Global Privacy and Personal Data Protection Standard

Policy Owner: Privacy Office

Date of Revision: October 2023

Table of Contents

Standard Effective Date

May 2018

Standard Implementation Date

December 2023

Standard Statement

The Global Privacy and Personal Data Protection Standard ("Privacy Standard") describes how State Street handles and protects the Personal Data we Process of our clients, vendors, employees, contingent workers and other third parties.

The Privacy Standard defines the minimum standards that must be satisfied in accordance with applicable laws in the places we operate. To the extent that the laws or industry expectations of a local jurisdiction require additional privacy, data security, or data protection measures, such measures are specified in related region or jurisdiction policies, standards, procedures and guidelines. Those terms are to be read in conjunction with this Privacy Standard.

Scope

This Privacy Standard applies to all State Street entities of which State Street owns 50 percent or more, including their respective branches, Business Units and Corporate Functions that operate within such entities, and their Employees, Contingent Workers, and other Personnel who many have access to, may Process, or may outsource to third parties the Processing of Personal Data.

Standard Details

Covered Data

> This Privacy Standard applies to all Personal Data (as defined in Key Terms and Definition below) we Process regardless of the media on which that data is stored or whether it relates to past or present employees, contingent workers, clients, client or vendor contacts, shareholders, website users or any other Data Subject.

Continuing Obligation with Regard to Personal Data Regardless of Entity Performing Processing

> State Street is responsible for the protection of Personal Data and for the preservation of a Data Subject's rights, regardless of whether a State Street entity Processes the information internally or outsources the Personal Data to a vendor or to an affiliate for Processing.

What the Privacy Standard Entails

This Privacy Standard articulates responsibilities, procedures, and accountability with respect to the Privacy Program ("Program"). This Privacy Standard also summarizes at a high level the administrative, technical, and physical safeguards that all State Street entities must reasonably assure are in place to protect the security, confidentiality, and/or integrity of electronic, paper, or other records containing Personal Data. It also details the steps that all State Street entities must take to identify and assess reasonably foreseeable internal and external risks to those records, and thereby protect against unauthorized access, use, disclosure, alteration, loss, or destruction of Personal Data that creates a risk of identity theft, fraud, or other risk of harm or inconvenience to the Data Subjects.

This Privacy Standard governs State Street's response to complaints by Data Subjects about State Street's or third parties that process Personal Data on behalf of State Street handling of their personal Data, as well as demands from Data Subjects for access to, correction or deletion, of their Personal Data.

This Privacy Standard is not intended to expand any of State Street's legal obligations, and it is not intended to create any liability other than that already imposed by law or regulation.

Region and Jurisdiction Specific Derogations

This Privacy Standard establishes a baseline for all State Street entities worldwide. In some jurisdictions, additional obligations may be imposed by law or by common practice in the financial services industry. Those obligations shall be set out in related region or jurisdiction specific policies, standards, procedures or guidelines, when determined necessary by the Chief Privacy Officer (CPO) or designee, to specify any additional privacy, data security and data protection obligations as appropriate. For example, in some jurisdictions data relating to legal entities falls within the scope of the local data protection law as opposed to most countries' data protection laws. Where this is the case, the State Street privacy controls framework also applies to the protection of information concerning legal entities.

I. Roles and Responsibilities

A. The CPO or designee is responsible for overseeing this Privacy Standard and, as applicable, developing region or jurisdiction specific policies, procedures, standards and guidelines.

B. The CPO or Privacy Office must be contacted before Processing data in the following circumstances:

- you are engaging in:
    - a new processing activity related to personal data,
    - a change in processing activities related to personal data,

    - a plan to use Personal Data for purposes other than that for which it was originally collected;
- you are unsure of the lawful basis that you are relying on to Process Personal Data, including the legitimate interests used by State Street;
- you need to rely on Consent and/or need to capture Explicit Consent;
- you need new or revised Privacy Notices;
- there has been a Data Incident involving Personal Data (but note the need to first escalate the Data Incident to Global Data Incident Management immediately upon discovery);
- you are initiating a transfer of Personal Data outside the jurisdiction in which it was collected;
- you receive a complaint from a Data Subject or a request to exercise data protection rights from a Data Subject (also follow ICAMS and Customer Complaints Policy-Global where applicable);
- you need to process Personal Sensitive Data such as ethnicity, political opinions, religious or philosophical beliefs, trade union membership, genetic/biometric data, health-related data, data concerning a person's sex life, sexual orientation, or criminal convictions or offenses;
- you need to process data of minors under the age of 18;
- you plan to undertake any activities involving Profiling or Automated Decision-Making;
- you need assistance with data minimization, anonymizing or pseudonymizing personal data (refer to II.C Data Minimization below);
- you need help complying with applicable law when carrying out direct marketing activities;
- you need help with contracts or engagements involving the sharing of Personal Data with third parties, including our Vendors; or
- you need assistance with ensuring the Personal Data you process is held only as long as necessary after checking with Business Unit/ Corporate Function aligned retention periods established by the Records Management Office.

