ONLINE MASTER SERVICES AGREEMENT

This Online Master Services Agreement ("**MSA**") is entered into as of the Effective Date (as defined in Section 1.1.) by and between **WhistleB Whistleblowing Centre AB**, Reg. No. 556873-2753, a limited liability company incorporated under the laws of Sweden ("**WhistleB**"), and the organisation as identified during the application process through WhistleB's website ("**Customer**"). In consideration of the mutual covenants and conditions contained in this MSA the parties agree as follows:

1.0 Purpose and Scope.

1.1. Account Creation; Effective Date. WhistleB provides organisations with the ability to apply for a service account online through WhistleB's website. In order to apply for an account, Customer must complete all application steps through WhistleB's website, including providing all required information. Customer represents and warrants that: (i) all required application information Customer submits is truthful and accurate; and (ii) Customer will maintain the accuracy of such information. Customer understands and acknowledges that submission of an application through WhistleB's website constitutes a binding offer to purchase the Services selected by Customer during the online application process, subject to WhistleB's acceptance of such offer. WhistleB will review all applications and notify Customer via email whether the application has been accepted. For avoidance of doubt, no contractual relationship shall be formed between the parties unless and until WhistleB notifies Customer in writing (which may be provided via email) that WhistleB has accepted Customer's application. This MSA shall be effective as of the date WhistleB notifies Customer in writing that WhistleB has accepted Customer's application ("**Effective Date**").

1.2. Master Services Agreement. This MSA establishes the general terms and conditions with respect to WhistleB's provision of Services to Customer. "**Service**" or "**Services**" means, collectively, the SaaS Offering (as defined in Section 2.1) and any other services provided to Customer by WhistleB. This MSA and all documents incorporated into the MSA by reference are, collectively, the "**Agreement**."

1.3. Online Applications; Order Forms and Change Orders. The initial Services to be provided are the Services selected by Customer during the online application process. The applicable Service-specific terms and conditions are set out in Exhibit B. Additional Services may be added pursuant to the execution of a separate ordering document that will be presented to Customer outside of the WhistleB website ("**Order Form**"). Certain additional Services which are not recurring and for which only one-time fees apply may be added pursuant to a simplified ordering document ("Change Order"). As used herein, the term "Order Form" includes Change Order. Customer's execution of an Order Form constitutes a binding commitment to purchase the Services specified in the applicable Order Form.

1.4. Affiliates. **"Affiliate**" means an entity controlling, controlled by, or under common control with a party to this MSA. Customer may authorize its Affiliates' use of the Services provided that (i) the combined use of the Services by Customer and its Affiliates shall not exceed the applicable Subscription Metrics (as defined in Section 2.1); (ii) Customer guarantees any such Affiliate's compliance with the applicable terms and obligations of the Agreement; and (iii) Customer shall be responsible for all use of and access to the Services by such Affiliates.

1.5. Order of Precedence. To the extent any terms and conditions of this MSA conflict with the terms and conditions of an Order Form, the terms and conditions of the Order Form shall control.

1.6. Applicable Law. "**Applicable Law**" means any law, rule, or regulation applicable to a party.

2.0 Services.

2.1. Grant of Use. During the applicable Services Term (as defined in Section 6.2), and subject to Customer's compliance with the Agreement, WhistleB grants Customer a non-transferable, non-assignable, worldwide right to access and use the proprietary software-as-a-service offering selected by Customer during the online application process and, if applicable, any subsequent Order Form, that WhistleB makes available to Customer online via a Uniform Resource Locator (URL) ("**SaaS Offering**") for Customer's internal use for purposes of managing and coordinating information. Customer's use is restricted to the applicable limitations designated and/or defined during the online application process and, if applicable, any subsequent Order Form ("**Subscription Metrics**").

2.2. Online Access; Environment; Hosting Infrastructure. WhistleB will provide Customer online access to and use of the SaaS Offering in accordance with the Services selected by Customer during the online application process, the terms set forth in Exhibit B and, if applicable, any subsequent Order Form, as well as the user instructions, release notes, manuals, and online help files that describe the operation of the Services in the form generally made available to WhistleB customers, as may be updated from time to time (collectively, the "**Technical Documentation**"). Customer will access the SaaS Offering by use of a supported Customer-provided browser. WhistleB is responsible for the hosting and management of the SaaS Offering, including obtaining and maintaining all computer hardware, software, communications systems, network, and other infrastructure necessary to permit Customer to access and use the SaaS Offering ("**Hosting Infrastructure**"), either directly or through its designated third-party supplier or data center. WhistleB will manage and install within the Hosting Infrastructure all updates and upgrades that WhistleB makes generally available to its customers for the SaaS Offering. Customer is solely responsible for obtaining and maintaining, at its own expense, all equipment and technology needed to access the SaaS Offering, including, without limitation, internet access and adequate bandwidth.

2.3. Service Levels. WhistleB shall ensure availability of the SaaS Offering of ≥ 99.5% of scheduled availability. WhistleB shall take an accounting of the availability of the SaaS Offering on a quarterly basis, measured each calendar quarter across all WhistleB customers.

2.4. Updates. Access is limited to the version of the Services in WhistleB's production environment. WhistleB regularly updates the Services and reserves the right to make updates to the Services in the event of Service unavailability, end of life, or changes to software requirements, provided that any such modification shall not result in a material reduction in the functionality of the Services.

2.5. Acceptable Use. Customer acknowledges and agrees that WhistleB does not monitor or evaluate Customer Data transmitted through the Services and WhistleB shall not be responsible for the content of any Customer Data. Customer shall use the Services exclusively for authorized and

legal purposes and consistently with Applicable Law. Customer is solely responsible and liable for ensuring the appropriate use of any reports and other materials prepared by WhistleB in a manner that will not violate Applicable Law or infringe upon the rights of any third party.

