DATA PROCESSING AGREEMENT WHISTLEBLOWING SYSTEM

1. Whistleblowing System

1.1 Compliance.One GmbH (hereinafter referred to as "Contractor" or "Compliance.One") provides the Client with its digital whistleblowing system (hereinafter referred to as "Whistleblowing System") as SaaS. The Client uses the Whistleblowing system to enable employees and possibly other third parties to report potential compliance violations in the company anonymously or confidentially. The Whistleblowing System processes the data collected in the course of submitting reports on behalf of the Client. As part of the main contract between the parties, this Data Processing Agreement specifies the obligations of both parties to comply with the applicable data protection law, in particular the requirements of the General Data Protection Regulation ("GDPR").

1.2 In the case of an **anonymous report**, the whistleblower shall provide neither name nor contact details.

In the case of a **pseudonymous report**, only Compliance.One has the contact details of the whistleblowers, but these are not disclosed to the Client. The Client irrevocably instructs Compliance.One not to disclose to the Client or any third party any personal data that would allow the whistleblower to be identified in the event of a pseudonymous report.

In the case of a **transparent report**, the internal reporting office responsible for processing reports at the Client has access to the data on the identity of the whistleblower and can communicate directly with the whistleblower. The Client is legally obliged to maintain the confidentiality of the whistleblower's identity; accordingly, only the employees of the Client's internal reporting office who process the respective report may know the identity of the whistleblower.

To make the whistleblowing website available, it is also necessary to process **personal data of a technical nature** (IP address and device information) for the duration of the whistleblowing website being accessed. This personal data is only processed for the duration of the whistleblowing website visit. The IP address is anonymized in the log files (replacement of the last octet of the IP address with "xxxx.xxxx"), the device information is not stored.

2. Scope

The Contractor shall process personal data on behalf of the Client. The subject of the processing, the nature and purpose of the processing, the type of personal data and the categories of data subjects are specified in the Service Agreement and in **Annex 1** to this Data Processing Agreement.

3. Instructions

3.1 The Contractor may process data of data subjects only within the scope of the order and the documented instructions of the Client. The instructions shall initially be determined by the main contract and may thereafter be amended, supplemented or replaced by the Client in text form, unless they have been issued irrevocably. Verbal instructions shall be confirmed by the Client in text form without delay.

3.2 If the Contractor is obliged to process personal data under the law of the Union or the Member State to which the Contractor is subject, the Contractor shall inform the Client thereof in writing prior to the respective processing, unless the law prohibits such information for important reasons of public interest. In the latter case, the Contractor shall inform the Client without undue delay as soon as this is legally possible for the Contractor.

3.3 The Contractor shall inform the Client without undue delay if it is of the opinion that an instruction violates applicable laws. The Contractor may suspend the implementation of the instruction until it has been confirmed or amended by the Client.

4. Technical and Organizational Measures

4.1 The Contractor undertakes vis-à-vis the Client to comply with the technical and organizational measures required to comply with the applicable data protection regulations. This includes in particular the requirements of Art. 32 GDPR.

4.2 The status of the technical and organizational measures existing at the time of conclusion of the agreement is documented in **Annex 2** to this Data Processing Agreement and additionally in the technical overview of the application in **Annex 3.** The parties agree that changes to the technical and organizational measures may be necessary in order to adapt to technical and legal circumstances. The Contractor reserves the right to change the security measures taken, but it must be ensured that the contractually agreed level of protection is not undercut. The Client may request a current overview of the technical and organizational measures taken by the Contractor at any time.

5. Data Subject Rights

5.1 The Contractor shall support the Client within the scope of its possibilities in fulfilling the requests and claims of data subjects pursuant to Chapter III of the GDPR (in particular information, correction, blocking or deletion). Insofar as the cooperation of the Contractor is necessary for the protection of data subject rights by the Client, the Contractor shall take the measures required in each case in accordance with the instructions of the Client. The Contractor shall support the Client as far as possible with suitable technical and organizational measures in fulfilling its obligation to respond to requests for the exercise of data subject rights.

5.2 The Contractor may only provide information to third parties or the person concerned with the prior consent of the Client. The Contractor shall immediately forward any inquiries addressed directly to it to the Client.

5.3 In the case of pseudonymous reports, the Client instructs the Contractor to directly fulfill the rights of the data subject vis-à-vis the respective whistleblower.

6. Other Obligations of the Contractor

6.1 The Contractor shall inform the Client without undue delay, at the latest within 24 hours, if it becomes aware of any violations of the protection of Client's personal data.

6.2 In connection with the processing, the Contractor shall support the Client in creating and updating the register of processing activities and, if necessary, in conducting a data protection impact assessment. All required information and documentation shall be made available to the Client without undue delay upon request.

