CUSTOMER AGREEMENT INTEGRITYLOG

TERMS AND CONDITIONS

1. Background

Euronext Corporate Services Sweden AB, 559141-7083 ("**The Supplier**"), provides *IntegrityLog*, a web-based tool that help companies handle internal whistleblowing matters ("**Software**"). The Software enables company personnel and anyone otherwise performing tasks through which they can become whistleblowers to anonymously report certain types of perceived or actual wrongdoing ("**Whistleblowing**"). The Supplier has agreed to provide the Software to **the Customer** (as defined in the Order) pursuant to the Order and these general terms and conditions (the "**Terms**"). The Software is a company service, not intended for use by natural persons but by legal entities.

By submitting the Order, the Customer agrees to be bound by these Terms and its appendices. The Terms have one appendix, the "**Data Processing Agreement**", which comprises a data processing agreement and its two Schedules (Schedule 1 – Data Processing Instructions and Schedule 2 – Technical and Organizational Security Measures).

The Order, the Terms and its appendices form the entire agreement between the Customer and Supplier with respect to the Software, (the "**Agreement**"). In case of conflict between the Order, the Terms and the Data Processing Agreement, the latter shall prevail in relation to topics regulated therein (processing of personal data). In case of conflict between the Order and the Terms, the Order shall take precedence over the Terms.

In these Terms the Supplier and Customer will collectively be referred to as the "**Parties**" and individually as a "**Party**". Where the context does not clearly indicate otherwise, words and expressions in these Terms shall have the same meanings as set out in the Order.

2. License

The Customer is granted a non-exclusive, non-sublicensable and non-transferable license to use the Software in the Customer's internal business operations for the term further specified in the Agreement (the "**License**"). For the avoidance of doubt, the Software is not sold and the Agreement does not constitute any transfer of ownership of the Software.

3. Fee, invoicing and license period

All fees stated in the Order are collectively referred to as the "**Fees**".

The Fees specified in the Order are excl. VAT. Predetermined Fees are invoiced in advance on an annual basis and the one-time Fees are invoiced after the end of the contract period. All invoices have a thirty (30) days' payment period.

Unless stated otherwise in the Order, the License is valid for one year starting from the date specified in the Order (the "**License Period**"). The License Period is automatically renewed, unless terminated at least two (2) months prior to the end of each License Period. Any amendments of these Terms for an upcoming License Period shall be communicated by the Supplier (by email or clearly through the Software interface) at least three (3) months prior to the end of the applicable License Period. Individuals that have been made main administrators in the Software shall be entitled to approve new terms on behalf of the Customer.

The Supplier may disable the Customer's access to the Software if the Customer does not, despite reminder, pay invoices that have fallen due.

The Customer must provide correct and up-to-date contact information to enable the Supplier to invoice the Customer in accordance with the foregoing. Accordingly, the Customer undertakes to promptly inform the Supplier of any changes to such contact information.

4. User restrictions and obligations

The Customer is responsible for all the Customer's physical users of the Software, including but not limited to, employees, consultants and advisors ("**Users**"). Accordingly, the Customer shall ensure that each such User complies with these Terms. Any login details and passwords necessary for a User to access the Software are personal and may not be shared.

The Customer is solely responsible and liable for the activities conducted under the Customer's accounts in the Software and for the User's use of the Software. The Customer undertakes to inform the Supplier of any unauthorized activities conducted under the Customer's accounts.

The Supplier has the right to wholly or in part suspend the Customer's access to the Software without prior notice if the Supplier has reasonable grounds to suspect that the Customer has violated the terms and conditions of the Agreement.

5. Updates and bug fixes

As long as the Customer has a valid License, the Customer will be given free access to minor general updates and bug fixes of the Software. The Software is set to automatically download and install such updates. General updates are installed between 00-05 CET.

The Customer is responsible for procuring and maintaining, at its own cost, its own equipment and other software required for using the Software.

The Customer accepts that the Software may become inactive when the Supplier makes any updates to the Software in accordance with the previous paragraphs. The Customer is advised not to work in the Software during any such updates, as such work may be lost once the updates have been completed.

Supplier may, from time to time, develop new functions which are not included in the Fees. No such functions are installed or invoiced without the Customer's consent.

