Dropbox

Privacy and Data Protection

Introduction

Personal data plays a huge part in society and the economy. Increasingly, people are seeking greater control and clarity about how their personal data is used and protected by organisations they interact with.

At Dropbox, trust is the foundation of our relationship with millions of people and businesses around the world. We value the confidence you've placed in us, and take the responsibility of protecting your personal data seriously.

Our Commitments to You

We're committed to protecting your personal data. Dropbox's Terms of Service outline your responsibilities when using our services. Our Privacy Policy describes our privacy commitments to users and explains how we collect, use and handle your personal data when you use our services. If you reside in North America (the United States, Canada and Mexico), Dropbox, Inc. acts as your service provider.

For all other users, Dropbox International Unlimited Company acts as a controller of your personal data.

If you are a Dropbox Business or Dropbox Education user, your organisation acts as the data controller for any personal data provided to Dropbox in connection with your use of Dropbox Business or Dropbox Education. The data controller determines the purposes and means of processing personal data. Dropbox acts as the data processor, processing data on your organisation's behalf when you use Dropbox Business or Dropbox Education, and our Business Agreement includes commitments related to data processing and international data transfer.

Our Track Record: Compliance

Compliance is an effective way to validate a service's trustworthiness. We encourage and are pleased to provide independent verification that our security and privacy practices comply with the most widely accepted standards and regulations, such as ISO 27001, ISO 27017, ISO 27018, HIPPA/HITECH, Germany BSI C5, and SOC 1, 2, and 3.

Furthermore, we were one of the first cloud service providers to achieve certification with ISO 27018, the internationally recognised standard for leading practices in cloud privacy and data protection. Our independent third-party auditors test our controls and provide their reports and opinions. We may share these with you whenever possible.

Please note, while the scope of our certifications and audit reports typically refers to Dropbox Business and Dropbox Education, the majority of our controls are applicable for Dropbox Basic, Plus and Professional users as well. More information on the standards that we comply with and how we verify our practices can be found on our compliance web page.

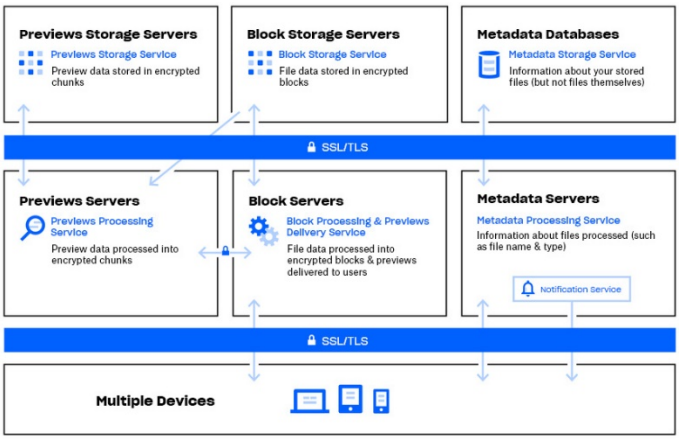
Dropbox

Dropbox Architecture: Protecting Your Personal Data

At Dropbox, we believe protecting your personal data begins with keeping your data secure. To that end, Dropbox is designed with multiple layers of protection, including secure file data transfer, encryption, and application-level controls that are distributed across a scalable, secure infrastructure.

Our Infrastructure: Files

Dropbox's infrastructure for files is comprised of the components depicted in the diagram below.



Metadata servers

Certain basic information about user data, called metadata, is kept in its own discrete storage service and acts as an index for the data in users' accounts. Metadata includes basic account and user information, like email address, name and device names. Metadata also includes basic information about files, including file names and types, that helps support features like version history, recovery and sync.

Metadata Databases

File metadata is stored in a MySQL-based database service, and is sharded and replicated as needed to meet performance and high availability requirements.

Block servers

By design, Dropbox provides a unique security mechanism that goes beyond traditional encryption to protect user data. Block Servers process files from the Dropbox applications by splitting each file into blocks, encrypting each file block using a strong cipher and synchronizing only blocks that have been modified between revisions. When a Dropbox application detects a new file or changes to an existing file, the application notifies the Block Servers of the change, and new or modified file blocks are processed and transferred to the Storage Server.

Block Storage Servers

The actual contents of users' files are stored in encrypted blocks with the Block Storage Servers. Prior to transmission, the Dropbox client splits files into file blocks in preparation for the storage. The Block Storage Servers act as a Content-Addressable Storage (CAS) system, with each individual encrypted file block retrieved based on its hash value.

