04.03 FIS Privacy Policy

Policy Owner:	Shea, Anna
Contact:	PrivacyOffice@fisglobal.com
Domain:	Corporate Privacy
Scope:	Enterprise Wide
Published Date:	November 29, 2022
Effective Date:	December 9, 2016
Mandatory Review Date:	November 6, 2023
Provision for Exception:	Exceptions require Policy Exception Committee approval unless otherwise delegated within the policy.

*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

Fidelity National Information Services, Inc., and its employees, contractors, managers, officers, directors, divisions, branches, subsidiaries, and controlled affiliates (collectively, "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. FIS has adopted this 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, but not limited to 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 four 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 Company Controlled Personal Data, as defined below.
- The **Online Privacy Notice** explains how FIS processes Personal Data it collects through FIS websites.
- The **Staff Privacy Notice** explains how FIS processes the Personal Data of its personnel, (e.g., employees, applicants for employment, and contractors.)
- The **Worldpay Privacy Notice** explains to individuals who access or use Worldpay's services, how the Worldpay business uses Personal Data as a controller (e.g., buyers, Worldpay merchants, Worldpay customers who trade as individuals, and website or application users.)

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 **MUST** 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 **SHALL** process 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 "**Company**

Controlled Personal Data." Company Controlled Personal Data includes the Personal Data referred to in the Worldpay Privacy Notice. Personal Data that is Company Controlled Personal Data will often, but not always, be collected directly by FIS.

Company Controlled Personal Data is Personal Data controlled and processed by FIS related to the collection of accounts receivable, the processing of accounts payable, sales, marketing, and vendor and customer relationship management purposes. In some circumstances, FIS **SHALL** use Controlled Personal Data for sanctions and anti-money laundering screening and to meet regulatory requirements.

FIS **SHALL** process some Personal Data solely on behalf of its clients while delivering FIS services ("**Services Personal Data**"). FIS **SHALL** process 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 data subject of the Services Personal Data.

Typically, Services Personal Data will have been collected by the client and provided to FIS for processing., FIS **SHALL** process Services Personal Data exclusively pursuant to contractual obligations, client's instruction, its Record Retention Policy, and/or regulatory purposes, and **SHALL** 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 **MUST** be 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 **MUST** 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 **SHALL** endeavor to verify the Company Controlled Personal Data it processes is accurate and where necessary, is kept current. FIS **SHALL** endeavor to verify the Company 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 confirming the data is accurate, current, adequate, relevant, and not excessive.
- **Transparency**. Individuals who are the subjects of Company 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 Company 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 Company Controlled Personal Data that may be processed, (iii) any categories of sensitive Company Controlled Personal Data that may be processed, and (iv) their rights in relation to the Company Controlled Personal Data for which they are subject. More information about the different rights held by data subjects of Company Controlled Personal Data is set out in the Privacy Notices referenced above.
- **Sensitive Personal Data**. Company 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 condition, genetic or biometric data, sexual life or sexual orientation, Personal Health Information (PHI), commission of any offense or criminal record of the individual that is the subject of the Personal Data **SHALL** always be classified as Sensitive Personal Data for purposes of this Policy. Such data **MAY** have additional layers of security or varying legal bases, such as explicit consent of data subject. Company Controlled Personal Data relating to children and to the financial history or circumstances of the subject of the Personal Data

may be classified as Sensitive Personal Data under some applicable law. Data that is Sensitive Personal Data **MUST 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 and a data protection impact assessment (DPIA) **SHALL** be conducted.

- **Data Subject Rights**. Where FIS is required by law or regulation to provide data subjects with rights over their data, then FIS **SHALL** enable these rights in accordance with said law or regulation. Where FIS acts as a Processor, FIS' client is responsible for compliance with applicable law or regulation. To submit a Data Rights Request
    - click here to submit electronically; or
    - email your request to DataRights@fisglobal.com or
    - call 866-728-7033.
- **Personal Data used for Marketing Purposes**. Where Company Controlled Personal Data is processed for the purpose of marketing and analytics, effective procedures exist allowing the data subject of the Personal Data, as required by applicable law or regulation, to opt in or opt out from such use. The opt in/opt out option refers to the marketing of consumer or commercial goods or services to an individual data subject and SHALL 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 or Sensitive Personal Data processed by FIS against accidental or unlawful destruction, accidental loss, alteration, or unauthorized disclosure or access are in place.
- **Data Access**. FIS **SHALL** take reasonable steps to determine who gains access to Personal Data. The Enterprise Identity and Access Management Policy is based on the "Principle of Least Privilege," and access to Personal Data shall be limited by that principle. The Principle of Least Privilege 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 **MUST** 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 Company 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 Company Controlled Personal Data, as directed by FIS, when it is no longer needed for the purposes for which it was provided.
- **Obsolete Personal Data**. In accordance with the FIS Records Management Policy, 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, **MUST** be destroyed in a secure manner or, where appropriate, returned to a client.
- **Disputes or Objections.** FIS **SHALL** address any complaints or disputes regarding Personal Data in order to settle in a timely fashion. All complaints or disputes regarding Personal Data should be sent to PrivacyOffice@fisglobal.com.

- **Asking Questions, Seeking Advice, and Reporting Violations of the Policy**
    - FIS employees and contractors **MUST** 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.
- **Training**
    - FIS employees and contractors **SHALL** 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 Colleagues, contractors, and applicable third-parties are required to adhere to established policies, procedures, and standards. Violation of Company Policies, procedures and/or standards **MAY** result in disciplinary action up to and including termination of employment, as permitted by local law. Any suspected violation of Company Policies, procedures, or standards **SHOULD** be reported to either an FIS manager or the Ethics Office at fisethicsoffice@fisglobal.com in accordance with the Code and Company Policies. Suspected violations of the Code **MAY** also be reported, through the FIS Ethics Helpline utilizing the phone numbers within the Code of Business Conduct and Ethics (Appendix A) or through the website at www.fnisethics.com. Concerns raised to the Ethics Helpline can be made anonymously where permitted under local laws. FIS does not tolerate any retaliation against anyone who, in good faith, reports a suspected violation of the Code, Company Policies, or the law or who cooperates with an investigation. Colleagues also have the option of raising employee relations concerns through TPO Support Center (Raise a Concern, Grievance or Complaint - Employee Service Center (service-now.com)). Concerns related to information security can be reported using **Service Now (SNOW): Technology Service Catalog > Security Services > FIS Security Incident Reporting Form**. For urgent or critical information security incidents, please call +1.414.357.FSIRT (3747) (U.S. and International). In addition, privacy incidents can be reported through FIS & me Workplace Services > RISC Resource Center > Report a Privacy Incident.