GENERAL DATA PROTECTION REGULATION (GDPR) POLICY

LAST UPDATE: OCTOBER 2020

Kuylenstierna & Skog S.A.
74, Grand Rue, L-1660 Luxembourg
Postal address: BP 574, L-2015 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. Who is responsible for your personal data and whom can you contact?

We, Kuylenstierna & Skog S.A., process information and personal data relating to you and/or any Related Person of yours (Related Person(s) and you, together the hereinafter "Data Subject(s)"). In substance, we do so in connection with our existing and/or prospective business relationships, including your use of our website (together hereinafter the "Business Relationship"). We can do so either as controller or as joint controller (hereinafter the "Controller").

A "Related Person" means an individual or entity whose information you or a third party provides to us and/or which otherwise comes to our knowledge in connection with our 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).

In this context, we ask that you liaise with and transmit to any and all of your Related Persons this Privacy Notice, respectively the information contained therein.

For any questions you may have in relation to this Privacy Notice, your Controller, or more generally the processing of your (or your Related Persons') personal data, you may contact your Account Manager with us or our Data Protection Officer (Elisabeth Skog) at the following addresses:

Kuylenstierna & Skog S.A.
74 Grand-Rue
L-1660 Luxembourg
GDPR@k-s.lu

We, and this policy, comply with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on General Data Protection (“GDPR”), and The Law of 1 August 2018 establishing the National Commission for Data Protection and the implementation of Regulation (EU) 2016/679.

2. How do we handle your personal data?

We are subject to certain confidentiality and/or secrecy obligations, e.g., arising under data protection, contract, professional or banking secrecy, as the case may be. Personal data we process are also subject to said obligations.

This Privacy Notice deals with the way we process (i.e., collect, use, store, transmit or otherwise handle or process, collectively defined hereinafter as the "Processing" or "Processing Operations") personal data. This Privacy Notice does not replace, and is subject to, our applicable contractual terms and conditions.

We may conduct our Processing Operations either directly or indirectly, through other parties which process personal data on our behalf (hereinafter the "Processors"). We are responsible only for the Processing of personal data as per this Privacy Notice.

3. General description of CRM IT system

The system uses pseudonymization for the organization of data. 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. 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 our IT Procedure for further information on security.

4. What personal data do we process?

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

- Identification data, e.g., names, addresses, telephone numbers, email addresses, business contact information;
- Personal characteristics, e.g., date of birth, country of birth;
- Professional information, e.g., employment and job history, title, representation authorities;
- Identifiers issued by public bodies, e.g., passport, identification card, tax identification number, national insurance number, social security number;
- Financial information, e.g., financial and credit history information, bank details;
- Transaction / investment data, e.g., 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;

5. For what Purposes and on what legal bases do we process personal data?

We collect and process personal data for the purposes (hereinafter the "Purposes") and based on the legal bases set forth herein.

As a general comment, we essentially base our Processing on (i) the performance of a contract to which you are a party or a Related Person is related (as well as to take pre-contractual steps at your or a Related Person's request), (ii) our obligation to comply with a legal or regulatory obligation, (iii) the pursuit of our legitimate interest and (iv) the performance of a task carried out in the public interest

(e.g., to prevent or detect offences).

More specifically, we collect and process personal data as necessary for the performance of a contract to which you are a party 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 your and/or Related Person's account or Business Relationship with us, including all related operations for your identification;
- any other related services provided by any service provider of the Controller(s) and Processors in connection with our 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.
- We also collect and process personal data in relation to compliance with legal and regulatory obligations to which we are subject, including to:
- provide offering documentation to Data Subjects about products and services;
- comply with legal obligations relating to accounting, compliance with legislation on markets in financial instruments;
- carry 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 (e.g., 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);
- prevent 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;
- deal 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;
- record conversations with Data Subjects (such as telephone and electronic communications), in particular 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, we may process personal data in relation to legitimate interests we pursue in order to:

- assess certain characteristics of the Data Subjects on the basis of personal data processed automatically (profiling)(see also Section 5 below);
- develop our Business Relationship with you;
- improve our internal business organisation and operations, including for risk management;
- use this information for market studies or advertising purposes, if relevant;
- assess our 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 Subjects (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, e.g., in relation to our compliance with legal and

regulatory obligations to which we are subject. Please be aware that not providing such information may preclude us from pursuing a Business Relationship with, and/or from rendering our services to you.

6. Do we rely upon profiling or automated decision making?

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

Furthermore, we generally do not use automated decision making in connection with our Business Relationship and/or Data Subjects. Should we do so, we shall comply with applicable legal and regulatory requirements.

7. What sources do we use to collect your personal data?

To achieve the Purposes, we collect or receive personal data:

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

8. Do we share your personal data with third parties?

If necessary or useful to achieve the Purposes, we reserve 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 (e.g., financial supervisory authorities) or financial market actors if needed (e.g., third-party or central depositaries, brokers, exchanges and registers);
- Third-party Processors that process personal data on our behalf and/or to which we outsource certain tasks of ours (outsourcing);
- auditors or legal advisors.

We undertake not to transfer personal data to any third parties other than those listed above, except as disclosed to Data Subjects 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.

9. Are personal data transferred outside of our 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).

10. What are your rights in connection with data protection?

You have the right, subject to applicable local data protection legislation, to:

- request access to, 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 Subjects have objected to the Processing;
- object to the Processing of personal data, in which case we will no longer process the personal data unless we have compelling legitimate grounds to do so (e.g., 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 we may have implemented for transferring the personal data outside of the European Union
- complain with our Data Protection Officer (see Section 1 above) in relation to the Processing of personal data and, absent 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, we are nevertheless allowed to continue the same 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, you can exercise the above rights free of charge by contacting our Data Protection Officer.

11. How long are your personal data kept or stored?

As a matter of principle, we retain personal data for as long as we need the same to achieve the

Purposes. By the same token, we 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) S.A. will perform a quarterly screening of all emails and files saved on the server and delete all emails and files which are last modified more than 10 years ago and no longer necessary to achieve the Purposes.

A screening will take place monthly in our 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 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 year 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.