6. Support and corrective measures

During the term of the Agreement, support for rectifying Defects in the Software is included. "**Defects**" means reproducible cases where the Software materially fails to perform as promised. Support levels for responding and resolving Defects:

Priority Level	Response time	Resolution time
A) Critical	30 min	8 hours
B) High	30 min	16 hours
C) Normal	30 min	7 days

Priority levels:

Critical: System failure or any issue causing major operational disruption

High: Any issue affecting the operational processes

Normal: Operational processes are not affected or affected lightly

The support request must be submitted via e-mail to support@complylog.com or any other e-mail designated by the Supplier. The support is available for receipt and handling of matters on working days between 09:00 and 18.00 CET. Response time and resolution time is only calculated between these hours. For example, if an issue is received at 17.45 and a response is sent the next working day at 09.05, that issue shall be deemed to have been handled within 20 minutes.

A support request shall include information about which web browser the Customer is using and the Defect that the Customer has experienced. Furthermore, the Customer shall co-operate with the Supplier and provide all reasonable assistance necessary for the Supplier to diagnose, reproduce and assess the Defect.

Support is primarily provided remotely via phone or e-mail. If the Defect cannot be corrected remotely, the Supplier may need to access the Customer's server instance where the Customer's data is stored. The Supplier shall use its' best endeavours to not access any sensitive data pertaining to the Customer unless it is necessary to correct the Defect.

The Customer will be credited an amount equivalent to a proportional amount of the Fee during the time that the Defect persisted from the support request. Such credit shall be granted to the Customer within sixty (60) days from the day the Defect was remedied in its entirety. If the Defect cannot be corrected within a reasonable time, the Customer may as its exclusive remedy terminate the Agreement prematurely and shall be compensated for any pre-paid Fees pertaining to the period the Software has not been used.

7. Intellectual property rights

The Supplier retains all ownership and all other rights to the Software, including source code, design and trademark etc. Even if the Software is modified after input and suggestions from the Customer, the Customer has no right to such modifications and they shall automatically be assigned to the Supplier which may use them freely without any obligation to compensate the Customer.

The Customer may not a) sub-license the Software or in any other way make the Software available to any third parties, b) copy, decompile, attempt to determine or receive access to the source code, methods, algorithms or procedures of the Software or otherwise engage in "reverse engineering", or modify, adapt or create new works or software based on the Software except as set out in mandatory applicable law, c) remove, conceal or circumvent the Supplier's trademark or copyright markings in the Software, d) attempt to circumvent license keys or other user restrictions in the Software, e) use the Software for illegal purposes, f) use the Software to spread viruses or other malware and/or g) use the Software to infringe or breach the intellectual property rights or other rights of others.

Unless the Customer has objected to it in writing, the Supplier may use the Customer as a reference case in the Supplier's sales materials (on its website, in printed materials or at meeting) and refer to the Customer as a user of the Software by using the Customer's name, trademark and logo.

8. Hosting and personal data

The Customer is responsible for ensuring that any information provided in the Software by the Customer complies with applicable laws and does not infringe any third-party rights.

The Supplier will be responsible for hosting of the Software.

The Customer is the controller of all personal data which is processed by the Software. It is the Customer's responsibility to make sure that such processing complies with applicable rules on personal data.

If the Supplier gets access to the Customer's data stored in the Software, or other sensitive and non-public data about the Customer, this information shall be treated as confidential and may not, neither during the term nor thereafter, be used or disclosed to a third party without the Customer's consent. The confidentiality does not apply if the information is or becomes publicly known through any other party than the Supplier or if the Supplier is required to disclose the information by law, court or authoritative order.

The Supplier is responsible for and assures that all its personnel and any other consultants employed by the Supplier to provide services to the Customer, are subject to confidentiality obligations.

9. Liability and limitation of liability

The Supplier does not manage any reporting channel or engage in any assessment of any case of any kind for the Customer, rather it provides the Software which simplifies the Customer's own administration and handling of Whistleblowing. In case of any perceived or actual Defect in the Software, the Customer cannot stop or delay the proper compliance with its obligations under laws, regulations and/or recommendations applicable to the Whistleblowing. Consequently, the Customer undertakes to return to manual management until the Defect is corrected by the Supplier. For the avoidance of doubt, the Customer acknowledges that the Software does not constitute any recommendation and/or instruction with respect to any applicable laws, regulations and/or recommendations applicable to Whistleblowing ("**Whistleblowing Laws**"). It is the Customer's sole responsibility to ensure it complies with Whistleblowing Laws and the Supplier can, under no circumstances, be held liable for the Customer's non-compliance with Whistleblowing Laws or any other applicable law and/or regulation.

