PRIVACY NOTICE

1. GENERAL INFORMATION

Data protection safeguards your (“You”; “Data Subject”) rights and freedoms when personal data is processed. The purpose of data protection is to define when and on what conditions personal data can be processed.

This Privacy Notice supplements the Privacy Policy available on . This Privacy Notice (“Privacy Notice”) explains in detail how we collect, use and disclose your personal data in connection with our whistleblowing process, which is explained deeply in the guidance available here.

2. WHY IS PERSONAL DATA PROCESSED IN CONNECTION WITH WHISTLEBLOWING?

Whistleblowing effectively supports transparency and a high level of business ethics. To investigate the notifications as well as address potential issues on organizational level, it is necessary to process personal data.

This means that we may process personal data of the person who blows the whistle as well as people who are potentially subject to notification or otherwise involved in the whistleblowing process. Their personal data is processed for the purposes of investigation, reporting, and fixing of potential issues raised.

3. BASIS FOR PROCESSING PERSONAL DATA

Processing of personal is based on mandatory legislation (whistleblower act, in Finnish “*Euroopan unionin ja kansallisen oikeuden rikkomisesta ilmoittavien henkilöiden suojelusta*”) and legitimate interest.

Haltian has legitimate interest for processing of personal data as the reporting channel is a way of monitoring compliance with the applicable legislation as well as ethical principles. Through the reporting channel, it is possible to obtain important and systematic information about any suspected misconduct and violations, and to respond to them in a timely manner.

A reporting mechanism is a key part of the UN's guiding principles for human rights and business conduct. The existence of a reporting channel supports a good business culture, by giving a channel for sharing grievances and suspicions. We cannot separately request the consent of a person who is the subject of a report.

4. PROCESSED PERSONAL DATA

We collect personal data that is necessary for the investigation of a case. Such data may include basic personal details, if a person provides these via the reporting channel. Some examples of such data are a person's name, phone number, or e-mail address.

It may also include details relevant to a case about a person who is the subject of the report -- e.g., the person's name and position within the company.

5. RECIPIENTS OF PERSONAL DATA

The personal data is processed in digital systems and services for the purposes specified in this Privacy Notice. We use external service providers in the production of system and support services. Personal data can be transferred to said service providers insofar as the service providers in question participate in the implementation of measures within the framework of the relevant assignment.

We work to ensure a sufficient level of protection for personal data that is in our partners' possession, according to what is required by law.

If a report requires a more detailed investigation, and if anyone's personal details are given in the report, this personal data may be handed over to the persons in the organisation who are responsible for internal investigations.

We disclose data to the authorities within the limits permitted and required by valid legislation when responding to authorities' requests for information.

6. TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS, AND THE SAFEGUARDS EMPLOYED

We do not transfer personal data to third countries outside the European Union or the European Economic Area, or to international organisations.

7. PERIOD FOR STORING PERSONAL DATA, OR CRITERIA FOR DETERMINING THE STORAGE PERIOD

The personal data referred to in this privacy notice is only stored for as long as, and to the extent that, it is needed, and the data controller will utilise it for actions related to the reported purposes of processing.

With all other things remaining equal, reports and any associated personal data are stored for 5 years after the receiving the information. If a case proceeds to court, and the proceedings in court require a longer period of storage, then the data will be stored for the period that the legal proceedings require. Reports that contain no basis for investigation will be anonymised immediately if they contain any personal data.

8. IMPORTANT INFORMATION ON AUTOMATED DECISION-MAKING OR PROFILING

No automated decision-making or profiling is associated with the personal data processing.

9. INFORMATION SECURITY

We protect personal data carefully throughout its entire life cycle, by employing the appropriate data protection and information security measures. The supplier of the anonymous reporting channel system (WhistleB) processes personal data at secure server facilities. WhistleB does not store IP addresses or other information that could be used to identify the sender of a report. All reports are encrypted and can only be decrypted by

designated personnel. Access to reports is restricted, and those who process reports have an obligation of confidentiality.

10. DATA SUBJECT RIGHTS

Your rights are further elaborated on Privacy Policy available on https://haltian.com/privacy/.

However, in connection with whistleblowing your rights may be limited if it is necessary and proportionate to ensure the accuracy of the notification or to protect the identity of the notifier.

For any further questions or complaints please address your request to privacy@haltian.com.

People also have the right to lodge a complaint with the supervisory authority if they consider the processing of their personal data to violate the applicable data protection provisions.