Previews Servers

The Previews Servers are responsible for producing previews of files. Previews are a rendering of a user's file in a different file format that is more suited for fast display on an end user's device. Previews Servers retrieve file blocks from the Block Storage Servers to generate previews. When a file preview is requested, the Previews Servers retrieve the cached preview from the Preview Storage Servers and transfer it to the Block Servers. Previews are ultimately served to users by Block Servers.

Previews Storage Servers

Cached previews are stored in an encrypted format in the Previews Storage Servers.

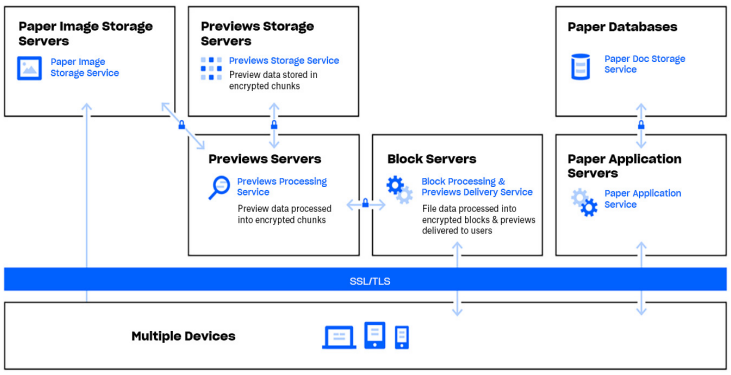
Notification service

This separate service is dedicated to monitoring whether or not any changes have been made to Dropbox accounts. No files or metadata are stored here or transferred. Each client establishes a long poll connection to the notification service and waits. When a change to any file in Dropbox takes place, the notification service signals a change to the relevant client(s) by closing the long poll connection. Closing the connection signals that the client must connect to the Metadata Servers securely to synchronise any changes.

Dropbox

Our Infrastructure: Paper

Dropbox Paper (Paper) is a feature of the Dropbox product. However, Paper uses a mostly distinct set of systems within the Dropbox infrastructure environment. Paper's infrastructure is comprised of the components depicted in the diagram below.



Paper application servers

The Paper Application Servers process user requests, render the output of edited Paper docs back to the user and perform notification services. Paper Application Servers write inbound user edits to the Paper Databases, where they are placed in persistent storage. Communication sessions between the Paper Application Servers and Paper Databases are encrypted using a strong cipher.

Paper databases

The actual contents of users' Paper docs, as well as certain metadata about these Paper docs, are encrypted in persistent storage on the Paper Databases. This includes information about a Paper doc (such as the title, shared membership and permissions, project and folder associations and other information), as well as content within the Paper doc itself, including comments and tasks. The Paper Databases are sharded and replicated as needed to meet performance and high availability requirements.

Paper Image Storage Servers

Images uploaded to Paper docs are stored and encrypted at rest on the Paper image servers. Transmission of image data between the Paper application and Paper image servers occurs over an encrypted session.

Previews Servers

The Previews Servers produce previews both for images uploaded to Paper docs, as well as hyperlinks embedded within Paper docs. For images uploaded to Paper docs, the Previews Servers fetch image data stored in the Paper Image Storage Servers via an encrypted channel. For hyperlinks embedded within Paper docs, Previews Servers fetch the image data and render a preview of the image using encryption as specified by the source link. Previews are ultimately served to users by Block Servers.

Previews Storage Servers

Paper uses the same Previews Storage Servers described in the Dropbox infrastructure diagram to store cached image previews. Cached preview chunks are stored in an encrypted format in the Previews Storage Servers.

Dropbox

Dropbox Controls: Our Internal Practices

We take comprehensive measures to protect our infrastructure, network and applications. Some of the security measures we have in place include encryption at rest, encryption in transit and the permanent deletion of files. We also offer robust privacy and security training for all our employees to build a culture where being worthy of trust is a priority. Details of some of our controls are described below:

Training

Part of protecting our users' personal data involves building and growing a culture of security and privacy awareness. Dropbox employees are required to agree to security policies, including a user data privacy policy, prior to being granted systems access. Only those employees with a specific need have access to such systems. Employees also take part in mandatory security and privacy training on an annual basis.

Encryption in Transit

To protect file data in transit between a Dropbox client (currently desktop, mobile, API or web) and Dropbox's front-end servers, an encrypted connection is negotiated to ensure secure delivery. Similarly, an encrypted connection is negotiated to protect Paper doc data in transit between a Paper client (currently mobile, API or web) and the hosted service. These connections are encrypted using Secure Sockets Layer (SSL)/Transport Layer Security (TLS) to create a secure tunnel protected by 128-bit or higher Advanced Encryption Standard (AES) encryption.