To the extent permitted under applicable mandatory law, the Software is provided on an "as is" basis. The Supplier has no liability for Defects or other damages that occur due to a) any event outside the Supplier's control, b) the Software not being used in accordance with the Supplier's instructions, c) the Software being modified by any other party than the Supplier, d) the Customer acting negligently, e) third party software being used in the Software except that the Supplier shall report the Defect to the concerned supplier and implement the proposed measures.

The Supplier's liability is limited to an amount corresponding to the fixed yearly Fee under the Agreement. The Customer can under no circumstances hold the Supplier responsible for loss of profits or savings, costs for sanctions or fines, lost goodwill, lost information, costs for cover purchases or any kind of indirect damages. The Customer understands that the Supplier would not be able to provide the Software at the current price if the Supplier was to assume liability for any sanction fees from a national competent authority.

The Customer is furthermore liable for all damages or costs caused by the Customer's breach of the obligations under Section 7.

The person signing the Agreement on behalf of the Customer warrants that they are an authorized representative of the Customer, capable of legally binding the Customer to the

Agreement, and they shall be personally fully liable for all direct or indirect damages, costs or losses relating to their breach of this warranty.

10. Termination

In addition to the provisions regarding termination of the License Period pursuant to the preceding Sections of these Terms, each Party has the right to terminate the Agreement with immediate effect if:

a) the other Party has committed a material breach of the Agreement and does not take full correction of such breach within thirty (30) days of the other Party giving written notice thereof; or

b) the other Party is declared bankrupt, enters into liquidation, is the subject of corporate reorganisation, cancels its payments or can otherwise reasonably be assumed to have become insolvent.

11. Miscellaneous

The Supplier may transfer all rights and obligations under the Agreement and the Terms to another company within the same group of companies as the Supplier. The Customer may not, without the Suppliers prior written approval, transfer the rights and obligations under the Agreement and the Terms.

If any provision of the Terms is held to be invalid or unenforceable, such provision shall be limited, modified or severed to the minimum extent necessary to eliminate its invalidation or unenforceability so that the Terms otherwise remain in full force and effect. Any provision of the Terms, which inherently should endure beyond termination, shall survive termination or expiration of the Terms.

Any dispute, controversy or claim arising out of or in connection with the Software, the Agreement or these terms, or the breach, termination or invalidity thereof, shall be finally settled by arbitration in accordance with the Rules for Expedited Arbitrations of the Arbitration Institute of the Stockholm Chamber of Commerce. Swedish law shall be applied, and the proceedings shall take place in Stockholm, Sweden and be held in the English language. The parties undertake to keep all information relating to such proceedings, including the award, as strictly confidential.

APPENDIX - PERSONAL DATA PROCESSING AGREEMENT

1. Background

This data processing agreement and its appendices ("**DPA**") are entered between the Customer ("**Controller**") and Supplier ("**Processor**"), individually referred to as a "Party" and collectively as the "Parties".

The Parties have entered into an agreement regarding the Processor's software ("**Agreement**") under which the Processor may process the Controller's personal data ("**Personal Data**") on behalf of the Controller. This DPA constitutes a written agreement in accordance with the General Data Protection Regulation (EU) 2016/679 ("**GDPR**") to provide adequate safeguards with respect to the transfer and processing of Personal Data.

If the terms concerning the processing of Personal Data of the DPA and the Agreement are in conflict, the Parties shall apply the terms of this DPA with respect to the matters stated herein (processing of personal data).

2. Definitions

The specific terms and expressions relating to Personal Data that are not defined herein, such as "personal data breach", "processing", "data subject" shall have the same meaning as in the Data Protection Legislation, and their cognate terms shall be construed accordingly.

The following terms, used in this DPA, have the following meaning:

"Data Protection Legislation" means the GDPR and laws implementing or supplementing the GDPR (including, when applicable, binding guidance, opinions and decisions published by supervisory authorities, court or other competent authority) applicable to the processing of Personal Data under this DPA, and as amended or supplemented during the term of this DPA;

"Sub-Processor" means any third-party sub-contractor engaged by the Processor to process Personal Data on behalf of the Controller.

"Third countries" means any country outside the European Economic Area which has not been deemed to ensure an adequate level of data protection by the European Commission pursuant to Article 25(6) of Directive 95/46/EC or Articles 44-50 (Chapter V) of the GDPR.

