Dropbox

隐私和数据保护

简介

个人数据对于社会和经济的发展至关重要。人们逐渐开始寻求进一步掌控并了解与其交往的企业如何使用和保护其个人数据。

在 Dropbox，信任是我们与全球范围内数百万用户和企业建立良好关系的基石。我们重视您给予我们的信心，并积极承担严密保护您的个人数据的责任。

我们对您的承诺

我们致力于保护您的个人数据。Dropbox 的服务条款概述了您在使用我们服务时需承担的责任。我们的隐私政策写明了我们对用户的隐私承诺，并解释了您在使用我们的服务时，我们是如何收集、使用和处理您的个人数据。如果您居住在北美地区（美国、加拿大和墨西哥），则您的服务提供商为 Dropbox, Inc.。

而其他所有用户的个人数据由 Dropbox International Unlimited Company 控制。

如果您是一名 Dropbox Business 或 Dropbox Education 用户，那么在使用 Dropbox Business 或 Dropbox Education 时向 Dropbox 提供的任何个人数据由您的企业控制。数据控制者决定处理个人数据的目的和方法。您在使用 Dropbox Business 或 Dropbox Education，以及使用包括我们对数据处理和国际数据转移做出的承诺在内的 Business 协议时，Dropbox 将代表您的企业处理相关数据。

我们的业绩记录：合规性

合规性是检验服务是否值得信任的有效方式。我们鼓励并乐意提供独立验证，以表明我们的安全和隐私措施符合普遍认可的标准和规定，如 ISO 27001、ISO 27017、ISO 27018、HIPPA/HITECH、德国 BSI C5 和 SOC 1、2 和 3。

此外，我们是最先获得 ISO 27018 认证的云服务提供商之一。ISO 27018 是一项公认标准，证明企业在云隐私和数据保护方面实现领先实践。我们的独立第三方审计师负责测试我们对数据的控制，并提供他们的报告和意见。我们会尽可能与您分享这些内容。

请注意，尽管我们的认证和审计报告的范围通常为 Dropbox Business 和 Dropbox Education，但我们对大部分的控制范围涵盖 Dropbox Basic、Plus 和 Professional 用户。更多有关我们遵从的标准和我们如何检验安全措施的信息，请参阅我们的合规性网页。

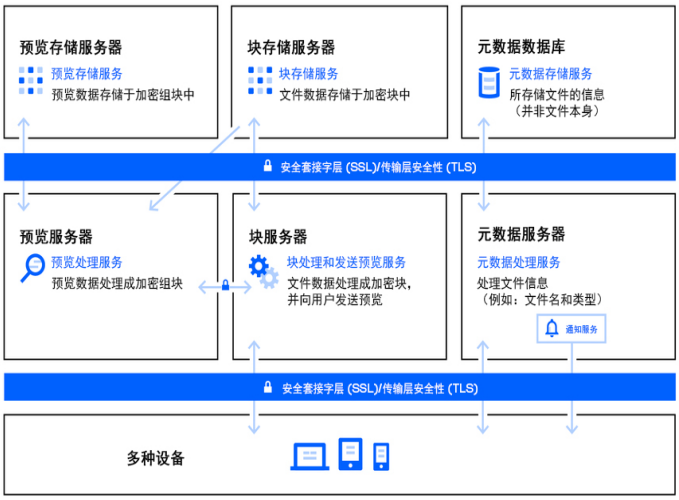
Dropbox

Dropbox 架构：保护您的个人数据

在 Dropbox，我们相信只有首先确保您的数据安全，才能保护您的个人数据。为此，Dropbox 设计了多层保护，包括在安全可扩展的基础设施中设置安全数据传输、加密和应用级控制功能。

我们的基础设施：文件

Dropbox 针对文件的基础设施由下图所示的组件构成。



元数据服务器

有关用户数据的特定基本信息被称为元数据，元数据存储在自己独立的存储服务中，在用户帐户中充当着数据索引的角色。元数据包括基本帐户和用户信息，如电子邮件地址、名称和设备名称。元数据还包括文件名和类型等有关文件的基本信息，这些信息可用于支持版本历史、恢复和同步等功能。

