KUYLENSTIERNA & SKOG S.A.
ASSETMANAGEMENT

GENERAL DATA PROTECTION REGULATION (GDPR) POLICY

LAST UPDATE: JULY 2023

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. Purpose, Intention and Definitions

According to regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016, and repealing Directive 95/46/EC, Kuylenstierna & Skog (“K&S” hereinafter “the Company”) have prepared the following General Data Protection Regulation Policy (GDPR).

This Regulation lays down rules relating to the protection of natural persons regarding the processing of “personal data” means any information relating to an identified or identifiable natural person (Data Subject). A (Data Subject) is one who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

This Regulation lays also down rules relating to the free movement of personal data. It protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data and the free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons regarding the processing of personal data “processing” means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction

“Controller” means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

“Processor” means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

2. Internal Information

The Company **processes** information and personal data relating to any natural person i.e., any data subject and/or any **Related Person** to the **Data Subject**.
In substance, the Company does so in connection with existing and/or prospective business relationships, this relates also to the use of the Company’s website.
The Company processes it as either Controller or as joint Controller.

A "**Related Person**" means an individual or entity whose information the data subject or a third party provides to the Company and/or which otherwise comes to the Company’s knowledge in connection with the Business Relationship. A Related Person may include, but is not limited to, (i) any director, officer or employee of a company (ii) any nominee or beneficial owner of an account, (iii) a substantial interest owner in an account, (iv) a controlling person, (v) a payee of a designated payment, or (vi) any representative(s) or agent(s) (e.g., with a power of attorney or a right of information on an account).

For any questions that may arise in relation to this GDPR Policy, the Controller, or more generally on the processing of the personal data, contact should be done directly to the Account Manager in charge of the relation or to the **Data Protection Officer** “DPO” (Rebecca Stenvall) of the Company.

The contact can be done to the following addresses:

Postal Address:

Kuylenstierna & Skog S.A.
74 Grand-Rue
L-1660 Luxembourg

or by E.Mail:

GDPR@k-s.lu

3. The handling of personal data

The Company is subject to certain confidentiality and/or secrecy obligations arising under data protection, contract, professional or banking secrecy.
Personal data processing is also subject to said obligations.

This GDPR Policy deals with the way the Company processes (i.e. collects, uses, stores, transmits, handles or processes collectively defined hereinafter as the "**Processing**" or "**Processing Operations**") personal data. This GDPR Policy does not replace and remains subject to the Company’s applicable contractual terms and conditions.

The Company may conduct the Processing Operations either directly or indirectly, through other parties which process personal data on the Company’s behalf (hereinafter the "**Processors**").

4. General description of CRM IT system

The system uses for the organization of data “**pseudonymization**” means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

Any data recorded for individuals, companies or accounts are given a unique key. The key is a sequence number with no connection with the data itself. This unique key is used throughout the system when storing information, separating the personal data from account records or any other data item. It is only possible to combine data about a person, company or account by using the unique key.

The data is kept on the server of the Data Provider of the company i.e., Calligo (Luxembourg) PSF S.A.
The location of the data is not accessible for users, and it is not possible to read, copy or modify the data directly. The data is encrypted according to the specification of the Data Provider.

Access to the data is only possible through the Databases server (MySQL). The server controls user access by a combination of:

- originating IP-address (location of user), only from the company internal network
- username, only for approved users
- password, only when correct password is provided for the user.

All users have designated access rules and may only insert, view, update or delete data that they have been given specific authorisation to by the user-access rules of the system. Any update is recorded with time and user making the update.

Please see the Company's IT Procedure for further information on security.

5. What personal data does the Company process?

"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.
- Professional information, employment and job history, title, representation authorities.
- Identifiers issued by public bodies, passport, identification card, tax identification number, national insurance number, social security number.
- Financial information, financial and credit history information, bank details.
- 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.

6. For what Purposes and on what legal bases does the Company process personal data?

The Company collects and processes personal data for the purposes (hereinafter "**the Purposes**") based on the legal bases set forth herein.

As a general comment, the Company essentially bases its Processing on (i) the performance of a contract to which the Data Subject or a Related Person is related (as well as to take pre-contractual steps at the Data Subject or a Related Person's request), (ii) the obligation to comply with a legal or regulatory obligation, (iii) the pursuit of the legitimate interest and (iv) the performance of a task carried out in the public interest (e.g., to prevent or detect offences).

