Scope and overview

Stifel Nicolaus Europe Limited (SNEL) and its EU and Swiss affiliates, subsidiaries, and related entities (collectively, "Stifel," "we," "us," or "our") are committed to protecting personal data, which means any information relating to an identified or identifiable natural person ("data subject," "you," or "your"). This document, together with any other documents referenced, explains how we may collect, use, disclose, or otherwise process your data. This Notice applies to your data irrespective of whether we obtain it from you or another source. This Notice also describes certain rights you have regarding such data.

This Notice is addressed to all data subjects except job candidates and employees. A separate disclosure addresses those other two categories of data subjects. You might interact with us in various capacities, including visitors to our website, clients and prospective clients (and individuals connected with our clients), contacts at firms we deal with in a non-client capacity, suppliers, visitors to our offices, etc.

Who is responsible for your data?

For the purposes of applicable data protection laws, notably the General Data Protection Regulation (GDPR), including its variants like the UK GDPR and the EU GDPR and all other applicable data protection laws, such as the Swiss Data Protection Act, Stifel is a data controller with associated responsibilities for your data. SNEL is incorporated in England and Wales (No. 03719559) with its registered address as shown in the footer below. SNEL is authorised and regulated in the United Kingdom by the Financial Conduct Authority (FCA) (Registration Number 190412). Stifel is also registered in other countries where it operates.

Collecting your data

- **Information you provide to us or to one of our authorized non-European affiliates.** This includes information you provide by filling in forms or communicating with us, whether face-to-face, by phone, e-mail, or otherwise. This information may include:
  - Basic personal data, such as first name, family name, national insurance number, e-mail address, telephone numbers, address (including city, postcode, and country), occupation and job title, identification documentation, date of birth, life events, and family information; and
  - Special categories of personal data, also known as sensitive data, such as data concerning health or data revealing political opinions.

- **Information we generate about you.** This may include:
  - Any file we may produce as a record of our relationship with our clients and prospective clients, including contact history; and
  - Any personal data we obtain in relation to your use of our websites.

- **Information we obtain from other sources.** This may include:
  - Information from publicly available sources, including third-party agencies, such as credit reference agencies, fraud prevention agencies, law enforcement agencies, public databases, registers and records, such as Companies House and the FCA Register, and other publicly available sources;
  - Information obtained from independent financial advisors, other professional advisers, product providers, event organisers, and other agents and/or representatives; and
  - Information obtained from sanctions checking and background screening providers.

Using your data

We may store, use, and otherwise process your data as applicable law permits or requires, including in the following ways and for the following purposes:

- To contact and interact with you to perform our contractual obligations to you or your organisation;
- To carry out our legal and regulatory compliance obligations, including anti-money laundering and terrorist financing checks and related actions which we consider appropriate to meet any legal or regulatory obligations imposed on us from time to time, or where the processing is in the public interest, or to pursue our legitimate interest to prevent fraud, bribery, corruption, tax evasion, and to prevent the provision of financial and other services

to persons who may be subject to economic or trade sanctions on an ongoing basis, in accordance with our anti-money laundering procedures;

- To monitor and record calls and e-mails to comply with our legal and regulatory obligations and ensure compliance with our policies and standards and for investigation and crime prevention purposes, and to enforce or defend our legal rights, or pursue our legitimate interests in relation to such matters;
- To report tax-related information to tax authorities in order to comply with our legal obligation;
- To monitor and record calls for quality, training, analysis, complaint resolution, and other related purposes in order to pursue our legitimate interest to improve service delivery;
- To manage our relationships with you, develop and improve our business and services, maintain and develop our IT systems, manage and host events, and to administer and manage our website, systems, and applications;
- To manage access to our premises and for security purposes;
- To protect the security of our communications and other systems and to prevent and detect security threats, frauds, or other criminal or malicious activities; and
- To provide you with information about our products and services that may be of interest to you as well as informing you of any changes to our service.

We may also process your data for purposes compatible with the ones listed above. If we need to process your data for an incompatible purpose, we will provide notice to you and, if required by law, seek your consent. We may process your data without your knowledge or consent where required by applicable law

We may process your data on the following basis:

- You consented to the processing;
- The processing is necessary to fulfil the performance of our contract with you, in our capacity as the data controller;
- The processing is necessary to comply with our legal obligations; and/or
- The processing is necessary for our legitimate interests, such as:
  - Managing and administering our business operations effectively and efficiently;
  - Maintaining compliance with internal policies and procedures;
  - Enabling quick and easy access to information on our services; and
  - Offering effective, up-to-date security solutions for mobile devices and IT systems.