Further, all Personnel of State Street are responsible for complying with this Privacy Standard and all applicable laws and regulations associated. State Street Personnel should contact the Privacy Office at PrivacyOffice@statestreet.com with any questions about this Privacy Standard or applicable data protection regulations, as well as report any concerns that this Privacy Standard is not or has not been followed.

II. Personal Data Protection Principles

State Street's Data Protection Principles aim to: (i) integrate standards for the protection of personal data across State Street; (ii) facilitate the accountable processing of personal data; and (iii) ensure respect for privacy rights of individuals. These Principles apply to personal data, contained in any form, and processed in any manner.

A. Lawfulness, Fairness and Transparency – Personal Data is required to be Processed lawfully, fairly and in a transparent manner in relation to the Data Subject. Our actions with regard to the Processing of Personal Data must be restricted to specified lawful purposes. Specific purposes for which the Processing of Personal Data is allowed include the following:

- the Data Subject has given Consent;
- the Processing is necessary for the performance of a contract with the Data Subject;
- to meet our regulatory and legal obligations;
- to protect the Data Subject's vital interests; or
- to pursue our legitimate interests for purposes where they are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects.

Where required, the purposes and legal basis for which we Process Personal Data need to be disclosed in applicable Privacy Notices upon the point of data collection.

B. Purpose Limitation – Personal Data is required to be collected only for specified, explicit and legitimate purposes. Personal Data must not be used for new, different or incompatible purposes from that disclosed when the data was initially obtained unless the Data Subject has been informed of the new purposes and they have Consented, where necessary. Processing Sensitive Personal Data is typically not allowed. However, it may occur under strict limited conditions which must be met prior to processing Sensitive Personal Data. Business Units and Corporate Functions should contact the Privacy Office to confirm requirements prior to the collection of Sensitive Personal Data. Equally, the processing of Personal Data concerning Criminal Convictions or Offences is typically restricted and is only allowed under specific circumstances.

C. Data Minimization – Personal Data is required to be adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed. Business Units and Corporate Functions must only collect or process the Personal Data needed to meet the objectives of the processing activity. When Personal Data is no longer needed for specified purposes, it must be destroyed in accordance with State Street's Record Retention and Destruction Policy-Global.

D. Accuracy – Personal Data is required to be accurate, complete, and, where necessary, kept up to date. It must be corrected or deleted without undue delay when inaccurate. For example, where a Business Unit or Corporate Function has a direct relationship with Data Subjects, reasonable efforts should be made to periodically verify the

data is accurate and complete. Where Business Units and Corporate Functions do not have a direct relationship with Data Subjects, they shall respond to client directives to correct inaccuracies and update Personal Data as needed upon request.

E. Storage Limitation – Personal Data must not be kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the Personal Data was originally collected and is Processed, including retaining Personal Data where it is necessary to satisfy any applicable legal, accounting or reporting requirements. The Records Management Office maintains retention policies and procedures that require deletion of Personal Data after a reasonable time for the purposes for which it was being held, unless a legal obligation requires such data to be kept for a longer period of time. All reasonable steps must be taken to destroy or erase Personal Data that we no longer require in accordance with State Street's Record Retention and Destruction Policy-Global and accompanying retention schedule. This includes requiring third parties to delete such Personal Data, where applicable. In addition, depending on the jurisdiction, Data Subjects may need to be informed of the period for which data is stored and how that period is determined in an applicable Privacy Notice.

F. Security, Integrity and Confidentiality – Personal Data is required to be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures ('integrity and confidentiality').

- Integrity means that Personal Data is accurate and suitable for the purpose for which it is processed.
- Confidentiality means that only people who have a need to know and are authorized to use the Personal Data can access it.

State Street develops, implements and maintains safeguards appropriate to its size, scope and business, our available resources, the type and amount of Personal Data that State Street is responsible for or maintains on behalf of others and the identified risks.

