WhistleB

WHISTLEBLOWING CENTRE

ONLINE SERVICE AGREEMENT FOR WHISTLEB SERVICE

This Service Agreement ("**Service Agreement**") is entered into between **WhistleB Whistleblowing Centre AB**, Reg. No. 556873-2753, a limited liability company incorporated under the laws of Sweden ("**WhistleB**", or "**Processor**"), and entity that subscribed to the WhistleB Service ("**Customer**" or "**Controller**"). WhistleB and the Customer are hereinafter referred to separately as "**Party**" or jointly as "**Parties**".

1. The Service

Subject to a duly paid license, the Customer have access to the WhistleB web-based whistleblowing service ("**Service**"), including the WhistleB Communication channel ("**Communication channel**") and the WhistleB Case management tool ("**Case management tool**"). Any future release, feature or update of the Service is covered by this Service Agreement.

2. Service accounts

2.1 Service account creation. In order to use the Service, the Customer applies for a Service account and provides information required for the account registration. The Customer represents and warrants that: (a) All required registration information the Customer submits is truthful and accurate, and (b) The Customer will maintain the accuracy of such information. The Customer acknowledges that WhistleB is not able to provide the Customer with the Service if the Customer does not comply with these provisions.

2.2 Service account responsibilities. The Customer is responsible for maintaining the confidentiality of its account login information and for all activities that occur in the Customer's account. WhistleB cannot and will not be liable for any loss or damage arising from the Customer's failure to comply with these requirements. Either Party agrees to notify the other Party immediately of any identified unauthorised use, or suspected unauthorised use, of the Customer's account or any other breach of security.

3. Access to the Service

3.1 License. Subject to due payment of a license fee for the subscription to the Service as agreed between the Parties and as invoiced by WhistleB ("**License Fee**"), WhistleB grants the Customer a non-transferable, non-exclusive, revocable, limited license to use and access the Service. The Customer is entitled to use the Service solely and in accordance with the subscribed functionalities of the service during the period which the License Fee has been paid for.

3.2 Restrictions. The rights granted to the Customer in this Service Agreement are subject to the following restrictions: (a) The Customer shall not license, sell, rent, lease, transfer, assign, distribute, host, or otherwise commercially exploit the Service, whether in whole or in part, nor any content included in the Service Agreement; (b) The Customer shall not copy, modify, make derivative works of, disassemble or reverse, engineer any part of the Service; and (c) The Customer shall not access the Service in order to build a similar or competitive Service.

3.3 Modification and discontinuation. The Service is being developed continuously. WhistleB reserves the right to modify the Service, where such modification does not notably and negatively affects the Customer's user experience with the Service. WhistleB will notify the Customer by available means on modifications of the Service that are likely to notably and negatively affect the Customer's user experience with the Service. The Customer is responsible for keeping WhistleB informed on the Customer's correct contact details. If the Customer doesn't accept the modifications, the Customer has the right to terminate the license and this Service Agreement with no liability and with immediate effect within thirty (30) days of WhistleB's notification of modifications. The remaining license subscription period will not be reimbursed, nor in whole nor in part. Continued use of the Service during a period of 30 days following notification implies the Customer's acknowledgement of such modification and agreement to be bound by the terms and conditions of such modifications.

3.4 Ownership. Excluding any Customer Data, the Customer acknowledges that all the intellectual property rights, including copyrights, patents, trademarks and trade secrets, included in the Service, the WhistleB web site and its content, are owned by WhistleB or WhistleB's suppliers. Neither this Service Agreement nor the Customer's use of the Service transfers to the Customer or any third party any rights, title or interest in, or to, such intellectual property rights, except for the limited access rights expressly set forth in section "The Service".