Encryption at Rest

Files uploaded by users are stored on Dropbox's Storage Servers as discrete file blocks. Each block is encrypted using 256-bit Advanced Encryption Standard (AES). Only blocks that have been modified between revisions are synchronised. Similarly, Paper doc data stored on Paper Databases is also encrypted at rest using 256-bit Advanced Encryption Standard (AES).

Permanent Deletion of Files and Paper docs

When any Dropbox user or an administrator for a Dropbox Business or Dropbox Education team marks a file for permanent deletion, it triggers a process to permanently delete the file. Likewise, when a user or an administrator for a Dropbox Business or Dropbox Education team marks a Paper doc for permanent deletion, there is a similar process to permanently delete Paper doc data and image data.

Personal Data Access Requests

For access to personal data beyond the files and Paper docs that are stored with Dropbox, users can sign in to the website and go to their account pages. The account page will show information like the name and email address associated with the account. Users can also view the IP addresses of connected sessions, computers and mobile devices, as well as apps connected to their accounts from the security page and connected apps page.

Dropbox users also have the option to request access to or deletion of other personal data that Dropbox may have collected about them. More information about this process can be found in the Dropbox Help Center.

Privacy Governance at Dropbox

The Privacy Programme team is responsible for operating the Dropbox Privacy Programme. It implements our key privacy initiatives and champions privacy by design in our data lifecycle. The Dropbox Privacy Programme is further supported by several cross-functional Legal sub-teams. These sub-teams provide the additional expertise required to operate and oversee the day-to-day tasks of the Privacy Programme.

The DPO team operates separately from the other privacy functions and serves as privacy compliance and oversight, directly supporting the Data Protection Officer in the execution of their duties. The Data Protection Officer (DPO) is the EU local representative and can be contacted at privacy@dropbox.com.

Dropbox

Government Data Request Principles

We understand that when users entrust us with their personal data, they expect us to keep that data confidential. Like most online services, Dropbox sometimes receives requests from governments seeking information about its users.

The principles below describe how we handle the government data requests we receive.

Be transparent

We believe online services should be allowed to publish the number and types of government requests they receive, and to notify individuals when information about them has been requested. This type of transparency empowers users by helping them better understand in- stances and patterns of government overreach. We will continue to publish detailed information about these requests and advocate for the right to provide more of this important information.

Fight overly broad requests

Government data requests should be limited in the information they seek and narrowly tailored to specific people and legitimate investigations. We will resist blanket and overly broad requests.

Provide trusted services

Governments should never install backdoors into online services or compromise infrastructure to obtain user data. We will continue to work to protect our systems and to change laws to make it clear that this type of activity is illegal.

Protect all users

Laws that give people different protections based on where they live or their citizenship are antiquated and don't reflect the global nature of online services. We will continue to advocate for the reform of these laws.

These principles, along with our annual transparency report, are made publicly available on the Dropbox website at: https://www.dropbox.com/transparency.

For additional details about our controls and our approach to protecting your personal data, please refer to our Dropbox Business Security Whitepaper.

Others Working for and with Dropbox

Dropbox manages the majority of activities related to the provision of our services, however, we do utilise some trusted third parties in relation to our services (for example, providers of customer support and IT services). These third parties will only access your information to perform tasks on our behalf in compliance with our Privacy Policy, and we'll remain responsible for their handling of your information in accordance with our instructions.

Each third party goes through a rigorous vetting process, including security reviews and regular contractual reviews, to evaluate their ability to meet our data protection commitments.

International Data Transfers

Dropbox relies upon a variety of legal mechanisms for its international transfer of personal data from the EU to the United States. We are certified under the EU-US and Swiss-US Privacy Shield Programs regarding the collection, use and retention of personal data and its transfer from the EU and Switzerland to the United States. In addition to Privacy Shield, Dropbox also provides strong contractual guarantees around the privacy of its services and has implemented EU Model Contract Clauses to cover its international transfers of data.

Dropbox

GDPR: The General Data Protection Regulation

The General Data Protection Regulation, or GDPR, is an EU regulation that establishes a legal framework to protect the personal data of EU data subjects.

The GDPR is the most significant piece of European data protection legislation since the EU Data Protection Directive of 1995, and many companies – including Dropbox – that do business in Europe have invested heavily in GDPR compliance.

The GDPR harmonises data protection laws across Europe and brings them up to speed with the rapid technological change that has occurred in the past two decades.