We will not use your data for any automated decision-making that affects you or for creating profiles other than as described above.

Sharing your data

Generally, we may disclose your data to third parties where required by law or to our employees, contractors, designated agents, or certain third parties who process your data on our behalf, whom we permit to process your data only for specified purposes in accordance with our instructions. Specifically, we may disclose your data as follows:

- To our affiliated companies (including those located in the United States) for the above-mentioned purposes.
- To companies providing services for money laundering and terrorist financing checks and other fraud and crime prevention purposes and companies providing similar services;
- To courts, law enforcement authorities, regulators, governmental officials, and other bodies as required by law or as requested;
- To third-party vendors in order to process the data for the above-mentioned purposes;
- To our and our affiliated companies' professional advisers, subject to confidentiality obligations;
- If we have collected your data in the course of providing services to any of our clients, we may disclose it to that client and, where permitted by law, to others for the purpose of providing those services; and
- To purchasers of the whole or part of our business or on any merger or group reorganisation.

Transferring your data to foreign destinations

Your data may be transferred to a foreign destination where it may be processed by staff working for our affiliates or suppliers (see here for all Stifel Europe locations – https://stifelinstitutional.com/global-coverage/europe/). For all such transfers, we will ensure that your data is protected to comply with applicable domestic data protection laws. This can be done in a number of ways. For instance:

- The destination might be approved as an adequate jurisdiction under applicable domestic laws;
- The recipient might have signed up to a contract based on "model contractual clauses" approved under applicable domestic laws, obliging them to protect the data; or
- Where the recipient is located in the United States, it might be a participant in an appropriately approved certification scheme, such as the EU-US Data Privacy Framework (DPF), or its UK extension that establishes the UK-US data bridge.

Securing your data

We have implemented appropriate physical, technical, and organizational security measures designed to secure your data against accidental loss and unauthorized access, use, alteration, or disclosure. In addition, we limit access to personal data to those employees, agents, contractors, and other third parties that have a legitimate business need for such access. We require our third-party service providers, by written contract, to implement appropriate security measures to protect your data consistent with our policies and any data security obligations applicable to us.

Retaining your data

How long we hold your data will vary. Except as otherwise permitted or required by applicable law, we will retain your data only for as long as necessary to fulfil the purposes we collected it for, as required to satisfy any legal, accounting, or reporting obligations, or as necessary to resolve disputes. To determine the appropriate retention period for your data, we consider applicable legal requirements; the amount, nature, and sensitivity of the data; the potential risk of harm from unauthorized use or disclosure of the data; the purposes we process the data for; and whether we can achieve those purposes in other ways.

Your rights

You have a number of legal rights in relation to your data we process. These rights include:

- The right to obtain information regarding our processing and access to the data;
- The right to withdraw your consent to our processing of the data at any time. Please note, however, that we may still be entitled to process the data if we have another legitimate reason;
- In some circumstances, the right to receive some data in a structured, commonly used, and machine-readable format and/or request that we transmit those data to a third party where this is technically feasible. Please note that this right only applies to data you provided to us;
- The right to request that we rectify the data if it is inaccurate or incomplete;
- The right to request that we erase the data in certain circumstances. Please note that there may be circumstances where you ask us to erase the data but we are legally entitled to retain it;
- The right to object to, and the right to request that we restrict, our processing of the data in certain circumstances. Under some circumstances, however, we might be legally entitled to continue processing notwithstanding your objection or restriction request.

If you think we have infringed any of your rights, you may lodge a complaint with the appropriate data protection regulator. If you are in the UK, please contact the Information Commissioner's Office (ICO), or search their website at https://ico.org.uk/. If you are elsewhere in Europe, please contact the local data protection authority (DPA) or another supervising authority (SA) designated under local law.

Changes to this Notice

We reserve the right to update this Notice from time to time to reflect changes to the way we process your data or legal requirements. Whenever we update this Notice, we will post it on our website and/or, where appropriate, notify you by e-mail. Please check back frequently to see any updates to this Notice.

Contacting us

If you have any questions about this Notice, seek further details about any matter mentioned here, or want to exercise your rights listed earlier, please contact us by e-mailing EuropeDataOffice@stifel.com.