Whistleblower Partners ApS
CVR-nr 43615661
Kultorvet 11 4,
1175 Copenhagen,
Denmark

DATA PROCESSING AGREEMENT

pursuant to Article 28(3) of Regulation 2016/679 (the General Data Protection Regulation) concerning the data processor's processing of personal data

between

The Customer

(hereinafter "the data controller")

and

Whistleblower Partners ApS
CVR Number: 43615661
Kultorvet 11, 4th floor
1175 Copenhagen
Denmark

(hereinafter referred to as "the data processor")

each referred to as a "Party" and, collectively, the "Parties"

HAVE AGREED the following standard contractual provisions (the Provisions) with a view to complying with the General Data Protection Regulation and ensuring the protection of privacy and the fundamental rights and freedoms of natural persons

Whistleblower Partners ApS
CVR-nr 43615661
Kultorvet 11 4,
1175 Copenhagen,
Denmark

1. PREAMBLE

1. These Provisions stipulate the data processor's rights and obligations when the data processor processes personal data on behalf of the data controller.
2. These Provisions are designed to ensure that the parties comply with Article 28(3) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and regarding the free movement of such data as well as ensuring that the parties comply with the repealing of Directive 95/46/EC (General Data Protection Regulation).
3. In connection with the delivery of Whistleblower Partners' Whistleblower solution, the data processor processes personal data on behalf of the data controller in accordance with these Provisions. According to The Whistleblower Directive, processing of personal data can take place when it is necessary to process reports received as part of a whistleblower scheme.
4. The Provisions take precedence over any similar provisions in other agreements between the parties.
5. There are four annexes to these Provisions, and the annexes form an integral part of the Provisions.
6. Annex A contains specifics on the processing of personal data, including the purpose and nature of the processing, the type of personal data, which is processed, the categories of data subjects and the duration of the processing.
7. Annex B contains the data controller's conditions for the data processor's use of data sub-processors and a list of data sub-processors that the data controller has approved the use of.
8. Annex C contains the data controller's instructions regarding the data processor's processing of personal data, a description of the security measures that the data processor must, as a minimum, implement, and information on how the data processor and any data sub-processors are supervised.
9. The Provisions and accompanying annexes must be stored in writing, including electronically, by both parties.
10. These Provisions do not release the Data Processor from any obligations imposed on the Data Processor under the General Data Protection Regulation or any other legislation.

Whistleblower Partners ApS
CVR-nr 43615661
Kultorvet 11 4,
1175 Copenhagen,
Denmark

2. RIGHTS AND OBLIGATIONS OF THE DATA CONTROLLER

1. The data controller is responsible for ensuring that the processing of personal data takes place in accordance with the General Data Protection Regulation (see the regulation's article 24), data protection regulations in other EU law or the Member States'[1] national law as well as in accordance with these regulations.

2. The data controller has the right and obligation to make decisions about the purpose(s) for and the means by which personal data may be processed.

3. The data controller is responsible for, among other things, ensuring that there is a processing basis for the processing of personal data which the data processor is instructed to carry out.

3. THE DATA PROCESSOR ACTS ACCORDING TO INSTRUCTIONS

1. The data processor may only process personal data in accordance with documented instructions from the data controller, unless otherwise required by EU law or the national law of the Member States to which the data processor is subject. These instructions must be specified in Annexes A and C. Subsequent instructions may also be given by the data controller while personal data is being processed, but the instructions must always be documented and kept in writing, including electronically, along with these Provisions.

2. The data processor shall inform the data controller immediately if, in their opinion, an instruction is contrary to the General Data Protection Regulation or data protection provisions in other EU law or the national law of member states.

1 References to "Member State" in these Provisions shall be construed as a reference to "EEA Member States".

4. CONFIDENTIALITY

1. The data processor may only grant access to personal data processed on behalf of the data controller to persons who are subject to the data processor's instructional powers and who have committed themselves to confidentiality or are subject to an appropriate statutory duty of confidentiality, and only to the extent necessary. The list of persons who have been granted access must be reviewed on an ongoing basis. Based on this review, access to personal data may be prevented if access is no longer necessary, in which case the personal data shall no longer be available to these persons.

2. The data processor must, at the request of the data controller, be able to demonstrate that the persons in question, who are subject to the data processor's instructional powers, are subject to the above-mentioned duty of confidentiality.

