The General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GPDR) is a European Union (EU) regulation that establishes a new framework for collecting, processing, storing and protecting the personal data of EU citizens. It introduces new obligations and liabilities for all organisations that handle personal data, and new rights for individuals over how their personal data is collected, processed, and stored.

Impacts of the GDPR

If your organisation must comply with GDPR, then there are a number of factors that should be considered. We highly recommend seeking legal advice to determine what may be required for your specific situation.

1. Understanding your data

Protecting data properly means understanding how it's treated in your organisation—how personal data is handled, shared, utilized, archived and deleted. Understanding what your data is, and how it's used and stored, is a key requirement in building your business' GDPR strategy.

2. Determining ownership and accountability

It is important to identify a responsible owner for data protection compliance. For some organisations, appointing a data protection officer is required. The GDPR also introduced a new "accountability" principle that requires organisations to adopt a data protection compliance programme. Organisations will need to develop internal data protection policies and provide staff training.

3. Ensuring a legal basis for processing

Another component of the GDPR that companies must ensure are documented are the legal grounds for processing the different types of personal data you handle. For example, if you are using consent as a basis for processing, you'll need to consider how you obtain it and must be able to clearly demonstrate how and when it's been given.

4. Understanding the rights of data subjects

To ensure your procedures accommodate them, you will want to make sure you understand the rights that people have in relation to their personal data. For example, data subjects have the right to access their personal data, as well as have it corrected, erased, or exported electronically. In certain circumstances, users also have the right to object to automated decision-making and profiling.

5. Ensuring privacy by design

Privacy by design is an explicit legal requirement for the first time, so it's important to build it into your business processes. In some circumstances, conducting privacy impact assessments is also necessary.

6. Preparing for breach management

Ensuring your r data breach management policies and processes are up to date and tested is crucial to a robust data protection programme. Detecting and reporting breaches to the correct authorities in a timely manner is required by the GDPR, as fines can be levied for reporting failures as well as for breaches.

7. Communicating essential information

Ensuring that your organization's online privacy policies and other notices are up to date and encompass the data protection practises . New requirements include detailing the legal basis for your processing and making users aware of the authority they can complain to if there's a problem.

8. Working with your providers

Fulfilling GDPR obligations goes beyond your organisation's own policies. Any third parties processing personal data on your behalf will also need to meet the necessary standards for data protection. Some questions you may want to ask your providers include:

- Do they have robust practices for network and information security, privacy, and data protection?
- Do they conform to internationally accepted standards and verify their compliance?
- How can they demonstrate a strong culture of trust and security? And what controls do they offer to help you manage your data and meet your obligations as a controller?

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 information seriously. To be worthy of your trust, we built and will continue to grow Dropbox with an emphasis on security, compliance, and privacy.

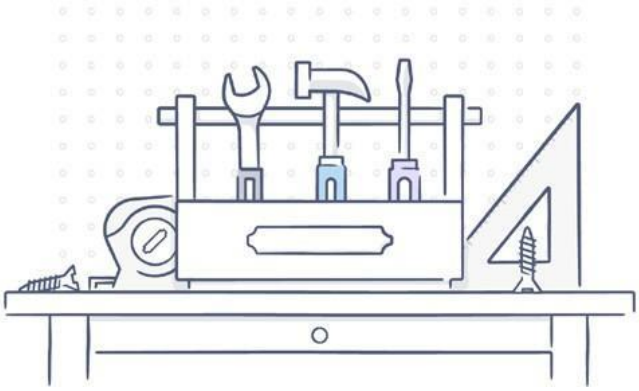
Security: Protect and control

Protect: Architecture and information security

Dropbox is designed with a secure, distributed infrastructure with multiple layers of protection including secure data transfer, encryption, network configuration, and application-level controls distributed across a scalable and secure infrastructure. Our robust information security management framework is designed to assess risks and build a culture of security at Dropbox. We regularly review and update security policies; provide our employees with security training; perform application and network security testing (including penetration testing); conduct risk assessments; and monitor compliance with security policies. Full details can be found in our Dropbox Business Security White Paper.

Control: Empowering IT administrators

Dropbox provides the control and visibility features that IT admins need, helping you to manage your compliance obligations more easily. Our admin dashboard enables you to monitor team activity, view connected devices, and audit sharing activity. You can create groups to easily manage team member access to specific folders, and team folder manager gives you visibility and control over team folders, including sync management. The link permissions feature means you can password protect shared links, set expiration dates to grant temporary access, and limit access to those within your organisation. Our account transfer tool allows you to easily transfer files from one user to another when responsibilities change. Remote wipe enables you to clear files from lost or stolen devices.



Compliance: Trust and verify

Compliance is an effective way to validate a service's trustworthiness. We encourage and expect you to verify that our security practices comply with the most widely accepted standards and regulations like ISO 27001, 27017, 27018 and SOC 1, 2, and 3. Our independent third-party auditors test our controls and provide their reports and opinions — which we share with you whenever possible. More information on the standards that we comply with and how we verify our security practices is available on our compliance web page.

Privacy: Our commitment

We are committed to protecting your data. Whether it's your personal or work information, we take our users trust seriously and work hard to ensure that all data in our systems is protected.
Our privacy policy clearly describes how we handle and protect your information. In addition, Dropbox Business adheres to the Cloud Security Alliance (CSA) Code of Conduct for GDPR Compliance. Furthermore, we publish a transparency report and our government data requests principles to share how often we receive, scrutinize, and respond to these requests, and we also try to reform laws to make them more protective of your privacy.

Working together to keep your data secure

Dropbox works with its business customers to keep their data secure. 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 audit. Customers also play a key role in ensuring their teams and data are protected and secure. Dropbox enables you to configure, use and monitor your account in ways that meet your organisation's security, privacy 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 team's data.