Privacy Impact Assesment (PIA) - Whistleblower Partners ApS

Whistleblower Partners ApS
Kultorvet 11, 4., 1175 Copenhagen C, Denmark

(Referred to as "the Controller")

Customers of Whistleblower Partners ApS

(Referred to as "the Data Subject")

Michael Erlitz, Data Protection Officer (Referred to as "DPO")
michael.erlitz@whistleblowerpartners.com

1. PREAMBLE

This Privacy Impact Assessment (referred to as "PIA") is conducted following Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (referred to as "GDPR").

1.1 The Scope of the PIA

It is stipulated in GDPR Article 32(1) that:

> *"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, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk".*

On the grounds of the above-mentioned, the Regulation, and to improve transparency, the Controller conducts following PIA. The PIA aims at describing the data processing and the risks of the Data Subjects in case of a data breach in relation to the Whistleblower System of the Controller.

The PIA is supplemented by the Data Protection Impact Assessment (DPIA), the data agreements between the Controller and the Data Subjects, as well as the Privacy Policy.

Furthermore, *this PIA contains a risk assessment of the data processing in relation to external Data Subjects*, which excludes persons inside the organization.

1.2 Overview of the Controller's Solutions

Under Directive (EU) 2019/1937 of the European Parliament and the Council of 23rd October 2019, on the protection of persons who report breaches of Union Law, the Whistleblower System is for persons designed to have the opportunity to report breaches of Union Law anonymously, and for legal entities, to be able to do a screening of breaches of Union Law.

The Controller provides the following solutions:

- Whistleblower System
- Screening Service
- Response Service
- Speak Up Universe

2. DATA PROCESSING

2.1 Data Processing Activities

In connection with the delivery of the Controller's software solution, the Controller processes personal data on behalf of the Data Subject. The Controller might be processing data concerning the following:

Online

- Website Operation
- Tracking

Customers

- Contract Processing, Sales, or Distribution
- CRM
- Marketing

General / Suppliers

- Accounts Payable and Receivable
- Project Management
- Production
- Audit
- Legal
- Compliance

Because of the nature of the business of the Controller, normal personal data, special categories of personal data (GDPR Article 9), and personal data relating to criminal convictions and offences (GDPR Article 10) might be processed.

2.2 Purpose of Data Processing

The purpose of the processing of data is mainly to fulfil the contractual obligations of the Controller in relation to the Whistleblower System. Data might therefore be processed in the following cases:

- Registration of the Customers for financial administration, invoicing, and to process and deliver orders.
- Manage the relationship with the Customers, e.g., responding to questions or complaints.
- Administer and protect the business and website, e.g., system maintenance and support, fixing problems, and hosting of data.
- Carry out data analytics to improve website, products, marketing, and customer experience on our website.
- Recommend products that may be of interest to users by email and contextual advertising.
- Provide email newsletters to users who have subscribed to this service.

- Detect and prevent fraudulent transactions.

- Verify user identity and provide a secure platform.
- Comply with regulatory or legal obligations.

3. DATA SHAREING

Personal data included in a reported breach of Union Law is shared with the Customer's contact persons under the Customer's internal policies. Alternatively, if these persons are disqualified from viewing the data, the personal data will be shared with other persons the Controller deems relevant to contact to process the report. If agreed with the customer, external parties, e.g., public authorities, may be notified if the details of a report merit such action.

The Controller disclose personal data to local Legal Partners, with whom the Controller collaborate to offer the Whistleblower Screening Service.

4. THE SCOPE OF THE DATA PROCESSING

To identify the level of risk of a personal data breach, as of 1st September 2023, the Controller processed Customer data of upwards to 850 Data Subjects.

The data specifically contained information regarding the Data Subject's:

- Company name,
- address,
- contact information (e.g., email, tel., fax, etc.),
- ownership and structure,
- person in charge of whistleblower incidents, and his / her contact information.

5. THE PRIVACY OF PHYSICAL PERSONS

Privacy and discretion are the fundamental values of the Whistleblower System. However, because of the nature of the personal data, it is assessed, that a personal data breach potentially could harm the Data Subjects physically, materially, or morally. Therefore, the Controller has a high level of awareness of data protection and data breach response, which is outlined in the Controller's DPIA.

6. PROBERBILITY

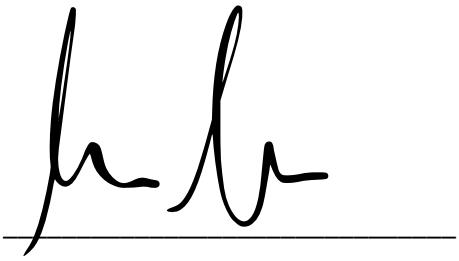
On the grounds of the conclusions reached in the DPIA, and the fact that there have not been detected any data breaches at the Controller yet, the threat of data breaches is evaluated to be of low risk. However, as the System and the surroundings are in constant change, the PIA and the DPIA will be reviewed continuously if changes to the initially identified risks occur.

7. OVERALL ASSESSMENT

After an examination of the data processing and the risks to the Data Subjects in case of a data breach, the following conclusions can be derived:

- That the Controller mainly processes data in relation to the Controller's contractual obligations to the Customers of the Whistleblower System,
- this information might consist of normal personal data, special categories of personal data (GDPR Article 9), and personal data relating to criminal convictions and offenses (GDPR Article 10), and therefore, a data breach could have great consequences on the privacy of the Data Subjects.
- The Controller has a high level of awareness of data protection and has identified the risk of a data breach as low.

This PIA enters into force on the *31st of August 2023* and will be reviewed if changes to the initial identified risks occur. The PIA has been reviewed by the DPO.



Signed by Michael Erlitz, DPO, the 15th of September 2023