元数据数据库

文件元数据存储在基于 MySQL 的元数据服务中，并会根据需要进行分片和复制，以满足性能和高可用性的要求。

屏蔽服务器

在设计过程中，Dropbox 所提供的独特安全机制超越传统的加密技术，可以保护用户数据。块服务器通过将每个文件分块，使用强密码对每个文件块进行加密，并仅同步修订版之间修改的块，从而处理来自 Dropbox 应用程序的文件。当 Dropbox 应用程序检测到新的文件或更改现有文件时，应用程序会向块服务器发送更改通知，新的或修改的文件块会被处理并传输到存储服务器中。

块存储服务器

块存储服务器会以加密数据块的形式存储用户文件的实际内容。在传输之前，Dropbox 客户端会将文件拆分为多个文件块，以为存储做准备。块存储服务器充当内容寻址存储 (CAS) 系统，并会根据哈希值检索每个单独的加密文件块。

预览服务器

预览服务器负责生成文件预览。预览会以不同文件格式呈现用户文件，更适合在最终用户设备上快速显示。预览服务器从块存储服务器中检索文件块以生成预览。请求文件预览时，预览服务器会从预览存储服务器中检索缓存预览，并将其传输到块服务器。预览最终通过块服务器提供给用户。

预览存储服务器

缓存预览在预览存储服务器中以加密形式存储。

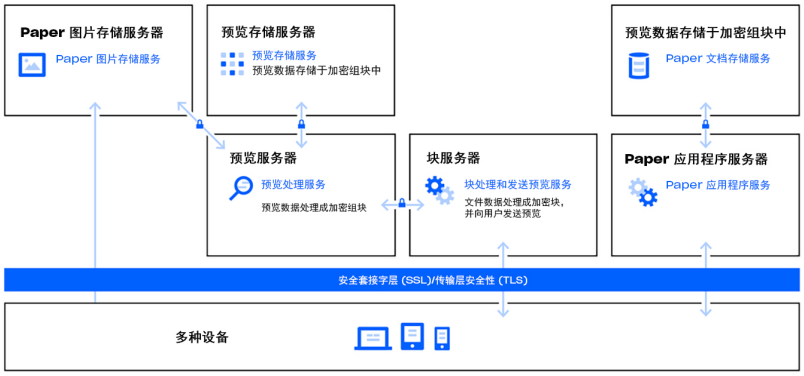
通知服务

这是一项单独的服务，专门监控 Dropbox 帐户是否有任何更改。此处不存储或传输任何文件或元数据。每个客户端都会与此通知服务建立长轮询连接并等待。当 Dropbox 中的任何文件出现更改时，通知服务会通过关闭长轮询连接来向相关客户端发出更改信号。关闭连接信号时，表明客户端必须安全连接到元数据服务器，以同步出现的任何更改。

Dropbox

我们的基础设施：文件

Dropbox Paper (Paper) 是 Dropbox 产品的一项功能。但 Paper 在 Dropbox 基础设施环境中使用一组截然不同的系统。Paper 的基础设施由下图所示的组件构成。



Paper 应用程序服务器

Paper 应用程序服务器处理用户请求，将编辑后的 Paper 文档的输出呈现给用户，并执行通知服务。Paper 应用程序服务器将用户编辑写入将其永久存储的 Paper 数据库。Paper 应用程序服务器和 Paper 数据库之间的通信会话使用强密码加密。

Paper 数据库

用户 Paper 文档的实际内容及有关这些 Paper 文档的特定元数据将以加密形式永久存储在 Paper 数据库中。其中包括 Paper 文档的相关信息（如标题、共享成员资格和权限、项目和文件夹关联以及其他信息），以及 Paper 文档本身的内容，包括评论和任务。Paper 数据库会根据需要被分片和复制，以满足性能和高可用性的要求。

Paper 图片存储服务器

上传到 Paper 文档的图片在 Paper 图片服务器上进行存储和静态加密。在 Paper 应用程序和 Paper 图片服务器之间的图片数据传输通过加密会话进行。

