DATA PROCESSING AGREEMENT

This Data Processing Agreement ("DPA") is entered into by the Customer and DE software & control GmbH ("DE software & control"), each a "Party" and together the "Parties".

Customer and DE software & control have entered into the Agreement under which Customer is provided access to and use of the Services during the Subscription Term. This DPA is incorporated into and made a part of the Agreement.

SECTION 1 GLOBAL PRIVACY OBLIGATIONS OF THE PARTIES

1.1 **Ownership of Customer Content.** DE software & control asserts no ownership right or interest to Customer Content processed under this DPA and, between the Parties, Customer Content owned by Customer remains the property of Customer.

1.2 **Personal Data.** The Parties agree that the nature, purposes, subject matter, duration of processing, categories of Personal Data or data subjects, and applicable retention periods are as described in Annex I.

1.3 **Applicable Data Protection Law.** DE software & control and Customer agree to comply with their respective obligations of Applicable Data Protection Law.

1.4 **DE software & control's Obligations.** DE software & control agrees to:

(i) process Personal Data according to Customer's documented instructions, unless otherwise permitted or required by applicable law. DE software & control will inform Customer immediately if its processing instructions infringe Applicable Data Protection Law;

(ii) not sell or share Personal Data;

(iii) ensure that all employees and contractors are fully aware of their responsibilities to protect Personal Data under this DPA and have committed to an appropriate contractual or statutory obligation of confidentiality;

(iv) notify Customer if it can no longer meet its obligations under Applicable Data Protection Law and allow Customer to take reasonable and appropriate steps to remediate unauthorized processing of Personal Data;

(v) implement and maintain appropriate technical and organizational measures designed to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access, taking into account the likelihood and severity of risks to the privacy rights of data subjects, including the measures in Annex II;

(vi) notify Customer of a confirmed personal data breach without undue delay and within 48 hours, unless prohibited by law or government agency; take appropriate measures designed to mitigate the cause(s) of the personal data breach; and provide Customer all necessary information as required under Applicable Data Protection Law;

(vii) reasonably assist Customer with its obligation to respond to data subject requests and, if DE software & control receives a request directly from Customer's data subject, direct the data subject to Customer unless prohibited by law; and

(viii) make available commercially reasonable information and assistance to enable Customer to conduct any data protection impact assessment or supervisory authority consultation, as required by Applicable Data Protection Law.

1.5 **Customer Obligations.** Customer, as data controller, determines what Personal Data is processed by the Services. Customer is responsible for assessing DE software & control's technical and organization measures as appropriate for the types of Personal Data Customer wishes to process by its use of the Services.

SECTION 2 USE OF SUB-PROCESSORS

2.1 **Sub-Processors.** Customer provides its general written authorization for DE software & control to use Sub-processors provided that:

(i) DE software & control remains liable to Customer for the acts or omissions of its Sub-processors with respect to their processing of Personal Data; and

(ii) each Sub-processor agrees to protect the Personal Data to standards consistent with the requirements of this DPA.

2.2 **Sub-Processor Updates.** DE software & control will update the list of sub-processors with any newly appointed Sub-processors at least 30 days before such change. Customer will receive email notifications of such changes.

2.3 **Sub-Processor Policy Objections.** Customer may object to any newly appointed Sub-processor on reasonable grounds relating to data protection. If Customer objects, it will inform DE software & control in writing within 30 days following the update to the list of Sub-Processors. In such event, the Parties will negotiate, in good faith, a solution to Customer's objection. If the Parties cannot reach resolution within 60 days of DE software & control's receipt of Customer's objection, DE software & control, in its sole discretion, will either:

(i) instruct the Sub-processor not to process Customer's Personal Data, and the DPA will continue unaffected, or

(ii) allow Customer to terminate any affected portion of the Services and provide Customer with a pro rata refund of Subscription credits paid in advance for the affected portion of the Services if they could not be used as of the effective date of termination.

SECTION 3 AUDIT

3.1 **External Auditors.** DE software & control uses independent and qualified external auditors to verify the adequacy of its information security system (e.g. TISAX).

3.2 **Audit Report.** At Customer's written request, DE software & control will provide Customer with an Audit Report, subject to the confidentiality provisions of the Agreement.

3.3 **Assistance.** To the extent Customer's audit requirements under Applicable Data Protection Law are not reasonably satisfied through the Audit Report or other documentation that DE software & control makes generally available to its customers, and Customer does not otherwise have access to the relevant information, DE software & control will reasonably assist Customer.

