Global Privacy Policy

Table of Contents

Introduction

Policy Overview

FedEx Corporation (together with its subsidiaries and affiliated companies, "FedEx") recognizes the importance of having effective privacy protections in place and is committed to compliance with applicable data privacy laws, regulations, internal policies and standards. These protections form the foundation of a trustworthy company, are necessary to maintain the confidence of customers and employees and ensure the company's own compliance with such local laws. This Global Privacy Policy ("Policy") is based on globally accepted, basic principles on data protection.

Scope

This Policy applies worldwide to all employees and companies of FedEx. Individual operating companies may not adopt policies inconsistent with this Policy. Supplemental data Protection requirements for individual operating companies, regions or countries may be created with the approval of the Global Chief Compliance and Governance Officer ("GCCGO").

Application of Local Laws

Each operating company of FedEx is responsible for compliance with this Policy. If there is reason to believe that local law requirements or other legal obligations contradict the duties under this Policy, the relevant operating company must inform the GCCGO. In the event of conflicts between applicable local laws, rules or regulations and the Policy, FedEx will work to find a practical solution that reconciles these requirements.

Definitions

Personal Data — Any information that can directly or indirectly be used to identify a natural person, whether that individual is an employee, a customer or employee of a customer, a vendor or employee of a vendor, a job applicant or any other third party.

Examples:

- Names
- Government-issued identification numbers (social security and driver's license numbers, etc.)
- Addresses
- Phone numbers
- Email addresses
- Photos

Processing — Any operation performed on Personal Data, with or without the use of automated systems, such as to collect, store, organize, retain, archive, record, view, modify, adapt, alter, query, use, retrieve, forward, transmit or combine data. This also includes disposing of, deleting, erasing, destroying or blocking data.

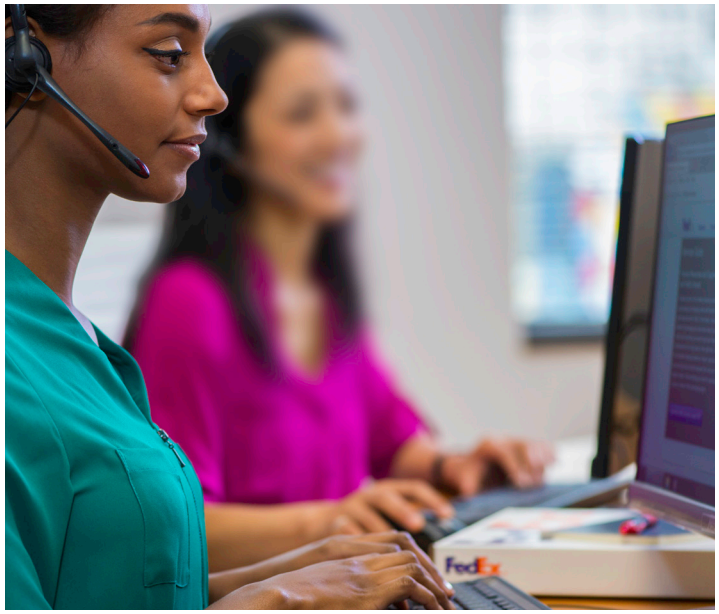
Examples:

- Storing information in databases
- Viewing information stored on another computer
- Transferring information from one database to another

Notes:

Data that has been anonymized such that individuals cannot be identified does not constitute Personal Data.

The transportation of physical media (documents, computers, etc.) containing Personal Data does not constitute Processing of that Personal Data.

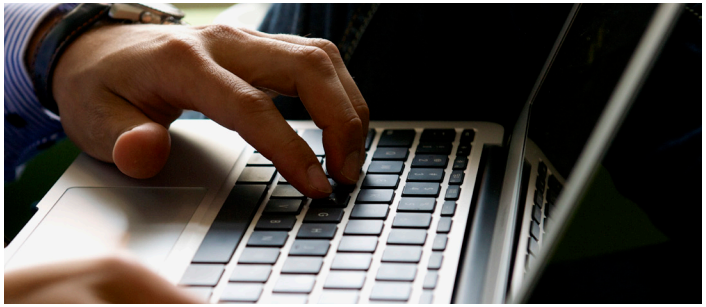


Data Protection Principles

Personal Data will be collected, recorded and used in a proper and professional manner, whether the Personal Data is on paper, in computer records or recorded by any other means.

FedEx is accountable for and must be able to demonstrate compliance with the following principles of data protection.

