);

1.1.11. "Protected Area" means (i) in the case of EU Personal Data, the member states of the European Union and the EEA and any country, territory, sector or international organisation in respect of which an adequacy decision under Art 45 GDPR is in force or (ii) in the case of UK Personal Data, the United Kingdom and any country, territory, sector or international organisation in respect of which an adequacy decision under UK adequacy regulations is in force; or (iii) in the case of Swiss Personal Data, any country, territory, sector or international organisation which is recognised as adequate by the FDPIC or the Swiss Federal Council (as the case may be);

1.1.12. "Services" means the product and data analytics services the Processor provides.

1.1.13. "Subprocessor" means any person appointed by or on behalf of Processor to Process Personal Data on behalf of the Company in connection with the Agreement.

1.2. The terms, "Controller", "Data Subject", "Member State", "Personal Data", "Personal Data Breach", "Processing" and "Supervisory Authority" shall have the same meaning as in the GDPR and UK GDPR, and their cognate terms shall be construed accordingly.

2. Processing of Company Personal Data

2.1. The Company shall:

2.1.1. ensure that any and all information or data, including without limitation Company Personal Data, is collected, processed, transferred and used in full compliance with Data Protection Laws;

2.1.2. be solely responsible for ensuring that it has all obtained all necessary authorizations and consents from any Data Subjects to Process Company Personal Data and in particular any consents needed to meet the cookie requirements in the ePrivacy Directive 2002/58/EC and any associated national legislation;

2.1.3. instruct the Processor to process Company Personal Data.

2.2. Processor shall:

2.2.1. comply with all applicable Data Protection Laws in the Processing of Company Personal Data; and

2.2.2. not Process Company Personal Data other than on the relevant Company's documented instructions including with regard to data

transfers outside of the Protected Area, unless required to do so by laws to which the Processor is subject; in such a case, Processor shall inform the Company of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest. The Company acknowledges that as part of the processing instructions, Processor may aggregate, anonymise, extract and combine or otherwise deidentify information resulting from the Company's use of the licensed materials and services for product improvement, benchmarking, and the development of new products; and

2.2.3. notify the Company immediately if, in the Processor's reasonable opinion, an instruction for the Processing of Personal Data given by the Company infringes applicable Data Protection Laws , it being acknowledged that the Processor shall not be obliged to undertake additional work or screening to determine if the Company's instructions are compliant.

3. Processor Personnel

Processor shall take reasonable steps to ensure the reliability of any personnel who may have access to the Company Personal Data, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality with respect to such Company Personal Data.

4. Security

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Processor shall in relation to the Company Personal Data implement appropriate technical and organisational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR and UK GDPR. These measures include those at Annex II.

5. Subprocessing

5.1. The Company provides Processor with general authorisation to engage Subprocessors.

5.2. Processor shall enter into a written contract with any Subprocessor and this contract shall impose upon the Subprocessor equivalent obligations as imposed by this Agreement upon the Processor. Where the Subprocessor fails to fulfil its

data protection obligations, Processor shall remain fully liable to the Company for the performance of the Subprocessors' obligations, provided such obligations are within the scope of this Agreement and the Processor's instructions..

5.3. The list of Subprocessors engaged by the Processor can be found at Annex III. Processor may update this list from time to time as applicable, providing the Company with notice of such update at least fourteen (14) days in advance of such updates.

6. Data Subject Rights and Cooperation

6.1. Taking into account the nature of the Processing, Processor shall assist the Company by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Company obligations, as reasonably understood by Company, to respond to requests to exercise Data Subject rights under applicable Data Protection Laws.

6.2. Processor shall:

6.2.1. notify Company if it receives a request from a Data Subject under any Data Protection Law in respect of Company Personal Data; and

6.2.2. ensure that it does not respond to that request except on the documented instructions of Company or as required by applicable laws to which the Processor is subject.

