EURONEXT CORPORATE SOLUTIONS

## EURONEXT CORPORATE SERVICES: INFORMATION SECURITY & DATA PRIVACY OVERVIEW

Dear Client,

We are pleased to share with you our Security and Data Privacy Overview, which outlines the comprehensive measures we have implemented to protect your data and ensure compliance with the General Data Protection Regulation (GDPR) and other applicable data protection laws.

At Euronext, safeguarding our clients' information is integral to everything we do. We have invested significantly in robust Technical and Organisational Measures (TOMs) that align with the requirements of Article 32 of the GDPR and industry best practices. These measures are regularly reviewed and enhanced to respond to evolving legislative, technological, and operational landscapes.

The enclosed overview highlights:

- Our adherence to the ECS Standard for Data Protection and Information Security, ensuring consistency and quality of data protection across all ECS entities.
- Our ISO/IEC 27001 certifications, which demonstrate our commitment to internationally recognised information security standards.
- Service-specific TOMs designed to meet the unique requirements of each service offering.
- Our structured approach to Data Processing Agreements (DPAs), which ensures that all contractual arrangements maintain the same high level of data protection and operational flexibility.

We understand that our clients have diverse needs and expectations, and we are committed to collaborating closely with you to address any specific requirements or concerns. Should you wish to discuss any aspect of this overview or require further clarification on how our practices align with your organisation's compliance obligations, please do not hesitate to reach out to me or your dedicated Euronext representative.
Thank you for placing your trust in Euronext. We look forward to continuing our partnership and supporting your business objectives with the highest standards of data protection and information security.

## OUR COMMITMENT TO INFORMATION SECURITY AND DATA PRIVACY

At Euronext, the protection of client data is a fundamental pillar of our operational philosophy. We are unwavering in our commitment to complying with the General Data Protection Regulation (GDPR) and all other applicable data protection laws. We have designed and implemented robust Technical and Organisational Measures (TOMs) that align with the principles set forth in Article 32 of the GDPR, ensuring an appropriate level of security tailored to the risks associated with our services.

Our TOMs are subject to regular and systematic review to adapt to changes in legislation, risk landscapes, and technological advancements, ensuring that our security practices remain effective, proportionate, and current.

## HOW WE SAFEGUARD PERSONAL DATA

### a. Adherence to the ECS Standard

All Euronext Corporate Services (ECS) entities operate under the ECS Standard for Data Protection and Information Security. This comprehensive internal framework ensures that personal data is consistently protected across all ECS entities, regardless of ISO certification status.

**Key features of the ECS Standard include:**

- **Physical and logical access controls:** Strict access management, including secure perimeter controls, secure entry points, and logging of physical access.
- **Role-Based Access and authorisation management:** Access to data is restricted to authorised personnel only, based on defined roles and business needs, ensuring adherence to the principle of least privilege.
- **Secure transmission of data:** All data in transit is encrypted using industry-standard protocols to ensure confidentiality and integrity.
- **Data integrity and audit logging:** Comprehensive audit logs and traceability mechanisms enable oversight and accountability for all data processing activities.
- **Data availability and redundancy:** Robust backup procedures, redundant systems, and failover mechanisms ensure continuity of service and data resilience.
- **Secure software development practices:** Secure coding standards, regular code reviews, and vulnerability management are integrated into the development lifecycle.
- **Incident response and review mechanisms:** Dedicated procedures for prompt detection, investigation, containment, and resolution of

security incidents, complemented by systematic post-incident reviews and improvements.

### b. ISO/IEC 27001 Certifications

Several ECS entities have achieved certification under the ISO/IEC 27001 standard, underscoring Euronext's commitment to internationally recognised best practices in information security management. Certification requires rigorous third-party audits covering areas such as governance, risk assessment, data encryption, monitoring, and continuous improvement.

**Currently certified ECS entities include:**

- **iBabs:** ISO/IEC 27001 and ISO 9001.
- **Company Webcast (CWC):** ISO/IEC 27001.
- **InsiderLog:** ISO/IEC 27001.
- **IntegrityLog:** ISO/IEC 27001.
- **IR.Manager:** ISO/IEC 27001.
- **Euronext Academy:** ISO9001.