More specifically, the Company collects and processes personal data as necessary for the performance of a contract to which the Data Subject and/or a Related Person is related, which includes the following **Processing Operations** (which may also be based upon other lawful bases):

- the opening and management of the Data Subject and/or Related Person's account or Business Relationship with the Company, including all related operations for the identification of the data subject.
- any other related services provided by any Service Provider of the Controller(s) and Processor(s) in connection with the Company's Business Relationship.
- the processing of subscription, conversion and redemption requests in investment funds, as well as for maintaining the ongoing relationship with respect to holdings in such investment funds.
- The Company also collects and processes personal data in relation to compliance with legal and regulatory obligations to which we are subject, including to:
- provides offering documentation to Data Subjects about products and services.
- complies with legal obligations relating to accounting, compliance with legislation on markets in financial instruments.
- carries out any other form of cooperation with, or reporting to, competent administrations, supervising authorities, law enforcement authorities and other public authorities (e.g., in the field of anti-money laundering and combatting terrorism financing ("AML-CTF")), for the prevention and detection of crime under tax law (reporting of name, address, date of birth, tax identification number (TIN), account number and account balance to the tax authorities under the Common Reporting Standard ("CRS") or Foreign Account Tax Compliance Act ("FATCA") or other tax legislation to prevent tax evasion and fraud as applicable);
- prevents fraud, bribery, corruption and the provision of financial and other services to persons subject to economic or trade sanctions on an on-going basis in accordance with our AML-CTF procedures, as well as to retain AML-CTF and other required records for screening purposes.
- deals with active intra-group risk management pursuant to which risks in terms of markets, credit, default, processes, liquidity and image as well as operational and legal risks must be identified, limited and monitored.
- records conversations with Data Subjects (such as telephone and electronic communications), to document instructions or detect potential or actual frauds and other offences.

The foregoing Processing Operations may rely on other lawful bases and eventually do substantially rely on the performance of a task carried out in the public interest.

Furthermore, the Company may process personal data in relation to legitimate interests the Company pursues in order to:

- assess certain characteristics of the Data Subjects based on personal data processed automatically (profiling) (see also Section 5 below).
- develop the Business Relationship with the Data Subject.
- improve the Company's internal business organisation and operations, including for risk management.
- use this information for market studies or advertising purposes, if relevant.
- assess the Company's risk and take related business decisions in case of risk management.
- establish, exercise and/or defend actual or potential legal claims, investigations or similar proceedings.
- record conversations with Data Subject(s) (such as telephone and electronic

communications) to verify instructions, enforce or defend our interests or rights, assess, analyse and improve the quality of our services, train our employees and manage risks.

The provision of personal data may be mandatory, i.e., in relation to the Company's compliance with legal and regulatory obligations to which the Company is subject to.

Please be aware that not providing such information may preclude the Company from pursuing a Business Relationship with, and/or from rendering services to the data subject.

7. Does the Company rely upon profiling or automated decision making?

The Company may assess certain characteristics of the Data Subjects based on personal data processed automatically, to provide Data Subjects with personalised offers and advice or information on the Company's products and services or those of the Company's affiliates and business partners. The Company may also use technologies that allow identifying the level of risks linked to a Data Subject or to the activity on an account.

Furthermore, the Company generally does not use automated decision making in connection with the Company's Business Relationship and/or Data Subject. Should the Company do so, it shall comply with applicable legal and regulatory requirements.

8. What sources are used to collect personal data?

To achieve the Purposes, the Company collects or receives personal data:

- directly from the Data Subject(s) when contacting the Company or through (pre-)contractual documentation directly sent to the Company.
- indirectly from other external sources, including any publicly available sources (i.e., UN or EU sanctions lists), and/or information available through subscription services. (i.e., Bloomberg/Infront) and/or information provided by other third parties.

9. Is personal data shared with third parties?

If necessary or useful to achieve the Purposes, the Company reserves the right to disclose or make accessible the personal data to the following recipients, provided this is legally or otherwise authorised or required:

- public / governmental administrations, courts, competent authorities (i.e., financial supervisory authorities) or financial market actors if needed (i.e., third-party or central depositaries, brokers, exchanges and registers).
- Third-party Processors that process personal data on the behalf of the Company and/or to which the Company outsources certain tasks (**outsourcing**).
- auditors or legal advisors.

The Company undertakes not to transfer personal data to any third parties other than those listed above, except as disclosed to Data Subject(s) from time to time or if required by applicable laws and regulations applicable to them or by any order from a court, governmental, supervisory or regulatory body, including tax authorities.