预览服务器

预览服务器为上传到 Paper 文档的图片和在 Paper 文档中嵌入的超链接提供预览。对于上传到 Paper 文档的图片，预览服务器通过加密通道获取存储在 Paper 图片服务器中的图片数据。对于嵌入 Paper 文档的超链接，预览服务器使用源链接指定的加密通道获取图片数据并呈现图像预览。预览最终通过块服务器提供给用户。

预览存储服务器

Paper 使用 Dropbox 基础设施图中描述的相同预览存储服务器来存储缓存图像预览。缓存预览块在预览存储服务器中以加密形式存储。

Dropbox

Dropbox 控件：我们的内部措施

我们采取全面措施来保护我们的基础设施、网络和应用程序。我们采取的一些安全措施包括静态加密、传输中加密和永久删除文件。

我们还为所有员工提供全面的隐私和安全培训，以建立重视用户信任的文化。有关数据控制的详细信息如下：

培训

保护用户的个人数据还包括建立和发展安全和隐私意识文化。在授予系统访问权限之前，Dropbox 员工必须同意安全政策，包括用户数据隐私政策。只有具有特定需求的员工才有权访问此类系统。员工每年还会参加强制性安全和隐私培训。

传输加密

为了保护在 Dropbox 客户端（当前为桌面、移动、API 或网页版）和 Dropbox 前端服务器之间传输的文件数据，我们协商实施加密连接，以确保安全传输。同样，我们还协商实施加密连接，以保护 Paper 客户端（当前为移动、API 或网页版）与托管服务之间传输的 Paper 文档数据。连接时，使用安全套接字层 (SSL) 或传输层安全性 (TLS) 进行加密，建立一个受 128 位或更高级别的高级加密标准 (AES) 保护的安全隧道。

静止加密

用户上传的文件以独立文件块的形式存储在 Dropbox 存储服务器中。每个文件块均采用 256 位高级加密标准 (AES) 进行加密。只有在修订版本之间修改过的文件块才会完成同步。同样，存储在 Paper 数据库的 Paper 文档数据采用 256 位高级加密标准 (AES) 进行静态加密。

永久删除文件和 Paper 文档

任何 Dropbox 用户或 Dropbox Business 或 Dropbox Education 团队的管理员为永久删除而标记文件时，均会触发永久删除文件的流程。同样，当一名用户或 Dropbox Business 或 Dropbox Education 团队的管理员为永久删除而标记 Paper 文档时，会触发永久删除 Paper 文档数据和图像数据的类似流程。

个人数据访问请求

如需获取使用 Dropbox 存储的文件和 Paper 文档之外的个人数据，用户可以登录网站并转到其帐户页面。帐户页面会显示与帐户有关的姓名和电子邮件地址等信息。用户还可以查看连接会话、计算机和移动设备，以及从安全页面连接其帐户的应用程序和已连接应用程序页面的 IP 地址。

Dropbox 用户还可以选择请求访问或删除 Dropbox 可能收集的与该用户有关的其他个人数据。更多有关此流程的信息，请参阅 Dropbox 帮助中心。

Dropbox 隐私管理

隐私计划团队负责实施 Dropbox 隐私计划。团队可在我们的数据生命周期开展重要隐私计划，并倡导“隐私始于设计”的理念。多个跨职能法律子团队进一步为 Dropbox 隐私计划提供支持。这些子团队为实施和监督隐私计划的日常任务提供所需的额外专业知识。

DPO 团队独立于其他隐私职能部门，负责隐私合规性和隐私监督，在执行职责的过程中直接为数据保护官提供支持。数据保护官 (DPO) 是欧盟的本地代表，可通过 privacy@dropbox.com 与其联系。