3.4 **Audit.** If Customer cannot satisfy its audit obligations under Applicable Data Protection Law through DE software & control's assistance provided in Section 3.3 and Customer has the right to conduct an audit under Applicable Data Protection Law, Customer may request such an audit by providing at least 30 days' advance written notice to DE software & control. Such audit may be conducted no more than once annually, must be conducted during normal business hours with reasonable duration, must not interfere with DE software & control's operations, and must only be conducted at DE software & control headquarters or an agreed business office. Such audit will not involve access to any data relating to other DE software & control customers, or to secured facilities or systems in any way that would violate DE software & control's security controls or cause DE software & control to violate its confidentiality obligations to any third party. Any information generated in connection with such audit is DE software & control's Confidential Information and will be promptly provided to DE software & control. Customer is responsible for costs and expenses relating to any audit it requests beyond the Audit Report.

SECTION 4 INTERNATIONAL DATA TRANSFERS

International Data Transfers. Customer acknowledges that it is necessary for the performance of the Services that DE software & control may process Customer Content within EEA in compliance with Applicable Data Protection Law.

SECTION 5 RETURN AND DESTRUCTION OF PERSONAL DATA

DE software & control will delete Customer's instructions in the system one month after the termination of the subscription term. After this period all data will be deleted.

SECTION 6 CONFLICTS

Unless otherwise agreed, the terms of this DPA will take precedence over any conflicting terms in the Agreement.

SECTION 7 DEFINITIONS

All terms used in this DPA will have the meanings given to them below. Where not defined in this DPA, the terms "sell", "share", "processing", "process", "processor", "controller", "data exporter", "data importer", "data subject", "personal data breach" (and similar terms), and "supervisory authority" will have the same meaning as in Applicable Data Protection Law. Any capitalized terms not otherwise defined in this DPA are as defined in the Agreement.

"Applicable Data Protection Law" means the German and European data protection laws and regulations applicable to each party in connection with its respective processing of Personal Data under this Agreement.

"Audit Report" means a confidential summary of any such certification or audit report.

"Personal Data" means any personal data relating, directly or indirectly, to an identified or identifiable natural person that is contained in Customer Content.

"Sub-processor" means any third-party data processor engaged by DE software & control who receives and processes Customer Content in accordance with Customer's instructions (as communicated by DE software & control) and the terms of its written subcontract with DE software & control, as listed in Annex III.

This DPA is agreed to by the Parties.

ANNEX I

Details of Processing

Data Controller: Customer (with respect to DE software & control)
Contact Details: Provided in the DPA signature block.

Data Processor: DE software & control GmbH
Contact Details: Provided in the DPA signature block

1. **Nature and Purpose of the Processing:** DE software & control will process Personal Data as specified in the Agreement and for the purposes determined by Customer.

2. **Processing Activities:** Processing activities will include hosting and processing of Personal Data as specifically instructed by the Customer programmatically or in the Agreement.

3. **Duration of Processing and Retention:** DE software & control will process and retain Personal Data on a continuous basis for the Subscription Term. Customer may delete Personal Data at any time.

4. **Data Subjects:** Customer may, at its sole discretion, submit Personal Data to the Services, which may include, but is not limited to: employees (including contractors and temporary employees), relatives of employees, customers, prospective customers, service providers, business partners, vendors, advisors (all of whom are natural persons) of Customer and any natural person(s) authorized by Customer to use the Services.

5. **Categories of Personal Data:** Customer may process any category of Personal Data at its sole discretion using the Services, which may include, but is not limited to, the following categories of Personal Data: first and last name, email address, title, position, employer, contact information (company, email, phone numbers, physical address), date of birth, gender, communications (telephone recordings, voicemail, metadata), and customer service information.

6. **Special Categories of Data:** Sensitive categories of data requiring special treatment under Applicable Data Protection Law and therefore must not be included in Customer's Personal Data.

ANNEX II

DE software & control Technical and Organizational Security Measures

This document describes the technical and organisational measures (TOMs) in accordance with Article 32 of the GDPR that have been implemented by DE software & control GmbH to protect personal data.

1. Management and Organisation

- **Security Incidents (Incident Response):** A documented process for security incidents is in place. Incidents are reported and handled centrally via an ISMS (Information Security Management System). Measures are then determined there, such as informing affected customers/users and initiating appropriate remedial actions.
- **Information Security Officer (ISO) / Data Protection Officer (DPO):** Information Security Officer and Data Protection Officer are appointed.

2. Physical security of the infrastructure

- **Server rooms:** The entire IT infrastructure is hosted in the cloud (e.g. AWS, Microsoft).
- **Office access control:** The business premises are physically secured by an electronic access system (access tokens/keys).
- **Visitor policy:** Guests and visitors are never left unattended on the premises.
- **Clean Desk Policy:** A strict clean desk policy is in place. Sensitive information and documents must never be left lying openly at the workstation.

3. Employee awareness

- **Training:** All employees receive initial training on data protection and IT security as part of the onboarding process.
- **Refresher** training**:** The training is then repeated annually.