10. Is personal data transferred outside of the Company's jurisdiction of incorporation?

In relation to our Business Relationship, we may disclose, transfer and/or store personal data abroad (hereinafter "International Transfer") (i) in connection with the conclusion or performance of contracts directly or indirectly related to our Business Relationship, e.g., a contract with you or with third parties in your interest, (ii) when the communication is necessary to safeguard an overriding public interest, or (iii) in exceptional cases duly foreseen by applicable laws (e.g., disclosures of certain trades made on an exchange to international trade registers).

International Transfers may include the transfer to jurisdictions that (i) ensure an adequate level of data protection for the rights and freedoms of Data Subjects as regards to Processing, (ii) benefit from adequacy decisions as regards their level of data protection (e.g., adequacy decisions from the European Commission) or (iii) do not benefit from such adequacy decisions and do not offer an adequate level of data protection. In the latter case, we will ensure that appropriate safeguards are provided, e.g., by using standard contractual data protection clauses established by the European Commission.

Should you wish to have further information as regards International Transfers or appropriate safeguards, you may of course contact our Data Protection Officer (see Section 1 above).

11. What are the rights of the Data Subject in connection with data protection?

The Data Subject has the right, subject to applicable local data protection legislation to request access and receive a copy of the personal data we hold.

- if appropriate, request rectification or erasure of the personal data that are inaccurate.
- request the erasure of the personal data when the Processing is no longer necessary for the Purposes, or not or no longer lawful for other reasons, subject however to applicable retention periods (see Section 10 below).
- request a restriction of Processing of personal data where the accuracy of the personal data is contested, the Processing is unlawful, or if the Data Subject has objected to the Processing.
- object to the Processing of personal data, in which case the Company will no longer process the personal data unless it has compelled legitimate grounds to do so (i.e., the establishment, exercise or defence of legal claims).
- receive the personal data in structured, commonly used and machine-readable format (data portability right).
- obtain a copy of, or access to, the appropriate or suitable safeguards which the Company may have implemented for transferring the personal data outside of the European Union
- complain with the Company's Data Protection Officer (DPO) (see Section 2 above)

in relation to the processing of personal data on absence on a satisfactory resolution of the matter, file a complaint in relation to the processing of personal data with the relevant data Protection Supervisory Authority.

Even if a Data Subject objects to the processing of personal data, the Company has nevertheless is allowed to continue if the Processing is (i) legally mandatory, (ii) necessary for the performance of a contract to which the Data Subject is a party, (iii) necessary for the performance of a task carried out in the public interest, or (iv) necessary for the purposes of the legitimate interests we follow, including the establishment, exercise or defence of legal claims.

Subject to the limitations set forth herein and/or in applicable local data protection laws, the Data Subject can exercise the above rights by contacting free of charge the company's Data Protection Officer (DPO).

12. How long is personal data kept or stored?

As a matter of principle, the Company retains personal data for as long as needed.
By the same key (as mentioned in point 4), the Company will delete or anonymise personal data (or equivalent) once they are no longer necessary to achieve the Purposes, subject however (i) to any applicable legal or regulatory requirements to store personal data for a longer period, or (ii) to establish, exercise and/or defend actual or potential legal claims, investigations or similar proceedings, including legal holds, which we may enforce to preserve relevant information.

Calligo (Luxembourg) PSF S.A. will perform a quarterly screening of all E-mails and files saved on the server and delete all E-mails and files which have been last modified more than 10 years ago and no longer necessary to achieve the Purposes.

A screening will take place monthly in the Company's D3fine Database system and the following information will be deleted automatically from the D3fine Database system as per below:

Delete all entries more than 10 years old for the following:

- account balances
- account fees
- account fundholding
- account NAV
- account positions
- appropriateness form data
- audit connect log
- currency rates
- delta report data
- documents with maturity date more than 10 years ago
- history updates (account, subject, document)
- orderbook
- scorecard data
- security prices
- suitability data

(regardless of if the client and/or account is active or not):

Selection on the following

- accounts inactive more than 10 years ago
- clients with accounts inactive more than 10 years ago
- companies/individuals inactive more than 10 years and not linked to any account

For selection above: delete any/all related data regardless of entry/maturity, if the relevant data is not linked to another account/client which is still active (or inactive less than 10 years ago).

In this event the related data will only be deleted after 10 years (in list above) or when the last related account/client is deleted.

Delete all raw bank data (data feed) more than 4 months.
This data has been converted and harmonized in the database and added to working tables. Consequently, these are only held for backup and bug-fixe control.