

Data Protection Impact Assessment (DPIA) - 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 Data Protection Impact Assessment (referred to as "DPIA") 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 DPIA

As stated in GDPR Article 35(3) a DPIA shall in particular be required in the case of e.g.:

- (a) *“Systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person.*
- (b) *Processing on a large scale of special categories of data referred to in GDPR Article 9(1), or of personal data relating to criminal convictions and offenses referred to in GDPR Article 10.*
- (c) *Systematic monitoring of a publicly accessible area on a large scale”.*

In addition, [the Danish Data Protection Agency's List of Activities Requiring a DPIA](#) states that companies need to conduct a DPIA when e.g., data breaches can have a direct effect on the health of a physical person or the safety of a physical person.

The DPIA is aimed at assessing and targeting potential high risks associated with the data processing activities related to the Whistleblower System of the Controller. The DPIA supplements data agreements between the Controller and the Data Subjects, as well as the Privacy Policy.

Furthermore, *this DPIA 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 Organization'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. 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. The data specifically contains 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.

2.2 Purpose of Data Processing

The purpose of the data processing 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:

- Online
Website Operation
Tracking
- Customers
Contract Processing, Sales, or Distribution
CRM
Marketing
- General / Suppliers
Accounts Payable and Receivable
Project Management
Production
Audit
Legal
Compliance

2.3 Legal Framework

As stated in GDPR Article 6(1) data processing shall be lawful only if and to the extent that the data processing has a legal basis.

The Controller can process data on the grounds of one or more of the following reasons:

- GDPR Article 6(1)(a). The Data Subject has given consent to the processing of his or her data for one or more specific purposes.
- GDPR Article 6(1)(b). Processing is necessary for the performance of a contract to which the Data Subject is party or to take steps at the request of the Data Subject before entering into a contract.
- GDPR Article 6(1)(c). Processing is necessary for compliance with a legal obligation to which the Controller is subject.
- GDPR Article 6(1)(d). Processing is necessary to protect the vital interests of the Data Subject or another natural person.
- GDPR Article 6(1)(e). Processing is necessary for the performance of a task carried out in the public interest or the exercise of official authority vested in the Controller.

The Controller ensures, in accordance with the principles in GDPR Article 5(1) that personal data is at any time processed lawfully, fairly, and in a transparent manner about the Data Subject, collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes, adequate, relevant and limited to what is necessary about the purposes for which they are processed.

3. RIGHTS & OBLIGATIONS

3.1 Rights of the Data Subject

At any time, the Data Subject has the rights as mentioned in the Regulation. These provisions include especially Article 16 (the Right to Rectification), Article 17 (the Right to Be Forgotten), Article 18 (the Right to Restriction of Processing), Article 19 (the Right to Data Portability), Article 21 (the Right to Object), and Article 22 (the Right to Be a Subject Matter of Individual Decision Making).

If the Data Subject has complaints regarding the use or collection of personal data, the Data Subject has the possibility to complain to the DPO.

3.2 Obligations of the Controller

The Controller is by GDPR Article 24(1) responsible for ensuring that the processing of personal data is conducted in accordance with the Regulation and other data protection rules in the EU or national law.

4. DATA SECURITY MEASURES

4.1 Data Retention

The Controller will store and use data collected from Customers as long as is necessary to implement, administer, and manage the contractual obligations concerning the Whistleblower System, or as required to comply with legal obligations, including Tax and Security Rules.

When the Customer contract has been terminated or repealed the Controller will retain data on the Data Subject for a maximum of twelve months in order to finalize the contract relation.

In any case, the Data Subject has the right to be forgotten following GDPR Article 17 and the right to restriction of processing in GDPR Article 18.

4.2 Data Sharing

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.

5. RISK ASSESSMENT

The Controller has in cooperation with the internal IT Department identified the following top score risks, that can pose a threat to the security of the data processing with a focus on the general rights and freedom rights of the Data Subject:

- (1) Poor DevOps Service Quality: Failure to deliver new features, improvements, bug fixes, or configuration changes, which leads to an exposure of personal data:

Any development or configuration change requests e.g., new features, improvements, bug fixes, change of infrastructure, etc. are backlogged, categorized, risk-rated, prioritized, and processed accordingly when a user story, expected result, and test cases are formalized. The development and delivery are processed according to agile development standards with continuous delivery. No change request is implemented before the full test process has been successfully committed including unit test, self-test, code review, quality assurance feature and smoke-test, and internal end-user test have been successfully performed. After deploying to PROD a feature and smoke tests are performed.