2.6. Security. WhistleB will implement commercially reasonable and appropriate measures designed to secure Customer Data against accidental or unlawful loss, access, or disclosure. WhistleB will be responsible for ensuring the security and confidentiality of account names and passwords residing within its systems and while being received and processed by the SaaS Offering for the purpose of permitting access thereto. Customer is responsible for instructing any individual who Customer authorizes to use the Services ("**Licensed User**") to keep their respective account names and passwords strictly confidential. Customer agrees to promptly notify WhistleB if account names or passwords are lost, stolen, or otherwise compromised. Customer will not (i) breach or attempt to breach the security of the Services or of any network, servers, data, computers, or other hardware relating to or used in connection with the SaaS Offering, or of any third party that is hosting or interfacing with any part of the SaaS Offering; or (ii) use or distribute through the SaaS Offering any software, files, or other tools or devices designed to interfere with or compromise the privacy, security, or use of the SaaS Offering or the operations or assets of any other customer of WhistleB or any third party. Customer will comply with the user authentication requirements for use of the SaaS Offering. Customer is solely responsible for monitoring the administration of access to and use of the SaaS Offering by its Licensed Users. A failure by a Licensed User to comply with a material term of the Agreement shall be deemed to be a material breach by Customer and WhistleB shall not be liable for any damages that Customer or any third party incurs resulting from such breach. Customer must immediately take all necessary steps, including providing Notice (as defined in Section 12.4) to WhistleB, to effect the termination of an access identification for any Licensed User if there is any compromise in the security of that access identification or if unauthorized use of such access identification is suspected or has occurred.

2.7. Support. WhistleB will provide Customer the self-help support resources WhistleB generally makes available to its customers as well as support with regard to Errors (as defined in Section 7.2). Requests for additional support may result in additional fees. WhistleB is not under any obligation to provide support with respect to (i) SaaS Offering(s) that have been altered or modified by anyone other than WhistleB or its licensors; (ii) SaaS Offering(s) used other than in accordance with the Technical Documentation and the Agreement; or (iii) errors and/or malfunctions caused by any systems or programs not supplied by WhistleB.

3.0 Proprietary Rights.

3.1. Ownership. Each party shall retain all right, title, and interest in any copyrights, trademarks, patent rights, and other intellectual property or proprietary rights it has acquired or developed prior to or outside the scope of the Agreement. Customer shall retain all right, title, and interest, including copyrights, trademarks and patent rights, in any and all Customer content provided under the Agreement and any and all derivative works thereof (collectively, "**Customer Intellectual Property**"). Any data collected, received, or processed by WhistleB as required by the Services, including Personal Data (as defined in Exhibit A) but excluding Use Data (as defined in Section 3.4) (collectively, "**Customer Data**"), will remain the exclusive property of Customer. WhistleB shall own and retain all right, title, and interest, including copyrights, trademarks, and patent rights in any and all Services provided under the Agreement and any and all derivative works thereof (collectively, "**WhistleB Intellectual Property**"). Neither party will acquire any right, title, or interest in the intellectual property rights of the other party by virtue of its performance under the Agreement. All rights not expressly granted are reserved exclusively by the respective owner; there are no implied rights.

3.2. License Rights.

(i) WhistleB grants Customer, for the Term, a limited, non-exclusive, worldwide, non-transferable, royalty-free license to reproduce, transmit, perform, copy, display, distribute, and otherwise use any and all WhistleB Intellectual Property for the sole and limited purpose of furthering Customer's business operations that use WhistleB Intellectual Property per the terms of this Agreement. Customer agrees that any use of WhistleB's trademarks or service marks will inure solely to the benefit of WhistleB and that Customer will not at any time acquire any rights in WhistleB's trademarks or service marks. Customer shall not take any action that jeopardizes WhistleB's rights in any WhistleB Intellectual Property. Customer may not obscure, alter, add, or remove any copyright, patent, trademark, service mark, or proprietary rights notices on any WhistleB materials.

(ii) Customer grants WhistleB, for the Term, a limited, non-exclusive, worldwide, non-transferable, royalty-free license to reproduce, transmit, perform, copy, display, distribute, create derivative works for the sole purpose of formatting, and otherwise use any Customer Intellectual Property for the sole and limited purpose of delivering the Services to Customer per the terms of this Agreement. WhistleB agrees that any use of any of Customer's trademarks or service marks will inure solely to the benefit of Customer and that WhistleB will not at any time acquire any rights in Customer's trademarks or service marks. WhistleB shall not take any action that jeopardizes any of Customer's rights in any Customer Intellectual Property. WhistleB may not obscure, alter, or remove any copyright, patent, trademark, service mark, or proprietary rights notices on any Customer materials.

3.3. Restrictions. Customer shall not: (i) except as authorized in a separate agreement between WhistleB and customer, sell, resell, distribute, host, lease, rent, license, or sublicense the Services or any portion thereof, including, without limitation, to provide processing services to third parties, or otherwise use the Services on a service bureau basis; (ii) reverse engineer or otherwise attempt to discover the source code of or trade secrets embodied in the Services or any portion thereof; (iii) write or develop any derivative works based upon the Services; (iv) modify, adapt, tamper with, or otherwise make any changes to the Services or any part thereof; (v) use the Services in a manner not authorized under the Technical Documentation or the Agreement, or in violation of Applicable Law; or (vi) use the Services, or permit them to be used, for purposes of evaluation, benchmarking, or other comparative analysis intended for external publication without WhistleB's prior written consent, which shall not be unreasonably withheld. Despite the foregoing subsection (vi), pursuant to Applicable Law, Customer may use WhistleB's name in internal or regulatory communications pertaining to Customer's agreement to use WhistleB's Services.

3.4. Data Aggregation and Use Data. Customer authorizes WhistleB, as part of the Services, to access and compile certain Customer Data (excluding Personal Data), for the purpose of analysis and reporting on the effectiveness and trends in corporate ethics and compliance programs. The Customer Data that WhistleB accesses and compiles shall be aggregated with other similar data across all WhistleB customers according to industry, company size, country, geographic region, or other relevant classification and shall not be used in any manner that would identify Customer.

Customer understands that WhistleB employs certain third-party software within its Services to enable WhistleB to better understand Licensed User behavior and provide Licensed Users with improved functionality and other relevant enhancements to the software application(s). The data gathered from such use ("**Use Data**") shall not contain Personal Data, but may include information such as browser type, pages visited, features used, and operating system version.

4.0 Processing of Personal Data. Customer acknowledges and agrees that WhistleB will collect, process, use, and/or store certain Personal Data in delivering the Services as detailed in Data Processing Addendum, attached hereto as Exhibit A.

5.0 Fees and Payment.

5.1. Fees. Fees are set forth during the online application process and, if applicable, any subsequent Order Form, and are based on the applicable Subscription Metrics. Except as otherwise specified herein, fees are not refundable or cancellable. WhistleB shall send all invoices and fee increase notices via email to the Customer email address provided by Customer during the online application process, unless otherwise specified herein or updated in accordance with Section 12.4.