3. The data processor may only pass on personal data processed on behalf of the data controller to the extent that this follows from The Whistleblower Directive, the General Data Protection Regulation or other legislation.

5. PROCESSING SECURITY

1. Article 32 of the General Data Protection Regulation stipulates that the data controller and the data processor, considering the current technical level, the implementation costs and the nature, scope, context and purpose of the processing concerned, as well as the risks of varying probability and seriousness to natural persons' rights and freedoms, take relevant technical and organisational measures to ensure a level of protection appropriate for these risks.

   The data controller shall assess the inherent risks of the processing to the rights and freedoms of natural persons and implement measures to address these risks. Depending on their relevance, measures may include:

   a. Pseudonymisation and encryption of personal data

   b. ability to ensure lasting confidentiality, integrity, availability and robustness of processing systems and services;

c. ability to restore the availability of, and access to, personal data in the event of a physical or technical incident in a timely manner;

d. a procedure for regular testing, assessment and evaluation of the effectiveness of technical and organisational measures to ensure processing safety.

2. Pursuant to Article 32 of the Regulation, the data processor – independently of the data controller – must also assess the inherent risks of the processing to the rights of natural persons and implement measures to address these risks. For the purposes of this assessment, the data controller shall provide the information to the data processor which is necessary for them to identify and assess such risks.

3. In addition, the data processor shall assist the data controller in complying with the data controller's obligation under Article 32 of the Regulation by i.a. providing the data controller with the necessary information regarding the technical and organisational security measures already implemented by the data processor in accordance with Article 32 of the Regulation as well as any other information necessary for the data controller to comply with its obligation under Article 32 of the Regulation.

   If the response to the identified risks, in the opinion of the data controller, requires the implementation of additional measures beyond those already implemented by the data processor, the data controller shall list the additional measures to be implemented in Annex C.

6. USE OF DATA SUB-PROCESSORS

1. The data processor must meet the conditions set out in Article 28(2) and (4) of the General Data Protection Regulation in order to utilise another data processor (a data sub-processor).

2. The processor has the controller's general authorisation for the engagement of sub-processors.

3. The data processor shall carefully select the sub-processors, particularly considering the suitability of the technical and organisational measures taken by the sub-processor.

Whistleblower Partners ApS
CVR-nr 43615661
Kultorvet 11 4,
1175 Copenhagen,
Denmark

4. The processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.

5. The list of data sub-processors already approved by the data controller is set out in Annex B.

6. When the data processor uses a data sub-processor to perform specific processing activities on behalf of the data controller, the data processor shall, through a contract or other legal document under EU or national law, impose the same data protection obligations on the data sub-processor as those that appear in these Provisions, in particular the necessary guarantees that the data sub-processor will implement the technical and organisational measures in such a way that the processing complies with the requirements of these Provisions and the General Data Protection Regulation.

   Thus, the data processor is responsible for ensuring that the data sub-processor, at a minimum, complies with the data processor's obligations under these Provisions and the General Data Protection Regulation.

7. Sub-processor agreement(s) and any subsequent amendments thereto are sent, at the request of the data controller, in a copy to the data controller, who thus can ensure that corresponding data protection obligations resulting from these Provisions are imposed on the data sub-processor. Provisions on commercial terms that do not affect the data protection content of the data sub-processing agreement shall not be sent to the data controller.

8. In its agreement with the data sub-processor, the data processor must include the data controller as a beneficiary third party in the event of the data processor's bankruptcy so that the data controller can accede to the data processor's rights and enforce these against data sub-processors, i.e. allowing the data controller to instruct the data sub-processor to delete or return the personal data.

9. If the data sub-processor fails to fulfil its data protection obligations, the data processor remains fully liable to the data controller for the performance of the sub-processor's obligations. This is without prejudice to the data subjects' rights deriving from the General Data Protection Regulation, in particular Articles 79 and 82 of the Regulation, vis-à-vis the data controller and the data processor, including the data sub-processor.

7. TRANSFER TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS

1. Any transfer of personal data to third countries or international organisations may only be carried out by the data processor based on documented instructions from the data controller and must always be done in accordance with Chapter V of the General Data Protection Regulation.

