GENERAL DATA PROTECTION REGULATION (GDPR) POLICY

LAST UPDATE: DECEMBER 2024

Kuylenstierna & Skog S.A.
74, Grand Rue, L-1660 Luxembourg
Tel: +352 22 95 15
Email: k-s@k-s.lu
www.k-s.lu
VAT: LU 18229523 – RCS: B 74203

Kuylenstierna & Skog S.A. – filial
Birger Jarlsgatan 55, S-111 45 Stockholm
Tel: +46 8 795 24 60
Email: k-s@k-s.se
www.k-s.se
Org. Nr. 516411-0586

CONTENTS

1. Introduction and Purpose

Kuylenstierna & Skog S.A.(“K&S”) has prepared this **GDPR Compliance Procedure** in the aim to establish a framework for the protection of personal data, define the roles and responsibilities of key stakeholders, and ensure that the handling and processing of personal data meet all legal and regulatory requirements.

The purpose of this procedure is to:

- Ensure that K&S is compliant with GDPR and relevant local regulations in Luxembourg, such as **CSSF Circular 20/750**.
- Safeguard the privacy and integrity of personal data processed by K&S.
- Define the legal and procedural bases for personal data processing.
- Establish clear guidelines for responding to data subject rights requests, handling data breaches, and maintaining proper documentation.

  www.cssf.lu/wp-content/uploads/cssf20_750eng.pdf

2. Scope

This procedure applies to:

- All **personal data** processed by K&S family office and portfolio management services.
- All activities involved in the collection, storage, processing, and transfer of personal data.
- Data subjects including clients (individuals and entities), employees, and third-party contractors.
- Data controllers who determine the reason for collecting personal data (purpose for managing client portfolios, ensuring compliance with regulations (i.e., **MiFID II**) and performing (KYC/AML).
- Data processors and sub-processors involved in personal data processing.

3. Relevant Regulations, Directives, and Circulars

K&S´s compliance with GDPR and Luxembourg law must consider the following:

- **General Data Protection Regulation (GDPR) (EU) 2016/679** of the European Parliament and the Council of 27 April 2016, and repealing Directive 95/46/EC: The central regulation for data protection and privacy in the EU.

- **Directive (EU) 2019/2034 on the prudential supervision of investment firms**: Sets requirements for firms supervised by the **CSSF**, particularly **Group 3 investment firms**.

- **MiFID II (Directive 2014/65/EU)**: Regulates investment services, including portfolio management and client protection.

- **CSSF Circular 20/750**: Outlines requirements for outsourcing arrangements and third-party data processors.

- **Luxembourg Data Protection Act (2018)**: Complements the GDPR at the national level.

4. Data Protection Officer (DPO) Responsibilities

The **Data Protection Officer (DPO)** plays a central role in the firm's GDPR compliance efforts.

The DPO's responsibilities include:

- **Monitoring Compliance**: Ensure that all data processing activities are in line with GDPR, relevant Luxembourg laws, and regulatory guidance.

- **Conducting Data Protection Impact Assessments (DPIAs)**: Lead the firm's DPIAs for new projects, products, services, or changes in data processing activities.

- **Advising on Data Protection**: Provide advice and recommendations to management regarding data protection and privacy matters.

- **Training and Awareness**: Develop and deliver regular data protection training programs for staff, ensuring they understand GDPR obligations and the firm's internal policies.

- **Handling Data Subject Rights Requests**: Act as the point of contact for data subjects exercising their rights (access, rectification, erasure, etc.).

- **Liaising with Authorities**: Communicate with the **National Data Protection Commission (CNPD)** and other supervisory authorities on data protection matters.

- **Notification of Data Breaches**: The DPO must notify the relevant supervisory authority (i.e., **CNPD**) of any personal data breach **within 72 hours of becoming aware of it**, as per **GDPR Article 33**. In certain cases, affected data subjects must also be informed. (See Point 8)

- **Record-Keeping**: Ensure proper documentation and maintenance of records related to data processing activities as required by GDPR Article 30.

5. Personal Data Handling: Types of Data and Purpose of Processing

5.1 Types of Personal Data Collected

Investment firms, family offices, and portfolio management firms process various types of personal data, including but not limited to:

"Personal data" includes any information that enables one to identify a natural person directly (first name, surname) or indirectly (passport number or data combination). Personal data of Data Subjects we process may include:

- **Identification data**: names, addresses, telephone numbers, email addresses, business contact information.
- **Personal characteristics**: date of birth, country of birth, nationality.
- **Professional information**: employment and job history, title, professional background, representation authorities.
- **Identifiers issued by Public Authorities**: passport, identification card, tax identification number, national insurance number, social security number.
- **Financial information**: financial and credit history information, bank details, financial assets, income.
- **Transaction / investment data**: current and past investments, investment profile, investment preferences and invested amount, number and value of shares held, role in a transaction (seller / acquirer of shares), transaction details.
- **Risk Profile:** Risk tolerance, financial objectives and other investment-related preferences

5.2 Purpose of Processing Personal Data

Personal data is processed for several purposes in accordance with **GDPR Article 6** and **Article 9** (for special categories of data):

- **Client Onboarding and KYC/AML Compliance**: Personal identification and financial information for the purposes of **Know Your Customer (KYC)** and **Anti-Money Laundering (AML)**.