6.3. To the extent required under Data Protection Laws, Processor shall (taking into account the nature of the processing and the information available to Processor) provide all reasonably requested information regarding the Service to enable the Company to carry out data protection impact assessments or prior consultations with data protection authorities and to assist the Company with meeting its obligations under Article 32 GDPR/UK GDPR as required by Data Protection Laws.

6.4. To the extent that assistance under this Agreement is not included within the Services, the Processor may charge a reasonable fee for such assistance, only if the requests are manifestly unfounded or excessive, in accordance with applicable Data Protection Laws., save where assistance was required directly as a result of the Processor's own acts or omissions, in which case such assistance will be at the Processor's expense.

7. Personal Data Breach

7.1. Processor shall notify Company without undue delay, and where feasible, no later than 72 hours after becoming aware of a Personal Data Breach affecting Company Personal Data, providing Company with sufficient information to allow the Company to meet any obligations to report or inform Data Subjects or

Supervisory Authorities of the Personal Data Breach under applicable Data Protection Laws.

7.2. Processor shall cooperate with the Company and take reasonable commercial steps as are directed by Company to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

8. Audits

The Processor shall make available to the Company all information reasonably necessary to demonstrate compliance with this Agreement, provided that such audits are conducted at a mutually agreed time and do not unreasonably disrupt the Processor's business operations.

9. Deletion or return of Company Personal Data

Following a request from the Company, Processor shall promptly and in any event within 10 business days of the date of cessation of any Services involving the Processing of Company Personal Data , return or delete and procure the deletion of all copies of the Company Personal Data unless applicable law or legitimate business interests require storage of such Company Personal Data.

10. General Terms

10.1. Confidentiality. Each Party must keep this Agreement and information it receives about the other Party and its business in connection with this Agreement (“Confidential Information”) confidential and must not use or disclose that Confidential Information without the prior written consent of the other Party except to the extent that:

10.1.1. disclosure is required by law;

10.1.2. the relevant information is already in the public domain.

10.2. All notices and communications under this Agreement, including those required by law, may be sent electronically and shall be deemed valid and legally binding if sent to the designated email addresses of the Parties, provided that delivery confirmation is obtained.

10.3. Governing Law and Jurisdiction. This Agreement is governed by the laws of Germany and the European Union.

ANNEX I

A. Processing Activities:

Subject matter of the processing

The personal data shall be processed in order to allow Processor to provide the Services.

Nature and purpose of the processing

Product provisioning, analytics, including insights, session recording and feature flags.

Duration

For the duration of the Principal Agreement.

Categories of data subjects

The personal data processed relates to the following categories of data subjects:

- Employees
- Customers
- Visitors
- Prospects

Categories of personal data processed

The personal data processed comprises the following categories of data:

- Identifying – name, email address
- Computer device – IP address, MAC address, browser footprint
- Contact – email address
- Location – country, territory, city
- Behavioral – product usage (page views, clicks, browsing behavior)

ANNEX II

Technical and Organizational Security Measures

1. Technical Measures

1.1 Data Encryption

Encryption in Transit: All data transmitted between users and our servers is encrypted using industry-standard TLS (Transport Layer Security) to prevent unauthorized interception.

Encryption at Rest: Data stored on our servers is encrypted using AES-256, ensuring that unauthorized access to physical hardware does not compromise data.

1.2 Access Control and Authentication

Single-Sign-On (SSO): Access to internal systems is protected by SSO (and MFA) where possible, centralizing authentication and requiring more than one authentication method where applicable.

Role-Based Access Control (RBAC): Access to sensitive data is restricted based on role and responsibility within the organization. Only authorized personnel have access to personal data.

Unique User IDs: Each user and employee is assigned a unique identifier to ensure accountability for system access and actions.

1.3 Data Minimization and Pseudonymization

Pseudonymization: Where applicable, personal data is pseudonymized so that it cannot be attributed to a specific individual without additional information, which is stored separately.

Data Minimization: We collect and process only the personal data necessary for the intended purposes of providing the service.

1.4 System Monitoring and Logging

Logging and Auditing: All access to data and actions taken within the system are logged and audited regularly. Logs are stored securely and protected against unauthorized access.

