Privacy Notice – FIS Staff Privacy Notice

Introduction

Fidelity National Information Services, Inc. and certain members of its affiliated group of owned and controlled subsidiary companies (collectively, "**FIS**"), including the FIS company that employs or contracts with you or to which you have made an application, have adopted a comprehensive program to safeguard and protect the personal data it processes relating to identified or identifiable employees, applicants for employment and independent or licensed contractors, as well as personal data of other persons in relationships with such employees, applicants for employment, and contractors that are relevant to their relationship with FIS, such as for global mobility, emergency contact, and benefits purposes, as applicable (collectively, "**Staff Personal Data**").

The purpose of this notice is to provide you further details regarding the Staff Personal Data that may be processed by FIS and how FIS collects and uses Staff Personal Data before, during, and after your employment or contract with FIS. FIS will only process your Staff Personal Data in accordance with this Privacy Notice and as permitted by applicable law. The term "processing" is used in this notice to cover all activities involving Staff Personal Data, including collecting, handling, updating, storing, deleting, sharing, accessing, viewing, using, transferring, and disposing of the Staff Personal Data. We encourage you to read this notice and the Appendix carefully and understand the contents. If you have any questions relating to FIS processing of Staff Personal Data, you should contact the FIS Privacy Office using the contact information listed in the Appendix.

The primary data controller for your Staff Personal Data is the FIS company which employs or contracts with you or to which you have made an application. If you have any questions about who this company is, please contact The People Office at the.people.office@fisglobal.com.

Description of Data Processing

Staff Personal Data includes all personal data collected and processed in the context of an individual's working relationship with FIS. For example, FIS processes Staff Personal Data regarding job candidates, temporary and permanent employees, contingent workers, independent contractors, retirees, and persons formerly in such roles with FIS. FIS also processes Staff Personal Data regarding relatives, dependents, or other persons in relation to job candidates, employees, contingent workers, independent contractors, retirees, and persons formerly in such roles with FIS when their personal data has been given to FIS by such persons with a working relationship with FIS. A list of the types of Staff Personal Data that may be processed is set out in the Appendix, together with the purposes of the data processing and the categories of the recipients of the data that may apply.

In some jurisdictions, Staff Personal Data that is considered "Sensitive Personal Data" under applicable laws may need to be collected as required or permitted by local law, for example, for the purposes of complying with equal opportunity measures or local tax requirements. In the attached Appendix, the relevant data categories in which Sensitive Personal Data might be included are listed separately.

The Staff Personal Data may be provided to FIS directly by the person to whom it relates, or by another person or company. For example, if you make an application for employment or accept employment with FIS, FIS may obtain information from recruiters, employment research firms, identity verification services, the references you provide, third-party websites, including through LinkedIn, and other publicly available sources. Where permitted by local law and with your consent, FIS may request background or credit checks from public authorities or financial institutions to evaluate your eligibility for employment or for certain tasks, as well as your medical information if required to evaluate your eligibility for employment benefits. For the purposes of meeting regulatory requirements, Staff Personal Data may be screened against third-party identification services and government-provided databases, which contain personal data and return results regarding potential matches to publicly available data.

Why FIS Collects, Uses, and Stores Staff Personal Data

FIS collects, uses, and stores Staff Personal Data where necessary to administer your contractual relationship with FIS, or in connection with services or opportunities which you request, where necessary to comply with a legal obligation, and where necessary pursuant to FIS' legitimate interests and where these interests are not overridden by your data protection rights. This means where we have a good legal reason to do so that does not prejudice your rights. For example, FIS has a legitimate interest in verifying the security and integrity of its facilities and systems and in verifying that relevant information for the conduct of our business is available across the FIS group. FIS may also process your Staff Personal Data in limited circumstances where you have given consent. Where FIS asks for consent, you are free to withhold or revoke it. Your revocation of consent will not invalidate prior processing of the Staff Personal Data by FIS based on the consent.

For more information on FIS' legal basis for processing Staff Personal Data, please consult the Appendix.

Who Do We Share Your Data With?