3. Obligations of the Processor

The Processor shall make sure that all processing of Personal Data is conducted in accordance with relevant provisions of any applicable Data Protection Legislation. The Processor specifically undertakes that it shall process Personal Data only in accordance with the Agreement and in accordance with the Controller's instructions (including the instructions attached hereto in Schedule 1).

The Processor shall immediately notify the Controller if, in its opinion, any instructions implies a breach of Data Protection Legislation. However, the Processor shall not be obliged to verify whether any instruction given by the Controller complies with Data Protection Legislation.

The Processor shall ensure that its personnel engaged in the processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities and are subject to obligations of confidentiality during the persons' engagement with the Controller.

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk to protect the Personal Data that is Processed on behalf of the Controller. A description of the Processor's security principles and measures is listed in schedule 2 of this DPA.

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 requests for exercising the Data Subject's rights laid down in Chapter III of the GDPR.

The Processor shall notify the Controller without undue delay, and no later than 24 hours, after becoming aware of a personal data breach. Taking into account the nature of processing and the information available to the Processor, the Processor shall provide reasonable assistance to the Controller as may be necessary to satisfy any notification obligations required under Articles 33 or 34 of the GDPR related to any Personal Data Breach.

The Processor shall, at the choice of the Controller, delete or return all the Personal Data to the Controller after the end of the provision of services relating to Processing, and deletes existing copies unless Union or Member State law requires storage of the Personal Data.

4. Sub-processors

The Processor hereby receives a general authorization to engage a new Sub-processor and/or replace a current Sub-processor. The Processor shall inform the Controller beforehand of new Sub-processors the Processor intends to use in processing the Personal Data pursuant to the Agreement and this DPA by giving notice to the Customer contact person stated in the Order. The Controller is responsible for ensuring that the email dress of the contact person is correct and updated at any given time and to notify the Processor without undue delay if the email address needs to be updated. The Controller has the right to object to the use of a new Sub-processor. The Controller shall notify the Processor of such objection within thirty (30) days of the Processor's notice to the Controller. If the Controller does not object within thirty (30) days of the Processor's notice to the Controller, the Controller shall be deemed to having accepted the use of the new Sub-processor. In the event that opposition to such Sub-processor, in the Processor's opinion, prevents effective provision of Processor's services in accordance with the Agreement, the Processor may terminate the Agreement without penalty or liability, with thirty (30) days' notice.

Any initially approved Sub-processors are set out in Schedule 1. The Processor shall enter into a personal data processing agreement with data protection obligations no less protective than this DPA with all Sub-Processor's approved by the Controller, unless otherwise stated in Schedule 1 or as agreed between the Parties. Where a Sub-processor fails to fulfil its data protection obligations, the Processor shall remain fully liable to the Controller for the performance of the Sub-processor's obligations.

5. Audit

The Processor shall make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 of the GDPR and allow for and contribute to audits, including inspections upon thirty (30) days' advance written notice to the Processor, conducted by the Controller or another auditor mandated by the Controller subject to what is set out in Schedule 1 in relation to Sub-Processors.

Any audit may only be conducted during the Processor's regular business hours so as not to cause disruption to the Processor's business, by a party who is subject to a confidentiality agreement with Processor; in accordance with Processor's security requirements, and in a way that does not impede the obligations of the Processor or its Sub-processors with regard to third parties. The Controller shall be responsible for all costs associated with the audit unless the audit evidences a significant material breach by the Processor of its obligations under this DPA that is not cured within a period of sixty (60) days.

6. Transfer to third countries

The Processor shall not transfer Personal Data to a Third Country unless (i) the Controller gives permission to such a transfer and the Processor ensures that the transfer is governed by and in accordance with a suitable framework recognized by the relevant authorities or courts as providing an adequate level of protection for Personal Data, including, without limitation binding, corporate rules for processors; or that the transfer is governed by and in accordance with the standard contractual clauses based on the European Commission Implementing Decision (2021/914) of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, or any subsequent or amended or new version thereof released by the European Commission, or (ii) required by law.

7. Limitation of liability

To the extent allowed under Data Protection Legislation, each Party's liability under this DPA shall be limited to liability for direct costs incurred by the other Party as a result of negligence, and consequently excluding lost profit and any form of indirect or consequential loss or damage.

8. Term and termination

The DPA is applicable from signing of the Agreement and for as long as the Processor processes Personal Data on behalf of the Controller. A Party is entitled to terminate this DPA with immediate effect if the other Party commits a material breach of its obligations pursuant to this DPA which is not remedied within thirty (30) days of such Party being notified of the breach by the non-defaulting Party.

