Privacy Notice – FIS Controlled Personal Data

Introduction

Fidelity National Information Services Inc. and certain members of the FIS group of companies (collectively, "FIS"), have adopted a comprehensive program to safeguard and protect the personal data it processes relating to identified or identifiable individual persons with whom, or representing other companies with whom, the FIS Group has or seeks to have business relationships in support of the business of the FIS Group ("FIS Controlled Personal Data").

This Notice does not apply to Personal Data relating to employees, applicants for employment, and temporary contractors providing services to FIS, or others in relationships with such persons that are relevant to their relationship with FIS, such as for global mobility, emergency contact, and benefits purposes. For information regarding FIS processing of such data, see the FIS Staff Privacy Notice.

In the normal course of business activities, FIS provides services for clients that result in FIS processing Personal Data on behalf of those clients. In many cases, FIS acts as a data Processor on behalf of the client, which is the data Controller of certain Personal Data, known as "Services Personal Data," provided to FIS for FIS' processing on the client's behalf. This Notice does not apply to such processing. The processing of Services Personal Data will be carried out by FIS in accordance with the terms of the relevant contract or contracts between FIS and the client that provides the personal data to FIS for processing.

For additional information, see also the FIS Privacy Policy.

The term "Processing" is used in this Notice to cover all activities involving FIS Controlled Personal Data, including, but not limited to: collecting, handling, updating, storing, deleting, sharing, accessing, using, transferring, and disposing of the FIS Controlled Personal Data.

"Personal Data" means any information that relates to or identifies an individual person that is collected and processed in the context of the individual's working relationship with FIS, and the "Data Subject" of the Personal Data is the person to which the information relates or identifies. The term "Controller" as used in this Notice describes the situation in which FIS may determine how and why the Personal Data is processed.

The Controller for Controlled Personal Data is the FIS company to which the data subject or the employer of the Data Subject has provided the Personal Data.

Description of Data Processing

This Notice is directed to those persons who are the Data Subjects of FIS Controlled Personal Data. The subject of this Notice 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 client relationship management purposes. In some cases, FIS also uses Controlled Personal Data for sanctions and anti-money laundering screening and to meet regulatory requirements.

The FIS Controlled Personal Data may have been provided to FIS directly by the person to whom it relates, or by another person or company, such as the vendor or customer that employs the subject of the data and with whom FIS has a business relationship. For the purposes of "know your customer" and other regulatory requirements, Controlled Personal Data may be screened against third-party identification services and government-provided databases, which return information regarding potential matches to publicly available information.

FIS may carry out some automated decision making such as credit and fraud checks. FIS may be unable to provide you with our services if you do not pass these checks.

For more detailed information on the categories of data processed, the purposes of Processing, and the legal basis on which FIS relies to process Controlled Personal Data, please consult the Appendix to this Notice.

International Transfers and Third Parties

In the ordinary course of global business operations, FIS may need to make international transfers of FIS Controlled Personal Data between its various branches and offices and selected service providers in many parts of the world. Some of the countries to which the data is transferred may not have equivalent privacy and data protection laws to those in the data subject's country of residence. FIS has established a data protection program and has put in place data processing agreements to confirm transfers of FIS Controlled Personal Data are subject to appropriate safeguards. This may include the use of European Commission-approved model clauses and other appropriate data transfer arrangements.

In support of FIS global operations, FIS may need to make FIS Controlled Personal Data available to selected external third-party service providers performing services at the request of FIS. Examples of third-party service providers with which the data could be shared include legal advisors and information technology service providers. Such third parties may be located in countries that may not have the same privacy and/or data protection laws and regulations as the FIS Controlled Personal Data subject's home country. FIS verifies transfers of FIS Controlled Personal Data among FIS group companies and third parties are subject to appropriate safeguards. This may include the use of European Commission-approved model clauses and other appropriate data transfer arrangements.

Security

FIS is committed to the confidentiality and security of the FIS Controlled Personal Data. FIS' systems and facilities in which the FIS Controlled Personal Data are processed are protected by secure network architectures that contain firewalls and intrusion detection devices. Access to the FIS Controlled Personal Data is limited to those individuals who need the information to perform their job duties.

Choices and Rights

FIS Controlled Personal Data subjects may request further details regarding FIS' processing of their FIS Controlled Personal Data in accordance with local, applicable law. Further, such Data Subjects are entitled, in certain circumstances, to review their FIS Controlled Personal Data and to request appropriate rectification, erasure, portability or restriction of their Controlled Personal Data. Where applicable, Data Subjects have the right to object to Processing based on legitimate interests and/or to withdraw consent where consent forms the legal basis for Processing. These rights may be limited, for example, if fulfilling a request would reveal Personal Data of another person, or if the Processing is required by law or other compelling legitimate interest. Subject to applicable law, Data Subjects may have the right to complain to a data protection authority.

