

# The General Data Protection Regulation

The General Data Protection Regulation, or GDPR, is a European Union regulation that establishes a new framework for handling 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 in respect of their personal data. Organisations must comply with the new rules by 25 May 2018.

How to prepare for the GDPR

If you think your organisation may be impacted by the GDPR, now's the time to start preparing. We highly recommend you seek legal advice to determine what may be required for your specific situation. However, there are a number of factors that all organisations should be considering.



## 1. Understanding your data

Protecting data properly means understanding how it's treated in your organisation—how your personal data is handled, shared, and used. With this information, you can build your GDPR strategy in a way that works for your organisation, and allows you to use the data the way your business needs to.

## 2. Determining ownership and accountability

It's important to identify a responsible owner for data protection compliance. For some organisations, this will mean appointing a data protection officer. The GDPR also introduces a new "accountability" principle that requires organisations to adopt a data protection compliance programme. In addition, you may need to develop internal data protection policies and provide staff training.

## 3. Ensuring a legal basis for processing

It makes sense to start determining and documenting what legal grounds you're using for processing the different types of personal data you handle. If you're using consent as a basis for processing, for example, you'll need to consider how you obtain it and 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 new rights that people have in relation to their personal data. For example, data subjects will have the right to access their personal data, as well as have it corrected, erased, or ported electronically. In certain circumstances, they'll also have the right to object to automated decision-making and profiling.

## 5. Ensuring privacy by design

Privacy by design will become an explicit legal requirement for the first time, so it's important to begin considering how to build it into your business processes. In some circumstances, conducting privacy impact assessments will also be necessary. It's important to start planning how, when, and by whom these will be conducted.

## 6. Preparing for breach management

You'll want to review and update your data breach management policies and processes. Detecting and reporting breaches to the correct authorities in a timely manner will be critical, as fines can be levied for reporting failures as well as for breaches.

## 7. Communicating essential information

Reviewing your online privacy policies and other notices will become important as the GDPR deadline nears. 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?

## Dropbox: Protecting your data

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.

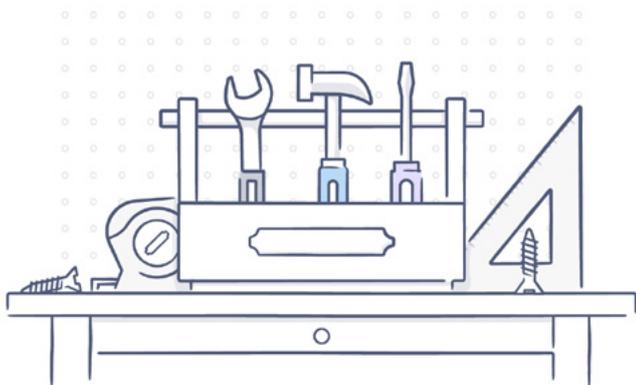
### Security: Protect and control

#### 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, 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

You own your data, and whether it's your personal or work information, we're committed to keeping it private. Our [privacy policy](#) clearly describes how we handle and protect your information. 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.

The contents of this guide are to assist access to information and do not constitute legal advice. Readers should obtain their own legal advice as may be required.

