Privacy and Data Protection

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 organizations they interact with.

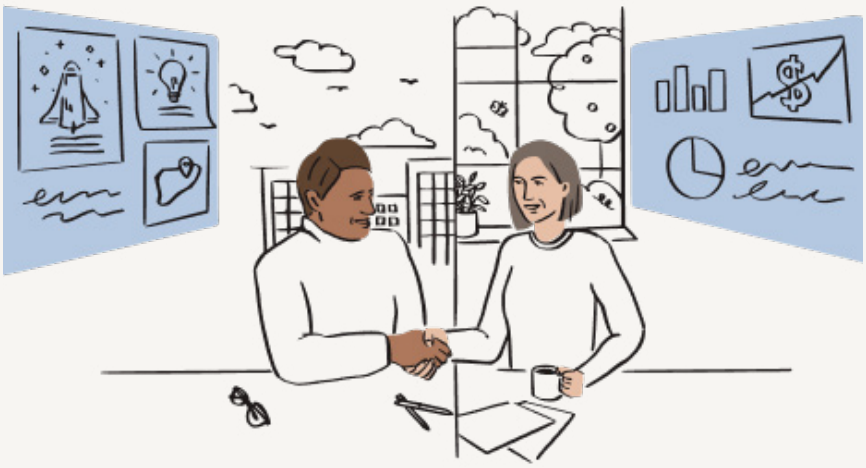
At Dropbox, trust is the foundation of our relationship with millions of people and businesses around the world. We value the confidence you've put in us and take the responsibility of protecting your personal data seriously.

Our commitments to you

We're committed to protecting your personal data. Dropbox's Privacy Policy describes our privacy commitments and explains how we collect, use, and handle your personal data when you use our services. We are also committed to sharing information about our privacy practices in a way that is easy to understand. We have made available a Privacy Policy: Frequently Asked Questions, as well as this document to address common questions.

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. A data controller determines the purposes and means of processing personal data.

If you use one of our Dropbox for teams plans (for example, Dropbox Business or Dropbox Education), your organization acts as the data controller for any personal data provided to Dropbox in connection with your use of Dropbox. In this case, Dropbox acts as the data processor, processing data on your organization's behalf in accordance with our Business Agreement, which outlines our commitments related to data processing and international data transfers.



Regardless of your plan, Dropbox employs the same principles when it comes to handling your personal data. The following sections lay out our company principles and offer a peek into how we comply with global certifications and privacy regulations.

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 government and law enforcement agencies seeking information about our users. We scrutinize each request and are committed to giving users notice, as permitted by law, when their accounts are identified in a request.

We maintain a transparency report and have established the following set of Government Data Request Principles:

Be transparent

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 instances 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.

These principles, along with our annual transparency report, are available on the Dropbox website at: Dropbox Transparency Overview.

Artificial intelligence principles

Some of Dropbox's features are powered by artificial intelligence (AI). Dropbox works to ensure that our AI innovations not only serve our customers, but also respect their rights and safety.

The following principles guide our teams as we develop AI products and features responsibly:

- Leverage AI to serve our customers
- Keep customers in control of their data
- Be transparent about how we use AI
- Champion fairness in AI technology
- Be accountable to our customers
- Respect people, their safety, and their rights

These principles are described in more detail on the Dropbox website at: Dropbox AI Principles.

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 access controls. These measures are outlined in detail in Dropbox's Security Whitepaper.

Our robust security controls are complemented by a suite of privacy controls. Some examples are:

Privacy training

Part of protecting our user' personal data involves building and growing a culture of privacy awareness. Dropbox employees are required to agree to a user data privacy policy and data classification 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 privacy training on an annual basis. These trainings teach the basics of privacy laws and describe best practices on how to handle personal data at Dropbox.

Anonymization and pseudonymization

In certain cases where we no longer need data to be attributable to an individual, we employ methods such as anonymization and pseudonymization to de-identify the data. Anonymization permanently removes or changes personal data so that it cannot be used to identify an individual. Pseudonymization temporarily removes or changes personal data, but the process can be reversed if someone has access to additional information. An example of when we use pseudonymization is when we de-identify customer feedback and use it to improve our products and services.

Permanent deletion of files and Paper docs

When any Dropbox user or an administrator for a Dropbox for teams account 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 for teams account marks a Paper doc for permanent deletion, there is a similar process to permanently delete Paper doc data and image data.

Privacy governance

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

The Office of the Data Protection Officer operates separately from the other privacy teams, and serves a privacy compliance and oversight function. They can be contacted at privacy@dropbox.com.

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, ISO 27701, HIPAA / HITECH, SOC 1, SOC 2, and SOC 3**.

We are proud to have been one of the first cloud service providers to achieve certification with ISO 27018, the internationally recognized 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 for teams, the majority of our controls are applicable to all Dropbox plans.