2. If a transfer of personal data to third countries or international organisations that the data processor has not been instructed to perform by the data controller is required by EU law or national laws of Member States to which the data processor is subject, then the data processor shall notify the data controller about this legal requirement before processing, unless the legislation in question prohibits such notification out of consideration of the public interest.

3. Thus, without documented instructions from the data controller, the data processor may not, within the limits of these Provisions:

    a. transfer personal data to a data controller or data processor in a third country or an international organisation

    b. transfer the processing of personal data to a data sub-processor in a third country

    c. process personal data in a third country

4. The data controller's instructions regarding the transfer of personal data to a third country, including any basis for transfer in Chapter V of the General Data Protection Regulation on which the transfer is based, shall be set out in Annex C.6.

5. These Provisions shall not be confused with the standard contractual provisions within the meaning of Article 46(2), points (c) and (d) of the General Data Protection Regulation, and these Provisions may not constitute a basis for the transfer of personal data within the meaning of Chapter V of the General Data Protection Regulation.

8. ASSISTANCE TO THE DATA CONTROLLER

1. Taking into account the nature of the processing, the data processor shall assist the data controller as far as possible by appropriate technical and organisational measures in compliance with the data controller's obligation to respond to requests for the exercise of data subjects' rights as set out in Chapter III of the General Data Protection Regulation.

   This means that, to the extent possible, the data processor must assist the data controller in complying with:

   a. the duty to inform the data subject when personal data is collected from the data subject;

   b. the duty to inform the data subject if personal data has not been obtained from the data subject;

   c. the right of access;

   d. the right of rectification;

   e. the right of erasure ("the right to be forgotten");

   f. the right to restriction of processing;

   g. the duty to inform in connection with the correction or deletion of personal data or restriction of processing;

   h. the right to data portability;

   i. the right to object;

   j. the right not to be the subject of a decision based solely on automatic processing, including profiling

Whistleblower Partners ApS
CVR-nr 43615661
Kultorvet 11 4,
1175 Copenhagen,
Denmark

2. Taking into account the nature of the processing and the information available to the data processor, the data processor shall also assist the data controller with the following:

   a. the obligation of the data controller to report the breach of personal data security 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 of personal data security poses a risk to natural persons' rights or freedoms

   b. the obligation of the data controller to notify the data subject of a breach of personal data security without undue delay when the breach is likely to entail a high risk to the rights and freedoms of natural persons

   c. the obligation of the data controller to carry out an analysis of the consequences of the intended processing activities for the protection of personal data prior to processing (impact assessment)

   d. the data controller's obligation to consult the competent supervisory authority, before processing if an impact analysis regarding data protection shows that the processing will lead to a high risk in the absence of measures taken by the data controller to limit said risk.

3. The Parties shall set out in Annex C the necessary technical and organisational measures with which the data processor is to assist the data controller, as well as the extent of these. This applies to the obligations that follow from Provisions 8.1. and 8.2.

Whistleblower Partners ApS
CVR-nr 43615661
Kultorvet 11 4,
1175 Copenhagen,
Denmark

9. NOTIFICATION OF BREACH OF PERSONAL DATA SECURITY

1. Without undue delay, the data processor shall notify the data controller after becoming aware that there has been a breach of personal data security.

2. The data processor's notification to the data controller shall, if possible, take place within 24 hours after they have become aware of the breach so that the data controller can comply with their obligation to report the breach of personal data security to the competent supervisory authority in accordance with Article 33 of the General Data Protection Regulation.

3. In accordance with Provision 8.2.a, the data processor shall assist the data controller in reporting the breach to the competent supervisory authority. This means that the data processor must assist in providing the following information, which, according to Article 33(3), must be stated in the data controller's notification of the breach to the competent supervisory authority:

    a. the nature of the personal data breach, including, where possible, the categories and approximate number of data subjects impacted as well as the approximate number of personal data records concerned;

    b. the likely consequences of the breach of personal data security

    c. the measures taken or proposed by the data controller to deal with the breach of personal data security, including, where appropriate, measures to limit the potential harmful effects of the breach.

4. The Parties shall set out in Annex C the information that the data processor must provide in connection with their assistance to the data controller in their obligation to report breaches of personal data security to the competent supervisory authority.