These certifications reflect our dedication to upholding the highest standards of information security management and our ongoing investment in best-in-class security practices.

## SERVICE-SPECIFIC SECURITY MEASURES

In addition to the ECS Standard, Euronext implements tailored Technical and Organisational Measures (TOMs) for each service, reflecting the unique operational, technical, and risk profiles of individual offerings.

**Our service-specific TOMs include:**

- **Access Control to Premises:** Implementation of multi-layered security measures, including ID readers, security badges, electronic locks, CCTV surveillance, and on-site security personnel.
- **System Access Control:** Enforcement of stringent password policies, session timeouts, automatic account blocking, and local storage encryption to prevent unauthorised access.
- **Data Access Control:** Application of role-based access controls, with documented authorisation processes and comprehensive audit logging to ensure accountability and transparency.

- **Data Disclosure Control:** Use of secure VPN connections, robust encryption protocols for data in transit, electronic signatures, and logging of all data transfers to mitigate risk of unauthorised disclosure.
- **Input Control:** Implementation of logging and audit trails capturing all data creation, modification, and deletion events to ensure data integrity and traceability.
- **Availability Control:** Deployment of data backup strategies, RAID disk mirroring, uninterruptible power supply (UPS), failover mechanisms, anti-virus and firewall protection, and comprehensive disaster recovery plans.
- **Segregation Control:** Logical and operational segregation of production and testing environments, as well as strict data separation between clients, to prevent unauthorised cross-access.
- **Ongoing Security Reviews:** Regular internal audits, ad-hoc reviews following significant business or regulatory changes, and external penetration testing-particularly for high-risk processing activities-to identify and remediate vulnerabilities.

These measures are designed not only to protect personal data but also to ensure the resilience, reliability, and continuity of our services.

## AI GOVERNANCE AND CONTRACTUAL SAFEGUARDS

Euronext Corporate Services (ECS) applies a responsible approach to Artificial Intelligence (AI). Whenever AI functionality is offered within our services, it is always optional, disabled by default, and can only be activated at a client's request. Clients retain full ownership of their data, while ECS and its technology partners retain ownership of the AI systems themselves. Data processed through AI assistants is handled exclusively within secure environments (such as Microsoft Azure in the EU/EEA) and is never used to train or fine-tune AI models. Clients are responsible for ensuring lawful use of AI outputs and for informing end users when they interact with AI tools, including obtaining consent where required.

AI outputs are provided on an "as-is" basis, with human validation remaining essential before any content is stored or shared. These principles are also embedded in our contractual framework. This contractual framework sets out clear rules on ownership, lawful use, security, and transparency. By applying these safeguards consistently, ECS ensures that AI within our services is deployed in a transparent, compliant, and responsible manner, with clients always in control.

## OUR APPROACH TO DATA PROCESSING AGREEMENTS (DPAS)

As part of our commitment to transparency and consistency, Euronext typically proposes its own DPA template to clients. This template is meticulously drafted to align with our TOMs, ensuring that data protection rights and obligations are consistently applied across all client relationships.

**Key features of our standard DPA include:**

- **Data Breach Notification:** Commitment to notify clients "without undue delay" following the discovery of a personal data breach, in line with Article 33 of the GDPR, while ensuring accuracy and coordinated communication.
- **Liability Limitations:** Inclusion of clear financial caps on liability aligned with contractual values, ensuring proportionate and manageable risk allocation under Article 82 GDPR.
- **Sub-Processor Management:** Adoption of a flexible approach allowing for sub-processor engagements with appropriate notice to clients, balanced with clients' rights to object-ensuring operational flexibility without compromising transparency. A list of our sub-processors can be found online.

In exceptional circumstances where clients propose their own DPA templates, Euronext undertakes a thorough legal and security review of all critical clauses. Particular attention is paid to data breach notification timelines, liability caps, and sub-processor approval requirements to ensure alignment with Euronext's risk management principles and operational requirements.

## SUPPORT WITH DATA PROTECTION IMPACT ASSESSMENTS (DPIAS)

Euronext Corporate Services (ECS) recognises the importance of Data Protection Impact Assessments (DPIAs) for clients under Article 35 GDPR. As the majority of ECS services are provided in the role of a data processor, ECS cannot conduct DPIAs on behalf of clients. However, we are committed to supporting our clients in meeting their obligations by providing the necessary technical, organisational, and contractual information.