5.2. Payment. Unless otherwise agreed to in writing by the parties, Customer will pay all undisputed fees due within thirty (30) calendar days following the invoice date. Customer shall send payment to the address included on the invoice, and such payments shall be made in the currency specified during the online application process and, if applicable, any subsequent Order Form. Interest accrues on past due balances until paid at the lesser of (i) one and one-half percent (1.5%) per month; and (ii) the highest rate allowed by law. Customer shall reimburse WhistleB for expenses incurred, including interest, court costs, and reasonable attorneys' fees, in collecting amounts due to WhistleB hereunder that are not under good faith dispute by Customer.

5.3. Taxes. All fees for the Services exclude any direct or indirect taxes, levies, duties, or similar governmental assessments, including without limitation, any sales, use, value-added, withholding, or similar taxes ("**Taxes**"). Customer is responsible for paying all Taxes associated with Customer's purchases hereunder directly to the taxing authority. As an exception to the foregoing, if WhistleB has the legal obligation to pay or collect Taxes for which Customer is responsible under this paragraph, the appropriate amount shall be invoiced to and paid by Customer to WhistleB, unless Customer provides WhistleB with a valid tax exemption certificate authorized by the appropriate taxing authority. WhistleB is solely responsible for taxes based upon WhistleB's net income, assets, payroll, property, and employees.

5.4. Subscription Metrics. At all times during the Services Term, Customer shall be responsible for ensuring sufficient Subscription Metrics to accommodate one hundred percent (100%) of its usage of the Services. If Customer's usage of the Services exceeds the current Subscription Metrics, Customer must promptly purchase additional Subscription Metrics or WhistleB may charge then-prevailing prices for the level of usage above Customer's current Subscription Metrics.

6.0 Term and Termination.

6.1. MSA Term. This MSA shall remain in effect until terminated as set forth herein ("**Term**").

6.2. Services Term. The initial term for each Service purchased, and any renewal rights or extensions, will be as set forth in the Exhibit B or, if applicable, any subsequent Order Form ("**Services Term**").

6.3. Suspension of Services for Non-Payment. If any fees which are not disputed by Customer in good faith are more than thirty (30) calendar days past due, WhistleB will have the right, in addition to all other rights and remedies available to it, to suspend delivery of or access to the Services.

6.4. Disputed Fees. Customer shall set forth in writing and in reasonable detail any amount(s) disputed in good faith and the basis or reason for the dispute. Upon receipt of a Notice of dispute, the parties will make reasonable, diligent, good faith efforts to quickly resolve the dispute, and WhistleB shall provide such information as Customer reasonably requests in order to audit or confirm the charges. Neither party shall be required to pay or refund, as applicable, any amounts disputed in good faith until such dispute is fully resolved. Once the dispute is fully resolved, the agreed-upon amounts shall be paid or refunded, as applicable, within ten (10) calendar days following such resolution.

6.5. Termination. The Agreement may be terminated (i) by either party if the other party materially breaches the Agreement and does not cure the breach within thirty (30) calendar days after receiving Notice thereof from the non-breaching party; (ii) as set forth in Section 7.5 (Infringement Remedies); (iii) as set forth in Section 12.6 (Compliance with Law); (iv) if the other party becomes insolvent (generally unable to pay its debts as they become due) or the subject of a bankruptcy, conservatorship, receivership, or similar proceeding, or makes a general assignment for the benefit of creditors; or (v) by WhistleB upon the expiration of ten (10) calendar days' Notice if any fees which are not disputed by Customer in good faith are more than thirty (30) calendar days past due.

6.6. Partial Termination. Where a party has rights to terminate the Agreement pursuant to Section 6.5 (Termination), such party may, at its discretion, either terminate the entire Agreement or the applicable Order Form(s). Order Forms that are not terminated shall continue in full force and effect under the terms of this MSA.

6.7. Effects of Termination or Partial Termination. Upon any termination, without prejudice to any other rights or remedies that the parties may have, all rights licensed and obligations required hereunder shall immediately cease, except as otherwise provided. Each party may retain, subject to this MSA, copies of Confidential Information required for internal record keeping purposes and for compliance with Applicable Law. If WhistleB terminates the Agreement or an Order Form per Section 6.5(v), Customer agrees that it shall remain responsible for all outstanding fees payable to WhistleB for the Services Term and WhistleB may declare all such fees immediately due and payable. Customer acknowledges that such amounts are liquidated damages reflecting a reasonable measure of actual damages and not a penalty.

7.0 Warranties and Disclaimers.

7.1. WhistleB Services Warranty. WhistleB warrants that: (i) the SaaS Offering, as updated in accordance with Section 2.4 and when used in accordance with the current Technical Documentation, will perform in all material respects as specified in such Technical Documentation during the

applicable Services Term; (ii) all Services will be performed in a professional manner, in accordance with industry standards; and (iii) WhistleB will not design its systems to include any "back door," "time bomb," "Trojan horse," "worm," "drop dead device," "virus," "preventative routines," or other similar computer software routines.

7.2. Breach of Services Warranty Remedies. In the event of any breach of Section 7.1, WhistleB shall diligently endeavor to remedy any material failures of a Service to conform to its functional specifications, as described in the Technical Documentation, that Customer reports to WhistleB and that WhistleB is able to replicate during the applicable Services Term ("**Errors**"). The foregoing shall be Customer's sole remedy, and shall be WhistleB's sole liability, for any uncured breach of Section 7.1. WhistleB shall not be obligated to correct Errors resulting from any (i) components or content that WhistleB does not provide; (ii) unauthorized use or use of the Services other than in accordance with the Technical Documentation and the Agreement; or (iii) viruses, malicious software, or other disruptive programs or applications that Customer, its agents, or its Licensed Users introduce into the Services or which are introduced into the Services as a result of Customer's use of the Services.

7.3. Customer Warranties. Customer represents and warrants that: (i) Customer and Licensed Users are authorized to provide all Customer Data and any other data and information submitted to the Services; (ii) Customer's and Licensed Users' use of the Services and provision of Customer Data will comply with Applicable Law; (iii) Customer Intellectual Property provided by Customer to WhistleB for use in performing WhistleB's obligations under this Agreement will not infringe the intellectual property or other proprietary rights of any third party; and (iv) Customer will not modify or create derivative works based on the SaaS Offering or any other Services, or attempt to decode, decipher, decompile, disassemble, or reverse engineer the SaaS Offering or any other Services or deliverables.

7.4. Mutual Warranties. Each party represents and warrants that: (i) the execution, delivery, and performance of this MSA has been and shall be duly authorized by the executing party; (ii) the executing party's performance of its obligations will not conflict with, result in a breach of, or constitute a default under any other agreement to which that party is bound; and (iii) the executing party is in material compliance with all Applicable Laws with regard to its obligations under the Agreement.

