Corporate Employee Personal Information Privacy Notice & Policy

Effective Date: June 2014

Last Reviewed: May 2014

Next Review: May 2015

In the course of your employment, Fidelity may collect information about you and your employment relationship with Fidelity, as well as information about your spouse, domestic/civil partner, and/or dependents. By collecting this information, Fidelity has certain responsibilities under the data protection legislation of the countries in which our employees reside, and employees also have obligations regarding the information.

Purpose and Scope

This policy addresses the collection and use of Personal Information of employees and the responsibilities of Fidelity, its employees, and employees of its affiliates regarding such Information.

This policy is applicable to all regular full-time, regular part-time, and temporary employees of Fidelity Investments, regardless of citizenship, residence or job location.

Information We Collect and Use

In the course of your employment, Fidelity may collect information about you and your employment relationship with Fidelity, as well as information about your spouse, domestic/civil partner, and/or dependents ("Dependents"). When that information is identifiable to an individual, we refer to such information as "Personal Information".

Fidelity takes reasonable measures to ensure that it uses Personal Information collected only in ways compatible with the purposes described in this policy, unless it is required or authorized by law, authorized by you, or is necessary for emergency purposes.

With the exception of certain information that is necessary to make possible your employment by Fidelity, required by law or important to the performance of our business, your decision to provide Personal Information to Fidelity is voluntary. However, if you do not provide certain information, Fidelity may not be able to accomplish some of the purposes outlined in this policy.

Transfer, Disclosure and Joint Use of Personal Information

Due to the global nature of Fidelity's operations and systems, Fidelity may disclose Personal Information to personnel and departments throughout the company, its affiliates, and unaffiliated third parties.

- This may include transferring Personal Information to other countries (including countries other than where you reside that may have different data protection regimes than are found in the country where you are based).
- If you are located in the European Economic Area (the "EEA") this may include countries outside of the EEA.

Access to Personal Information within Fidelity will be limited to those who have a need to know the information for the purposes described here, and may include your managers, their designees, and other personnel at Fidelity such as, but not limited to, Human Resources, Compliance, Security, IT and Audit.

All personnel within Fidelity will generally have access to your business contact information, or other similar information classified as "Fidelity Internal Information". This information includes data elements such as name, position, work telephone number, work address, work email address, organizational information, photo, "tags", preferred personal contact information, and other data you submit to the company directory ("Who's Who") for public viewing. For a list of Personal Information that is classified as "Fidelity Internal Information" please see the supplemental hard card.

From time to time, Fidelity may need to make Personal Information available to unaffiliated third parties. For a list of the categories of unaffiliated third parties, please see the definitions section.

- Some unaffiliated third parties may not be located in your home jurisdiction.
- Third party service providers and professional advisors are required to protect the confidentiality and security of Personal Information, and only use Personal Information for the provision of services to Fidelity and its affiliates, and in compliance with applicable law.

All Personal Information is classified as "Fidelity Highly Confidential" unless deemed "Fidelity Internal" or otherwise as approved by the appropriate BU ISO, Chief Privacy Officer or Workforce Data Privacy Program Office

Data Security

Fidelity takes reasonable measures to protect Personal Information that are consistent with applicable privacy and data security laws and regulations and Fidelity policies, including requiring service providers to use appropriate measures to protect the confidentiality and security of Personal Information.

Data Integrity

Fidelity takes reasonable steps to ensure that any Personal Information processed is reliable, accurate and complete for its intended use.

Data Retention

Fidelity retains Personal Information at least for the period necessary to fulfill the purposes for which it was collected unless a longer retention period is required or permitted by law.

Questions and Concerns

If you have any questions or concerns about how Fidelity processes Personal Information, or if you wish to access, correct, restrict or delete your Personal Information, please contact HR Solutions, your Human Resources Representative, your regional Data Privacy or Grievance Officer (India), or the Workforce Data Privacy Program Office, as applicable (refer to the contact section for more information). Please note Fidelity may be exempt from such requests pursuant to applicable law.