Whistleblower Partners ApS
CVR-nr 43615661
Kultorvet 11 4,
1175 Copenhagen,
Denmark

10. DELETION AND RETURN OF DATA

1. Upon termination of the personal data processing services, the data controller is obligated to delete all personal data that has been processed on behalf of the data controller and to confirm to the data controller that the data has been deleted, unless EU law or the national law of the Member States provides for the storage of the personal data.

11. AUDIT, INCLUDING INSPECTION

1. The data processor shall make available to the data controller all information necessary to demonstrate compliance with Article 28 of the General Data Protection Regulation and provide for and contribute to audits, including inspections carried out by the data controller or another auditor authorised by the data controller.

2. The procedures for the data controller's audits, including inspections, with the data processor and sub-processors are detailed in Annex C.7.

3. The data processor is obligated to give supervisory authorities who, in accordance with applicable law, have access to the data controller's or data processor's facilities, or representatives acting on behalf of the supervisory authority, access to the data processor's physical facilities against proper identification.

12. AGREEMENT BY THE PARTIES ON OTHER MATTERS

1. The Parties may agree on other provisions regarding the service and concerning the processing of personal data on e.g. liability, as long as these other provisions do not directly or indirectly contravene the Provisions or impair the data subject's fundamental rights and freedoms arising from the General Data Protection Regulation.

13. ENTRY INTO FORCE AND TERMINATION

1. The Provisions shall enter into force on the date of signature of both Parties.

2. Both Parties may demand that the Regulations be renegotiated if changes to legislation or inexpediencies in the Regulations give rise to this.

3. The Provisions apply as long as the personal data processing service lasts. During this period, the Clauses may not be terminated unless other provisions governing delivery of the personal data processing service are agreed between the Parties.

4. If the delivery of the services relating to the processing of personal data ceases and the personal data is deleted or returned to the data controller in accordance with Provision 10.1 and Annex C.4, the Provisions may be terminated by written notice by either party.

Whistleblower Partners ApS
CVR-nr 43615661
Kultorvet 11 4,
1175 Copenhagen,
Denmark

ANNEX A – INFORMATION ABOUT THE PROCESSING

A.1 THE PURPOSE OF THE DATA PROCESSOR'S PROCESSING OF PERSONAL DATA ON BEHALF OF THE DATA CONTROLLER

The purpose of the processing of personal data is to receive and store reports and make these available to case handlers appointed by the data controller to process reports as part of the data controller's advisory service in connection with whistleblower schemes, cf. The Whistleblower Directive.

A.2 THE DATA PROCESSOR'S PROCESSING OF PERSONAL DATA ON BEHALF OF THE DATA CONTROLLER PRIMARILY CONCERNS (THE NATURE OF THE PROCESSING)

To receive and store reports from end users and make these reports available to case handlers appointed by the data controller to process information.

A.3 THE PROCESSING INCLUDES THE FOLLOWING TYPES OF PERSONAL DATA ABOUT THE DATA SUBJECTS

The data processor receives and processes personal data in accordance with the data processing agreement. The data owner transfers the following types of personal data to the data processor:

ARTICLE 6, GENERAL PERSONAL DATA

- ✓ Contact information *(e.g., name, email, phone number)*
- ✓ Master data *(e.g., birth data)*
- ✓ Registration numbers *(e.g., userID, databaseID, customerID)*
- ✓ Information on employment conditions *(e.g., contract, title, staff file)*
- ✓ Information relating to salary *(e.g., salary, bank details)*
- ✓ Qualifications and certifications
- ✓ Performance *(e.g., overtime, KPIs)*
- ✓ Relationships *(e.g., customer status, contact roles)*
- ✓ Behavioural information *(e.g., usage preferences, usage history)*

ARTICLE 9, SENSITIVE PERSONAL DATA

Information about…

- ✓ Race or ethnic origin.
- ✓ Political beliefs or affiliation.
- ✓ Religious or philosophical beliefs.
- ✓ Trade union membership.
- ✓ Health.
- ✓ Sex life.
- ✓ Sexual orientation.
- ✓ Genetic data.
- ✓ Biometric data.
- ✓ Information about children.
- ✓ Other sensitive information.

