Data Processing and Privacy Notice

Last Updated: June 2019

At State Street, we are committed to transparency regarding how we provide services to our clients, the regulatory obligations to which we adhere and our strategy for data privacy and integrity. In addition to our established disclosure documents, we are pleased to provide this privacy notice. This notice addresses our global operating model and related policies, as well as how we store and control access to our clients' data. We believe that it is important for our global operating model to be understood by you in your relationship with State Street and its affiliates.

State Street Bank and Trust Company or one of its subsidiaries or affiliates companies (collectively "State Street"), needs to collect and process data, including personal data, in relation to providing contracted financial services. This Data Processing and Privacy Notice ("Notice") explains how that personal data is used. This Notice applies to all clients from whom State Street collects data in the course of providing the contracted for services.

How we use your personal data

We collect and use your data, including personal data, to enable us to manage our relationship with you effectively, lawfully and appropriately, during the course of providing you the above services both during and after the contractual period. This includes using information to enable us to comply with the contract, to comply with any legal requirements, pursue the legitimate interests of State Street and protect our legal position in the event of legal proceedings.

While any component of our services may be performed by our Global Processing Centers or any other State Street affiliate, the State Street affiliate with which you contract remains fully responsible for the delivery of services to you. In our operating model, the entity with which you contract is responsible for the quality of the services being provided by other members of our group and is ultimately responsible for determining whether to rely upon or require improvements to this operational footprint.

Types of Data We Collect and Process

The types of data relating to our clients that may be accessed by any of our affiliates, agents or service providers to provide services to clients, meet our regulatory obligations and/or manage our business may include the following:

- Information needed to comply with Anti Money Laundering (AML), Know Your Customer ("KYC") and Counter-Terrorism Financing (CTF) requirements.
    - Such information may include: name, date of birth, residential address, nationality, job title, passport or other state or national identification documents which may contain a photograph.
    - We collect this type of information when we are required to do so to comply with applicable laws or regulations or State Street's internal policy requirements. Examples of when this would be the case are if you are a controlling party (CP) (such

as a CEO, director, trustee, investment adviser, partner or agent) or ultimate beneficial owner (UBO) of a client or prospect of State Street.
    - When we collect information for AML/KYC/CFT purposes, we may also collect certain special categories of personal data such as political opinions or affiliations or trade union memberships. We will only process such special categories of personal data to the extent permitted by applicable law or regulation.
- Information about a client's business, financial affairs, end customers or operations
- Transactional data
- Holdings information
- Compliance, audit and risk reporting
- Cash availability reporting
- Fees and rates negotiated with State Street and other contractual terms
- Information regarding securities settlements, overdrafts, lines of credit, securities lending positions, and trading relationships with State Street
- Personally identifiable information, or personal data, with respect to client's personnel, associated parties, beneficial owners, investors and clients

This is not intended to be an exclusive list of data that is required in our global operating model. Given our operating model, you should assume that such data may be accessed at any of our affiliated operating locations; however, this access is provided within a comprehensive controls infrastructure that we are pleased to describe to you below.

Profiling and Screening

In order to comply with applicable financial crime related laws and regulations and sanctions regimes, State Street engages in PEP, negative news and financial sanctions screening programmes, including those defined by the European Union, the United Nations, Her Majesty's Treasury the Office of Foreign Assets Control and other applicable laws or regulations. Depending on the nature of your relationship with State Street, these activities may involve State Street processing your personal data and/or conducting screening on you. These activities may also involve State Street processing certain special categories of your personal data, such as your political opinions or trade union memberships. Such processing is considered lawful on the grounds of substantial public interest. Other than as specified above, as a general rule, State Street does not require such sensitive personal data from you.

Security

The overall end-to-end controls environment surrounding the services State Street provides and the manner in which we process data and information incorporates a variety of procedural, operational and automated controls. All State Street affiliates, including our Global Processing Centers, are subject to this controls environment. At their core, these controls are designed to promote the security and confidentiality of data and information we process and store.

Our objective is to protect against any anticipated threats or hazards to the security or integrity of such data and information and to protect against its unauthorized access or use. Data protection

controls include systems access and authorization and the division of responsibilities for particular tasks or functions. Periodic and spot testing of the foregoing procedures and controls are conducted by State Street's corporate information security and compliance departments and business unit controls teams, and both internal audit and independent third parties conduct periodic examinations and/or reviews of operating procedures and controls, and/or information technology systems and controls. State Street also has an Incident Management framework that requires that all relevant parties are made aware in the event of any breach of data.