It builds upon past legal frameworks in the EU, including the EU Data Protection Directive, and introduces new obligations and liabilities for organisations that handle personal data, as well as new rights for individuals in respect of their personal data. Organisations that are established in the EU, as well as organisations that process personal data of EU data subjects, are required to comply with the GDPR.

Dropbox's GDPR Compliance Journey

Dropbox is committed to GDPR compliance. Respect for privacy and security was built into our business from the beginning, and as we've grown, our focus on handling and protecting the data that our users entrust to us has remained a priority. Dropbox has a track record of staying ahead of the compliance curve – as described above, we were one of the first cloud service providers to achieve ISO 27018 certification for our business users. Given this strong foundation, Dropbox views GDPR compliance as an evolution of our existing practices and controls, and represents an ongoing, evolving set of initiatives to ensure that our users' personal data is always protected.

Dropbox's journey to GDPR compliance began as soon as the regulation was adopted in 2016. Our first step was to form a cross-functional team of data protection specialists consisting of legal counsel, security and compliance professionals and product and infrastructure engineers. Our team then completed a full assessment of our current security and data protection practices against the GDPR requirements.

Our next step was to perform an evaluation of our personal data processing activities and trace the lifecycle of personal data through our systems. These exercises are sometimes referred to as performing Data Mappings and completing Data Protection Impact Assessments.

Since then, we have continued to build on our existing internal processes and procedures to ensure we meet the accountability principles under the GDPR requirements. This is important as the GDPR places an increased focus on documenting decisions and practices affecting personal data.

Dropbox

Empowering our Users on their GDPR Journeys

Dropbox provides control and visibility features that can help you manage your data protection obligations, including GDPR compliance obligations, more easily. Of course, GDPR compliance across your organisation does not begin or end with the relationship with your suppliers, such as Dropbox. While our features can help you manage your obligations, they cannot ensure compliance in and of themselves. GDPR compliance requires thinking more broadly about how data moves around and is protected in your organisation. Each organisation should undertake its own steps to reach compliance, with suppliers as important partners on that journey.

Data Minimisation

An important element of the GDPR's Privacy by Design requirement is that organisations should design their services in a data minimising way. This means having good visibility and control of the data within your organisation in order to help you manage it. The Dropbox Business admin dashboard is a useful tool to help with this, as it enables you to monitor team activity, view connected devices and audit sharing activity. We work to embed the Privacy by Design principles into new products and features.

Protection and Restoration of Data

Lost device protection, version history and file recovery can help protect against accidental loss, damage or destruction of personal data, and can help with the ability to restore availability of, and access to personal data in a timely manner in the event of an incident. Two-factor authentication is another important measure that we encourage to help protect your data.

Record Keeping

The GDPR also increases obligations on organisations to keep detailed records of their processing activities. Our audit logs and activity logs can help your better understand your processing activities to support your record keeping.

Access Administration

Within the Dropbox Business admin dashboard, you easily manage team member access to files, folders and Paper docs. For shared file links, our link permissions feature allows you to password protect the shared links, set expiration dates to grant temporary access, and limit access to those within your organisation. In the event that responsibilities change between users, our account transfer tool allows you to easily transfer files and ownership of Paper docs from one user to another.

Administrators also have the ability to disable a user's access to their account while preserving their data and sharing relationships to keep your organisation's information safe. Lastly, the remote wipe feature allows you to clear files and Paper docs from lost or stolen devices.

EU Infrastructure

While the GDPR does not require personal data to be hosted within the EU, Dropbox does offer qualified Dropbox Business and Dropbox Education customers the ability to store files (blocks) in the EU. EU-based file storage is provided on Amazon Web Services (AWS) infrastructure. To learn more about our EU infrastructure, contact our sales team.

Dropbox

Working Together to Protect Your Personal Data

Dropbox works with its users to protect their personal data. We take comprehensive measures to protect our infrastructure, network and applications, train employees in security and privacy practices, build a culture where being worthy of trust is the highest priority and put our systems and practices through rigorous third-party testing and auditing.

However, users also play a key role in protecting their personal data. Dropbox enables you to configure, use and monitor your account in ways that meet your organisation's privacy, security and compliance needs. Our shared responsibility guide can help you to understand more about what we do to keep your account safe and what you can do to maintain visibility and control over your personal data.

Summary

Every day, millions of users place their trust in Dropbox. To be worthy of that trust, we built and will continue to grow Dropbox with an emphasis on security and privacy. Our commitment to protecting our users' personal data is at the heart of each decision we make. For more information, please email privacy@dropbox.com. For more information on GDPR, you can also visit our GDPR guidance centre.