All Business Units and Corporate Functions are responsible for protecting the Personal Data we hold and must implement reasonable and appropriate security measures (including use of encryption and Pseudonymization, where applicable) against unlawful or unauthorized Processing of Personal Data and against the accidental loss of, or damage to, Personal Data.

State Street Personnel must exercise particular care in handling Personal Data to protect it from loss and unauthorized access, use or disclosure. Personal Data may only be transferred to third-party service providers who contractually agree to comply with State Street's security and data protection requirements for Personal Data and who have implemented adequate measures for the protection of Personal Data. Data security must be maintained by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

All Personnel must comply with and not attempt to circumvent the administrative, physical and technical safeguards State Street implements and maintains. These include, but are not limited to, the requirements set forth in this Privacy Standard, as well as the State Street Cybersecurity (GCS) Standards - Global.

G. Transfer Limitation – Personal Data must not be transferred to another country without appropriate safeguards being in place. Mechanisms for cross border data transfers vary by jurisdiction and thus, the Privacy Office should be contacted prior to the transfer or Personal Data to another country.

H. Data Subject's Rights and Requests – In certain jurisdictions, Personal Data is required to be made available to Data Subjects, and Data Subjects are allowed to exercise certain rights in relation to their Personal Data (e.g., the right to access, rectify, erase, object, restrict processing of their data). Business Units and Corporate Functions must immediately escalate any request received from a data subject to exercise a data protection right or a complaint regarding the handling of the data subject's Personal Data to the Privacy Office at PrivacyOffice@statestreet.com.

State Street is responsible for and must be able to demonstrate compliance with the Personal Data protection principles listed above.

III. Registration with Local Data Protection Authorities and Appointment of Data Protection Officer

Where applicable, each State Street legal entity that is a wholly owned or a controlled and consolidated subsidiary shall cooperate with the CPO or their designee to meet all applicable legal and regulatory requirements regarding the registration of that legal entity and (where relevant) the appointment and registration of a Data Protection Officer (DPO) with the local Data Protection Authority, including any renewal registrations.

IV. Cross-Border Data Transfers

Cross-border data transfers occur when Personal Data that originated in one country is electronically or manually transferred to or accessed (viewed) from a different country. Certain data protection regulations restrict the cross-border data transfer of Personal Data from one country to another unless there are appropriate safeguards in place. Cross-border data transfers (new and modified cross-border data transfers) need to go through the Privacy Impact Assessment process (as described in section VII below) prior to implementation to determine whether appropriate safeguards exist or need to be implemented.

V. Notification and Consent of Data Subjects

A. Each Business Unit and Corporate Function must cooperate with the CPO or their designee to meet all applicable legal and regulatory requirements regarding the notification and consent (where applicable) of Data Subjects with regard to the Processing of their Personal Data. Business Units and Corporate Functions must contact the Privacy Office for guidance on requirements and for the Privacy Office to draft any new or revised Privacy Notices and consent forms prior to collection and processing of the data.

- Examples of such notice and consent requirements include the Gramm-Leach-Bliley Act and the EU General Data Protection Regulation (GDPR).
- Employee notice and consent may be necessary in certain circumstances. For example, Business Units and Corporate Functions that use recorded telephone lines must take steps to reasonably ensure that all employees with recorded lines are aware that such recording will occur, as well as the purpose(s) for recording calls.
- Specific disclosures at the point of data collection are usually necessary. Such disclosures shall explain, at a minimum: what types of Personal Data will be collected; how that data will be collected (e.g., directly from the Data Subject, from a Data Subject's device); how State Street will use the data and for what purposes; the types of service providers, business partners, government entities, or other third parties with which State Street will share the data and if the data will be transferred outside the jurisdiction of collection or residence of the Data Subject, the jurisdictions to which the data will be transferred or otherwise processed.

For advice on the specific content of such disclosures, contact the CPO and/or delegate in the Privacy Office.

B. When processing the Personal Data of children or minors under the age of 18 is done on the basis of consent, State Street shall take into consideration the child's competence and make sure that the child understands what is being consented to, or the consent must be given or authorized by the holder of parental or other legal responsibility over the child. If a Business Unit or Corporate Function has a need to process the Personal Data of children or minors under the age of 18, then the Privacy Office must be contacted prior to any such Personal Data being requested or collected.