It is the responsibility of FIS Controlled Personal Data subjects to request such benefits by contacting the FIS Privacy Office.

FIS will retain Controlled Personal Data only for as long as needed. FIS may need to retain Controller Personal Data for reasons including, but not limited to the following: FIS' legitimate interests or other Processing in accordance with applicable law, e.g., to perform a requested service, to meet a legal requirement, etc.

Changes to this Notice

As this Notice is updated or modified, the current version will be posted on the Corporate Governance section of fisglobal.com.

Contact Us

The purpose of this Notice is to provide FIS Controlled Personal Data subjects the appropriate details regarding specific FIS Controlled Personal Data which may be processed by FIS. This includes how FIS collects and uses such FIS Controlled Personal Data. If you are an FIS Controlled Personal Data subject and have any questions related to FIS Processing of your personal data, please send your inquiries to:

Chief Privacy Officer
FIS
601 Riverside Avenue
Jacksonville, FL 32204

privacyoffice@fisglobal.com

If you are based in the European Economic Area (EEA) or Switzerland, you may contact the FIS Data Protection Officer at the following address:

Data Protection Officer
FIS
25 Canada Square, Canary Wharf
London E14 5LQ
United Kingdom

data.protection@fisglobal.com

APPENDIX

Description and Use of FIS Controlled Personal Data that is not Staff Personal Data

Purposes of the Processing

With respect to Data Subjects whose Personal Data is Processed by FIS as FIS Controlled Personal Data, for example, related to the collection of accounts receivable, the Processing of accounts payable, sales, marketing, vendor and customer relationship management purposes, the Personal Data may be transferred and processed for the following purposes:

Purpose of processing		Legal ground(s) for use
Designing, evaluating, benchmarking, and administering:	FIS product and service offerings and their fitness to purpose for particular clients	FIS relies on: • Consent to collect any information provided directly and to send promotional material; • FIS' legitimate interests in protecting its rights; • FIS' legitimate interests in developing and improving products and services; and • The need to process Personal Data to provide a requested product or service.
	Diversity programs, including compliance with diversity objectives	
	FIS controlled recognition and rewards programs	
	Education, training, and awareness programs	
	Sales and marketing campaigns	
	Offers of products and services, and contracting	
	Accounts receivable, Accounts payable, Bad debt and reserves; bank accounts for payments and receipts	
Assembling, maintaining, and disseminating:	Job assignments for sales, marketing, and collections	FIS relies on: • FIS' legitimate interests in the administration of its business.
	Company directories	
	Emergency contact information	
	Identification credentials	
Supporting, monitoring, auditing, executing, and facilitating:	Business conferences and travel	FIS relies on: • Consent to collect any information provided directly; • FIS' legitimate interests in the administration of its business; and • FIS' legitimate interests in protecting the integrity of FIS services, facilities and systems, and staff.
	Business negotiations and transactions	
	Business operations, including staffing proposals and client billing	
	Business transition activities, including mergers, acquisitions, and divestitures	
	Company marketing efforts, including websites, conferences, brochures, and	

Purpose of processing		Legal ground(s) for use
	other promotional media events and materials Compliance with contractual obligations; customer service and support Identification for security and systems/ facility authentication Internal and external business communications and management reporting	• FIS' legitimate interests in preserving records for business purposes, assuring security at its facilities and systems, and making contact information available to relevant employees; • FIS' legitimate interests in promoting, developing, and improving products and services; and • The need to process Personal Data to provide a requested opportunity, product or service, or to fulfil a contract.
Complying with:	Applicable laws, regulations, and legal requirements, including reporting and disclosure obligations	FIS relies on: • Legal requirements to process Personal Data; • FIS' legitimate interests in conducting sanctions and anti-money laundering screening, and meeting regulatory requirements; and • FIS' legitimate interests in protecting its rights.
Conducting:	Audits and accounting, financial and economic analyses In accordance with local law, investigations into alleged policy or contractual violations, misconduct related to work safety and security concerns Opinion and engagement surveys	FIS relies on: • FIS' legitimate interests in analyzing performance, understanding FIS client and customer preferences, and preserving the integrity of the FIS workplace; • FIS' legitimate interests in protecting the integrity of FIS services, operations, facilities and systems, and staff; • FIS' legitimate interests in protecting its rights; and • Legal requirements to process Personal Data.
Protecting:	Safety and security of personnel, workplaces, and company assets, by implementation of identity authentication and other security measures, control of access to company and client workplaces and systems, monitoring of activity in company work locations, and execution of backup and storage procedures	FIS relies on: • FIS' legitimate interests in protecting its rights, the integrity of FIS services, operations, facilities and systems, and staff, and preventing fraud or the misuse of FIS services.
Preventing and detecting:	Crime	FIS relies on: • FIS' legitimate interests and legal obligations; • FIS' legitimate interests in conducting sanctions and anti-money laundering screening, and meeting regulatory requirements; and