6.3 If the Client is subject to inspection by supervisory authorities or other bodies or if data subjects assert rights against it, the Contractor undertakes to support the Client to the extent necessary insofar as the processing under the contract is affected.

6.4 The persons employed by the Contractor for processing have committed themselves in writing to confidentiality, have been familiarized with the relevant provisions of data protection and are instructed and monitored appropriately on an ongoing basis with regard to compliance with data protection requirements.

6.5 The Contractor shall assist the Client in complying with the obligations set out in Articles 32 to 36 of the GDPR, taking into account the nature of the processing and the information available to it.

6.6 The Client may contact the Contractor's data protection officer at any time with questions regarding data protection at the Contractor. The Contractor's data protection officer is attorney Conrad Graf, e-mail privacy@compliance.one.

7. Rights and Obligations of the Client

7.1 The Client alone is responsible for assessing the permissibility of the processing and for safeguarding the rights of data subjects.

7.2 The Client shall be entitled to monitor the Contractor's compliance with the provisions on data protection and the contractual agreements to a reasonable extent itself or through third parties. The persons entrusted with the control shall be given access and insight by the Contractor to the extent

necessary and possible. The Contractor shall be obliged to provide the necessary information, demonstrate processes and provide evidence required to carry out an inspection. Inspections at the Contractor's premises shall be carried out without any avoidable disruptions to business operations. Unless otherwise indicated for urgent reasons to be documented by the Client, inspections shall take place after reasonable advance notice and during the Contractor's business hours and not more frequently than every 12 months.

8. Sub-processors

8.1 The commissioning of sub-processors by the Contractor shall only be permitted with the consent of the Client.

8.2 The Client agrees to the engagement of sub-processors in accordance with the Sub-Processor Overview, attached hereto as **Annex 4.** The Sub-Processor Overview also defines the process for future changes of sub-processors.

8.3 The Contractor shall carefully select the sub-processors and check before commissioning that they are able to comply with the agreements made between the Client and the Contractor. In particular, the Contractor shall check that all sub-processors have taken the technical and organizational measures required under Art. 32 GDPR to protect personal data.

8.4 Services which the Contractor uses from third parties as a purely ancillary service in order to carry out the business activity shall not be regarded as subcontracting relationships within the meaning of this Data Processing Agreement. This includes, for example, cleaning services, pure telecommunications services without any specific reference to services that the Contractor provides for the Client, postal and courier services, transport services and guarding services.

8.5 The commissioning of sub-processors shall not affect the contractual and data protection obligations of the Contractor towards the Client. The Contractor shall be liable for any poor performance of a sub-processor as for its own fault.

9. Data transfer to Third Countries

The processing shall take place exclusively within the European Union or the EEA and/or in third countries for which an adequacy decision of the EU Commission is available. A relocation of the processing to an "unsafe" third country requires the explicit approval of the Client.

10. Deletion and return of Personal Data

10.1 Copies or duplicates of the data will not be made without the knowledge of the Client. Excluded from this are security copies, insofar as they are necessary to ensure proper data processing, as well as data that is required with regard to compliance with statutory retention obligations.

10.2 After termination of the service agreement or earlier upon request by the Client, the Contractor shall hand over the personal data processed in the order to the Client or delete them in accordance with data protection requirements. Pseudonymous reports are excluded from the handover. The Contractor shall store these on the instructions of the Client in accordance with the statutory retention period.

10.3 Documentation that serves as proof of the orderly and proper data processing shall be retained by the Contractor in accordance with the respective retention periods beyond the end of the service agreement.

ANNEX 1: DESCRIPTION OF THE PROCESSING

Controller and Processor

The Client is a controller within the meaning of the GDPR and uses the Contractor's whistleblowing system to enable its employees and other third parties to report potential compliance violations in the Client's company.

The Contractor shall provide the whistleblowing system as a Software-as-a-Service (SaaS) to the Client as a data processor.

Data Subjects

The personal data processed relates to whistleblowers who use the whistleblowing system to confidentially report potential compliance violations in the Client's company. The Client decides whether to make the whistleblowing system available only to its employees or also to other third parties (customers, suppliers, etc.).

Furthermore, the Contractor shall process personal data of the persons indicated by the person providing the information in the context of a notification, e.g., as an accused of a potential compliance violation or in any other context.

Categories of Data

As part of the processing, the personal data that the whistleblower provides as part of his or her report and/or that is collected and recorded in the whistleblowing system as part of the follow-up activities is processed.

These can be:

- Name;
- Address;
- Employer or branch in which the activity is carried out;
- E-mail address; telephone/mobile number;
- Function in the company or relationship to the Client;
- Data of those accused of a potential compliance violation;
- Contents of the messages;
- other data provided to the Contractor by the Client for the performance of its services or collected by the Contractor for the Client in the course of the performance of the Contractor's services;
- technical information required to provide the whistleblowing website (IP address and device information).