C. Where relevant, contracts with State Street clients shall contain appropriate disclosures as to what Personal Data is collected, where it will flow, what types of parties will Process it, and the duties of each party with regards to it. Such disclosures shall be drafted in a manner consistent with all guidelines, regulations, and laws applicable to State Street.

VI. Management and Reporting of Incidents Involving Personal Data (Data Incidents)

A. State Street may be required to notify the applicable regulator, and in certain instances, the Data Subject, when a Data Incident constitutes a Personal Data Breach. State Street has implemented procedures to deal with any suspected Data Breach involving Personal Data and will notify Data Subjects and/or any applicable regulator where State Street is legally obligated to do so or when State Street believes notification is the rightful course of action based on the facts and circumstances of the Data Incident. Business Units and Corporate Functions are responsible for identifying, monitoring, reporting, and escalating all Data Incidents, deliberate or inadvertent, that cause improper destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data by any means (physical or electronic) that is classified as "Limited Access" or above as defined in State Street Cybersecurity (GCS) Standards - Global. Business Units and Corporate Functions are also

responsible for reporting Data Incidents that are reported to them via vendors, clients, or any other third parties.

B. Inadvertent data incidents must be reported immediately upon discovery to Global Data Incident Management (GDIM) via ICAMS, while all potential deliberate data incidents must be reported immediately to GDIM via email and are only to be entered into ICAMS once the investigation is complete and with the approval of the lead investigators.

   • GDIM Email Address: GlobalDataIncidentMgmt@statestreet.com

C. Business Units and Corporate Functions must cooperate with any requests for additional information that are made by the Privacy Office as part of the investigation. As such, Business Units and Corporate Functions need to provide the Privacy Office with the additional information requested promptly and no later than the deadline communicated by the Privacy Office. In situations where additional time may be required to gather the information, the Business Unit or Corporate Function must notify the Privacy Office to confirm when the information will be provided.

D. Refer to the Data Incident Policy-Global and Data Incident Playbook-Global and Incident Capture and Management Policy - Global for more details.

VII. Privacy Impact Assessment

Privacy Impact Assessments (PIAs) and/or Data Protection Impact Assessments (DPIAs) are required for all Business Unit and Corporate Function projects that involve the Processing of Personal Data and are in place for the Privacy Office to meet our regulatory requirements to:

- assess the level of privacy risk associated to the project;
- determine whether the appropriate processes and controls are in place to mitigate the privacy risk exposure;
- effectively uphold the Personal Data Protection Principles (Refer to Section II).

A. Business Units and Corporate Functions are required to contact the Privacy Engineering Team (PrivacyEngineering@StateStreet.com) whenever there is:

   a) a new processing activity related to personal data,

   b) a change in processing activities related to personal data, or

   c) a plan to use Personal Data for purposes other than that for which it was originally collected.

B. Business Units and Corporate Functions are required to remediate any privacy risks that are identified and communicated by the Privacy Office prior to the Processing of Personal Data being implemented. For projects that require remediation of privacy risks, the project sponsor will be asked to provide the Privacy Office with evidence of the actions taken in order for the Privacy Office to verify that the privacy risk(s) were adequately mitigated prior to the Processing of Personal Data.

C. If any material changes regarding the Processing of Personal Data are considered post-approval (e.g. expanding the scope to include additional jurisdictions, collecting new types of personal data, etc.), the Business Unit or Corporate Function must notify the Privacy Office of the proposed changes in order for a PIA to be conducted and for the remediation of any unmitigated privacy risks prior to implementation.

VIII. Sharing Personal Data with Third Parties

A. Personal Data may not be shared with third parties unless certain safeguards are in place. Personal Data we hold may only be shared with third parties, such as our service providers and joint ventures, if:
   - they have a need to know the information for the purposes of providing the contracted services;
   - sharing the Personal Data complies with the Privacy Notice provided to the Data Subject and, if required, the Data Subject's Consent has been obtained;
   - the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;
   - the transfer complies with any applicable cross border transfer restrictions; and
   - a fully executed written contract that contains approved privacy and data protection clauses has been obtained.

B. This Privacy Standard applies to all engagements with a Vendor where the Vendor will process Personal Data. The Vendor must contractually agree to maintaining appropriate technical and security measures to protect Personal Data in accordance with the Privacy Standard.