- (2) Refresh of TEST and DEV Database: Failure to clean Whistleblower Platform PROD DB being deployed to TEST and DEV environment.

DEV and TEST DB are not freshened from PROD. Hence the risk was removed.

In case a specific bug cannot be regenerated in TEST or DEV, the PREPROD APP server can be pointed to PROD within the same security regime of the PROD environment. An internal case administrator, outside of the IT Department, will be assigned the task of regenerating the bug. Hence the PROD data will still not be shared in the TEST or DEV database.

- (3) Vendor and Third-Party Risks: Relying on third-party vendors or service providers without ensuring they have robust data protection measures in place can lead to breaches that affect Data Subjects' rights.

Microsoft has been chosen to provide the system framework and hosting in Microsoft Azure in-side the European Union.

- (4) Poor Authentication Practices: Weak authentication methods or improperly configured access controls can make it easier for unauthorized individuals to gain access to personal data, compromising Data Subjects' rights to security and privacy.

Internally, password weak-authentication approval and 3D verification are processed via Microsoft and Microsoft Authenticator controlling system access.

Externally, access to the WB System is 3D secured via SMS password authentication. The access to the SMS Provider system is controlled by the DPO on request.

- (5) Failure to Patch and Update Systems: Neglecting to apply security patches or updates to IT systems can leave them vulnerable to known exploits, putting Data Subjects' rights to the security of their personal information at risk.

The Whistleblower System is hosted by the service provider in the Microsoft Azure hosting center in Frankfurt, Germany. (Security) patches for Windows Server OS, MS SQL, and MS Frameworks are processed on recommendation from Microsoft firstly on DEV for TEST and following on PROD. All patches are monitored and controlled by the DPO.

- (6) Lack of Data Encryption: Failing to encrypt data both in transit and at rest can expose it to interception or unauthorized access, potentially infringing on data subjects' rights to data security.

Internally, any data transmission is encrypted by the internal network and externally via the use of a VPN.

Externally, any access to the Whistleblower Platform is encrypted via the use of best development practices.

6. MITIGATION MEASURES

Concerning the identified threats under *Risk Assessment (Section 5)* the Controller has taken the mitigation measures (marked in cursive) in the above-mentioned section to reduce the risk of a data breach.

7. DATA BREACH RESPONSE

In the unlikely event of a data breach, defined as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed in GDPR Article 4(12), the Controller has created following guidelines to handle breaches, based on [the Danish Data Protection Agency's Guidelines](#):


- (1) In accordance with GDPR Article 33(2), the DPO will be informed about the breach within 24 hours, and conduct an assessment of the breach.
- (2) The DPO will report the breach to the competent supervisory authority, without undue delay, and if possible, no later than 72 hours after the breach, unless it is unlikely that the breach poses a risk to natural persons' rights or freedom rights (GDPR Article 33(1)).
- (3) Without undue delay, the DPO will notify the Data Subject after becoming aware that there has been a breach of personal data.
- (4) The DPO will document and store the breach, comprising the facts relating to the personal data breach, its effects, and the remedial action taken. (GDPR Article 33(5)).

8. OVERALL ASSESSMENT

After an examination of the data processing of Customers at the Controller, the following conclusions can be derived:

- The data processing activities and the purpose of these are lawfully, fairly, transparent, and compliant with the Regulation.
- The Controller has ensured that the Data Subjects' access to general rights and freedom rights is maintained.
- By systematically evaluating the technical factors, the Controller has gained valuable insights into the potential impacts and likelihood of adverse events. Implementing robust mitigation measures is crucial in safeguarding assets, personnel, and reputation. The combination of proactive measures and providing comprehensive awareness has significantly reduced the overall risk profile.
- There has been a review of the data breach response so that the organization has an up-to-date response mechanism.

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



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