Purpose of processing		Legal ground(s) for use
		• FIS' legitimate interest in protecting its rights and property.
Monitoring, auditing, and reviewing:	Communications and information on company systems, including email and website usage Compliance with company policies, procedures, and processes Activity in company work locations	FIS relies on: • FIS' legitimate interests in protecting the integrity of FIS services; and • FIS' legitimate interests in protecting its rights, the integrity of FIS services, operations, facilities and systems, and staff, and preventing fraud or the misuse of FIS services.
Preparing for, defending, participating in, or responding to:	E-discovery requests for information Litigation or potential litigation and other types of dispute resolution	FIS relies on: • Legal requirements to participate in legal process; • FIS' legitimate interests in conducting sanctions and anti-money laundering screening and meeting regulatory requirements; and • FIS' legitimate interests in protecting its rights.
Communicating and sharing of information with FIS companies or potential or actual acquirers of FIS companies or businesses for:	Internal administration and business management and planning purposes	FIS relies on: • FIS' legitimate interests to structure its business appropriately and legal obligations.
Processing and administering:	Tax and other required withholdings Reimbursements for business travel and other reimbursable business expenses Invoices, payments, cash balances and accounting	FIS relies on: • Legal recordkeeping and reporting requirements; • FIS' legitimate interests in protecting its rights; and • The need to process Personal Data to fulfil contractual and legal obligations.

Categories of data

With respect to Data Subjects whose Personal Data is processed by FIS as FIS Controlled Personal Data, such as Processing related to the collection of accounts receivable, the Processing of accounts payable, sales, marketing, vendor and customer relationship management purposes, the FIS Controlled Personal Data Processed may concern the following categories of data.

Data Category	Example
Advice, opinions, and other comments	Engagement surveys, exit interviews.
Bank and financial details	Payment and/or expense reimbursement; direct deposit banking information, credit card information, wire clearing information, bank account number and sort codes, invoicing details, and payment details.
Business travel and movement data	Travel data, including travel schedules, lodging, conveyance, meals, and other expenses.
Grievance data	Complaints, tribunal data.
Information recorded on or in company systems, equipment, or documents	Emails, text messages, web site usage, voicemail recordings, calendar or diary entries, correspondence, including Personal Information included in or on company systems, equipment, or documents by the Data Subject.
Access records	Dates, times, and locations of entry and exit from controlled facilities and systems, computer, and system logon/off audit trails.
Organizational data	Name, company structure, organizational charts, reporting relationships, titles, work contact details, email, and accounting code details.
Personal details and contact information	Name, gender, birth date, home and business address, phone numbers, email, government-issued identification numbers, identification numbers issued by or on behalf of the company, signatures, and handwriting.
Photo, video, or audio recordings	Information collected by security systems, closed-circuit television, profile photographs, voice mail, recorded trainings, conferences, or marketing materials.
Reports of disputes, defaults, or policy violations	Records of oral, written, email, telephone or similar reports pertaining to alleged and confirmed staff misconduct, contract issues, payment defaults, audits, or violations of company policies.
Talent, education, and training details	Education, skills, work experience, prior employment, training, language skills, technical skills, educational background, professional certifications and registrations, and membership in professional bodies and organizations.
Work schedule data	Planned and actual working times.
Workplace safety data	Reports, photographs, and video recordings.

Sensitive data

In some jurisdictions, Personal Data that is considered “Sensitive Personal Data” or “Special Categories of Data,” under applicable laws may be subject to more stringent protection and limitations on use than other Controlled Personal Data. What is considered Sensitive Personal Data varies by country, but generally includes information relating to a person’s sex life or sexual orientation, racial or ethnic origin, alleged or actual criminal offense, physical or mental health or condition, trade union membership, political opinions, religious belief, or genetic data.