- **Contractual Obligations**: Data processing necessary for the execution of client contracts, including portfolio management, investment advice, and related services.

- **Regulatory Compliance**: Processing personal data to comply with legal obligations under **MiFID II**, **CSSF Circulars**, **AML laws**, and tax regulations.

- **Risk Management**: Assessing the financial risks associated with investments and managing the portfolios of clients.

- **Client Communications**: statements and regulatory disclosures related to the investments.

- **Outsourcing**: If outsourced services are used (K&S) has outsourced their IT Services to Convotis (i.e. IT services, data hosting), personal data may be processed by third-party service providers under **CSSF Circular 20/750**.

5.3 Legal Basis for Processing

As per **GDPR Article 6**, personal data processing must have one or more lawful bases, such as:

- **Consent**: For processing sensitive data or for marketing purposes.
- **Contractual Necessity**: For providing investment services under client agreements (i.e., portfolio management).
- **Legal Obligation**: To comply with regulations like **KYC/AML**, tax obligations, and other regulatory requirements.
- **Legitimate Interests**: Where processing is necessary for the firm's legitimate interests, such as fraud prevention or direct marketing.

6. Data Subject Rights

Investment firms must establish procedures to facilitate the exercise of data subject rights under **GDPR Chapter III**.

These include:

- **Right to Access**: Data subjects can request access to their personal data and obtain information on how it is processed.
- **Right to Rectification**: Data subjects can request the correction of inaccurate or incomplete personal data.
- **Right to Erasure**: Also known as the "Right to be Forgotten", data subjects can request deletion of their data in specific situations.
- **Right to Restriction of Processing**: In cases where data processing should be limited but not erased (i.e., when contesting the accuracy of the data).
- **Right to Data Portability**: Data subjects can request their data in a structured, commonly used format to transfer it to another service provider.
- **Right to Object**: Data subjects can object to data processing on the grounds of legitimate interest or for direct marketing purposes.

Procedure for Handling Data Subject Requests:

- Ensure that requests are processed within **30 calendar days**.
- Provide clear communication to the data subject about their rights.

- Verify the identity of the individual making the request to avoid unauthorized access.

7. Data Protection Impact Assessments (DPIAs)

A **Data Protection Impact Assessment (DPIA)** must be conducted in situations where data processing is likely to result in high risks to the rights and freedoms of data subjects, such as:

- New investments or financial products that involve large-scale data processing.
- Use of new technologies (i.e., AI, blockchain) in portfolio management or client analytics.
- Outsourcing to third-party data processors, especially those outside the EU.

The DPO is responsible for leading DPIAs, ensuring that any identified risks are mitigated appropriately.

8. Data Breach Management

A **Data Breach** occurs when there is an accidental or unlawful destruction, loss, alteration, or unauthorized access to personal data. Firms must have clear procedures for detecting, reporting, and mitigating data breaches, including:

- **Detection and Reporting**: Employees must promptly report any potential data breaches to the DPO.
- **Notification to Authorities**: Under **GDPR Article 33**, breaches must be reported to the **CNPD** within **72 hours** of detection if the breach is likely to result in a risk to data subjects' rights.
- **Notification to Affected Individuals**: If the breach poses high risk to individuals, they must be notified without undue delay.
- **Mitigation and Record-Keeping**: After handling a breach, the firm must assess the cause and take steps to prevent recurrence.

9. Data Retention and Disposal

- **Retention Policy**: Personal data should only be kept for as long as necessary to fulfill the purpose for which it was collected. Retention periods should comply with regulatory requirements such as **MiFID II** and **CSSF Circular 19/712**.
- **Data Disposal**: When personal data is no longer needed, it must be securely erased or anonymized.

10. Outsourcing and Third-Party Data Processors

When outsourcing services (i.e., IT support, data storage), the firm must ensure that third-party processors comply with GDPR requirements:

- **Due Diligence**: Conduct thorough vetting of third-party processors to ensure their compliance with data protection standards.

- **Data Processing Agreements (DPA)**: Enter into legally binding agreements that specify the data protection measures, audit rights, and responsibilities of third-party processors under **GDPR Article 28**.

11. Record-Keeping and Documentation

The firm must maintain accurate records of data processing activities as required by **GDPR Article 30**. These records must include:

- The purposes of processing.

- Categories of personal data and data subjects.

- Data recipients, including third parties.

- Retention periods.

- Technical and organizational measures in place to ensure data security.

12. Training and Awareness

- **Staff Training**: Regular data protection training for employees to ensure they understand their responsibilities and the firm's obligations under GDPR.

- **Ongoing Monitoring**: Periodic reviews and refresher courses to keep up with regulatory updates and best practices.

13. Internal Audits and Compliance Checks

The firm must conduct **regular internal audits** to assess GDPR compliance, review data protection practices, and identify areas for improvement. The **DPO** should oversee this process and ensure that any non-compliance issues are addressed promptly.

14. Sanctions and Penalties

Failure to comply with GDPR can result in significant penalties, including:

- **Fines** of up to **€20 million** or **4% of global turnover**, whichever is higher.

- **Corrective actions** may be imposed by the CNPD, such as warnings, suspension of processing, or orders to rectify violations.