04.03 FIS Privacy Policy

Policy Owner:	Bussard, Cliff
Contact:	PrivacyOffice@fisglobal.com
Domain:	Corporate Privacy
Scope:	Enterprise Wide
Published Date:	December 11, 2017
Effective Date:	December 9, 2016
Mandatory Review Date:	December 11, 2018
Provision for Exception:	These provisions apply to all business units with no exceptions.

Empowering the Financial World

FIS

*The key words **"MUST"**, **"MUST NOT"**, **"REQUIRED"**, **"SHALL"**, **"SHALL NOT"**, **"SHOULD"**, **"SHOULD NOT"**, **"RECOMMENDED"**, **"MAY"**, and **"OPTIONAL"** in this document are to be interpreted as described in Best Current Practice – Key Words.*

04.03 FIS Privacy Policy

Purpose

FIS respects the privacy of all Personal Data it holds, and is committed to protecting and limiting the use of such information in accordance with applicable data protection and privacy laws wherever it does business. "Personal Data" means any information relating to an identified or identifiable natural person. Consequently, Fidelity National Information Services, Inc., and its employees, contractors, managers, officers, directors, divisions, branches, subsidiaries, and controlled affiliates (collectively, "FIS") have adopted this Personal Data Privacy Policy (the "Policy") to protect the individuals whose Personal Data FIS controls or otherwise processes. The term "processing" is used in this Policy to cover all activities involving Personal Data, including collecting, handling, updating, storing, deleting, sharing, accessing, using, transferring and disposing of the Personal Data.

This Policy reflects global principles and standards on handling Personal Data. This Policy governs all FIS business activity and the conduct of all FIS employees, contractors, representatives and third parties with respect to Personal Data processed on behalf of FIS at any location globally.

This Policy is supplemented by three Privacy Notices, which are intended to provide individuals with more detailed information about how FIS processes their Personal Data:

- The Controlled Personal Data Notice explains how FIS processes all FIS Controller Personal Data (as defined below);
- The Online Privacy Notice explains how FIS processes personal data it collects through the FIS websites; and
- The Staff Privacy Notice explains how FIS processes the personal data of its personnel (e.g. employees, applicants for employment and contractors).

Statement

It is FIS policy and practice to comply with all applicable data protection and privacy laws wherever it does business. In the event an applicable data protection or privacy law requires any action or imposes any standard more stringent than this Policy, the requirements of the law shall control and take precedence over the requirements of this Policy. References to applicable law and regulations in this Policy are references to those laws and regulations directly applicable to FIS.

04.03.01 Personal Data Covered by this Policy

All Personal Data processed by FIS for any purpose will be processed in compliance with this Policy. FIS may obtain such Personal Data directly from the individual ("**data subject**"), for example through website registrations, or indirectly through employees and third parties, for example through contact information.

FIS processes some Personal Data on its own behalf for its own business purposes. When FIS has the right to control when and how Personal Data will be collected and used, and for what purposes, the Personal Data is considered "**FIS Controlled Personal Data.**" Personal Data that is FIS Controlled Personal Data will often, but not always, be collected directly by FIS. If the subject of Personal Data is an employee, applicant for employment or temporary contractor, or any other person or entity relevant to the FIS relationship with the data subject, then Personal Data processed by FIS related to the employment, applicant or contractor relationship will always be considered FIS Controlled Personal Data, regardless of the source of that Personal Data.

In addition, FIS processes some Personal Data solely on behalf of its clients in the course of delivering FIS services ("**Services Personal Data**"). FIS processes Services Personal Data to accomplish the business purposes of the client for whom the services are provided, and often will not have a direct relationship with the subject of the Services Personal Data. Typically, Services Personal Data will have been collected by the client and provided to FIS for processing, but that is not always the case. In some cases, FIS may not even know that the data it processes for a client includes Services Personal Data.

FIS processes Services Personal Data exclusively pursuant to contractual obligations and authorization of its client, and will be required to return the Services Personal Data to the client, or to destroy it, after it is no longer needed in accordance with those contractual obligations.

04.03.02 Standards Applicable to the Processing of Personal Data

The following standards are applied by the employees, contractors, representatives and third parties acting on behalf of each affiliated FIS entity covered by this Policy with respect to Personal Data that is processed by FIS:

- **Fairness.** FIS shall process Personal Data fairly and lawfully.
- **Limitation on Purpose.** FIS shall process Personal Data only in support of legitimate FIS business purposes that are specified and explicit or apparent from the circumstances. Services Personal Data will not be processed by FIS for any purpose other than the delivery of the services to be provided by FIS in accordance with the client contract governing such data or another purpose authorized or instructed by the client who provided the Services Personal Data to FIS for processing.
- **Data Quality and Proportionality.** FIS endeavors to verify the FIS Controlled Personal Data it processes is accurate and, where necessary, is kept up to date. FIS also endeavors to verify the FIS Controlled Personal Data is adequate, relevant and not excessive in relation to the purposes for which it is collected and/or processed. For Services Personal Data, FIS' client is responsible for ensuring the data is accurate, up-to-date, adequate, relevant and not excessive.
- **Transparency.** Individuals who are the subjects of FIS Controlled Personal Data will be provided with information necessary to verify fair processing of their Personal Data, including notice of (i) the purposes for which the FIS Controlled Personal Data may be processed, unless the reason for the collection of the Personal Data is apparent from the circumstances, (ii) the categories of FIS Controlled Personal Data that may be processed, (iii) any categories of sensitive FIS Controlled Personal Data that may be processed, and (iv) their rights in relation to the FIS Controlled Personal Data for which they are subject. More information about the different rights held by data subjects of FIS Controlled Personal Data is set out in the Privacy Notices referenced above.
- **Sensitive Personal Data.** FIS Controlled Personal Data and Services Personal Data that reveal the racial or ethnic origin, political opinions, religious or other beliefs of a similar nature, trade union membership, physical or mental health or condition, sexual life or commission of any offense or criminal record of the individual that is the subject of the Personal Data will always be classified as Sensitive Personal Data for purposes of this Policy. FIS Controlled Personal Data relating to children and to the financial history or circumstances of the subject of the Personal Data may also be classified as Sensitive Personal Data under some applicable local laws. Data that is Sensitive Personal Data will not be processed without the consent of the subject of the Personal Data if such consent is required by applicable law. Prior to collecting or otherwise processing data that is Sensitive Personal Data, the lawfulness of such collection or processing shall be verified by consultation with the FIS Legal Department.
- **Data Subject Rights.** Where FIS is required by law or regulation to provide data subjects with rights over their data then FIS will fully enable these rights in accordance with said law or regulation.
- **Personal Data used for Marketing Purposes.** Where FIS Controlled Personal Data are processed for the purpose of direct marketing, effective procedures exist allowing the subject of the Personal Data to "opt out" from such use. This option refers to the marketing of consumer or commercial goods or services to an individual data subject, and will not limit normal and customary communications by or on behalf of FIS regarding the individual's relationship with FIS.

- **Data Security.** Appropriate physical network and process security measures designed to protect Personal Data processed by FIS against accidental or unlawful destruction, accidental loss, alteration, or unauthorized disclosure or access will be in place.
- **Data Access.** FIS takes reasonable steps to determine who gains access to Personal Data. FIS Access Control Policy is based on the "Principle of Least Privilege," and access to Personal Data shall be limited by that principle, which requires that privileged access must be provisioned with the minimum level of access to non-public data which is required to satisfy a user's job responsibilities. This premise is in addition to this Policy as well as other FIS policies, as applicable.
- **Data Transfers.** Personal Data will not be transferred across any political or geographic boundary unless such cross-border data flow is authorized by agreement of the individual that is the subject of the Personal Data or the transfer is otherwise permitted by applicable laws. Any third party authorized by FIS to process FIS Controlled Personal Data on behalf of FIS must first agree by written contract to (i) respect and maintain the confidentiality and security of such Personal Data in accordance with standards that meet the requirements of this Policy, (ii) to process such Personal Data pursuant to FIS instructions, and (iii) to return, or delete the FIS Controlled Personal Data, as directed by FIS, when it is no longer needed for the purposes for which it was provided.
- **Obsolete Personal Data.** FIS shall not retain Personal Data longer than necessary to accomplish the legitimate business purpose for which the Personal Data was collected and processed by FIS or as required by the terms of a client contract or applicable law. Such obsolete Personal Data, and the media on which it is contained, will be destroyed in a secure manner or, where appropriate, returned to a client.
- **Disputes or Objections.** FIS will address any complaints or disputes regarding FIS Controlled Personal Data with a view to settling them amicably in a timely fashion.

1. **Asking Questions, Seeking Advice, and Reporting Violations of the Policy**
    - FIS personnel have a duty to seek advice in the case of any doubt about the lawfulness of a particular activity involving Personal Data or other requirements for compliance with this Policy. The FIS Chief Privacy Officer is responsible for the general administration of this Policy.
2. **Training**
    - FIS personnel receive Information Security and Privacy Awareness Training, which includes specific education on personal data protection, compliance, and risk management topics. Privacy training is provided annually and required of all employees and contractors. FIS specialized training on handling health-related information is also annually assigned to employees and contractors who may handle this type of data.

All FIS employees, contractors and applicable third parties are required to adhere to established policies and standards. Violation of FIS policies and/or standards may result in disciplinary action up to and including termination. Any suspected violation of an FIS policy or standard should be reported to either a management representative, the People Office or to the FIS Ethics Officer or FIS Chief Compliance Officer (CorporateCompliance@fisglobal.com). Violations may also be reported using the FIS Ethics Web site (www.fnisethics.com) or Hotline**.** FIS does not tolerate any retaliation against anyone who, in good faith, reports a violation of FIS policy or law or cooperates with an investigation. To report a potential security incident, you should email the FIS Security Incident Response Team (FSIRT) at FSIRT@fisglobal.com. For urgent or critical security incidents, you should call 414.357.FSIRT (3747) (U.S. and International).