As FIS operates internationally, FIS needs to make Staff Personal Data available to other FIS entities, in limited circumstances to FIS clients, and to select external third-party service providers, such as payroll, benefit, and pension providers as well as tax advisors and information technology service providers performing services at FIS' request. FIS may also make Staff Personal Data available to other third parties, such as law enforcement, tax authorities, other public bodies, potential and actual acquirers of FIS companies or businesses if a change of ownership or business transfer is anticipated or occurs, and to marketing companies where such transfers are lawful and appropriate. In some circumstances, such as travel service companies, credit reporting agencies, payment service providers and the providers of corporate credit cards, the third party may be required or authorized to retain personal data about you to process for their own business purposes. In those circumstances the personal data as held and processed by the third party loses its character as Staff Personal Data subject to this Notice, and the third party will become responsible to safeguard the personal data and limit its use in accordance with their privacy policies and applicable laws.

Is Your Data Sent Abroad?

Such entities and third parties may be located in countries that may not have the same privacy and data protection laws and regulations as your home country. FIS will protect Staff Personal Data as required by applicable law and regulations, even when transferred across borders to a third party including, but not limited to, the use of European Commission-approved model clauses and other data transfer safeguards.

For more information on how FIS safeguards Staff Personal Data transfers, please contact the FIS Privacy Office as provided below.

Security

FIS works to maintain your confidence and trust and has implemented physical, technical, and organizational security measures designed to secure Staff Personal Data against accidental loss, misuse, and unlawful, unauthorized or accidental access, acquisition, disclosure, alteration, destruction, blocking, copying, or other unlawful forms of processing. FIS is committed to the confidentiality and security of Staff Personal Data. Access to Staff Personal Data within FIS is limited to those individuals who need the information to perform their job duties.

Choices and Rights

You may request further details regarding FIS' processing of your Staff Personal Data in accordance with local applicable law.

You may have certain rights over your personal data, depending on the applicable jurisdiction, including but not limited to:

- A right to receive information about your data or to access your data,
- A right to erase certain data,
- A right to stop your data being processed in certain circumstances,
- A right related to automated profiling,
- A right to data portability,
- A right to correct your data, and
- A right to opt-out of the sale of your data.

There are limitations in relation to these rights. Please consult the FIS Privacy Office or your local data protection authorities for more details.

It is your responsibility to correct the relevant FIS People Office information system (Workday, RMSystems, Oracle, and Kronos) with any change to either your own Staff Personal Data or that of others in a relationship with you, which are relevant to your relationship with FIS (e.g. for global mobility, emergency contact, and benefits purposes), such as home address, next of kin, bank account details, etc., so the Staff Personal Data remains accurate and complete.

If you are a job applicant, retiree, or other person without access to an FIS People Office information system, such requests should be directed to TPO.Privacy@fisglobal.com or the FIS Privacy Office using the contact information listed below.

Where Staff Personal Data is processed for the purposes of direct marketing, procedures will exist to allow you to opt-out of having your Staff Personal Data used for such marketing. This option refers to offers marketing consumer goods or FIS products or services to you and will not permit the opt-out of normal and customary communications regarding your employment relationship, including employee benefits and health and wellness programs made available by FIS.

Changes to this Notice

As this notice is updated or modified, the current version will be posted on the Corporate Governance section of our externally facing website, fisglobal.com, and on the company intranet within the Corporate Compliance page of FISandMe.

Contact Points for Data Protection Enquiries:

Chief Privacy Officer
FIS
601 Riverside Avenue
Jacksonville, FL 32204
E-mail: privacyoffice@fisglobal.com

Data Protection Officer
FIS
25 Canada Square, Canary Wharf
London E145LQ
United Kingdom
E-mail: data.protection@fisglobal.com

Please include your question regarding data privacy/security along with your contact details. EU individuals can contact the EU Supervisory authority if they have a complaint about how their data has been processed. Please contact the FIS Privacy Office if you are unsure where to direct a complaint.