Special Categories of Data

The personal data processed on behalf may include special categories of personal data pursuant to Art. 9 GDPR (e.g. health data) if such data are included in a notification or collected in the context of follow-up actions and recorded in the whistleblowing system.

Subject and Duration of Processing

The personal data processed shall be processed for the performance of the Contractor's services agreed in the Service Agreement and/or this Data Processing Agreement. The data shall be processed on the instructions of the Client as defined in this Data Processing Agreement.

The data, as defined above, will be deleted at any time upon instruction of the Client. The Client may also define specific retention and deletion periods. The data will be deleted upon termination of the Service Agreement.

The Client may export the data at any time (with the exception of the data on the identity of the person providing the information in the case of pseudonymous reports, which will be processed in accordance with the specific instruction regarding pseudonymous reports).

The term of this Data Processing Agreement is based on the term of the Service Agreement.

ANNEX 2: TECHNICAL AND ORGANIZATIONAL MEASURES

Compliance.One has taken the following technical and organizational measures to ensure data protection and information security within the whistleblowing system:

1. CONFIDENTIALITY

1.1 Physical Access Control

The software is hosted in data centers operated by Hetzner Online GmbH in Germany.

The technical and organizational measures taken in the data centers of the subcontracted processor Hetzner Online GmbH are described in detail here: https://www.hetzner.com/AV/TOM.pdf

1.2 System Access Control

The following measures have been taken by Compliance.One for system access control:

To gain access to IT systems, users must have the appropriate access authorization. For this purpose, corresponding user authorizations are assigned by administrators.

The user is then given a username and an initial password, which must be changed the first time the user logs in. The password defaults include a minimum password length of 8 characters, where the password must consist of upper/lower case letters, numbers and special characters.

A password history is stored. This ensures that the past 10 passwords cannot be used again. Incorrect login attempts are logged. If the wrong password is entered 3 times, the respective user account is blocked.

Remote access to Compliance.One IT systems always takes place via encrypted connections.

An intrusion prevention system is in use on Compliance.One's servers. All server and client systems have antivirus software that ensures a daily supply of signature updates. All servers are protected by firewalls that are constantly maintained and supplied with updates and patches.

Access by servers and clients to the Internet and access to these systems via the Internet is also secured by firewalls. This also ensures that only the ports required for the respective communication can be used. All other ports are blocked accordingly.

All employees are instructed to lock their IT systems when they leave them. Passwords are always stored in encrypted form.

1.3 Data Access Control

Authorizations for Compliance.One IT systems and applications are set up exclusively by administrators.

Authorizations are always granted according to the need-to-know principle. Accordingly, only those persons are granted access rights to data, databases or applications who maintain and service these data, applications or databases or are involved in their development.

The prerequisite is a corresponding request for authorization for an employee by a supervisor.

There is a role-based authorization concept with the option of differentiated assignment of access rights, which ensures that employees receive access rights to applications and data depending on their respective area of responsibility and, if necessary, on a project basis.

Employees are generally prohibited from installing unauthorized software on IT systems.

All server and client systems are regularly updated with security updates.

1.4 Separation

All IT systems used by Compliance.One for clients are multi-client capable. The separation of data from different clients is always guaranteed.

1.5 Pseudonymization & Encryption

Administrative access to server systems is always via encrypted connections. In addition, data on server and client systems is stored on encrypted data carriers. Corresponding hard disk encryption systems are in use.

2. INTEGRITY

2.1 Input Control

The entry, modification and deletion of personal data processed by Compliance.One on behalf is generally logged.

Employees are required to work with their own accounts at all times. User accounts may not be shared or used jointly with other persons.

2.2 Transfer Control

Personal data may only be disclosed on behalf of Compliance.One's clients to the extent agreed with the client or to the extent necessary to provide the contractual services to the client.

All employees working on a customer project are instructed with regard to the permissible use of data and the modalities of data disclosure.

As far as possible, data is transmitted to recipients in encrypted form.

The use of private data carriers is prohibited for Compliance.One employees.

Employees at Compliance.One are regularly trained on data protection topics. All employees are obligated to handle personal data confidentially.

3. AVAILABILITY AND RESILIENCE

Data on Compliance.One server systems is backed up incrementally at least daily and "fully" weekly. The backup media are encrypted and moved to a physically separate location.

The import of backups is tested regularly.

The IT systems have an uninterruptible power supply. The server room has a fire alarm system and a CO2 extinguishing system. All server systems are subject to monitoring, which immediately triggers messages to an administrator in the event of malfunctions.

There is a contingency plan in place at Compliance.One, which includes a restart plan.

4. ORDER CONTROL

The data processing takes place exclusively in the European Union.