7.5. Infringement Remedies. If the SaaS Offering infringes, or if WhistleB believes that the SaaS Offering infringes, on the intellectual property or other proprietary rights of any third party, WhistleB may, in its sole discretion, (i) modify the SaaS Offering to be non-infringing, (ii) obtain for Customer a license to continue using the affected SaaS Offering, or (iii) if neither (i) nor (ii) are practical in WhistleB's sole judgment, terminate the affected SaaS Offering and return to Customer the unused portion of any fees paid for the affected SaaS Offering. Subject to the parties also meeting their express indemnification obligations under this MSA, WhistleB's satisfactory performance of any one or all of the remedies set forth in the preceding sentence shall be Customer's sole and exclusive remedy for WhistleB's breach of the infringement warranty or for any damages incurred from early termination due to a third-party infringement claim.

7.6. Disclaimer of Warranties. EXCEPT FOR THE WARRANTIES SET FORTH HEREIN AND THOSE EXPRESSLY SET FORTH IN AN ORDER FORM, ALL SERVICES ARE PROVIDED ON AN "AS IS," "AS AVAILABLE" BASIS, AND WHISTLEB DISCLAIMS, TO THE MAXIMUM EXTENT PERMITTED BY LAW, ALL OTHER WARRANTIES, WHETHER EXPRESS, IMPLIED, OR STATUTORY WITH RESPECT TO THE SERVICES, DELIVERABLES, MARKS, OR WHISTLEB'S PERFORMANCE UNDER THE AGREEMENT, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OF MERCHANTABILITY, ACCURACY, QUIET ENJOYMENT, TITLE, NON-INFRINGEMENT, OR FITNESS FOR A PARTICULAR PURPOSE, AND THOSE THAT ARISE FROM ANY COURSE OF DEALING OR COURSE OF PERFORMANCE. WHISTLEB EXPRESSLY DOES NOT WARRANT THAT CUSTOMER'S USE OF THE SERVICES WILL SATISFY THE SPECIFIC REQUIREMENTS OF ANY FEDERAL, PROVINCIAL, STATE, OR LOCAL LAWS, REGULATIONS, OR GUIDELINES.

7.7. Additional Disclaimers and Agreements.

(i) LEGAL SERVICES. WHISTLEB IS NOT ENGAGED IN THE PRACTICE OF LAW. IN THE PROVISION OF SERVICES, CERTAIN ISSUES MAY ARISE THAT ARE QUASI-LEGAL IN NATURE. ANY STATEMENTS OR ASSISTANCE WHISTLEB PROVIDES IN THESE MATTERS SHOULD BE INTERPRETED AS OPINIONS OR ADVICE CONCERNING BUSINESS ISSUES TO BE CONSIDERED IN CONNECTION WITH THE SERVICES. CUSTOMER REPRESENTS AND WARRANTS IT IS NOT RELYING UPON WHISTLEB TO PROVIDE LEGAL SERVICES.

(ii) USE. CUSTOMER AGREES AND ACKNOWLEDGES THAT IT IS FULLY RESPONSIBLE FOR ITS USE OF THE SERVICES. WHISTLEB EXPRESSLY DISCLAIMS ANY LIABILITY AS A RESULT OF CUSTOMER'S USE OF THE SERVICES OR CUSTOMER'S ACTIONS OR INACTIONS WITH RESPECT TO ANY INFORMATION DERIVED THEREFROM, EXCEPT WHERE SUCH LIABILITY FIRST AROSE AS A DIRECT RESULT OF WHISTLEB'S (a) MATERIAL BREACH OF THIS MSA, OR (b) GROSSLY NEGLIGENT ACT OR OMISSION IN DELIVERING THE SERVICES. WHISTLEB WILL NOT BE RESPONSIBLE FOR PAYMENT OF ANY FINES ASSESSED AGAINST CUSTOMER OR ITS LICENSED USERS BY ANY REGULATORY AUTHORITY FOR CUSTOMER'S FAILURE TO COMPLY WITH STATUTORY OR REGULATORY REQUIREMENTS OF ANY KIND.

8.0 Indemnification.

8.1. By WhistleB. WhistleB will indemnify and defend Customer and its officers, directors, employees, and agents against any costs and expenses (including reasonable attorneys' fees and disbursements), liability, and costs from suits, actions, or proceedings threatened, made, or brought by any third party in connection with any and all allegations, claims, or demands ("**Losses**") to the extent such Losses relate to or arise from (i) WhistleB's violation of Applicable Law; or (ii) a claim that the SaaS Offering infringes or misappropriates any third-party intellectual property rights. WhistleB's obligations under Section 8.1(ii) do not apply (a) to the extent that the allegedly infringing SaaS Offering, portions or components thereof, or modifications thereto result from any change made by Customer or any third party for Customer; (b) if the infringement claim could have been avoided by using an unaltered current version of a SaaS Offering that WhistleB provided; (c) to the extent that an infringement claim is based upon any information, design, specification, instruction, software, data, or material not furnished by WhistleB, or any material from a third-party portal or other external source that is accessible to Customer within or from the SaaS Offering (e.g., a third-party web page accessed via a hyperlink) or a third-party product; (d) to the extent that an infringement claim is based upon the combination of any material with any products or services not provided by WhistleB; or (e) to the extent that an infringement claim is caused by Customer providing to WhistleB materials, designs, know-how, software, or other intellectual property with instructions to WhistleB to use the same in connection with the SaaS Offering.

8.2. By Customer. Customer will indemnify and defend WhistleB and its officers, directors, employees, and agents against any and all Losses to the extent such Losses relate to or arise from: (i) Customer's violation of Applicable Law; (ii) a claim that any Customer Intellectual Property infringes or misappropriates any third-party intellectual property rights; (iii) Taxes for which Customer is liable; or (iv) Customer's and Customer's Affiliates' use of the Services, provided that such use is the sole and proximate cause of the request for indemnification under this subsection.

8.3. Mutual Obligations. The party from whom indemnification is being sought pursuant to this Section 8.3 ("**Indemnifying Party**") shall indemnify the party seeking indemnification from the Indemnifying Party ("**Indemnified Party**") only on the following conditions: (i) the Indemnified Party has a valid claim for indemnification pursuant to Section 8.0; (ii) the Indemnified Party promptly provides the Indemnifying Party with Notice of any Losses; and (iii) the Indemnified Party promptly tenders control of the defense and settlement of any such Losses to the Indemnifying Party (at the Indemnifying Party's expense and with the Indemnifying Party's choice of counsel); with the exception that failure to give such Notice shall not relieve the Indemnifying Party of its obligations hereunder except to the extent that the Indemnifying Party is materially prejudiced by such failure. The Indemnified Party shall cooperate fully with the Indemnifying Party at the Indemnifying Party's request and expense in defending or settling such claim, including, without limitation, providing any information or materials necessary for the Indemnifying Party to perform the foregoing. The Indemnifying Party will not enter into any settlement or compromise of any such claim without the Indemnified Party's prior written consent if the settlement would require admission of fault or payment by the Indemnified Party.