Transferring Data

In connection with the services we provide, the discharge of our other obligations under client agreements and the management of our business, State Street (or our agents or service providers on our behalf) continuously receives, processes and maintains data and information regarding our clients. We recognize the competitive importance to our clients of their data and the trust they place in State Street in allowing us to access this data. Examples of the types of data and information we receive and access include information about a client's business, financial affairs, end customers or operations, transactional data, holdings information, compliance reporting, cash availability reporting, and fees and rates negotiated with State Street. This data may also include personally identifiable information, or personal data, with respect to our client's personnel, investors and clients.

We may also need to access data in our possession to meet our regulatory or corporate needs. For example, to meet regulatory disclosure requirements relating to our significant client credit exposure, our Finance team requires access to information on securities settlements, overdrafts, lines of credit, securities lending positions, and trading relationships with State Street. Your data will only be used to: (i) allow State Street to perform services you have hired us to perform and (ii) carry out management of our business including, but not limited to, financial and operational management reporting, risk management, legal and regulatory compliance and client service management. We may also use such data to better understand how our clients use services that we and others provide and to determine if other services that we offer that may be appropriate for our clients. State Street will not, without prior consultation with you, use your data in any product or service nor will it be provided to third parties for their commercial use other than at your direction.

In addition, in connection with the enhancements we are making to our operating model, we are augmenting our data management with cloud-based content management platforms and other cloud-based systems for a portion of our data management needs. Although some of our data storage and management systems are proprietary, others are third party systems that we employ to support the storage, access and transmission of client data. Access to data transferred or stored on such third party systems, which meet or exceed standard established under our third party risk management framework, is controlled by State Street and granted only to authorized employees of State Street group companies (and, where appropriate, entities that support State Street group companies). The benefits of cloud-based systems and solutions include enabling State Street to employ enhanced security protocols and data loss prevention tools, permitting State Street to classify data (*e.g.*, personal sensitive, highly confidential) in accordance with our information security policies and procedures and providing State Street with the ability to comply with country-specific data access and storage requirements using geographically dispersed data centers designated by State Street.

We may share some of your data, including personal data, within the State Street Group, and other service providers, who are outside of the jurisdiction in which the personal data was collected. For example, information collected within the EEA, or about European citizens may be transferred, stored, and processed outside of the EEA. For these transfers State Street has the relevant legal safeguards in place by way of contractual arrangements based on sets of standard contractual clauses pre-approved by the European Commission to ensure adequate protection. This reflects our commitment to protecting your personal data regardless of where your personal data resides.

Rights With Respect to Personal Data

Depending on the jurisdiction, individuals may have the following rights with respect to their personal data:

- To be informed about the personal data we hold
- Access the personal data we are holding
- Have their personal data rectified where it is inaccurate or incomplete
- Have their personal data erased in certain circumstances (e.g., where the personal data is no longer necessary in relation to the purposes for which it was collected)
- Obtain restriction of processing in certain circumstances (e.g., where the accuracy of the personal data is contested, for the period enabling us to verify the accuracy of that personal data)
- To object to the processing
- To data portability, i.e., to receive their personal data in a structure, commonly used and machine-readable format, and to have that personal data transmitted directly to another data controller
- The right to lodge a complaint to the relevant data protection authority

Retention of Personal Data

We will retain your personal data for as long as is necessary for the purposes set out above, or for as long is required by the applicable law and/or regulation.

Applicability and Changes to this Notice

If we make changes to this privacy notice, we will communicate those changes to you. We recognize that many of our clients have their own regulatory obligations to understand our arrangements and data access rights and, importantly, to be comfortable that we are processing transactions in a secure manner. We hope that this information is helpful to you in carrying out those obligations and in understanding our global footprint strategy and related approach to data sharing among affiliates.

Further Information

Our relationship management team is always available to address any questions that you may have and, work with you to provide you with additional information to assist you in your evaluation of our controls environment. For queries specifically related to protection of personal data, please contact the State Street Privacy Office at PrivacyOffice@StateStreet.com.