KUYLENSTIERNA & SKOG S.A.
ASSETMANAGEMENT

# GENERAL DATA PROTECTION REGULATION (GDPR) POLICY

LAST UPDATE: April 2026

**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 established this GDPR Compliance Procedure to provide a structured framework for the protection of personal data, define the roles and responsibilities of key stakeholders, and ensure that the collection, processing, storage, and transfer of personal data comply with applicable legal and regulatory requirements.

The objectives of this Procedure are to:

- Ensure compliance with the General Data Protection Regulation (GDPR) (EU) 2016/679 and relevant Luxembourg regulations, including CSSF Circular 20/750.
- Safeguard the privacy, integrity, and confidentiality 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 requests, managing data breaches, and maintaining accurate and complete records.

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

## 2. Scope

This Procedure applies to:

- All personal data processed by K&S in the context of family office and portfolio management services.
- All activities related to the collection, storage, processing, and transfer of personal data.
- Data subjects including clients (natural persons and legal entities), employees, and third-party contractors.
- Data controllers, who determine the purposes and means of processing personal data (e.g., portfolio management, KYC/AML compliance).
- Data processors and sub-processors engaged by K.

**Outsourced ICT Services**: IT and data hosting services are outsourced to Convotis, a Luxembourg PSF under CSSF supervision, which must comply with GDPR and CSSF Circular 22/806 on outsourcing arrangements.

www.cssf.lu/wp-content/uploads/cssf22_806eng.pdf

## 3. Relevant Regulations, Directives, and Circulars

K&S's GDPR compliance framework aligns with the following legal and regulatory instruments:

- **General Data Protection Regulation (GDPR) (EU) 2016/679** – the core EU regulation governing personal data protection and privacy.
- **CSSF Circular 22/806** – requiring PSFs to comply with GDPR and Luxembourg supervisory expectations (CNPD).

- **Directive (EU) 2019/2034** – prudential supervision of investment firms, particularly relevant for Group 3 IFs.

- **MiFID II (Directive 2014/65/EU)** – investment services and client protection requirements.

- **CSSF Circular 20/750** – outsourcing arrangements and third-party data processors.

- **Luxembourg Data Protection Act (2018)** – national complement to GDPR.

## 4. Data Protection Officer (DPO) Responsibilities

The Data Protection Officer (DPO) is responsible for overseeing K&S's GDPR compliance.

Key responsibilities include:

- **Monitoring Compliance** – Ensuring all data processing activities comply with GDPR, Luxembourg law, and regulatory guidance.

- **Data Protection Impact Assessments (DPIAs)** – Leading DPIAs for new projects, products, services, or material changes in processing activities.

- **Advisory Role** – Providing guidance and recommendations to management on privacy matters.

- **Training and Awareness** – Conducting regular staff training to ensure understanding of GDPR obligations.

- **Handling Data Subject Rights Requests** – Acting as the primary contact for individuals exercising GDPR rights (access, rectification, erasure, etc.).

- **Liaison with Authorities** – Communicating with the CNPD and other supervisory authorities as needed.

- **Data Breach Notification** – Notifying CNPD within 72 hours of a personal data breach per GDPR Article 33 and informing affected data subjects where high risk exists.

- **Record-Keeping** – Ensuring proper documentation of processing activities in accordance with GDPR Article 30 for a minimum of 10 years.

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

## 5.1 Types of Personal Data Collected

K&S processes various personal data categories, including:

- **Identification data** – Names, addresses, phone numbers, email, business contacts.

- **Personal characteristics** – Date and place of birth, nationality.

- **Professional information** – Employment history, title, professional background, representation authorities.
- **Identifiers issued by public authorities** – Passport, national ID, tax ID, social security numbers.
- **Financial information** – Bank details, income, financial assets, credit history.
- **Transaction and investment data** – Investment history, profile, preferences, number/value of shares, transaction roles.
- **Risk profile** – Risk tolerance, financial objectives, investment preferences.

## 5.2 Purpose of Processing Personal Data

Personal data is processed for:

- **Client onboarding and KYC/AML compliance** – Verifying identity and assessing financial risks.
- **Contractual obligations** – Executing client agreements including portfolio management and advisory services.
- **Regulatory compliance** – Fulfilling obligations under MiFID II, CSSF Circulars, AML/CTF, and tax laws.
- **Risk management** – Assessing investment and financial risks.
- **Client communications** – Sending statements, disclosures, and regulatory reports.
- **Outsourcing** – Allowing third-party service providers to process personal data under binding agreements.

## 5.3 Legal Basis for Processing

Processing is conducted based on:

- **Consent** – For sensitive data or marketing purposes.
- **Contractual necessity** – To deliver services under client agreements.
- **Legal obligation** – To comply with regulatory requirements (e.g., KYC/AML, tax, reporting).
- **Legitimate interests** – Where necessary for fraud prevention or other business purposes, balanced against data subjects' rights.

## 6. Data Subject Requests

- Requests must be processed within **30 calendar days**.
- Identity verification of the requester is mandatory.
- Clear communication on the rights and actions taken must be provided.

## 7. Data Protection Impact Assessments (DPIAs)

DPIAs must be conducted for high-risk processing, including:

- Large-scale financial data processing for new investment products.
- Use of emerging technologies (AI, blockchain) affecting personal data.
- Outsourcing to third-party processors, especially outside the EU.

The DPO is responsible for ensuring mitigation of identified risks.

## 8. Data Breach Management

- Detection & Reporting – Employees must report suspected breaches immediately to the DPO.
- Notification to Authorities – CNPD must be notified within 72 hours per GDPR Article 33.
- Notification to Data Subjects – Required if breach poses high risk.
- Mitigation & Documentation – Breaches are investigated, mitigated, and documented with corrective actions

## 9. Data Retention and Disposal

### 9.1. Retention Periods

- Client data – Retained for 5 years, extendable to 7 years if required by authorities, maximum 10 years after end of business relationship.
- Employee data – Retained for 5 years, extendable to 7 years if required, maximum 10 years post-employment.
- Transaction records – Retained for 5–7 years, maximum 10 years, per CSSF and AML requirements.

### 9.2. Archiving

- Archived data is **encrypted, access-controlled, and restricted** to authorized personnel.
- Annual review of archived data ensures continued necessity or safe deletion.

- Records of Processing Activities (RoPA) are maintained and reviewed yearly alongside the Business Continuity Plan (BCP).

See our: **Record of Processing Activities (RoPA) saved under: T/IT/KS01 GDPR**

## 10. Outsourcing and Third-Party Data Processors

- **Due diligence** – Third-party processors are assessed for GDPR compliance.

- **Data Processing Agreements (DPA)** – Legally binding agreements per GDPR Article 28, defining responsibilities, audit rights, and safeguards.

## 11. Record-Keeping and Documentation

Records of processing activities are maintained for **10 years** in accordance with GDPR Article 30.

## 12. Training and Awareness

- **Annual training programs for all staff.**

- **Ongoing monitoring and refresher courses aligned with regulatory updates.**

## 13. Internal Audits and Compliance Checks

- DPO oversees periodic audits of data protection practices.
- Non-compliance issues are documented and remediated promptly.

## 14. Sanctions and Penalties

- Non-compliance can result in fines up to **€20 million or 4% of global turnover**.

- Supervisory corrective measures may include warnings, suspension of processing, or orders to rectify violations.