9.0 Confidential Information.

9.1. Definition of Confidential Information. "**Confidential Information**" means any information disclosed at any time by either party, its Affiliates, directors, officers, employees, and agents (collectively, "**Representatives**"), to the other party or its Representatives in anticipation of or during the parties' relationship, either directly or indirectly, in writing, orally, or by inspection of tangible objects that pertain to such party's business, including, without limitation, information concerning technology, marketing, planned functionality, market strategies, finances, employees, planning, product roadmaps, service or product purchases, performance agreements and documentation, performance results, pricing, and other confidential or proprietary information, including information a reasonable person would understand to be confidential or proprietary. Confidential Information of either party will not, however, include any information that: (i) was publicly known and that the disclosing party made generally available in the public domain prior to the time of disclosure; (ii) becomes publicly known and that the disclosing party made generally available after disclosure to the receiving party through no action or inaction of the receiving party; (iii) is already in the possession of the receiving party without a breach of any third party's obligations of confidentiality at the time of disclosure by the disclosing party, the burden of proof of prior possession being on the party asserting such prior possession; (iv) the receiving party obtains from a third party without a breach of such third party's confidentiality obligations; or (v) the receiving party independently develops without use of or reference to the disclosing party's Confidential Information, the burden of proof of independent development being on the party asserting such independent development.

9.2. Disclosure of Confidential Information. Each party shall (i) hold all Confidential Information of the other party in confidence and use it only as permitted in connection with the Services provided under the Agreement; (ii) use the same care to prevent unauthorized disclosure of the disclosing party's Confidential Information as the receiving party uses with respect to its own Confidential Information of a similar nature, which shall not, in any case, be less than the care a reasonable business person would use under similar circumstances; (iii) disclose only the Confidential Information required to comply with a court order or Applicable Law in conjunction with fulfilling obligations under Section 9.4; and (iv) only disclose the Confidential Information to its Representatives who have a need to know such information in order to perform their job, have been informed of its confidential nature, and have agreed to and are bound by no less restrictive confidentiality obligations than those in this MSA. Each party shall be liable for their respective Representative's breach of this MSA. Confidential Information shall not be disclosed to third parties without the other party's prior written consent unless required by Applicable Law.

9.3. Injunctive Relief. Each party acknowledges that a party's actual or threatened breach of its confidentiality obligations under Section 9.0 would likely cause irreparable harm to the non-breaching party that could not be fully remedied by monetary damages. Each party, therefore, agrees that the non-breaching party may seek such injunctive relief or other equitable relief as may be necessary or appropriate to prevent such actual or threatened breach without the necessity of proving actual damages. Each party waives the requirement to post a bond in the event of such actual or threatened breach.

9.4. Legal Process. If either party receives notice of a witness summons, request for production of documents, court order, or requirement of a governmental agency to disclose any information or respond to an official inquiry ("**Legal Process**"), the recipient thereof shall, if permitted by law, give prompt Notice to the other party so the other party may move for a protective order or other relief. Each party agrees to cooperate with the other party to respond to any notice or inquiry from a third party related to the Agreement.

10.0 Liability Exclusions and Limitations.

10.1. Liability Limitations. THE FOLLOWING LIMITATIONS SHALL NOT APPLY TO (i) BREACHES OF CONFIDENTIALITY OBLIGATIONS; (ii) VIOLATIONS OF EITHER PARTY'S INTELLECTUAL PROPERTY RIGHTS; (iii) EITHER PARTY'S INDEMNIFICATION OBLIGATIONS; OR (iv) PAYMENT OF FEES:

(a) TO THE MAXIMUM EXTENT PERMITTED BY LAW, IN NO EVENT SHALL EITHER PARTY BE LIABLE TO THE OTHER, WHETHER UNDER THEORY OF CONTRACT, TORT, OR OTHERWISE, FOR ANY INDIRECT, INCIDENTAL, PUNITIVE, CONSEQUENTIAL, OR SPECIAL DAMAGES (INCLUDING ANY DAMAGE TO BUSINESS REPUTATION, LOST PROFITS, OR LOST DATA), WHETHER FORESEEABLE OR NOT, AND WHETHER OR NOT SUCH PARTY IS ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

(b) TO THE MAXIMUM EXTENT PERMITTED BY LAW, EACH PARTY'S AGGREGATE CUMULATIVE LIABILITY TO THE OTHER IN CONNECTION WITH THE AGREEMENT SHALL NOT EXCEED THE AGGREGATE CONTRACT VALUE FOR THE ONE- (1) YEAR PERIOD PRIOR TO THE DATE THAT SUCH LIABILITY FIRST ARISES.

10.2. Time Limit for Bringing Action. No claim or action, regardless of form, arising out of the Agreement, other than a claim or action relating to a breach of confidentiality or infringement, may be brought by either party more than two (2) years after the cause of action has arisen.

11.0 Governing Law; Dispute Resolution. This contract shall be governed by the substantive law of Sweden without regard to conflict of laws rules. Any dispute, controversy or claim arising out of or in connection with this contract, or the breach, termination or invalidity thereof, shall be finally settled by arbitration in accordance with the Arbitration Rules of the Arbitration Institute of the Stockholm Chamber of Commerce. The seat of arbitration shall be Stockholm, Sweden. The language to be used in the arbitral proceedings shall be English.

12.0 General Provisions.

12.1. Publicity. WhistleB shall not use Customer's name, trademarks, or logos for marketing purposes except as specifically authorized by Customer in writing in advance of any such use.

12.2. Third-Party Beneficiaries. Unless otherwise prohibited by Applicable Law, nothing in the Agreement shall be construed to give any person or entity other than the parties hereto any legal or equitable claim, right, or remedy; rather, the Agreement is intended to be for the sole and exclusive benefit of the parties.

12.3. Assignment. The terms of the Agreement shall be binding on the parties and their respective successors. Neither party may assign, transfer, or delegate its rights or obligations under the Agreement (in whole or in part) without the other party's prior written consent, except (i) to an Affiliate; or (ii) pursuant to a transfer of all or substantially all of such party's business and assets, whether by merger, sale of assets, sale of stock, or otherwise. Any attempted assignment, transfer, or delegation in violation of the foregoing shall be null and void.