Company Systems

All information, including Personal Information, placed on or sent using Fidelity's systems (including third party systems provided by Fidelity or accessed through Fidelity's systems) may be monitored, examined, recorded, copied, disclosed, and used in accordance with Fidelity's policies (for example, The Electronic Communications, Social Media and Systems Usage Policy) and applicable law.

Employees' Obligations

You must keep Personal Information up to date and inform Fidelity of any significant changes to your Personal Information.

If you provide Personal Information about your spouse, domestic/civil partner, dependents or related parties, Fidelity will assume that you have informed them about the content of this Policy, and have obtained their consent (provided they are legally competent to give consent or you have the right to grant consent) for the use (including transfer and disclosure) of that Personal Information by Fidelity.

You must agree to follow applicable law and Fidelity's policies, standards and procedures when handling any Personal Information about others to which you have access in the course of your employment relationship with Fidelity. In particular, you have agreed that you will not access or use any such Personal Information for any purpose other than in connection with and to the extent necessary for your work for Fidelity.

You understand that these obligations continue to exist after termination of your relationship with Fidelity.

Exception Approval Process

Any exceptions to this policy, or related policies and procedures must be approved in writing and in advance by the appropriate BU ISO, HR ISO, local Data Protection Officer, or Workforce Data Privacy Program Office.

Definitions

As used in this policy, the terms below have the following meanings.

Personal Information Any data, or combination of data, collected or maintained by Fidelity for its business purposes, by which a particular individual can be identified or that would allow an unauthorized person to access or use an individual's financial or benefits account, or health or compensation information.

Third Parties Any unaffiliated entities, such as external service providers or vendors, with whom Fidelity may share Personal Information. Categories of third parties include the following:

- Professional Advisors: Accountants, auditors, lawyers, insurers, bankers, and other outside professional advisors
- Service Providers: Companies that provide products and services to Fidelity or its employees such as payroll, pension administrators, medical and health benefits, human resources, performance management, training, expense management, travel services, technology systems and support, equity compensation programs, credit card companies, and trade bodies and associations, and other services providers
- Public and Governmental Authorities: Entities that regulate or have jurisdiction over Fidelity such as regulatory authorities, law enforcement, and public and judicial bodies
- Corporate Transaction: A third party in connection with any proposed or actual reorganization, merger, sale, joint venture, assignment, transfer or other disposition of all or any portion of Fidelity business, assets or stock (including in connection with any bankruptcy or similar proceedings)

Types Of Personal Information We May Collect

Personal Details

Name, employee identification number, work and home contact details (email, phone numbers, physical address) language(s) spoken, gender, date of birth, national identification number or social security number where applicable, marital/civil partnership status, domestic partners, dependents, disability status, emergency contact information and photograph, or similar information.

Documentation Required under Immigration Laws

Citizenship, passport data, details of residency or work permit, or similar information.

Compensation, Payroll and Related Financial Information

Base salary, bonus, benefits, compensation type, salary step within assigned grade, details on stock options, stock grants and other awards, currency, pay frequency, effective date of current compensation, salary reviews, banking details, working time records (including vacation and other absence records, leave status, hours worked and department standard hours), pay data and termination date, or similar information.

Employment Details

Description of current position, job title, corporate status, management category, job code, salary plan, pay grade or level, job function(s) and subfunction(s), company name and code (legal employer entity), branch/unit/department, location, employment status and type, full-time/part-time, terms of employment, employment contract, work history, hire/re-hire and termination date(s) and reason, rehire eligibility, length of service, retirement eligibility, promotions and disciplinary records, date of transfers, and reporting manager(s) information, and similar information.

Talent Management Information

Details contained in letters of application and resume/CV (previous employment background, education history, professional qualifications, language and other relevant skills, certification, certification expiration dates, securities licenses), information necessary to complete a background check, details on performance management ratings, development programs planned and attended, e-learning programs, performance and development reviews, willingness to relocate, driver's license information, and information used to populate employee biographies, and similar information.