4. Customer Data. Customer Data means any and all information available in the Communication channel or in the Case management tool ("**Customer Data**"). Customer is solely responsible for the Customer Data. The Customer assumes all risks associated with use of the Customer Data, including any reliance on its accuracy, completeness or usefulness, or any disclosure. The Customer is responsible for secure password management, the Customer's backup encryption file, its use and secure storage. The so-called "secondary password" is set up by the Customer upon the Service launch and used to decrypt received reports. If the secondary password is lost, the Customer can restore and access the Customer Data with the backup encryption file. A lost secondary password in combination with a lost backup encryption file means that the Customer Data cannot be accessed. WhistleB cannot be held liable for any loss of Customer Data connected to the loss by the Customer of secondary password or of the backup encryption file.

5. Acceptable use policy. The following terms constitute WhistleB's Acceptable use policy ("**Acceptable use policy**"). The Customer agrees not to intentionally: (i) upload, transmit, or distribute to or through the Service, any computer viruses, worms, or any software intended to damage or alter a computer system or data; (ii) interfere with, disrupt, or create an undue burden on servers or networks connected to the Service; or (iii) attempt to gain unauthorised access to the Service (or to other computer systems or networks connected to, or used together with, the Service), whether through password mining or any other means.

6. Service levels and support. WhistleB ensures availability of the Service 24 hours a day, every day of the year. If the availability per calendar month is below 99 % the Customer has the right to extend the license period, free of charge, by ten (10) times the amount of time the Service was not available. WhistleB reserves the right to temporarily suspend the Service for maintenance reasons, with a maximum of one (1) hour per month. Within this time frame, maintenance time is not calculated as downtime. Support can be reached via e-mail: support@whistleb.com. The support service is open on weekdays, excluding public holidays in Sweden, between 9am and 5pm (CET).

7. Remuneration. The annual License Fee for the Service is invoiced annually and in advance. The invoice shall be paid no later than the date specified in the invoice. In the event of late payment, WhistleB has the right to charge statutory payment reminder fees and penalty interest according to applicable local laws and regulations or suspend the service. Additional services, whenever required, not included in the annual License Fee, will be charged at the applicable current rate.

8. Disclaimers. WhistleB provides the Service in accordance with its description and with the limitations described in the section "The Service" of this Service Agreement. WhistleB does not provide legal advice. Information provided by WhistleB, such as recommendations, shall not be considered as legal advice. WhistleB is not responsible for the Customer's use of the Service in compliance with applicable laws and regulations.

9. Liability. To the maximum extent permitted by law, WhistleB is not liable to the Customer or any third party for any lost profits, costs of procurement of substitute products, or any indirect damages arising from, or relating to, this Service Agreement or the Customer's use of, or inability to use the Service. Access to, and use of, the Service and the WhistleB web site is at the Customer's own discretion. To the maximum extent permitted by law, and subject to the final paragraph in this section, WhistleB's liability to the Customer for any damages arising from, or related to, this Service Agreement, will at all times be limited to an amount equivalent to the yearly License Fee under this Service Agreement. The existence of more than one claim will not extend this limit. The above stated limited liability shall not apply should damage have been caused intentionally or by gross negligence.

10. Force majeure. Neither Party shall be responsible for failure or delay of performance if caused by: an act of war, sabotage, pandemic, electrical, internet, or telecommunication outage that is not caused by the obligated Party, government restrictions, official decisions or other event outside the reasonable control of the obligated Party. The Parties will use reasonable efforts to mitigate the effect of a force majeure event. If such event continues for more than 30 days, either Party may cancel unperformed Service upon written notice. This provision does not excuse either Party's obligation to take reasonable steps to follow its normal disaster recovery procedures nor the Customer's obligation to pay for the Service.

11. Terms and termination. The term of the Service Agreement is twelve (12) months. After a twelve (12) months term the Service Agreement will upon

payment of the License Fee continue in full force and effect for a commencing twelve (12) months term. Each Party has the right to terminate this Service Agreement with immediate effect if (i) the other Party is guilty of a material breach of its undertakings according to this Service Agreement, and does not take action to rectify such breach no later than within thirty (30) days of a written request to do so; (ii) the other Party is declared bankrupt, suspends its payments, initiates composition proceedings, goes into liquidation or can otherwise be assumed to be insolvent; or (iii) termination is instructed by an authority or legislation.