ARTICLE 10, PERSONAL DATA REGARDING CRIMINAL CONVICTIONS AND OFFENCES

Information about…

- ✓ Convictions and offences

- ✓ Preferences
  (e.g., settings, user surveys, personal settings)
- ✓ Logins
- ✓ Technical information
  (e.g., OS version, browser version, IP addresses)
- ✓ Purchase history
  (e.g., book purchases, subscriptions)
- ✓ Confidential information
  (e.g., civil registration/CPR number)
- ✓ Serious or repeated violations of legislation or internal guidelines or code of conduct.
- ✓ Other personal information

A.4 THE PROCESSING INCLUDES THE FOLLOWING CATEGORIES OF DATA SUBJECTS

- ✓ Whistleblowers (*e.g. employees of the end customer who add information about legal offences to the whistleblower solution*),
- ✓ Customers or end users (*e.g. intermediaries of user access, system administrators, case handlers and the Customer's contact persons*),
- ✓ Suppliers (login information for persons who provide a service to the data processor, e.g. in the form of maintenance or engineering),
- ✓ Employees of the data processor
- ✓ Parties to criminal proceedings or involved in offences
  (*e.g. end-customer employees who are involved in serious or repeated offences or violations of internal guidelines or codes of conduct*)

Whistleblower Partners ApS
CVR-nr 43615661
Kultorvet 11 4,
1175 Copenhagen,
Denmark

A.5 THE DATA PROCESSOR'S PROCESSING OF PERSONAL DATA ON BEHALF OF THE DATA CONTROLLER MAY COMMENCE AFTER THE ENTRY INTO FORCE OF THESE CLAUSES. THE PROCESSING HAS THE FOLLOWING DURATION

- ✓ The processing is not time-limited and continues until the agreement is terminated or cancelled by one of the Parties. The data processing agreement persists beyond the duration of the main agreement between the parties and is effective for as long as the data processor processes, including stores, personal information received from or collected on behalf of the data controller or otherwise processed as part of the contractual relationship between the data controller and the data processor until the data processor has documented return and destruction of personal data, cf. section 10.1 of the data processing agreement.

ANNEX B – DATA SUB-PROCESSORS

B.1 AUTHORISEDDATA SUB-PROCESSORS

Upon entry into force of the Clauses, the data controller has approved the use of the following sub-processors:

SERVICE	CRN (CVR no.)	ADDRESS	BRIEF DESCRIPTION OF THE ACTIVITY
Microsoft Azure Services	IE8256796U	Microsoft Ireland Operations Ltd One Microsoft Place, South County Business Park, Leopardstown, Dublin, D18 P521, Ireland	Storage and backup of data Hosting application layers
Hosting and development	35248021	Unica Net ApS Agenavej 35, DK-2670 Greve, Denmark	Storage and backup of data

Upon the entry into force of the Provisions, the data controller has approved the use of the above data sub-processors for the described processing activity. The data processor may not – without the written consent of the data controller – make use of a data sub-processor for a processing activity other than the one described and agreed or make use of another data sub-processor for this processing activity.

B.2 NOTICE OF APPROVAL OF DATA SUB-PROCESSORS

Information about data processors is issued to the contract manager at the data controller in writing.

ANNEX C – INSTRUCTIONS REGARDING PROCESSING OF PERSONAL DATA

C.1 THE OBJECT/INSTRUCTION OF THE PROCESSING

The data processor's processing of personal data on behalf of the data controller shall take place as follows:

The data processor provides access to the data processor's whistleblower system in accordance with the subscription terms. The end customer and the end customer's users have the opportunity to anonymously file notices of matters and to process cases in a protected environment. The data controller is authorised to instruct the data processor about changes in end customer data, and the data processor shall make these changes without further charge if the end customer or the data controller is unable to exercise control over personal information.

The data processor and their sub-processors are authorised to process personal information for the purpose of operating and supporting the end customer's or whistleblowers' use of the product, as well as for development, subscription management and ensuring security, which are necessary for the delivery of a stable and secure product that complies with applicable legal requirements, cf. The Whistleblower Directive as well as EU2016/679 and EU2019/1937.

C.2 SECURITY OF PROCESSING

Taking into account the large amount of personal data classified under the General Data Protection Regulation (GDPR)'s Article 6, sensitive personal data covered by GDPR Article 9, information about criminal convictions or offences covered by GDPR Article 10, and information concerning vulnerable data subjects, defined as parties in an unequal power relationship with the data controller or data subjects, including children, who might be abused by the data controller, the data processor or third party due to the nature of the information, it is found that the processing poses a high risk for the data subject, which is why a correspondingly high level of processing and data security is established.