12.4. Notice. "**Notice**" means written notification to a party that shall be sent via email only, unless otherwise indicated herein. Any Notice to WhistleB shall be sent to: legalnotice@navexglobal.com. Notice to Customer shall be sent to the Customer email address provided by Customer during the online application process. Provided, however, that Customer may update its email address for Notice purposes at any time by providing WhistleB with Notice in accordance with the terms of this section.

12.5. No Agency. The Agreement shall not be construed to create a joint venture or partnership between the parties. Neither party shall be deemed to be an employee, agent, partner, or legal representative of the other for any purpose, nor shall either party have any right, power, or authority to create any obligation or responsibility on behalf of the other.

12.6. Compliance with Law.

(i) Each party shall be responsible for compliance with Applicable Law related to the performance of its obligations under the Agreement.

(ii) WhistleB's Services are subject to U.S. sanctions laws and may not be sold or licensed to any party listed on the Specially Designated Nationals List maintained by the U.S. Department of the Treasury ("**Restricted Party**") or in U.S.-sanctioned countries (the most up-to-date lists can be found at http://www.treasury.gov/resource-center/sanctions/Programs/Pages/Programs.aspx). Customer represents and warrants that neither Customer, its Representatives, nor, to Customer's knowledge, its Affiliate's Representatives are currently the subject of any investigation by the Office of Foreign Assets Control (OFAC), Department of the Treasury, or any other governmental authority pursuant to any laws that OFAC or any other governmental authority administers ("**Sanctions Investigation**"). Customer shall promptly notify WhistleB if it or any of its Representatives or its Affiliates' Representatives become the subject of any Sanctions Investigation. Customer agrees not to transfer or provide access to the Services (a) to any Restricted Party; or (b) in, or for the benefit of individuals or entities from, such U.S.-sanctioned countries. Further, Customer agrees not to use the Services for the benefit of a Restricted Party or individuals or entities from such U.S.-sanctioned countries. Customer represents and warrants that it is not directly or indirectly owned by, controlled by, owning, controlling, or named as a Restricted Party. WhistleB and its Affiliates may not do business with a Restricted Party under U.S. law (the most up-to-date lists can be found at http://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx and http://www.bis.doc.gov/index.php/the-denied-persons-list).

(iii) Customer represents and warrants that its use of WhistleB's Services will in all respects comply with U.S. export controls regulations and requirements, including, without limitation, those promulgated by U.S. Departments of State, Commerce, Homeland Security, Treasury, and Defense. Any breach of this Section 12.6 is a material breach of the Agreement for which no cure period shall apply.

12.7. Force Majeure. Except for payment of fees, neither party shall be liable for failure to perform, or the delay in performance of, any of its obligations under the Agreement if and to the extent that such failure or delay is caused by events beyond its reasonable control, including, without limitation, acts of the public enemy or a governmental body in its sovereign or contractual capacity, war, fire, flood, unusually severe weather, outside electrical failure, the limitations or failures of third-party internet service providers and/or telecommunication providers, the performance or failures of internet service providers, or acts of terrorism, including cyberattacks on WhistleB's computer systems or those of third parties, including, without limitation, internet service providers and telecommunication providers. If so affected, the affected party shall use commercially reasonable efforts to avoid or remove such causes of non-performance or delay and shall continue performance hereunder with reasonable dispatch whenever such causes are removed or otherwise resolved.

12.8. Waiver. No waiver or delay in enforcement of any breach of any provision of the Agreement shall constitute a waiver of any prior, concurrent, or subsequent breach of the same or any other provision hereof, and a waiver shall not be effective unless made in writing and signed by an authorized representative of the waiving party.

12.9. Survival. The terms and conditions of the Agreement that by their nature require performance by either party after the termination of this MSA, including, without limitation, confidentiality obligations, limitations of liability, exclusions of damages, indemnification obligations, governing law, fees owed prior to the date of termination, and any other provision or partial provision that by its nature would reasonably extend beyond the termination of this MSA shall be and remain enforceable after such termination of this MSA for any reason whatsoever.

12.10. Severability. If any provision of the Agreement conflicts with governing law or if any provision is held to be null, void, or otherwise ineffective or invalid by a court of competent jurisdiction, (i) such provision shall be deemed to be restated to reflect as nearly as possible the original

intentions of the parties in accordance with Applicable Law; and (ii) the remaining terms, provisions, covenants, and restrictions of the Agreement shall remain in full force and effect.

12.11. Entire Agreement. The Agreement constitutes the complete agreement between the parties and supersedes all prior or contemporaneous agreements, proposals, responses to requests for proposals, representations, and warranties, written or oral, concerning the subject matter of the Agreement, including any prior non-disclosure or confidentiality agreement(s), which shall be replaced by those terms and conditions set forth in Section 9.0 unless otherwise expressly agreed to in writing by the parties. The Agreement may be modified or amended only in writing signed by a duly authorized representative of each party; any other act, usage, or custom shall not be deemed to amend or modify the Agreement. It is expressly agreed that the terms of the Agreement shall supersede the terms in any Customer purchase order, and the terms included in any such purchase order or other Customer policy shall not (i) apply to the Services ordered; or (ii) in any way modify, revise, supplement, or otherwise affect the terms and conditions of the Agreement. If Customer requests processing of payments through a third-party payment vendor, it is understood and agreed that any such use of a third-party payment vendor is solely for the convenience of Customer and documentation associated with payment submission shall not in any way modify, add to, or delete any of the terms and conditions of the Agreement. Any costs associated with such use of a third-party payment vendor shall be borne exclusively by Customer.

12.12. Section Headings. The Section headings are for reference purposes only and shall not in any way affect the meaning or interpretation of this MSA.

12.13. Counterparts. The parties may execute Order Forms in counterparts. An exchange of scanned and emailed executed copies or electronic signatures is acceptable. In the event of such an exchange, such Order Forms shall become binding, and any scanned and emailed signed copies or electronic signatures shall constitute admissible evidence of the existence Order Form.

EXHIBIT A
DATA PROCESSING ADDENDUM

This Data Processing Addendum ("DPA") sets out the terms and conditions with regard to the Processing of Personal Data by WhistleB and/or WhistleB's Sub-Processors. In the course of providing the Services to Customer pursuant to the Agreement, WhistleB ("Processor") may Process Personal Data of Customer and may therefore be 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 with regard to the Processing of personal data and on the free movement of such data ("GDPR").