12. Consequences of termination. WhistleB offers, upon request of the Customer, to transfer encrypted Customer Data. Any requests for WhistleB's additional assistance, or requests for specific data formats, in exporting Customer Data will be subject to WhistleB's applicable current hourly rate fee. Obligations which, by their nature, are intended to continue after termination of this Service Agreement will continue to apply after termination of this Service Agreement.

13. General

13.1 Entire Service Agreement. This Service Agreement constitutes the entire agreement between the Customer and WhistleB regarding the use of the Service.

13.2 Waiver. Parties' failure to exercise or enforce any right or remedy under this Service Agreement shall not operate as a waiver of such right or remedy, nor shall it prevent any future exercise or enforcement of such right or remedy. No, or partial, exercise of a right or remedy shall preclude or restrict the further exercise of any such right or remedy or other rights or remedies.

13.3 Severability. If any part of this Service Agreement is declared unenforceable or invalid, the remaining parts of the Service Agreement will continue to be valid and enforceable.

13.4 Assignment. This Service Agreement, and Party's rights and obligations herein, may not be assigned, subcontracted, delegated, or otherwise transferred by a Party without the other Party's prior written consent. Such consent is not required for assignment within a Party's group of companies.

14. Governing law and dispute resolution. This Service Agreement, and any non-contractual obligations in connection therewith, shall be governed by the substantive laws of Sweden without regard to conflict of laws rules. Any dispute, controversy or claim arising from or regarding this Service Agreement, contractual as well as non-contractual, or the existence, breach, termination or invalidity thereof, shall be finally settled by arbitration administered by the Arbitration Institute of the Stockholm Chamber of Commerce. The language to be used in the arbitral proceedings shall be English.

15. Contact information. If the Customer wishes to contact WhistleB in writing, or if this Service Agreement requires the Customer to give notice to WhistleB in writing, please contact WhistleB at**:**

WhistleB Whistleblowing Centre AB
World Trade Centre, Klarabergsviadukten 70, Stockholm, Sweden 10724
legal@whistleb.com

ANNEX 1 Data Processing Agreement ("DPA")

This DPA sets out the terms and conditions with regard to the Processing of Personal data by WhistleB and/or WhistleB's Sub-Processors. Use of WhistleB's Service constitutes acceptance of these terms on behalf of the Controller. WhistleB processes Personal Data and is therefore considered a Processor within the meaning of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons ("**GDPR**"). The Controller may be considered a controller within the meaning of the GDPR.

1. DEFINITIONS.

Data Breach is a security breach within the meaning of article 4.12 of the GDPR.

Data Subject is the person to whom Personal Data refers to within the meaning of article 4.1 of the GDPR.

Personal Data are any data regarding an identified or identifiable natural person within the meaning of article 4.1 of the GDPR.

Processing means any operation or set of operations which is performed on personal data within the meaning of article 4.2 of the GDPR ("Process", "Processes" and "Processed" shall have the same meaning).

Special Categories of Personal Data are Personal Data within the meaning of Article 9.1 of the GDPR.

Sub-Processor is anyone who has been engaged by the Processor for the performance of specific Processing on behalf of the Controller and who Processes Personal Data as a sub-contractor and on behalf of the Controller.

User is an individual authorised by the Controller to use the Service in accordance with this Service Agreement, to access messages and manage them in the Case management tool, with defined User rights.

2. GENERAL. The Processor undertakes to Process Personal Data on the terms and conditions of this DPA in accordance with the documented instructions of the Controller, including with regard to transfers of personal data to a third country (i.e. a country outside the EU) or an international organisation. However, the Processor may Process Personal Data if required by union or member state law to which the Processor is subject to. In such case, the Processor shall inform the Controller of the legal requirement before the Processing, unless that law prohibits such information on important grounds of public interest. The Processor shall Process the Personal Data properly, with due care and in accordance with the GDPR and other applicable legislation and regulations relating to the Processing of Personal Data. The Processor carries out the Processing to the extent necessary to provide the Service to the Controller as described in the Service Agreement. The Processor shall not retain Personal Data shared with the Processor in the context of the Service Agreement any longer than is necessary (i) for the performance of this Service Agreement; or (ii) to comply with any of its statutory obligations. The Annex 1-A hereafter describes the applicable retention periods. The Processor is obligated to immediately inform the Controller regarding any changes in the performance of the Service Agreement, so that the Controller can monitor compliance through arrangements made with the Processor. This also includes the engagement of Sub-Processors, without prejudice to the provisions in section "Use of Sub-Processors" and section "Change".

