全球隐私政策

目录

简介 2

政策概述
范围
当地法律的适用

定义 3

数据保护原则 4

安全和访问权限 5

特殊情况 6

由第三方传输或处理数据
处理特殊类别的个人数据
电信和互联网

通信和责任 7

相关政策
反报复政策
政策保管人
通过日期

简介

政策概述

FedEx Corporation（与其子公司和关联公司一起统称为“FedEx”）认识到设置有效隐私保护措施的重要性，并承诺遵守适用的数据隐私法律、法规、内部政策和标准。这些保护措施是构成一家值得信赖公司的基石，是维持客户与员工信心所必要的，并能确保公司自身符合当地此类法律的要求。本全球隐私政策（以下简称“政策”）基于全球公认的有关数据保护的基本原则制定。

范围

本政策适用于FedEx全球范围内的全体员工和公司。各自运营的公司所采用的政策可能与本政策不一致。经全球首席合规与治理官（Global Chief Compliance and Governance Officer，以下简称“GCCGO”）批准后，可创建针对各自运营的公司、地区或国家的补充数据保护要求。

当地法律的适用

FedEx的每家运营公司都有责任遵守本政策。如果有理由认为当地法律要求或其他法律义务与本政策下的规定相矛盾，相关运营公司必须告知GCCGO。如果当地适用的法律、规则或法规与本政策之间发生冲突，FedEx将努力寻求切实可行的解决方案，以兼顾这些要求。

定义

个人数据 — 可直接或间接用于识别自然人的任何信息，无论该个人是员工、客户或客户的员工、供应商或供应商的员工、求职者或者任何其他第三方。

示例：

- 姓名
- 政府签发的身份识别号码（社会安全号码和驾驶证号码等）
- 地址
- 电话号码
- 电子邮件地址
- 照片

处理 — 对个人数据所执行的任何操作（无论是否使用自动化系统），例如收集、存储、组织、保留、存档、记录、查看、修改、调整、更改、查询、使用、检索、转发、传输或合并数据。此类操作还包括处置、删除、清除、销毁或阻止数据。

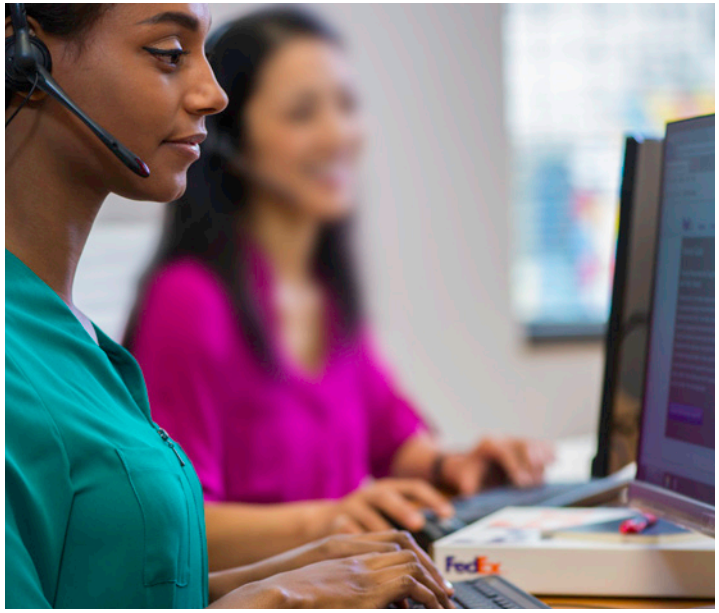
示例：

- 在数据库中存储信息
- 查看存储在其他计算机上的信息
- 将信息从一个数据库传输到另一个数据库

备注：

经过匿名处理而导致无法识别个人信息主体的数据不应视为个人数据。

包含个人数据的物理介质（文档、计算机等）的运输不应视为该个人数据的处理。

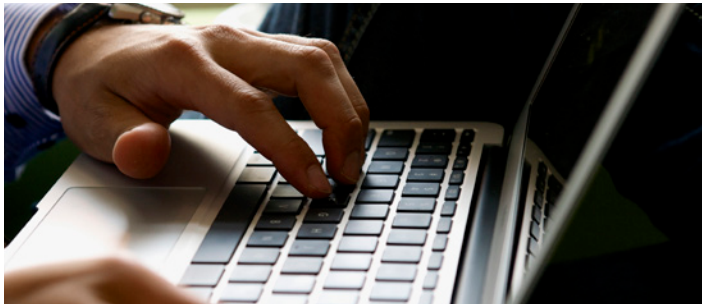


数据保护原则

个人数据将以适当且专业的方式收集、记录和使用，无论该个人数据是记录在纸上、存在于计算机记录中，还是通过任何其他方式记录。

FedEx有责任且必须能够证明其遵守下列数据保护原则。

1. **公平及合法。**处理个人数据时，与个人数据相关的个人的权利必须受到保护。个人数据的收集和处理应符合公平合法的原则。
2. **目的说明。**使用或处理个人数据的目的必须与收集时定义的目的一致，不得以违背该目的的任何方式进一步使用或处理个人数据。除非当地法律允许，否则不得收集或存储个人数据以备将来可能使用。
3. **收集限制。**FedEx仅收集满足收集时所述目的所必需的个人数据，且不得超出当地法律允许的范围。
4. **删除。**个人数据若不再适用于收集时所述目的，应根据适用的保留时间表予以删除，除非法务部另有要求。
5. **数据质量。**个人数据应准确，如有必要还应及时更新。
6. **安全保护。**必须使用技术、管理和物理安全措施来保护个人数据，避免丢失、未经授权的访问、销毁、使用、修改或泄漏等风险。
7. **透明。**收集个人数据时，必须告知相关个人将如何使用或处理其数据。他们必须知道收集个人数据的人员、处理个人数据的目的，以及如果将由第三方处理个人数据则是否有足够的保护措施。所有此类通知都必须由法务部批准。
8. **个人参与。**在当地法律允许的前提下，个人有权访问其个人数据，并在适当情况下，更正或删除该数据并行使当地法律赋予的任何其他权利。