In addition, Dropbox adheres to the **EU Cloud Code of Conduct**. The EU Cloud Code of Conduct is a voluntary instrument that enables a cloud service provider, such as Dropbox, to demonstrate their commitment to GDPR compliance. Dropbox for teams has been declared adherent to the EU Cloud Code of Conduct and received a Compliance Mark of "Level 2," which means that these services have implemented technical, organizational, and contractual measures in-line with the requirements of the Code. For more information, please visit the Code's official website.

More information on the standards that we comply with and how we verify our practices can be found on our Trust Center and our compliance web page.

International data transfers

When transferring data from the European Union, the European Economic Area, the United Kingdom, and Switzerland, Dropbox relies upon a variety of legal mechanisms, such as contracts with our customers and affiliates, Standard Contractual Clauses, and the European Commission's adequacy decisions.

Dropbox complies with the EU-U.S. and Swiss-U.S. Data Privacy Frameworks, as well as the UK Extension to the EU-U.S. Data Privacy Framework, as set forth by the U.S. Department of Commerce regarding the processing of personal data transferred from the European Union, the European Economic Area, the United Kingdom, and Switzerland to the United States. Dropbox has certified to the U.S. Department of Commerce that it adheres to these Data Privacy Frameworks with respect to such data, but this does not include the FormSwift portion of the Services.

To learn more about the Data Privacy Framework, and to view Dropbox's certification, visit https://www.dataprivacyframework.gov/.

Complaints and disputes related to our Data Privacy Framework compliance are investigated and resolved through JAMS, an independent third party. To learn more, please see our Privacy Policy.

Others working for and with Dropbox

Dropbox manages the majority of activities related to the provision of our services; however, we do utilize 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, privacy, and contractual reviews, to evaluate their ability to meet our data protection commitments. Based on this vetting process, Dropbox affirms that its trusted third parties commit to comply with applicable data protection laws in connection with processing personal data on Dropbox's behalf. Customers can monitor Dropbox's trusted third parties by reviewing Dropbox's ISO 27001 and 27018 certifications. Under appropriate obligations of confidentiality, customers can also monitor Dropbox's trusted third parties by examining Dropbox's controls and audit results for Trust Services Criteria P6.1, P6.4, and CC.9.2 of the SOC 2 Type II Report.

In addition, to enable the provision of services for Dropbox for teams customers, Dropbox may engage sub-processors with access to customer personal data. Before we engage sub-processors, Dropbox performs due diligence on sub-processor privacy, security, and confidentiality practices, and executes appropriate contractual measures regarding protection of personal data. You can view the list of sub-processors, and sign up for sub-processor changes, by visiting our Sub-processor List.

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 companies—including Dropbox—that do business in Europe have invested heavily in 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, GDPR compliance was a natural evolution of our existing practices and controls.

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 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, including maintaining records of processing in accordance with Article 30 of the GDPR.

For more information about the GDPR, visit our GDPR guidance center.

Data subject rights

The GDPR affords individuals the right to access, correct, delete, and object to the processing of their personal data. These consumer rights can also be found in a number of other privacy laws such as the California Consumer Privacy Act (CCPA). Here is how Dropbox complies with these privacy rights:

Right to access and correct

Users can access or correct data about themselves by signing into https://www.dropbox.com and going to their account page. The "General" tab shows information like the name and email address associated with the account; the "Security" tab shows the IP addresses of connected sessions, computers, and mobile devices; and the "Apps" tab lists the apps connected to the account.

Dropbox has also launched a "Privacy" tab, where users can generate access reports. Individuals who are unable to log in to their account or who do not have one can submit a data access request by filling out this form: Data Subject Request Form.

Right to delete

Users who want to delete their account contents can do so directly from within their accounts. More information on how to delete content can be found here.

Users can visit the "Privacy" tab to delete their non-account related data (e.g., contact information in our marketing systems). Individuals who are unable to log in to their account or who do not have one can submit a deletion request by filling out this form: Data Subject Request Form.

Right to object

Depending on the processing activity, individuals can request that we stop or limit processing of their personal data. If you would like to object to the processing of your personal data, please email us at privacy@dropbox.com.

Individuals can opt-out of receiving marketing materials at any time by changing their preferences in the Notifications section of their account or by clicking the Unsubscribe link in the footer of marketing emails.

Individuals can also opt-out of the collection of their personal data through cookies by updating their preferences in the Dropbox cookie banner. For more information on Dropbox's use of cookies and similar technologies, visit this page.

Empowering our users

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 organization 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 organization. Each organization should undertake its own steps to reach compliance, with suppliers as important partners on that journey.

Data minimization

An important element of the GDPR's Privacy by Design requirement is that organizations should design their services in a data minimizing way. This means having good visibility and control of the data within your organization in order to help you manage it. The Dropbox for teams 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 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 organizations to keep detailed records of their processing activities. Our audit logs and activity logs can help you better understand your processing activities to support your record keeping.

Access administration

Within the Dropbox for teams 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 organization. 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 organization'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 eligible Dropbox for teams 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.

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's Terms of Service outline your responsibilities when using our services. Dropbox enables you to configure, use, and monitor your account in ways that meet your organization'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.

For more information about the content of this document, please email privacy@dropbox.com.