1.5 Secure Development and Code Practices

Vulnerability Management: We have a proactive vulnerability management process, including patch management and prompt updates for security vulnerabilities.

1.6 Data Backup and Disaster Recovery

Regular Backups: Data is regularly backed up, with backups stored in a secure location. Backup integrity is tested periodically.

Disaster Recovery Plan: In case of a catastrophic event, we maintain a disaster recovery plan to restore services and data availability within an agreed timeframe.

1.7 Network Security

Firewalls: We employ advanced firewall protection to secure our network and restrict access to systems and data.

DDoS Mitigation: Protection against Distributed Denial of Service (DDoS) attacks is in place to prevent downtime or service disruption.

VPN for Internal Access: Internal systems can only be accessed via secure Virtual Private Networks (VPNs).

2. Organizational Measures

2.1 Employee Awareness

Confidentiality Agreements: All employees and contractors must sign confidentiality agreements and are contractually bound to maintain the security and privacy of personal data.

2.2 Data Breach Response

Data Breach Notification: In case of a data breach involving personal data, we notify affected users within 48 hours after becoming aware of the breach, as required by GDPR.

2.3 Access Management

Least Privilege Principle: Access to systems and data is granted based on the principle of least privilege, ensuring that individuals only have access to the data necessary for their specific tasks.

User Access Reviews: We perform regular reviews of user access rights to ensure that only authorized personnel have access to sensitive systems and data.

2.4 Contractual Measures with Third Parties (Subprocessors)

Data Processing Agreements (DPA): We have Data Processing Agreements in place with all subprocessors to ensure that they comply with GDPR and other relevant regulations.

2.5 Data Retention and Disposal

Data Retention Policy: We have a clear data retention policy to ensure that personal data is only kept for as long as necessary for the purposes it was collected. Data is automatically deleted after 60 days following account termination.

2.6 Privacy by Design and Default

Default Settings: Our platform defaults to the highest privacy settings, and users are required to opt-in to any data sharing or processing that is not essential to the provision of the service.

ANNEX III

Subprocessors

Sub-Processor Name, Address & Details	Type of Service Provided	Hosting Location
Fly.io, Inc. 2045 West Grand Avenue Ste B Chicago, IL 60612 USA	Hosting	Amsterdam
OpenAI Ireland Ltd The Liffey Trust Centre 117-126 Sheriff Street Upper Dublin 1, D01 YC43 Ireland	AI-services	USA
Supabase Pte Ltd 65 Chulia Street #38-02/03 OCBC Centre SINGAPORE 049513 Singapore	Hosting	Frankfurt
Hubspot Ground Floor, Two Dockland Central Guild Street Dublin 1 Ireland	Marketing	EU
Sentry Functional Software, Inc. dba Sentry 132 Hawthorne Street San Francisco CA 94107 USA	Error Tracking & Monitoring	EU
Plausible	Analytics	EU

Plausible Insights OÜ Västriku tn 2 50403 Tartu Estonia		
Microsoft Microsoft Corporation One Microsoft Way Redmond, WA 98052-6399 USA	Analytics	USA

Niklas Karbaum

Niklas Karbaum

Co-Founder & Managing Director

2025-03-28

Audit trail

Details

FILE NAME	Data Processing Agreement - Pre-Signed.pdf - 3/28/25, 9:51 AM
STATUS	Signed
STATUS TIMESTAMP	2025/03/28 08:52:07 UTC

Activity

SENT	nik@dealday.io **sent** a signature request to: • Niklas Karbaum (nik@dealday.io)	2025/03/28 08:51:24 UTC
SIGNED	**Signed** by Niklas Karbaum (nik@dealday.io)	2025/03/28 08:52:07 UTC
COMPLETED	This document has been signed by all signers and is **complete**	2025/03/28 08:52:07 UTC

The email address indicated above for each signer may be associated with a Google account, and may either be the primary email address or secondary email address associated with that account.