3. USE OF SUB-PROCESSORS. The Controller grants general written permission to Processor to engage a Sub-Processor for the provision of the Service. The Processor shall not grant access to Personal Data to third parties, including Sub-Processors, if not strictly necessary to provide the Service. The Processor is responsible for ensuring compliance with Articles 28.2 and 28.4 GDPR when engaging Sub-Processors and ensuring that Sub-Processors provide sufficient guarantees to implement appropriate technical and organisational measures, in such a manner that the Processing meets the requirements of GDPR. When the Processor engages a Sub-Processor, the Processor enters into a written agreement with the relevant Sub-Processor, in which data processing obligations corresponding to what is set out in this DPA are imposed upon the Sub-Processor. If new Sub-Processors are engaged, the Processor will notify the Controller without delay. If the Controller disagrees with engagement of new Sub-Processors, the Controller may terminate the Service Agreement. The Processor will upon request export all Controller Data to the Controller free of charge. Requests for data export in other than standard data formats, will be subject to Processor's applicable hourly rate fee. If a Sub-Processor fails to fulfil its data protection obligations, the Processor remains liable to the Controller for the performance of the Sub-Processor's obligations.

4. SECURITY. The Processor shall implement appropriate technical and organisational measures to secure Personal Data against loss or any form of unlawful Processing. Taking into account the state of the art and the costs of their implementation, these measures guarantee an appropriate security level given the risks associated with Processing and the nature of the Personal Data to be protected. The measures are, in part, aimed at preventing unnecessary collection and further Processing. The Processor shall record the measures in writing and shall ensure that the security as referred to in this paragraph meets with the security requirements under the GDPR. Furthermore, the Processor shall take all other measures required pursuant to Article 32 GDPR. On request, the Processor shall provide the Controller with written information relating to (the organisation) of the security of Personal Data.

5. OBLIGATION TO REPORT DATA BREACHES AND SECURITY BREACHES. In the event of a suspected or actual (i) Data Breach; (ii) breach of security measures; (iii) breach of the confidentiality obligation or (iv) loss of confidential data, the Processor shall notify the Controller without undue delay, the Processor shall take all measures reasonably necessary to prevent or limit (further) unauthorised examination, change, and provision or otherwise unlawful Processing and to stop and prevent any future breach of security measures, breach of the confidentiality obligation or further loss of confidential data, without prejudice to any right the Controller might have to damages or other measures. This provision applies to incidents at the Processor and its Sub-Processors, if any. At the Controller's request, the Processor shall cooperate, in so far as possible, in informing the competent authorities and Data subject(s). The Processor shall make written arrangements with Sub-Processors about the reporting of incidents to the Processor, which will enable the Processor and the Controller to comply with obligations in the event of an incident. These arrangements must in any event include the obligation that the Sub-Processors shall notify the Processor without undue delay after the first discovery of an incident, and at the Controller's request shall cooperate, in so far as possible, in informing the competent authorities and the Data Subject(s). The Processor shall ensure that all of the Processor's employees that has access to the Personal Data shall meet the Processor's obligations.

6. AUDIT. The Processor shall make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 GDPR. The Processor is responsible for and bears the costs of yearly penetration testing and information security audits. If the Controller requests additional audits to be carried out by an independent auditor or expert mandated by the Controller, the Controller shall bear the costs of this audit. Upon request, the Processor is obliged to make the findings of the IT auditor or expert available to the Controller in the form of a third-party memorandum. If it is established during an audit that the Processor has failed to comply with the provisions of the Service Agreement and the DPA, the Processor shall take all reasonably necessary measures to ensure compliance.