### How ECS supports clients

When ECS acts as data processor, we will:

- Provide detailed documentation on our Technical and Organisational Measures (TOMs), including encryption, access controls, monitoring, and audit logging.
- Share information about our hosting environments, security certifications, and service-specific measures.
- Make available an up-to-date list of sub-processors and their safeguards.
- Respond to specific questionnaires or requests for clarification to support your own DPIA process.

- 

When ECS acts as data controller, we will:

- Carry out our own DPIA assessments where required, in line with Article 35 GDPR and the ECS Standard for Data Protection and Information Security.
- Provide transparency about the scope of processing, the categories of data processed, and applicable risk mitigation measures.
- Ensure that clients are informed of their own obligations when sharing personal data with ECS in a controller-to-controller context.

**Collaboration with clients**

While the responsibility for performing and finalising a DPIA always remains with the data controller, ECS ensures that all relevant information is accessible and that our teams are available to support clients' risk assessments. Clients may contact their ECS representative or the Euronext DPO (dpo.ecs@euronext.com) to request documentation or assistance in connection with DPIAs.

## OUR ROLES UNDER DATA PROTECTION LAW: CONTROLLER OR PROCESSOR

Euronext Corporate Solutions (ECS) delivers a wide range of products and services, each with distinct operational models and data flows. Depending on the nature of the service and the associated processing activities, ECS may act either as a data processor (processing personal data on behalf of the client) or as an independent data controller (determining the purposes and means of the processing).

This distinction is clearly reflected in our contractual framework and supports compliance with Article 28 and Article 24 of the GDPR. The data processing role is defined per product and formalised in the signed contract documents, including the service-specific terms and applicable data processing addenda (DPAs).

**a. When ECS acts as a data processor**

For most ECS products, ECS acts as a data processor. This includes situations where ECS processes personal data strictly based on the client's documented instructions and for the performance of the contracted service. Examples include:

- IR.Manager
- Company Webcast
- iBabs
- InsiderLog
- IntegrityLog

 

• Shareholder Analysis

In these cases, the relevant DPA is included either in the ECS General Terms or appended as a signed document. It outlines data protection obligations, sub-processing rules, notification timelines, and other GDPR-aligned safeguards.

**b. When ECS acts as an independent controller**

In certain contexts, ECS determines its own purposes and means of processing. This typically applies where ECS delivers expertise-based services or engages in direct client relationship management, training, or advisory work. In such cases, ECS operates as an independent data controller. Examples include:

- Post Listing & ESG Advisory
- Euronext Academy (unless ECS processes personal data on the client's behalf, in which case a DPA is added under Article 15.5 of the Master Services Agreement)

When ECS acts as a controller, the data protection obligations are outlined in the General Terms and service-specific terms. These include transparency commitments, data subject rights, and security standards.

The ECS contract framework, including General Terms, Service Terms, Order Forms, and DPAs, ensures that roles and responsibilities are clearly documented, transparently assigned, and compliant with applicable law.

## SCOPE OF ECS PRODUCTS AND APPLICABILITY

The information security and data protection measures described in this overview apply across the full suite of Euronext Corporate Services (ECS) products and platforms. These include both long-standing and newly introduced services, all of which are subject to the ECS Standard for Data Protection and Information Security, as well as product-specific Technical and Organisational Measures (TOMs).

ECS continuously reviews and updates its risk assessments and data protection practices for each product. For new or evolving services, Data Protection Impact Assessments (DPIAs) are conducted to ensure compliance and to anticipate privacy risks.

The following ECS products and services are covered by our security and privacy framework:

- iBabs

- Company Webcast
- ComplyLog:
  - InsiderLog
  - IntegrityLog
  - TradeLog
  - LiabilityLog
- Shareholder Analysis
- ECS Academy
- Post-Listing Advisory
- ESG Advisory

## CONCLUSION

Information security and data privacy are cornerstones of Euronext's commitment to our clients. We invest continuously in maintaining and enhancing the security of our systems, processes, and contractual frameworks to safeguard personal data and uphold the trust our clients place in us.

For further information regarding our information security measures, or to discuss your specific requirements, please contact your Euronext representative.