C. Disclosures of Personal Data to third parties may be carried out where such third parties have contractually agreed to maintaining appropriate technical and security measures to protect Personal Data in accordance with the Privacy Standard, the State Street Privacy Notice under which the Personal Data was collected, as well as any applicable terms contained in contracts between State Street and the Data Subject, or between State Street and the third party that provided the Personal Data to State Street.

D. Engagement managers are responsible for accurately classifying their vendor engagements to ensure the required due diligence is carried out. Please contact the Privacy Engineering Team (PrivacyEngineering@StateStreet.com) if you have any questions related to the data classification of personal data involved in the third-party engagement.

IX. Records of Processing Activities

Business Units and Corporate Functions collecting and processing personal data are required to and are responsible for implementing appropriate data governance over such personal data, in line with the requirements of this Privacy Standard and the Global Data Governance Policy. Requirements include maintaining accurate metadata and lineage information related to personal data processing activities across applications, repositories and vendors. The implementation of data governance practices over personal data is critical to the maintenance of regulatory reporting

prepared by the Privacy Office, including the Records of Processing Activities (RoPA) report required under Article 30 of the European Union (EU) General Data Protection Regulation (GDPR).

X. Training of Personnel

A. All Employees in every Business Unit or Corporate Function must successfully complete Privacy Standard compliance training annually.

B. Privacy Standard compliance training will be provided to Contingent Workers subject to the applicable State Street policy.

C. Business Units and Corporate Functions who are identified by the Privacy Office as Processing Personal Data as a primary function are required to provide role-specific privacy training to Personnel annually. Role-specific privacy training may be limited to select role(s) within the Business Units and Corporate Functions.

Key Term Definitions and Acronyms

Affiliate	means an entity that owns or controls, is owned or controlled by or is under common control or ownership with State Street, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise.
Anonymization	means information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.
Automated Decision-Making	means when a decision is made which is based solely on automated processing (including profiling) which produces legal effects or similarly significantly affects an individual.
Availability	means that authorized users are able to access the Personal Data when they need it for authorized purposes.
Business Unit	means a component of State Street with profit and loss responsibility for the provision of products and services to clients or customers (e.g., Investment Servicing, Investment Management, Investment Research and Trading).
Chief Privacy Officer or CPO	means the Chief Privacy Officer appointed by State Street to head its Corporate Compliance Privacy Office.
Consent	means agreement which must be freely given, specific, informed and an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signifies agreement to the Processing of Personal Data relating to them.
Contingent Worker	means any individual performing work for State Street who has been provided a State Street e-mail account who is not a State Street Employee. This includes, but is not limited to, employees of Vendors and sub-contractors, as well as individuals directly engaged as independent contractors by State Street.
Corporate Function	means a component of State Street that does not have profit and loss responsibility for the provision of products and services to clients or customers (e.g., Legal, Global Procurement Services, IT, Corporate Compliance, Global Human Resources, etc.).

	Criminal Convictions and Offences	means Personal Data about criminal allegations, proceedings or convictions. Personal Data relating to criminal convictions and offences is high risk data which must be classified as such and protected as Sensitive Personal Data at State Street.
	Data Incident	means a deliberate or inadvertent improper destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data by any means (physical or electronic) that is classified “Limited Access” or above as defined in State Street’s Cybersecurity (GCS) Standards - Global.
	Data Privacy Impact Assessment (DPIA)	means tools and assessments used to identify and reduce risks of a data processing activity. DPIA may be carried out by the Privacy Office as part of Privacy Impact Assessment for high risk projects involving the Processing of Personal Data.
	Data Protection Authority (DPA)	means the public authority responsible for monitoring and enforcing the application of data protection and privacy laws.
	Data Subject	means an individual to whom Personal Data relates.
	Employee	means an individual (including an intern) who is employed directly by State Street on either a temporary or permanent basis.
	Encryption	means an overt secret writing technique that uses a bidirectional algorithm in which humanly readable information (referred to as plaintext) is converted into humanly unintelligible information (referred to as ciphertext).
	Explicit Consent	means Consent which offers individuals real choice and control and requires a very clear and specific statement (that is, not just action).
	Personal Data	means any information related to an identified or identifiable individual. It also includes Sensitive Personal Data that requires the highest levels of protection and stringent justification for processing. Refer to Sensitive Personal Data definition for more details.
	Personnel	means all Employees and Contingent Workers.
	Profiling	means any form of Automated Processing of Personal Data to evaluate certain personal aspects relating to an individual, in particular to analyze or predict aspects concerning that individual’s performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements. Profiling is a type of Automated Processing.
	Privacy Impact Assessment or PIA	means the process the Privacy Office has implemented to assess the level of privacy risk associated with projects involving the processing of Personal Data.
	Privacy Office	means the Corporate Compliance Privacy Office at State Street.
	Privacy Oversight Committee	means the cross-functional committee responsible for exercising oversight over privacy and data protection matters at State Street.
	Privacy Notices	means notices setting out information that may be provided to Data Subjects when State Street collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, employee privacy notices or a website privacy policy) or they may be stand-alone, one time privacy statements covering Processing related to a specific purpose.
	Processing or Process	means anything that can be done with or to Personal Data, including collecting, recording, organizing, storing, adapting, altering, retrieving, consulting, using, disclosing, disseminating, transferring, blocking, erasing, or destroying such data. Other forms of “Process,” such as