The data processor is thus entitled and obligated to make decisions about which technical and organisational security measures must be implemented to establish the necessary (and agreed) level of security.

However, the data processor must – in all cases and as a minimum – implement the following measures, which have been agreed with the data controller:

- Ensure that data is stored in an encrypted state in accordance with best practice for data that may contain confidential or sensitive information, at least encrypted to AES256 or an equivalent encryption standard.
- Ensure that encrypted data and encryption keys are stored separately. If possible, control over encryption keys is handed over to the end user.
- Ensure that communication between the service and the end user is secured via SSL or takes place via a similarly secured connection that meets applicable requirements.
- Ensure that data stored in the solution is segregated so that the end user's information cannot be accessed by unauthorised persons without the end user's direct permission.
- Ensure that data can be recovered following technical or physical incidents and have procedures in place in the form of disaster recovery and business continuity plans to ensure continued operations.
- Ensure that personal data in the solution is limited to what is absolutely necessary, and that, to the extent possible, data processors and sub-processors are restricted to processing pseudonymised personal data and do not possess, or are unable to access without the Customer's permission or knowledge, sensitive or confidential personal data contained in reports.
- Ensure that, on the basis of the Customer's instructions, the data controller can control access to the Customer's solution, and that changes in access conditions are logged and stored for up to one year, or as long as the Customer relationship lasts.
- Ensure that all access from development and support teams, who may provide access to personal data, comply with ISO2700 standards for securing access as a minimum.
- Ensure that third parties who gain legitimate access to the solution can only get access to encrypted data, that activities that involve access to sensitive or confidential personal data are logged, and that third parties are subject to a non-disclosure clause.

Whistleblower Partners ApS
CVR-nr 43615661
Kultorvet 11 4,
1175 Copenhagen,
Denmark

- Ensure that access to systems is controlled and subject to validation in the form of, for example, MFA, and that access identifiers and login times are recorded and stored for up to 30 days.
- Have procedures in place to detect and handle data breaches so that the data controller may inform users of the solution without undue delay.
- Ensure that, upon discovery of a data breach, the necessary information is registered for the purpose of case analysis and for possible follow-up investigations requested by the Customer.
- Ensure that necessary security measures are in place to prevent and limit the execution of malware or similar code, including through ongoing timely updating of software, hardware and communication systems, code validation, and by continuously testing the hardness and resistance of the solution through penetration testing.
- Have procedures for the correct and secure processing of physical material taken from the solution for legal purposes, including storage, distribution and data extracted from home offices, and ensure that the data processor's employees are instructed in the correct processing of personal data, have received security training, are subject to non-disclosure clauses and similar or equivalent organisational measures.
- Ensure that the Customer can see if the content of the solution has been changed and by whom.
- Ensure that the end user who has used the solution has the opportunity to correct or add information in the solution themselves, and that the end user has the opportunity to withdraw their report.
- Ensure that the Customer can extract the necessary data from the solution if the Customer wishes to stop using the solution. Data can be extracted in a machine-readable format by the Customer themselves so that the data controller's or data processor's access to sensitive or confidential personal data is minimised.

C.3 ASSISTANCE TO THE DATA CONTROLLER

The data processor shall, to the extent possible – within the scope and extent below – assist the data controller in accordance with Provisions 8.1 and 8.2 by implementing the following technical and organisational measures:

The data processor shall develop necessary technical information which can be disclosed for use in the data controller's risk analysis.

The data processor's other obligations are determined in the cooperation agreement between the data processor and the data controller under the following delivery parameters:

- The data processor must initiate assistance no later than 3 working days after the data controller's request.
- If the request is made on the basis of an urgent situation, the data controller can ask the data processor to start the assistance no later than on the same working day as the request is submitted.
- If emergency assistance entails a cost for the data processor, and the emergency assistance is not the result of errors or defects or inappropriate or opaque workflows or processes in the product which mean that the data processor is unable to live up to their responsibility towards the data controller, the data controller must reimburse documentable costs and losses. If the data processor wishes to enforce this clause, the data processor must assert this to the data controller before the assistance begins.