1. DEFINITIONS

As used in this DPA, Controller is the Customer pursuant to the Agreement which determines the purposes and means of the Processing of Personal Data. WhistleB is Processor, where it Processes Personal Data on behalf of the Customer.

Capitalized terms used herein without definition shall have the meanings ascribed to them in the Agreement, unless the context shall otherwise require.

Data Protection Requirements means all data protection and privacy laws and regulations, as applicable to a party, including the GDPR and any other local or regional data protection, data privacy or data security laws.

Data Subject is the natural person to whom Personal Data pertains.

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

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

Personal Data are any data regarding an identified or identifiable natural person, which are or will be Processed by Processor in any way whatsoever in the context of the Agreement, as further specified in Annex 1.

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

Processing is any activity or combination of activities involving Personal Data, in any event including but not limited to the collecting, recording, organising, storing, updating, amending, accessing, consulting, using, providing by way of forwarding, distributing or any other form of supplying, compiling, linking, as well as safeguarding, deleting or destroying of data ("Process", "Processes" and "Processed" shall have the same meaning).

Controller Data is any and all Customer Data, including Personal Data, submitted to the Services which includes information in the dialogue with a person reporting via the Services as well as all the data that is collected and stored in the case for the investigation purposes.

2. GENERAL

a. Processor undertakes to Process Personal Data on the terms and conditions of this DPA and only in accordance with the documented instructions of 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, Processor may Process Personal Data if required by union or member state law to which Processor is subject to. In such case, Processor shall inform Controller of the legal requirement before the Processing, unless that law prohibits such information on important grounds of public interest.

b. Processor shall Process the Personal Data properly, with due care and in accordance with the Data Protection Requirements relating to the Processing of Personal Data, including ensuring that persons authorized to Process the Personal Data are bound to obligations of confidentiality or are under an appropriate statutory obligation of confidentiality.

c. Controller shall, in its use of the Services, Process Personal Data in accordance with the requirements of Data Protection Requirements. Controller's instructions to Processor, for the Processing of Personal Data, shall comply with Data Protection Requirements.

d. In the event that Processor believes that Controller's instructions conflict with the requirements of the GDPR or other Data Protection Requirements, Processor shall immediately inform Controller.

e. Processor shall only carry out the Processing to the extent necessary to provide the Service to Controller as described in the Agreement, as more fully set out in Annex 1.

f. Processor shall not retain Personal Data made available to Processor in the context of the Agreement any longer than is necessary (i) for the performance of the Agreement; or (ii) to comply with any of its statutory obligations. Annex 1 describes the applicable retention periods.

g. Processor is obligated to inform Controller regarding any future changes in the performance of the Agreement, so that Controller can monitor compliance with arrangements made with Processor. This also includes the engagement of (new) Sub-processors, without prejudice to the provisions in section "Use of Sub-processors" and section "Change".

h. Taking into account the nature of processing and the information available, Processor shall assist Controller in meeting its obligations pursuant to Articles 32 to 36 of the GDPR.

3. USE OF SUB-PROCESSORS

Processor may continue to use those Sub-processors already engaged as of the date of this DPA, as set forth in the following link: https://whistleb.com/sub-processors/. The foregoing link contains a mechanism to subscribe to notifications of the addition of any new Sub-processors for each applicable Service, to which Controller may subscribe. Such updates provided via this mechanism shall operate as the notification of changes concerning the addition of any new Sub-processors, as required by Data Protection Requirements.

Processor will notify Controller in advance of any changes to the list of Sub-processors in place (except for deletions of Sub-processors without replacement) at least thirty (30) days in advance of any Processing by the proposed Sub-processor in accordance with the procedure set forth in this section 3. If Controller has a reasonable objection that relates to the Sub-processors' Processing of Personal Data, Controller may object to Processor's use of a Sub-processor by notifying Processor in writing at privacy@navexglobal.com within thirty (30) days after receipt of Controller's notice. In such event, the Parties will work in good faith to discuss a resolution. Processor may choose to: (i) not use the Sub-processor to Process Personal Data for Controller or (ii) take the corrective steps requested by Controller in its objection and use the Sub-processor. If neither of these options are reasonably possible and Controller continues to object, Controller may provide notice of termination of the affected portion of the Service as to Controller.

Processor shall impose the same data protection obligations as set forth in this DPA, on each Sub-processor by way of a contract, providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of Data Protection Requirements.

Processor shall be liable for the acts and omissions of its Sub-processors to the same extent Processor would be liable if performing the services of each Sub-Processor directly under the terms of this DPA.

4. SECURITY

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. 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, Processor shall take all other measures required pursuant to Article 32 GDPR.

On request, Processor shall provide Controller with written information relating to (the organisation) of the security of Personal Data.

5. OBLIGATION TO REPORT DATA BREACHES AND SECURITY BREACHES

To the extent permitted by law, Processor shall notify Controller without undue delay if it becomes aware of a Data Breach. To the extent available, such notification shall describe the nature of the incident, including the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned.

Processor shall: (i) reasonably cooperate with Controller to investigate and resolve the Security Incident; (ii) make reasonable efforts to identify and remediate the cause of such Security Incident; and (iii) keep Controller up-to-date about developments in connection with the Security Incident. At Controller's request, Processor shall cooperate, in so far as possible, in informing the competent authorities and Data subject(s).

6. Audit

Processor is required, upon request from Controller, to have an independent IT auditor or expert conduct an audit, including inspections, regarding the organisation of Processor in order to have it established that Processor complies with the provisions regarding the confidentiality, integrity, availability and security of Personal Data, as defined in the Agreement and DPA. Furthermore, Processor shall make available to Controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 GDPR.

Processor is responsible for and bears the costs of yearly penetration testing and its own information security audits. Upon request, Processor is obliged to make the findings of the IT auditor or expert available to Controller in the form of a third-party memorandum.

If it is established during an audit that Processor has failed to comply with the provisions of the Agreement and the DPA, Processor shall take all reasonably necessary measures to ensure compliance.

7. INTERNATIONAL TRANSFER

Should transfers of Controller 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 Requirements, including the European Commission's Standard Contractual Clauses.

8. INVESTIGATION REQUESTS

If 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, Processor shall notify Controller without undue delay, to the extent permitted by applicable law. When handling the request or order, Processor shall observe all of Controller's instructions (including the instruction to leave the handling of the request or order in full or in part to Controller) and provide all reasonably required cooperation to Controller.