APPENDIX - Description and Uses of Staff Personal Data

Purposes of the Processing

Staff Personal Data may be processed for the following purposes:

Purpose of Processing		Legal ground(s) for use
Designing, evaluating, benchmarking, and administering:	Compensation and benefits programs, including: salary, bonuses, pensions, medical benefits, insurance policies, vacation, and leaves of absence for employees and dependents	FIS relies on: • The need to process Staff Personal Data to fulfill the employment relationship or requests for employee benefits; • FIS' legitimate interests in conducting sanctions and anti-money laundering screening and meeting regulatory requirements; • FIS' legitimate interests in developing and managing its workforce; • FIS' legitimate interest in verifying meaningful equal opportunity monitoring and reporting. • The consent of the employee where legally required.
	Diversity programs, including compliance with diversity objectives, FIS controlled recognition and rewards programs, Employment-related education, training, and awareness programs	
	Global mobility programs and the transfer, relocation and movement of employees and dependents	
	Job descriptions	
	Manpower, staffing, and succession programs	
	New hire and departing staff activities and programs	
	Recruitment programs	
	Workplace safety and security measures	
Assembling, maintaining, and disseminating:	Business employment records for past, present, and potential employees	FIS relies on: • The need to process personal data to fulfill the employment / working relationship; • FIS' legitimate interests in preserving records for business purposes, assuring security at its facilities and systems, and making contact information available to relevant employees and clients; and • The consent of the employee where legally required.
	Company directories	
	Emergency contact information	
	Identification credentials	
	Business conferences and travel	FIS relies on:
	Business negotiations and transactions	

Purpose of Processing		Legal ground(s) for use
Supporting, executing, and facilitating:	Business operations, including staffing proposals and client billing, business transition activities, including mergers, acquisitions, and divestitures	• The need to process Staff Personal Data to fulfill the employment relationship or requests for employee benefits; • FIS' legitimate interests in developing and managing its workforce; • FIS' legitimate interests in promoting and delivering its products and services, developing business opportunities, and maintaining the security and integrity of its facilities, systems, and IT infrastructure; and • The consent of the employee, where legally required.
	Company marketing efforts, including websites, conferences, brochures, business cards, and other promotional media events and materials	
	Compliance with contractual obligations	
	Identification for security and systems authentication	
	Internal and external business communications, including email	
Complying with:	Applicable laws, regulations, and legal requirements, including reporting and disclosure obligations and tax filings	FIS relies on: • Legal record-keeping and reporting requirements; • FIS' legitimate interests in conducting sanctions and anti-money laundering screening and meeting regulatory requirements; • The need to process Staff Personal Data to fulfill the employment relationship or requests for employee benefits; • FIS' legitimate interests in developing and managing its workforce; • FIS' legitimate interests in promoting and delivering its products and services, developing business opportunities, and maintaining the security and integrity of its facilities, systems and IT infrastructure; and • The consent of the employee where legally required.
Conducting:	Audits and accounting, financial and economic analyses	FIS relies on: • FIS' legitimate interests in developing and managing its workforce; • FIS' legitimate interests in conducting sanctions and anti-money laundering screening and meeting regulatory requirements; • The need to process Staff Personal Data to fulfill the employment
	In accordance with local law, workplace investigations into alleged policy violations, misconduct related to work, safety, and security concerns	
	Opinion and engagement surveys	

Purpose of Processing		Legal ground(s) for use
		relationship or requests for employee benefits; • FIS' legitimate interests in preserving the integrity of the FIS workplace and understanding employee preferences; and • The consent of the employee where legally required.
Considering and evaluating:	Applicants for employment or engagement	FIS relies on: • The need to process Staff Personal Data for evaluation and tracking absences as an integral component of the employment relationship; • The need to process Staff Personal Data to fulfill the employment relationship or requests for employee benefits; • FIS' legitimate interests in managing its workforce and hiring appropriate personnel; • FIS' legitimate interests in analyzing performance and providing adequate compensation; • The consent of the employee where legally required; and • FIS' legitimate interest to satisfy legal requirements and to provide reasonable accommodations and assess fitness for duty.
	FIS controlled conduct, job performance and attendance, including for the purposes of performance appraisals, compensation decision-making, promotion, transfer, redeployment, and termination	
	Leaves of absence	
	Requests for reasonable accommodations, fitness for duty	
Maintaining and improving:	Workplace and staff health, i.e., vaccination status, temperature scanning, mask usage, etc.	FIS relies on: • FIS' legitimate interests in promoting and improving health, safety, security and performance; • FIS' legitimate interests in promoting and delivering its products and services, developing business opportunities, and maintaining the security and integrity of its facilities, systems and IT infrastructure; • Legal requirements to provide a safe and healthy work environment; and • The consent of the employee where legally required.
	Workplace and staff safety and security, i.e., thumbprints, facial identification/recognition, etc. used for device and security access for computers, phones, building and room access.	
	Workplace operations and performance	
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	FIS relies on: • FIS' legitimate interests in promoting and delivering its products and services, developing business opportunities, and maintaining the