4. Authentication & Roles/Permissions Framework

- **Password policies:** Passwords are managed centrally via password manager. Each service is assigned its own secure password. Minimum length and complexity requirements are pre-set in the password manager and are enforced.
- **Two-factor authentication (2FA/MFA):** For centralised systems (such as AWS, Microsoft, HubSpot and Halerium), 2FA is always used, provided the respective service offers this option. Alternatively, login takes place via single sign-on (SSO) using Microsoft Entra ID accounts.
- **Role and access rights framework (need-to-know principle):**
  - In SharePoint, workspaces are segregated using specific groups (e.g. the marketing team does not have access to project data).
  - The Halerium platform implements granular access rights management: only employees who are actively working with a client's data are members of the relevant tenant or workspace.
  - In project management (e.g. Jira/Asana), employees are likewise only added to the projects on which they are actively working.

5. End devices (clients) & mobile data storage

- **Hard drive encryption:** The hard drives of all laptops are encrypted by default. This is enabled by default during laptop configuration. Employees are instructed and trained to ensure this encryption is maintained at all times.

- **Bring Your Own Device (BYOD):** Personal devices may generally be used for work, but they are subject to exactly the same encryption policies as company devices.
- **Mobile Device Management (MDM):** The standard features of Microsoft Azure Entra ID (MDM) are used to manage the devices.
- **Endpoint protection (anti-virus):** Windows Defender is used as the default endpoint protection or anti-virus software.

6. Server Systems, Network & Web Applications

- **Server Administration:** The cloud servers are administered exclusively by authorised staff members. Dedicated admin access is provided for this purpose (without VPN or IP whitelisting).
- **Network architecture:** The network topology is designed to be restrictive. Only those services on the platform that absolutely must be accessible from outside are publicly accessible. All other internal services run in isolation within Virtual Private Clouds (VPCs).
- **Automated configuration (CI/CD):** Updates and deployments of the cloud infrastructure are carried out automatically via API keys set up specifically for this purpose. These keys have only the minimum necessary access rights (least privilege principle).
- **Vulnerability scans:** Web applications are regularly scanned manually. For the platform, a solution is also firmly integrated into the CI/CD pipeline.
- **Patch management:**
  - Security patches are applied to web applications using version pinning (manual updates).
  - Security updates for the platform are applied with every release.

7. Cryptography & Data Transfer

- **Encryption in transit:** Data is always transmitted in encrypted form (TLS/HTTPS).
- **Encryption at rest:** Data stored with cloud services (e.g. AWS) is encrypted whilst at rest. This applies to both database services and file storage.

8. Business Continuity, Backup & Logging

- **Backup strategy:** Data backups are created at least once a day. Data is retained according to a retention schedule: daily retention for the last week, followed by weekly and finally monthly retention. The maximum retention period is one year.
- **Restore Tests:** Backups are regularly tested for restorability every six months.
- **Logging:** Access to core AWS systems is documented via standard access logs. In SharePoint, the standard logging mechanisms are also used. No additional documentation or tracking software is used.
- **Log** analysis**:** Log files are analysed only on an ad hoc basis (e.g. in the event of a suspected security incident).

9. Data processors, development & data erasure

- **Data processors:** Appropriate data processing agreements are concluded with all service providers that process personal data.
- **Security & Privacy by Design:** In our own software development, we place great emphasis on Security by Design and Privacy by Design.
- **Development Guidelines:** Development is strictly unidirectional. Development or testing is never carried out on the production system. Development takes place in isolation within feature branches, which are thoroughly tested prior to final deployment.

- **Data deletion:** Customer data is logically structured into tenants and workspaces. To completely delete customer data (e.g. upon project completion or contract termination), it is sufficient to delete the relevant workspace or tenant. This process ensures that all associated data (files, database entries, personal data) is completely removed.

Annex III - Sub-Processors

Below the list Sub-Processors engaged to provide processing activities on Customer Content as defined in the DPA.

Sub-Processor	Form	Registered Office	Purpose
Erium GmbH	GmbH	Lichtenbergstraße 8, 85748 Garching bei München, Germany	Data storage, data processing, and provision of computing resources
Microsoft Ireland Operations Limited	Private Company Limited by Shares	One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, Irland	Data storage, data processing, and provision of computing resources
Amazon Web Services EMEA SARL	Société à responsabilité limitée (SARL)	38 Avenue John F. Kennedy, L-1855 Luxembourg, Luxemburg	Data storage, data processing, and provision of computing resources
Mixpanel, Inc.	Corporation (Inc.)	405 Howard Street, Floor 2, San Francisco, CA 94105, USA	Collection and analysis of user behavior to gain insights into usage patterns and improve the user experience.
Google Cloud EMEA Limited	Private Company Limited by Shares	Velasco, Clanwilliam Place, Dublin 2, Ireland	Data storage, data processing, and provision of computing resources
Stripe Technology Europe, Limited	Private Company Limited by Shares	25/28 North Wall Quay, Dublin 1, D01 H104, Ireland	Billing, invoicing, and payment processing