Dropbox

政府数据请求原则

我们理解，用户将其个人数据托付给我们时，是希望我们对其数据进行保密。与大部分在线服务类似，Dropbox 需要应政府请求收集其用户信息。

以下原则说明我们如何应对政府提出的数据请求。

公开透明

我们认为，应允许在线服务发布政府请求的数量和类型，并在政府提出获取用户信息时，通知相关用户。通过这种透明公开的方式，可以帮助用户更好地理解政府过度监控的情况和模式，以便赋予用户权利。我们将继续发布有关此类请求的详细信息，并争取获得提供更多此类重要信息的权利。

反对过于宽泛的请求

政府提出的数据请求应限于其要求收集的信息，且主要针对特定人员及合法调查。我们将抵制一揽子请求和过于宽泛的请求。

提供可信赖的服务

政府绝不应将后门程序安装到在线服务中或破坏其基础设施以获取用户数据。我们将继续努力保护我们的系统并推动法律修改，以明确表明此类活动非法。

保护所有用户

根据居住地或公民身份向人们提供不同保护的法律已过时，无法体现在线服务的全球化性质。我们将继续倡导政府对此类法律进行变更。

此类原则和我们的年度透明度报告已在网上公开，如需获取相关内容，请访问 Dropbox 网站：https://www.dropbox.com/transparency。

如需详细了解我们对数据的控制和保护您个人信息的方式，请参阅 Dropbox Business 安全白皮书。

为 Dropbox 工作以及与 Dropbox 合作的其他方。

Dropbox 负责管理与提供服务相关的大部分活动，但也确实寻求了第三方的帮助。这些第三方与我们的服务有关且值得信赖（如客户支持和 IT 服务提供商）。这些第三方仅在符合我们的隐私政策的前提下，可代表我们访问您的信息以执行任务，并且我们仍将根据相关说明，对第三方处理用户信息的行为负责。

每个第三方都将经过严格的审查程序，包括安全审查和定期合同审查，以评估其是否由履行我们数据保护承诺的能力。

国际数据传输

Dropbox 依靠各种法律机制，将个人数据从欧盟转移到美国。在收集、使用和保留个人数据并将数据从欧盟和瑞士转移到美国方面，Dropbox 已获得欧盟-美国和瑞士-美国隐私护盾框架认证。除了隐私护盾以外，Dropbox 还为其服务的隐私提供强有力的合同保证，并实施欧盟示范合同条款，以保护其国际数据传输。

Dropbox

GDPR：通用数据保护条例

通用数据保护条例 (GDPR) 是一项欧盟条例，此条例建立了保护欧盟数据主体的个人数据的法律框架。

自 1995 年欧盟数据保护指令颁布以来，GDPR 成为了欧洲数据保护立法中最重要的一部分。许多在欧洲开展业务的公司（包括 Dropbox）在 GDPR 合规性方面投入了大量资金。

GDPR 统一了整个欧洲地区的数据保护法律，赶上了过去二十年日新月异的技术变革。

GDPR 建立在包括欧盟数据保护指令在内的原有法律框架基础之上，对处理个人数据的企业提出新的义务和责任，并为用户提供了有关个人数据方面的新权利。

个人数据。在欧盟地区建立的企业，以及处理欧盟数据主体个人数据的企业都必须遵循 GDPR。

Dropbox 的 GDPR 合规性之旅

Dropbox 努力遵守 GDPR。从一开始，我们就将尊重隐私和安全性植入我们的公司理念。随着公司的成长，我们依然将处理和保护用户委托于我们的数据作为首要关注事项。Dropbox 在合规性方面已取得过保持领先地位的成绩。如上方所述，为了企业用户的数据安全，我们成为了最先获得 ISO 27018 认证的云服务提供商之一。在这一坚实基础之上，Dropbox 将 GDPR 合规性视为现有实践和控制体系之上的一次变革，并体现了 Drop-box 为始终保护用户的个人数据，不断变革发展一系列相关计划。

2016 年这项法规一经生效后，Dropbox 便开启了 GDPR 合规性之旅。我们采取的第一步，便是组建一支跨职能的数据保护专家团队。团队成员包括法律顾问、安全和合规性专业人员以及产品和基础设施工程师。随后，我们的团队根据 GDPR 的要求，对现有安全和数据保护措施进行全面评估。