C.4 RETENTION PERIOD/DELETION ROUTINE

Personal information is stored as long as the relationship between the parties exists, after which it is deleted by the data processor.

Upon termination of the Agreement regarding the processing of personal data, the data processor must return and delete the personal data in accordance with Provision 10.1, unless – after signing these provisions – the data controller has changed their original decision. Such changes must be documented and stored in writing, including electronically, in conjunction with the Provisions.

C.5 LOCATION OF PROCESSING

Without the prior written consent of the data controller, the processing of the personal data covered by the Provisions may not take place at locations other than the following:

- **Whistleblower Partners ApS,** Kultorvet 11, 4th floor, DK-1175 Copenhagen, Denmark.
- **Unica Net ApS**, Agenavej 35, DK-2670 Greve, Denmark.
- **Microsoft Ireland Operations Ltd**, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18 D18 P521, Ireland.

C.6 INSTRUCTIONS REGARDING THE TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES

The data processor is not permitted to transfer personal data about EU citizens, customers, employees, applicants, guests or other categories of data subjects to locations in third countries without the express written consent of the data controller.

If the data controller does not in these Regulations, or subsequently, provide documented instructions regarding the transfer of personal data to a third country, the data processor is not entitled to make such transfers within the framework of these Regulations.

Support for Microsoft Azure Cloud is provided directly to Microsoft Ireland Operations from:

- **Microsoft**,
  One Microsoft Way,
  Redmond, Seattle,
  Washington State,
  USA.

Details of the service delivery and support provided by data processors in third countries can be found at: https://azure.microsoft.com/da-dk/support/legal

C.7 PROCEDURES FOR THE DATA CONTROLLER'S AUDITS, INCLUDING INSPECTIONS, WITH THE PROCESSING OF PERSONAL DATA PROVIDED TO THE DATA PROCESSOR

The data controller's supervisory activities are carried out as an integral part of the ongoing status meetings between the Parties, cf. the model for cooperation set out in the main agreement between the Parties. At status meetings, security issues and data processing issues are discussed on the basis of the Parties' mutual assessment of the threat picture, updated assessments of critical vulnerabilities, identified security breaches and the like which affect the overall security of the processing activities regulated by the agreement.

IN THE EVENT OF A HIGH RISK LEVEL, THE FOLLOWING IS OBTAINED ON AN ANNUAL BASIS:	IF THE RISK LEVEL IS NOT HIGH, THE FOLLOWING IS OBTAINED ON AN ANNUAL BASIS:
✓ ISAE-3000 period statement,	× ISAE-3000 period statement,
× ISAE-3402 period statement,	× ISAE-3000 report,
× SOC 3 report,	× ISAE-3402 period statement,
× Similar audit material, defined below:	× SOC report,
	× Similar audit material, defined below:

✓ The data processor completes the security questionnaire from the data controller and reports the result and method to the data controller.	× The data processor completes the security questionnaire from the data controller. The data processor reports the result and method to the data controller.
✓ Physical inspection of the data processor with associated inspection report.	× Physical inspection of the data processor with associated inspection report.

Whistleblower Partners ApS
CVR-nr 43615661
Kultorvet 11 4,
1175 Copenhagen,
Denmark

The parties' shared assessment is that there is a high level of risk for data subjects, and it is stipulated that at least once a year, at no additional cost to the data controller, the data processor shall produce and submit an ISAE 3000 period report to the data controller as documentation of the data processor's compliance with the data processing agreement. This implies that the data controller is given the opportunity to carry out inspections at data processing locations, just as the data processor can be required to complete a security questionnaire on an annual basis describing the data processor's security measures and behaviour.

Without undue delay, documentation is forwarded to the data controller for informational purposes, with the understanding that the data controller may share the content with the Customer. The data controller can challenge the framework for and/or the audit method, and may in such cases request that new documentation is produced under a different framework and/or using a different method.

Based on the result, the data controller is entitled to request the implementation of additional measures to ensure compliance with the Data Protection Regulation, data protection provisions of other Union law or the national law of the Member States and these Regulations.

In addition, the data controller or a representative of the data controller has access to carry out inspections, including physical inspections, of the sites from which the data processor processes personal data, including physical sites and systems used for or in connection with the processing. Such inspections may be carried out when the data controller deems it necessary.