If the request or order prohibits Processor from complying with its obligations on the basis of the above, Processor shall promote Controller's reasonable interests.

9. RIGHTS OF DATA SUBJECTS

Processor shall promptly notify Controller if 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, and to the extent Controller in it use of the Services does not have access to the Personal Data or the ability to manage Data Subject Rights on its own as required by Data Protection Requirements, Processor shall assist Controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of Controller's obligation to respond to a Data Subject Request under applicable data protection laws. If a Data Subject, in relation to the execution of its rights under the Data Protection Requirements, directly requests Processor to correct, delete or block Personal Data, Processor shall refer such Data Subject to Controller.

10. INDEMNIFICATION AND LIMITED LIABILITY

Processor shall indemnify and keep indemnified Controller against direct damages, claims, and losses incurred by Controller which arise directly from Processor's Processing activities under this DPA. Notwithstanding anything to the contrary, the indemnification obligations pursuant to this DPA shall remain subject to the limitations of liability set forth in Section 10 of the MSA. The existence of more than one claim will not extend such limitation.

11. CHANGE

If a change in Data Protection Requirements results in this DPA no longer meeting applicable requirements for a data processing agreement, the parties will work together to implement any required changes in writing in order to meet such new or additional requirements.

12. TERMS AND TERMINATION

The terms of the DPA are equal to the terms of the Agreement. The DPA cannot be terminated separately from the Agreement.

Controller will have access and the ability to download and save Controller Data during the Term. All Controller Data shall be deleted within forty-five (45) days of expiration or termination of services, and Controller Data stored in backups shall be overwritten in accordance with Processor's backup and retention cycle. Unless there is a statutory obligation to store Personal Data, 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 Agreement and following delivery of the Personal Data.

13. GOVERNING LAW AND DISPUTES

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

14. CONTACT INFORMATION

If Controller wishes to contact Processor, or if this DPA requires Controller to give notice to Processor in writing, please contact Processor at:

WhistleB Whistleblowing Centre AB
PO Box 70396,
107 24 Stockholm
Sweden
E-mail: privacy@navexglobal.com

ANNEX 1: Data processing details

Data Controller

Data Controller is the legal entity that has executed the DPA.

Data PROCESSOR

Processor is a provider of the Services set forth in the Agreement, which Processes Personal Data upon the instruction of Controller in accordance with the terms of the Agreement.

Categories of Data subjects

Data subjects comprise of all persons given access to the Services by Controller.

Categories of Personal Data to be processed

The Personal Data captured by the Services concern the following categories of data:

- name, job title, job position, location, employer, relationship with the organization, e-mail address, telephone number;
- for whistle-blower hotline reports, in addition to the foregoing, the following may also be captured:
    - facts reported by a reporter about a suspected violation, including how and where the suspected violation occurred and how the reporter learned about the suspected violation;
    - identity, function and contact details of individuals allegedly involved in the suspected violation; and
    - identity, function and contact details of individuals who could provide information relating to the suspected violation.

Special Categories of Personal Data

The Personal Data captured by the Services concern the following special categories of data:

Controller, reporters or authorized users of the Services may submit special categories of data to the Services, the extent of which is determined and controlled by the data exporter in its sole discretion, and which is for the sake of clarity Personal Data that may include information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.

Data Protection Officer

Processor has appointed a data protection office where such appointment is required by Data Protection Requirements. The appointed person may be reached at privacy@navexglobal.com.

Retention periods

When a report is closed, 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. Deletion of Controller Data upon termination is addressed in Section 12.

ADDITIONAL Security measures

Processor ensures the security of Personal Data. Processor has no access to reporter data with regard to contents, as Processor will at no time have access to any encrypted data of Controller without prior authorisation.

Back up routines

The Service is delivered to 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.

EXHIBIT B
SERVICE TERMS

WhistleB

1. The Term shall begin on the Effective Date and run for 1 year (the "Initial Term").
2. The implementation fee and 100% of the Initial Term annual fees will be invoiced upon the Effective Date and Customer shall remit payment within 30 days of said invoice's date.
3. Each subscription will automatically renew for successive 1-year periods (each a "Renewal Term"). However, either party may elect to not renew by providing written notification to the other party at least 30 days prior to the start of a Renewal Term.
4. The annual fees for subsequent years will be invoiced to Customer at least 30 days prior to the start of the upcoming year and will be due by the start of such year.
5. Annual fees will be fixed for a period of 12 months from the Effective Date. Thereafter, WhistleB may increase annual fees not more than once per year by providing 60 days prior written notification of the increase.

SERVICE TERMS

ENCRYPTION OF CUSTOMER DATA. Customer Data is encrypted in flight and at rest when stored in the Services. Customer Data is accessible to Customer by use of a "secondary password" which is set up by Customer upon launch of the Services and used by Customer to decrypt Customer Data within the Services. The secondary password is shared among case managers and it is Customer's responsibility to share the secondary password with the case managers Customer wishes to authorise to access and manage reports. If the secondary password is lost, Customer can restore and access Customer Data with the backup encryption file, which is provided to Customer upon launch of the Services. Customer is responsible for secure password management, including use and secure storage of Customer's backup encryption file. WhistleB does not know Customer's encryption keys necessary to decrypt Customer Data and cannot access Customer Data unless such access to decrypted Customer Data is authorized in writing by Customer. **A lost secondary password, in combination with a lost backup encryption file, means that the Customer Data will no longer be accessible.** WhistleB cannot be held liable for any loss of Customer Data related to Customer's loss of the secondary password and backup encryption file.

ACCESS TO CUSTOMER DATA. During the Services Term, Customer will have sole responsibility for determining whether Customer Data residing in the Services will be maintained within the Services or deleted. WhistleB will have no responsibility, liability or obligation with respect to any Customer Data that has been deleted, purged, overwritten, or otherwise destroyed by or as directed by Customer. Customer will have access and the ability to download and save Customer Data during the Services Term. Upon termination and at the request of Customer made within thirty (30) days following the effective date of termination, WhistleB will create and deliver to Customer, at Customer's cost and expense, a copy of all encrypted Customer Data then in existence in the Services.

SUB-PROCESSORS.
Hosting Location: EU
Customer consents to the use of the applicable sub-processors set forth in the following link: https://whistleb.com/sub-processors/. The foregoing link contains a mechanism to subscribe to notifications of the addition of any new sub-processors for each applicable Service, to which Customer may subscribe. Notwithstanding any provision to the contrary, updates provided via this mechanism shall operate as the notification of changes concerning the addition of any new sub-processors

WhistleB Online MSA v.57