Purpose of Processing		Legal ground(s) for use
	company work locations, and execution of backup and storage procedures	security and integrity of its facilities, systems and IT infrastructure; • FIS' legitimate interests in protecting the safety and security of staff, systems, and facilities; and • The consent of the employee where legally required.
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; • FIS' legitimate interest in protecting its rights and property; • FIS' legitimate interests in managing its workforce and hiring and retaining appropriate personnel; • The consent of the employee where legally required.
Monitoring and reviewing:	Communications and information on Company systems, including email and website usage, in connection with workplace investigations into alleged policy violations, misconduct related to work, safety, and security concerns	FIS relies on: • FIS' legitimate interests in protecting the integrity of FIS services, facilities, systems and staff; • FIS' legitimate interests in developing and managing its workforce; and • The consent of the employee where legally required.
	Compliance with company policies, procedures, and processes	
	FIS controlled attendance	
	Activity in FIS work locations	
Preparing for, defending, participating in, or responding to:	E-discovery requests for information	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; • FIS' legitimate interests in protecting its rights; and • The consent of the employee where legally required.
	Litigation or potential litigation	
Communicating and sharing of information	Internal administration and business management and planning purposes	FIS relies on:

with FIS companies or potential or actual acquirers of FIS companies or businesses for:	Reporting purposes and activities as part of the FIS group of companies Anticipated or occurring business transfers, company sales and re-organizations or changes in ownership	• FIS' legitimate interests to structure its business appropriately and legal obligations; • The need to process Staff Personal Data to fulfill the employment relationship or requests made by the employee; • The consent of the employee where legally required.
Processing and administering:	Payroll, tax, and other required withholdings (such as court-ordered garnishments) Reimbursements for business travel and other reimbursable business expenses	FIS relies on: • The need to process Staff Personal Data to fulfill the employment relationship or requests made by the employee; • Legal requirements to participate in legal process; and • The consent of the employee where legally required.

Categories of Staff Personal Data

Staff Personal Data processed concern the following categories of data:

Data Category	Examples
Advice, opinions, and other comments	Engagement surveys, exit interviews.
Attendance data	Work absences, leave entitlements and requests, attendance records, paid and unpaid leave records.
Bank and financial details	Payroll and/or expense reimbursement direct deposit banking information, credit card information.
Benefit data	Insurance, powers of attorney, benefit plans records for employees and/or dependents enrolled in benefit continuation records.
Business travel and movement data	Travel data, including travel schedules, lodging, conveyance, meals, and other expenses.
Company property issuance data	Records of Company-issued assets, equipment, and vehicles.
Compensation data	Base salary, bonus, and other compensation elements, pay type, pay grade, pay level, full-time equivalent (FTE), currency, compensation requests (past and current), employment terms.
Dependent information	Personal contact and identity data on dependents and significant others.
Disciplinary data	Warnings, letters of reprimand, written and oral counselling.

Data Category	Examples
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 Staff Personal Data included in or on company systems, equipment, or documents by employees or independent contractors, background and credit check data.
Key card and access records	Dates, times, and locations of entry and exit from controlled facilities, computer and system logon/off audit trails.
Military status	Branch of service, rank, dates of enlistment or discharge, discharge status, disabled veteran status, awards or medals granted, protected veteran status.
Organizational data	Name, company structure, organizational charts, reporting relationships, titles, resumes, work contact details, email, accounting code details, employment terms, job descriptions, and salary levels.
Payroll processing data	Name, government-issued ID, home address, email, time attendance, remuneration, compensation data, hire date, termination date, employment terms, dependents data, bank and financial data, benefit data, accounting code details, withholdings and deductions, and benefit enrolments with employee contribution.
Performance and employment	Performance assessments, Performance Improvement Plan (PIP), performance counselling, disciplinary action(s), letters of appreciation, details of performance complaints.
Personal details and contact information	Name, gender, birth date, place of birth, home address, phone numbers, email, government-issued identification numbers, identification numbers issued by or on behalf of the company, signatures, handwriting, and photographs.
Photo, video, or audio recordings	Information collected by security systems, closed-circuit television; profile photographs, photo security badges, voicemail, recorded trainings, conferences, or marketing materials.
Recruiting and application data	Application details, applicant testing, background check, notes compiled by recruiter pertaining to the applicant and screening results.
Reports of misconduct or policy violations	Records of oral, written, email, telephone or Ethics Helpline website, Ethics Helpline, InTIRT, FSIRT, SIRI-P and similar reports pertaining to alleged and confirmed staff misconduct or violations of company policies.
Right to work / immigration data	Right to work documents, nationality, residency, citizenship, passport, and visa information.
Software applications	Use of software applications to process employee data including in relation to employee engagement and collaboration, in order to improve efficiency at FIS.
Talent, education, and training details	Education, skills, work experience, prior employment, accomplishments, projects, development and training, language skills, technical skills, educational background, professional certifications and registrations, membership in professional bodies and organizations.