我们采取的下一个步骤，是对个人数据的处理活动进行评估，并通过我们的系统跟踪个人数据的生命周期。这些行动有时是指执行数据映射并完成数据保护影响评估。

自此，我们在现有内部流程和程序的基础上进行构建，以确保我们符合 GDPR 要求下的问责原则。GDPR 更加注重对影响个人数据的决策和实践进行记录，因此这一点非常重要。

Dropbox

在 GDPR 合规性之旅中赋予用户权利

Dropbox 提供相关控制和可见性功能，可帮助您更轻松地履行 GDPR 合规性等数据保护义务。当然，您整个企业范围内的 GDPR 合规性不会开始或结束于与 Dropbox 等供应商之间的关系。虽然我们提供的功能可以帮助您履行义务，但无法确保义务本身的合规性。为保障 GDPR 合规性，您需要更广泛地思考数据传输的方式，以及您所在企业内部是如何保护数据。在 GDPR 合规性之旅中，每家企业都应将其供应商视作重要的合作伙伴，并采取相应措施来实现合规性。

数据最小化

企业应在设计服务时确保数据最小化，这是 GDPR“隐私始于设计”要求中的一大要素。即在您的企业中，确保能够有效查看和控制数据，以便更好地管理数据。Dropbox Business 管理员面板是协助实现这一目的的有效工具，可以帮助您监控团队活动、查看关联设备和审核共享活动。我们致力于在新产品和新功能中遵循“隐私始于设计”的原则。

保护和恢复数据

通过防范设备丢失、版本历史和文件恢复，可以防止个人数据意外丢失、损坏或销毁，并在出现意外时及时恢复数据，确保可以使用和访问个人数据。为保护您的数据，我们还鼓励采取双因素身份验证的方式。

保持记录

GDPR 还对企业提出了新的义务，即保持记录相关的数据处理活动。借助审核日志和活动日志，您可以更好地了解您的数据处理活动，为您保持相关记录提供支持。

访问管理

在 Dropbox Business 管理员面板中，您可以轻松管理团队成员对文件、文件夹和 Paper 文档的访问。对于共享文件链接，您可以借助链接权限功能，通过设置密码来保护共享链接、设置到期日以提供临时访问权限，并限制对企业内文件的访问。如果用户之间的职责发生变化，借助帐户转移工具，您可以轻松将 Paper 文档中的文件和所有权从一名用户转移到另一名用户。

管理员还可以在保留其数据和共享关系的同时，禁用用户对其帐户的访问权限，以确保企业的信息安全。最后，借助远程清除功能，您可以清除丢失或被盗设备中的文件和 Paper 文档。

欧盟基础设施

虽然 GDPR 并不要求将个人数据保留在欧盟境内，但 Dropbox 允许符合资格的 Dropbox Business 和 Dropbox Education 客户在欧盟境内存储文件（块）。借助 Amazon Web Services (AWS) 基础设施，用户可将文件存储在欧盟境内。如需了解更多有关欧盟基础设施的内容，请联系我们的销售团队。

Dropbox

共同致力于保护您的个人数据

Dropbox 及其用户共同致力于保护其个人数据。我们采取全面措施保护我们的基础设施、网络和应用程序，在安全和隐私措施方面培训员工，以建立重视用户信任的文化，并通过第三方，严格测试和审核我们的系统和措施。但是，用户在保护其个人数据方面也发挥着重要作用。Dropbox 可帮助您在符合企业隐私、安全和合规性要求的前提下，让您配置、使用和监控您的帐户。通过查看我们的《责任分担指南》，您可以进一步了解我们如何保障您的帐户安全，以及您可以如何持续查看和控制您的个人数据。

摘要

每天，数百万用户因信任而使用 Dropbox 产品。为了不辜负用户的信任，我们在建立和发展 Dropbox 的过程中充分重视安全和隐私。我们制定每项决策时，坚持遵守保护用户个人数据的承诺。如需了解更多内容，请发送电子邮件至 privacy@dropbox.com。如需了解更多有关 GDPR 的内容，请访问我们的 GDPR 指导中心。