7. INTERNATIONAL TRANSFER. Should transfers of Controllers Personal Data under this DPA be made from the European Union, the European Economic Area and/or their member states, Switzerland and the United Kingdom to countries which do not ensure an adequate level of data protection within the meaning of data protection laws of the foregoing territories, the Parties shall together take the required measures to ensure that the transfer is made in accordance with data protection laws.

8. INVESTIGATION REQUESTS. If the Processor receives a request or order from a supervisory authority, government agency or investigation, prosecution or national security agency to provide (access to) Personal Data, the Processor shall immediately notify the Controller. When handling the request or order, the Processor shall observe all of the Controller's instructions and provide all reasonably required cooperation to the Controller. If the request or order prohibits the Processor from complying with its obligations on the basis of the above, the Processor shall promote the Controller's reasonable interests.

9. RIGHTS OF DATA SUBJECTS. The Processor shall promptly notify the Controller if the Processor receives a request from a Data Subject to exercise the Data Subject's right of access, right to rectification, restriction of Processing, erasure ("right to be forgotten"), data portability, object to the Processing, or Data Subject's right not to be subject to an automated individual decision

making ("**Data Subject Request**"). Taking into account the nature of the Processing, the Processor shall assist the Controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Controller's obligation to respond to a Data Subject Request under applicable data protection laws. The Processor shall also assist the Controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 GDPR taking into account the nature of Processing and the information available to the Processor. If a Data Subject, in relation to the execution of its rights under the GDPR, directly requests the Processor to correct, delete or block Personal Data, Processor shall refer such Data Subject to the Controller. The costs for assistance under this section shall be calculated and allocated in accordance with section "Remuneration".

10. NATURE AND PURPOSE OF PROCESSING

(i) General nature and purpose of the Processing. The nature and purpose of the Processing is to deliver whistleblowing functions for the Controller. Processor does not own Controller data. Processor handles encrypted Controller data on behalf of the Controller and for purposes decided by the Controller. The Controller data is Processed and collected by the Controller for its own purposes. **(ii) The Categories of Data Subjects.** The categories of Data Subjects concerned comprise all persons who have access to the Communication channel. **(iii) Categories of Personal Data.** The following categories of Personal Data are concerned by the Processing: contact data of Users of the WhistleB whistleblowing system, the accused individuals and the authorized users – name, function, address, email, phone number; facts of the alert, investigation results and reports; follow-up measures for the confirmed misdeeds; encrypted whistleblower reports (Controller Data), **(iv) Transfers of Personal Data.** Personal Data is processed in line with the GDPR. **(v) Use of Sub-Processors:** Please see Article 3 of this DPA.

11. INDEMNIFICATION AND LIMITED LIABILITY. Processor shall indemnify and keep indemnified Controller against direct damages, claims, and losses incurred by the Controller which arise directly from the Processor's Processing activities under this DPA. The limitations of liability agreed between the Parties in the Service Agreement apply equally to this DPA. The existence of more than one claim will not extend such limitation.

12. CHANGE. If a change in the Personal Data to be Processed or a risk analysis of the Processing of Personal Data gives reason to do so, upon the Controller's first request the Parties shall consult on amending the arrangements made in the DPA. The arrangements to be newly made must be recorded in writing and form part of the DPA prior to their application. The changes must not result in the Controller becoming non-compliant with GDPR and other relevant laws and regulations relating to Personal data. If the data protection rules change during the term of this DPA, or if the Supervisory Authority issues guidelines, decisions or regulations concerning the application of the data protection rules resulting in this DPA no longer meeting the requirements for a DPA, this DPA may be amended to meet such new or additional requirements. The Controller grants to the Processor to make such amendments by this general written permission.