Data Category	Examples
Work history	Dates of hire and/or termination, title, dates of promotion, training courses attended, acknowledgement of company policies, completion of various mandatory company trainings with quiz scores, if applicable, reason for resignation or termination, public offices held, publications.
Work schedule data	Planned and actual working times, billable and administrative time records, employment terms, alternative working arrangements (remotely).
Workplace safety data	Reports, photographs, video recordings.

Sensitive Data (if appropriate)

In some jurisdictions, Staff Personal Data that is given special treatment as "Sensitive Personal Data", "Special Categories of Personal Data" or similar designations under applicable laws may need to be processed as permitted or required by local law. For example, for the purposes of equal opportunity measures or tax requirements. We refer to such personal data as "Sensitive Personal Data" in this Notice. What is considered Sensitive Personal Data varies from country to country, but it generally includes information relating to a person's sexual orientation, racial or ethnic origin, alleged or actual criminal offense, physical or mental health or condition, trade union membership, political opinions, religious beliefs, or biometric data. Please note, this does not mean that all the listed examples of Sensitive Personal Data will be processed for every employee, but only insofar as deemed necessary for the purposes of the legitimate interests pursued by FIS from time to time and always in compliance with applicable laws. Applicable local law may in some circumstances require the data subject's consent to process Sensitive Personal Data.

Potential Categories of Sensitive Personal Data:

Sensitive Data Category	Examples
Biometric and Health Data	Fingerprints, thumbprints, temperature scanning, facial identification/recognition
Data revealing offenses, criminal convictions, or information deriving from security measures	Criminal proceedings, outcomes, and sentences, driving history, prior employment, substance abuse screening, court records, and background check information.
Data revealing sex life	Personal contact and identity data on dependents and significant others, marital/partnership status, accommodation, and housing information.
Data revealing personal credit and financial information	Credit check, child support, debt payments, bankruptcy, foreclosure.
Data revealing physical or mental health or condition	Physical limitations and special needs, on-site screenings, company referrals for medical or counselling support, substance abuse testing, health certifications.
Data revealing racial or ethnic origin	Racial designations, nationality, and cultural identity.
Data revealing religious affiliation or beliefs or other beliefs of a similar nature	Affiliation with religious organizations, declaration of religious preference.

Sensitive Data Category	Examples
Data revealing trade union membership	Union or works council records, directories, meeting documentation and other materials.
Data revealing political opinions	Professional and other affiliations, offices held, publications and writings.

Recipients

Staff Personal Data may be disclosed to the following recipients or categories of recipients for a legitimate business need and/or process: FIS People Office, Legal, Corporate Compliance, RISC, Internal Audit, Finance and Accounting, Security, Information Systems, members of the Board of Directors, management personnel, FIS Clients, and FIS-selected service providers. FIS may also make Staff Personal Data available to other third parties as authorized, such as law enforcement, tax authorities, other public bodies, potential and actual acquirers of FIS companies or businesses if a change of ownership or business transfer is anticipated or occurs.

Storage limits and other relevant information

Staff Personal Data will be retained for as long as there is a business need or as required by law and regulation. More information on FIS' data retention standards may be found in the Record Management Policy found in the FIS Enterprise Policy Office on the company's intranet, FISandMe. If you are a job applicant, retiree, or other person without access to FIS systems to review such policies, requests for such information should be directed to the FIS Privacy Office.