A company data protection officer has been appointed at Compliance.One.

When subcontractors are involved, a contract processing agreement is concluded in accordance with the requirements of the applicable data protection law following a prior audit by Compliance.One's data protection officer. Contractors are also regularly monitored during the contractual relationship.

5. PRIVACY BY DESIGN AND PRIVACY BY DEFAULT

At Compliance.One, care is taken during the development of the software to ensure that the principle of necessity is already taken into account in connection with user interfaces. For example, form fields and screen masks can be designed flexibly.

Compliance.One's software supports input control with a flexible and customizable audit trail that enables immutable storage of changes to data and user permissions. Authorizations on data or applications can be set flexibly and granularly.

6. PROCEDURES FOR REGULAR REVIEW, ASSESSMENT AND EVALUATION

A comprehensive data protection management system is implemented at Compliance.One. There is a guideline on data protection and information security and policies to ensure the implementation of the guideline's objectives.

The guideline and the policies are regularly evaluated and adjusted with regard to their effectiveness.

A Data Protection and Information Security Team is in place to plan, implement, evaluate and make adjustments to data privacy and information security measures.

In particular, it is ensured that data protection incidents are recognized by all employees and reported to the team without delay. The team will investigate the incident immediately. If data processed on behalf of customers is affected, care is taken to ensure that they are informed immediately about the nature and scope of the incident.

ANNEX 3: TECHNICAL OVERVIEW OF THE WHISTLEBLOWING SYSTEM

- **Encryption in Transit**

  The contractor always uses SSL or https as transport layer for all accesses to its systems. Our SSL certificates have a maximum lifetime of 12 months and are replaced regularly. RSA SHA-256 is used for SSL.

  This ensures that unauthorized persons cannot read any data in transit.

- **Encryption at Rest**

  All data is stored encrypted by default. We use Hashicorp Vault to store hints and personal data for this purpose. Data is stored this way with AES256 GCM.

  Data can only be decrypted and accessed after unlocking the vault with at least three keys (Shamir's Secret Sharing). These three keys are distributed to different people in our organization and are not stored together in any place.

- **Application Security when Accessing Data**

  To provide additional protection for the data, a separate instance is created within the vault for each customer. Each individual access is protected with a one-time password (token), so that application access data is only valid for a fraction of a second at a time.

  This ensures that passwords cannot be used more than once and makes it impossible for attackers to use them more than once.

- **Authentication**

  Authentication against our public services is protected by a username + password authentication.

  The requirements for a password are at least 8 characters, a number, a special character and a capital letter Passwords can be changed at any time. We regularly ask our customers to change their passwords.

  We also log every failed login attempt and block access after a predefined number of failed attempts.

  To increase the security of our customers, we also offer 2-factor authentication. Here we support Yubikey tokens and software-based tokens (e.g. Authy or Google Authenticator).

- **Server Access**

  Access to servers is only possible directly for a very small group of employees. PKI-based access methods (SSH) with a minimum key length of 4096 bits are used here.

  In addition, access via firewall is reserved for certain IP addresses only.

- **Server Location and On-site Security Measures**

  All our servers are located in data centers in Germany. Our data center partners are DIN ISO/IEC 27001 certified. This includes access to the hardware, emergency power supply, access to the data center and operation of the infrastructure.

ANNEX 4: SUB-PROCESSOR OVERVIEW

Compliance.One shall use the following sub-processors in the performance of the services under the Service Agreement:

Sub-processor	Services of the Sub-processor	Location of Processing
Hetzner Online GmbH	Hosting of the whistleblowing system	Germany
Sendinblue GmbH	Sending transactional emails	EU
Friendly Captcha GmbH	Fraud and bot prevention	Germany

The Contractor may terminate the commissioning of individual sub-processors or commission additional sub-processors. When commissioning additional sub-processors, the Contractor shall inform the Client electronically about the planned use of the additional sub-processor at least 30 days prior to its use. If the Client has a material reason to object to the use of a sub-processor, the Client shall notify the Contractor thereof in writing no later than 15 days after being informed of the planned use of the sub-processor, stating the material reason. If the Client does not object within this period of time, the use of the additional subcontracted processor shall be deemed approved by the Client.

If Client objects, Contractor may cure the objection as follows: (1.) Contractor shall not use the additional sub-processor for the processing of Client's Personal Data; or (2.) Contractor shall take steps to eliminate the substantial reason for Client's objection; or (3.) Contractor may temporarily or permanently cease providing the aspect of the service affected by the use of the additional sub-processor to Client and refund to Client any compensation already paid in advance for the provision of the aspect of the service. If none of these three options is feasible and the objection has not been remedied within 15 days of receipt of the objection, either party may terminate the contract extraordinarily with reasonable notice.