		"Processing" or "Processes," have the same meaning for purposes of this Privacy Standard.
	Project	means new or modified processing of Personal Data through a cross-border data transfer, manual process, automated process, vendor, or technology.
	Project Sponsor	individual responsible for implementing or facilitating the implementation of the project; the individual can be a person within the business, project team, or information technology.
	Pseudonymization or Pseudonymized	means replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.
	Record of Processing Activities Report (RoPA)	means the report generated by the Privacy Office that is required to be updated and maintained by applicable Business Units and Corporate Functions (depending on local regulatory obligations) and serves as a central record of the personal data processing activities that the applicable Business Units and Corporate Functions engages in. The RoPA must be made available to authorities upon request.
	Regulatory Obligations	means applicable final rules, laws, statutes and regulations, formal regulatory guidance, Self-Regulatory Organization standards and codes of conduct adopted by State Street that regulate State Street's financial services activities and functions that support those activities.
	Sensitive Personal Data	means information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data. In addition, Personal Data relating to criminal convictions and offences is high risk data which must be classified as such and protected as Sensitive Personal Data at State Street.
	State Street	means, collectively, State Street Corporation and each State Street legal entity that is a wholly owned subsidiary, or a controlled and consolidated subsidiary.
	Vendor	means a person or entity that provides goods or services to State Street, including contractors, and that may Process or have access to Personal Data.

Related Policies, Standards and Guidance

This Privacy Standard provides a high-level summary of State Street's key privacy and data protection measures for Personal Data. As such, this Privacy Standard is not intended to be comprehensive, nor is it intended to enumerate any new requirements. Instead, all elements of the Privacy Standard are drawn from, and subject to, more detailed guidance in existing State Street policies and standards, including the following:

- Standard of Conduct
- Cybersecurity (GCS) Standards – Global
- Data Incident Policy – Global
- Data Incident Playbook - Global
- Incident Capture and Management Policy – Global
- Record Retention and Destruction Policy – Global
- Global Data Governance Policy
- Data Minimization Principle Guidance Note
- Third Party and Outsourcing Risk Management Policy – Global
- Performance Improvement and Disciplinary Process Policy (as applicable based on location)

- Conduct Standards Policy - Global and Framework
- Recorded Line Policy – Global
- Customer Complaints Policy – Global

Standard Administration

The Corporate Compliance Privacy Office maintains this Privacy Standard. Questions should be directed to the CPO or designee. Business Units and Corporate Functions may be audited for compliance with this Privacy Standard at any time.

Review and Approvals

The CPO or designee shall review this Privacy Standard on a biennial basis, and propose amendments to this Privacy Standard to comply with the applicable data protection regulations, best practices in the financial services industry, and any other applicable laws, regulations, or orders.

Any material changes to this Privacy Standard shall be submitted to the Privacy Oversight Committee (POC) for approval. This Privacy Standard, and amendments thereto, is effective from the date that the Privacy Standard is approved by the POC. Once approval has been granted it will be provided to the Core Compliance and Ethics Committee for noting.

This Privacy Standard shall be made available to all Personnel via the State Street intranet site.

Disciplinary and Enforcement Actions for Violations of the Privacy Standard

Disciplinary action (which may include training and counselling, as well as formal disciplinary or enforcement action up to and including termination of employment) in accordance with the Conduct Standards Policy – Global may be imposed for the violation of this Privacy Standard or parts thereof.

Investigations of potential privacy violations by Personnel shall be conducted by the Chief Security Officer and Global Human Resources, partnering as appropriate with Legal, Risk, Compliance, Audit, CIS, and other groups, as needed.

End of Record