System and Application Access Data

Information required to access company systems and applications such as System ID, LAN ID, email account, instant messaging account, mainframe ID, previous employee ID, previous manager employee ID, system passwords, branch, state, country code, previous company details, previous branch details, previous department details, and electronic content produced by you using Company systems, or similar information.

Facilities Access Data

Key card ("badge") number and CCTV recordings which may be associated with the building(s) to which you have access, the floors to which you have access, the hours during which you have access to each location, the reason(s) for which you were given access, "access data" (including the time you entered and exited security checkpoints using your badge or as a recording on CCTV), or similar information, all in accordance with applicable law.

Regulatory and Compliance Information

We may also collect certain types of information required to confirm compliance with laws or regulations, such as business entertainment and workplace gifts; personal security transactions; Conflicts of Interest; and political contributions.

Sensitive Information

Types of sensitive information required only when needed for business purposes and as permitted by local law, such as health/medical information, place of birth, trade union membership information, religion or church affiliation, sexual orientation, biometric information including fingerprint, financial information,(e.g. bank account/credit or debit card or other payment instrument details), and race or ethnicity in order to comply with legal obligations and internal policies (such as relating to diversity and anti-discrimination).

Purposes For Which We May Use and Disclose Personal Information

Managing Workforce

Managing workplace and personal activities, including recruitment, hiring, appraisals, performance management, promotions and succession planning, rehiring, salary, and payment administration and reviews, wages and other awards (such as stock options, stock grants and bonuses), healthcare, pensions and savings plans, training, leave, transfers, secondments, other contractual benefits, providing employment references, loans, performing workforce analysis and planning, employee surveys, background checks, providing access to facilities, managing disciplinary matters, grievances and terminations, reviewing employment decisions, making business travel arrangements, managing business expenses and reimbursements, planning and monitoring of training requirements and career development activities and skills, and creating and maintaining one or more internal employee directories.

Communications, Facilities and Emergencies

Facilitating communication with you, ensuring business continuity, providing references, protecting the health and safety of employees and others, safeguarding IT infrastructure, office equipment, facilities and other property, facilitating communication with you and your nominated contacts in an emergency.

Business Operations

Operating and managing the IT and communications systems, managing product and service development, improving products and services, managing company assets, allocating company assets and human resources, strategic planning, project management, business continuity, compilation of audit trails (including records of changes you may make to customer accounts) and other reporting tools, maintaining records relating to business activities, budgeting, financial management and reporting, communications, managing mergers, acquisitions, sales, re-organizations or disposals and integration with purchaser.

Compliance

Complying with legal and other requirements, such as income tax and national insurance deductions, record-keeping and reporting obligations, physical access policies, conducting audits, compliance with government inspections and other requests from government or other public authorities, responding to legal process such as subpoenas, pursuing legal rights and remedies, defending litigation and managing any internal complaints or claims, conducting investigations and complying with internal policies and procedures.

Contacts & Web resources

General Program and Policy Questions or Violations

Corporate Workforce Data Privacy Program

HR Solutions (800) 835-5099, option 2

Chairman's Line (800-242-4762)

For US Associates with Health Privacy Questions

HIPAA Privacy Officer

Mailzone: Z1J

For Indian Associates

India Data Privacy Grievance Officer

Phone: +91 080 6691 6079

Grievance.Officer@fmr.com

For Canadian Associates

Canada Chief Privacy Officer

fax (416)307-5349

phone (800)263-4077

mail: Attention Chief Privacy Officer

Fidelity Investments

483 Bay Street, Suite 200,

Toronto, Ontario, M5G 2N7

General Program Information

Employee Data Privacy Ribbit Site

Supplemental Hard card

Related policies and procedures

Corporate Employee Personal Information Privacy Policy - India Supplement

Privacy Information Security Policy (CS-004)

Information Protection Policy (SP2I) (CS-601)

Corporate Policy on Electronic Communications, Social Media, and Systems Usage (CS-506)

Vendor Management Oversight Policy

Vendor Framework Policy (CS-606)

Vendor Privacy Oversight policy

Privacy Governance Framework: Third-Party Vendor Oversight

All other Information Security Policies: pcs.fmr.com