Upon termination of the Agreement, the Processor shall cease with all processing activities conducted on behalf of the Controller. The Processor must delete or return all Personal Data to the Controller as requested at the end of the Agreement.

9. Governing law and dispute resolution

The provisions on governing law and dispute resolution in the Agreement shall apply also to this DPA.

SCHEDULE 1 - DATA PROCESSING INSTRUCTIONS

Purposes and subject matter	The purposes of the processing are the delivery of the following services or tasks by the Processor to the Controller: The cloud-based service Integrity which facilitates the management of reporting channels under Whistleblowing Laws (as defined in the Terms).
Categories of data	Categories: initially, the information provided in the report by the data subject is registered. Such information may include a) contact information (e.g. name, address, e-mail address and telephone number) of the individual who submitted the report and the individual(s) to whom the complaint relates and b) details of the wrongdoing as well as c) any other personal data related to individuals mentioned in the report or in consequential messages in the Software (which may include sensitive personal data such as information about sexual harassment in the workplace). In the event the report leads to an investigation, additional information required to investigate the suspicious wrongdoing will be added. This includes primarily the name of the suspected wrongdoer, position, details of the wrongdoing and such circumstances that form the basis for the report. Information will further be collected from the sources considered necessary to investigate the suspicious wrongdoing.
Categories of Data Subjects	"whistleblowers", which means all persons who files a report through the Software and who are working for the Controller under a contract of employment, or otherwise performing tasks through which they can become whistleblowers "suspected wrongdoers", which means all persons mentioned in a report, message and/or investigation who are working for the Controller under a contract of employment, or otherwise performing tasks through which they can become suspected wrongdoers
Physical location of servers	Ireland
Location ofProcessing	France, Ireland, Luxembourg, Netherlands, Portugal and Sweden
Storage, disposaland processing of Personal Data	The Processor shall promptly delete Personal Data upon the Controller's written request.
Approved Sub-processor(s)	- Euronext Corporate Services B.V. Company location: Netherlands. Processing in France, Portugal, Ireland, Luxembourg and Netherlands. <u>Euronext Corporate Services in turn engages:</u> - Amazon Web Services EMEA SARL ("AWS"). Company location: Luxembourg. Processing in France, Ireland, Luxembourg. <u>We have configured the engagement of AWS consciously to steer processing to companies within EU/EEA. AWS engages the following sub-processors:</u> Digital infrastructure and storage: - Amazon Data Services Ireland Limited. Company location: Ireland. Processing location: Ireland Support: - Amazon Development Centre Ireland Limited. Company location: Ireland. Processing location: Ireland.
Transfer to Third Countries	Personal Data may only be transferred to Third Countries in accordance with the terms of this DPA, unless otherwise agreed between the Parties.
Reporting of Personal Data Breach	The Processor shall notify the Controller of any personal data breach in connection with the processing of Personal Data to the email address set out in the Agreement.

SCHEDULE 2 - TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES

Access control to premises and facilities *Technical and organizational measures to control access to premises and facilities, particularly to check authorization*	• Access control system • ID reader, magnetic card, chip card • (Issue of) keys • Door locking (electric door openers etc.) • Security staff, janitors • Surveillance facilities • Alarm system, video/CCTV monitor
Access control to systems *Technical (ID/password security) and organizational (user master data) measures for user identification and authentication*	• Password procedures (incl. special characters, minimum length, change of password) • Automatic blocking (e.g. password or timeout) • Encryption of data media
Access control to data *Requirements-driven definition of the authorization scheme and access rights, and monitoring and logging of accesses*	• Differentiated access rights (profiles, roles, transactions and objects) • Reports • Access • Change • Deletion
Disclosure control *Measures to transport, transmit and communicate or store data on data media (manual or electronic) and for subsequent checking*	• Encryption/tunneling (VPN = Virtual Private Network) • Electronic signature • Logging
Input control *Measures for subsequent checking whether data have been entered, changed or removed (deleted), and by whom*	• Logging and reporting systems
Availability control *Measures to assure data security (physical/logical)*	• Backup procedures • Mirroring of hard disks, e.g. RAID technology • Uninterruptible power supply (UPS) • Remote storage • Anti-virus/firewall systems • Disaster recovery plan
Segregation control *Measures to provide for separate processing (storage, amendment, deletion, transmission) of data for different purposes*	• “Internal client” concept / limitation of use • Segregation of functions (production/testing)