13. TERMS AND TERMINATION. The terms of the DPA are equal to the terms of the Service Agreement. The DPA cannot be terminated separately from the Service Agreement. Upon termination of the Service Agreement and prior to deletion, the Processor will transfer to the Controller all required Controller data it has access to in a readable manner and common format, in order for the Controller to be able to continue using the Controller Data in other contexts. Unless there is a statutory obligation to store Personal Data, the Processor (and any Sub-Processor) shall delete or destroy in a secure and definite manner all Personal Data (including back-up copies) without undue delay after termination or expiry of the Service Agreement and following delivery of the Personal Data.

14. CONFIDENTIALITY

The Parties shall keep confidential all Personal Data and other data or information, the confidential nature of which they are aware of or can reasonably suspect, and that have come to their attention or to which they obtained access in the context of the performance of the Service Agreement or the DPA, and shall refrain from disclosing these internally or externally and/or providing these to third parties, except in so far as:

1. Disclosure and/or provision of said Personal Data and other data or information is necessary in the context of the performance of the Service Agreement or the DPA;
2. Any mandatory statutory provision or court decision requires the Parties to disclose and/or provide said (Personal) data or other information, in which case the Parties shall first notify the other Party;
3. Disclosure and/or provision of said Personal Data and other data or information takes place with the prior written consent of the other Party; or
4. It concerns information that has already been legitimately disclosed in a manner other than through the acts or omissions of one of the Parties.

The Parties shall contractually require the persons working for them (including employees) who are involved in the Processing of confidential Personal Data and other data or information to keep said information confidential.

Upon a Party's request, the Parties shall cooperate in the exercise of supervision by or on behalf of the other Party on the safekeeping and use of confidential Personal Data and other data or information.

Upon the Controller's first request, the Processor shall provide the Controller with all Personal Data and other data or information the Processor holds in the context of the performance of the Service Agreement, including any copies.

The Processor shall ensure that persons authorized to Process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

This confidentiality obligation shall remain in force after the termination of this DPA for a period of two years.

15. GOVERNING LAW AND DISPUTES

The DPA and its performance are subject to the relevant provisions on governing law and dispute resolution of the Service Agreement.

16. CONTACT INFORMATION

If the Controller wishes to contact the Processor, or if this DPA requires the Controller to give notice to the Processor in writing, please contact the Processor at: WhistleB Whistleblowing Centre AB, PO Box 70396, 107 24 Stockholm, Sweden E-mail: legal@whistleb.com

ANNEX 1-A Data processing details

Categories of Data subjects: Data subjects comprise of all persons given access to the Communication channel by the Controller.

Categories of Personal Data to be processed: The data is encrypted when stored in the Service and only available to the Controller. WhistleB is not able to decrypt and read communication through the WhistleB-system, if not authorised by the Controller.

Retention periods: When a whistleblower's report is closed, the Controller data is permanently deleted after 30 days from scheduling for deletion or archiving – and cannot be restored. Personal Data such as User name is deleted when an account is deleted.

Security measures taken: WhistleB ensures the security of Personal Data and whistleblower's anonymity. WhistleB has no access to a whistleblower's report data with regard to contents, as WhistleB will at no time have access to any encrypted data of the Controller without his written consent.

Back up routines: The Service is delivered to the Controller through Microsoft Azure data centres, each designed to run 24/7/365, and each employing various measures to protect operations from power failure, physical intrusion, and network outages. Personal Data is kept secure through encrypted communications as well as threat management and mitigation practices, including regular penetration testing. Database and blob storage (used for logs, backups and report attachments) are replicated with failover nodes, storing three copies within Microsoft Azure's primary data centre.

System operations: The availability, performance and security of the Service is monitored 24/7/365, and alerts are sent to the support manager and the WhistleB management team. Administrative access to the Service uses multi-factor authentication. For information on access, control and deletion of Personal data, please visit the online WhistleB Trust Centre (https://whistleb.com/trust-centre/), also for further information on data privacy and security.

Sub-Processors: The Processor has the Controller's permission to engage the following Sub-Processors in the performance of the Service:

TrueSec AB (Sweden), Microsoft Ireland Operations (Ireland), Lingo24 (France).