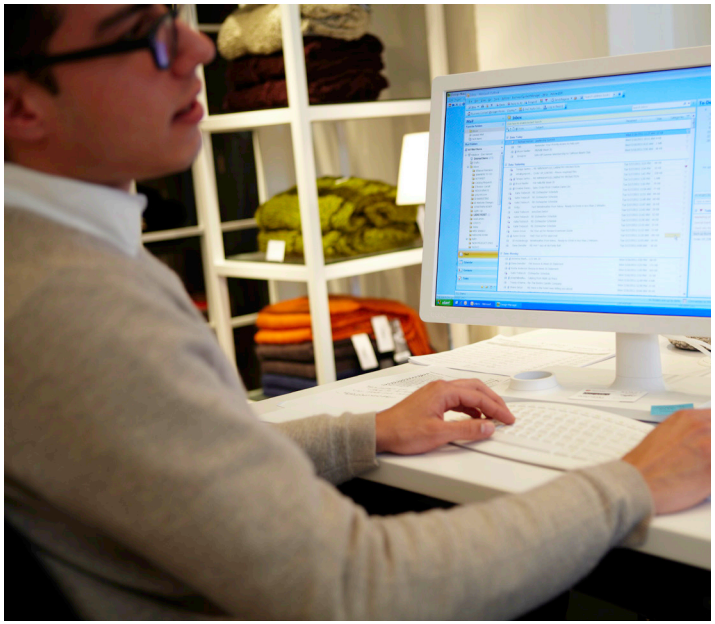
1. **Fair and Lawful.** When Processing Personal Data, the rights of the individual related to their Personal Data must be protected. Personal Data must be collected and Processed fairly and lawfully.
2. **Purpose Specification.** Personal Data can be used or Processed only for the purpose defined at the time of collection and shall not be further used or Processed in any manner incompatible with that purpose. Personal Data may not be collected and stored for potential future use unless allowed by local law.
3. **Collection Limitation.** FedEx only collects Personal Data necessary to meet the specified purpose at the time of collection and only to the extent allowed by local law.
4. **Deletion.** Personal Data no longer needed for the purpose specified at the time of collection shall be deleted according to applicable retention schedules unless it is subject to an exception from the Legal Department.
5. **Data Quality.** Personal Data should be accurate, and if necessary, kept up to date.
6. **Security Safeguards.** Personal Data must be protected using technical, managerial and physical security measures against risk of loss or unauthorized access, destruction, use, modification or disclosure.
7. **Transparency.** Individuals must be notified at the time of collection how their Personal Data is being used or Processed. They must be aware of who is collecting the Personal Data, the purpose for the Processing of the Personal Data and if third parties will Process the Personal Data, that adequate safeguards are in place. All such notices must be approved by the Legal Department.
8. **Individual Participation.** To the extent required by local law, individuals have a right to access their Personal Data and, where appropriate, to correct or delete it and exercise any other right provided by local law.



Security and Access

Personal Data is classified as confidential. Any unauthorized Processing of such data by employees is prohibited. Any Processing undertaken by an employee that is not part of his or her legitimate duties is prohibited. Employees may have access to Personal Data only as is appropriate for the type and scope of the task in question. This requires the definition and separation, as well as implementation, of roles and responsibilities.

Employees are prohibited from using Personal Data outside of the scope of their employment at FedEx, to disclose it to unauthorized persons or to make it available in any other way outside the permitted business use. Supervisors must inform their employees at the start of the employment relationship about the obligation to protect Personal Data. This obligation shall remain in force even after employment has ended.



Personal Data must be safeguarded from unauthorized access and unlawful Processing or disclosure. This applies regardless of whether data is Processed electronically or in paper form. Before the introduction of new methods of data Processing, a privacy impact assessment should be performed for new IT systems, which may lead to implementing technical and organizational measures to protect Personal Data.

Employees are expected to follow FedEx Information Security Standards, which can be found by searching keyword "standards." Note that Information Security classifies all data as Sensitive, Internal or Public. Depending on its classification, Personal Data must be protected in accordance with the applicable Information Security Standards.

In the event of suspicious activity, suspected cyberattack, suspected security incident, or possible breach of Personal Data, all FedEx employees must notify Information Security immediately via the Incident Notification Website, keyword "incident" or call 901/224- 2021 or 901/224-2022 to report the incident.

Special Circumstances

Data Transferring or Processing by Third Parties

Personal Data may not be transferred to a country outside the country of origin unless the transfer has been approved by the Legal Department, who will ensure an adequate level of data protection or suitable safeguards are in place. If a vendor or third party is engaged to Process Personal Data, a data transfer agreement must be in place with that external provider. An external provider can Process Personal Data only in accordance with instructions from FedEx.

Processing of Special Categories of Personal Data

Special categories of Personal Data that are highly sensitive can be Processed only under certain conditions. These categories include an individual's racial and ethnic origin, political beliefs, religious or philosophical beliefs, union membership or the health and sexual life of the data subject. Under local law(s), further data categories may necessitate special treatment. Personal Data that relates to a crime can often be Processed under special requirements of local law. Leave requests, that include special categories of data, will be handled by local Human Resources and Legal Departments.

If there are plans to implement a new system, procedure or Process that includes Personal Data in a special category, the GCCGO must be informed in advance.

Telecommunications and Internet

Telephone equipment, email addresses, intranet and Internet, along with internal social networks are provided primarily for work-related assignments. They can be used within the applicable legal regulations and internal policies. In the event of limited acceptable usage for private purposes, the local laws on secrecy of telecommunications and any local telecommunication laws must be observed.

Communication and Responsibilities

All Employees are responsible for:

- Reading and complying with this Policy and related policies, along with related documents/guidelines that may be developed and maintained to implement the requirements of this Policy.
- Reporting violations of this Policy.

Management is additionally responsible for:

- Ensuring all reporting personnel understand the requirements of this Policy.
- Ensuring appropriate safeguards are in place to protect Personal Data.
- Providing all necessary training and/or guidance to assist with the implementation process, and for monitoring compliance with this Policy.

Related Policies

- Code of Business Conduct and Ethics
- Information Security Standards
- Your company's Use of Computer Resources Policy
- Your company's Pre-employment Screening Policy
- Your company's Recruitment Policy
- Your company's Data Retention and Destruction Schedules
- Keyword "incident"

Anti-Retaliation Policy

FedEx prohibits any form of retaliation for reporting in good faith a suspected violation of this Policy.

Policy Custodian

Global Chief Compliance & Governance Officer

Adoption Date

This Policy was adopted effective May 1, 2018.