安全和访问权限

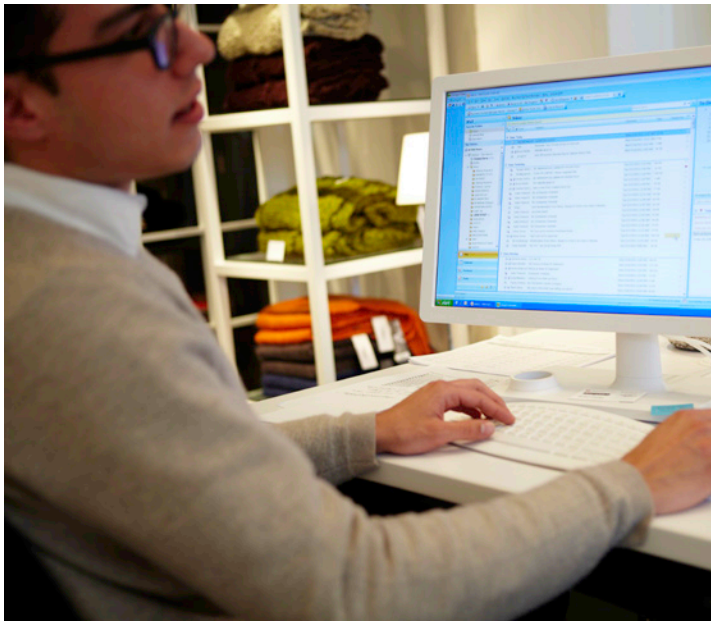
个人数据被归为“机密信息”。禁止员工在未经授权的情况下处理此类数据。禁止员工进行不属于其合法职责范围内的任何处理。员工仅可访问所执行任务的类型和范围所对应的相应个人数据。为此，需要对职务和责任进行定义、划分和落实。

禁止员工在其FedEx工作范围外使用个人数据、将该数据泄露给未经授权的人员，或者以任何方式在允许的商业用途之外提供该数据。在雇用关系开始之时，主管必须告知员工保护个人数据的义务。即使在雇用关系结束之后，该项义务仍应继续有效。

必须保护个人数据的安全，避免未经授权的访问以及非法处理或泄露。该项规定对于以电子方式或纸质方式处理数据均适用。在引入新的数据处理方法之前，应对新的IT系统执行隐私影响评估，评估的结果可能要求实施技术和组织上的措施来保护个人数据。

员工应遵守FedEx信息安全标准，可通过搜索关键字“标准”找到该标准。请注意，信息安全部将所有数据分类为“敏感”、“内部”或“公共”。必须根据信息安全部的分类，按照适用的信息安全标准来保护个人数据。

如遇可疑活动、疑似网络攻击、疑似安全事件或可能的个人数据违规行为，FedEx全体员工都必须立即通过事件通知网站、搜索关键字“事件”或拨打901/224-2021或901/224-2022，向信息安全部报告上述事件。



特殊情况

由第三方传输或处理数据

不能将个人数据传输到数据来源国以外的国家/地区，除非该传输已经过法务部批准，该部门将确保采取足够的数据保护水平或适当的保护措施。如果委托某个供应商或第三方处理个人数据，则必须与该外部提供商签订数据传输协议。外部提供商只能根据FedEx的指示处理个人数据。

处理特殊类别的个人数据

只能在特定条件下处理高度敏感的特殊类别个人数据。这些类别包括个人的种族和民族、政治信仰、宗教或哲学信仰、工会成员身份，或者健康状况和性生活。视当地法律而定，可能还有其他数据类别需要特殊对待。与犯罪相关的个人数据通常可以根据当地法律的特殊要求进行处理。包含特殊类别数据的休假申请将由当地人力资源部和法务部进行处理。

如果计划实施包含特殊类别个人数据的新系统、程序或流程，必须提前通知GCCGO。

电信和互联网

所提供的电话设备、电子邮件地址、内部网、互联网以及内部社交网络主要用于工作相关的任务。可以在适用的法律法规和内部政策允许的范围内使用这些资源。如因私人目的而需在有限的、可接受的范围内使用这些资源，则必须遵守当地有关电信保密的法律以及任何当地电信法律。

通信和责任

所有员工都有责任：

- 阅读和遵守本政策、相关政策以及为履行本政策要求而制定及维持的相关文件/准则。
- 报告违反政策的行为。

管理层另外还负有以下责任：

- 确保所有下属人员了解本政策的要求。
- 确保有适当的措施保护个人数据安全。
- 提供所有必要的培训及/或指导，协助执行流程并监督政策的遵守。

相关政策

- 职业道德和商业行为规范
- 信息安全标准
- 所在公司的计算机资源使用政策
- 所在公司的聘用前筛选政策
- 所在公司的招聘政策
- 所在公司的数据保留和销毁时间表
- 关键字“事件”

反报复政策

FedEx禁止对善意举报疑似违反政策行为的举报人实施任何形式的报复。

政策保管人

全球首席合规与治理官

通过日期

本政策于2018年5月1日通过并生效。