Dropbox's GDPR Compliance Journey

Dropbox

Introduction

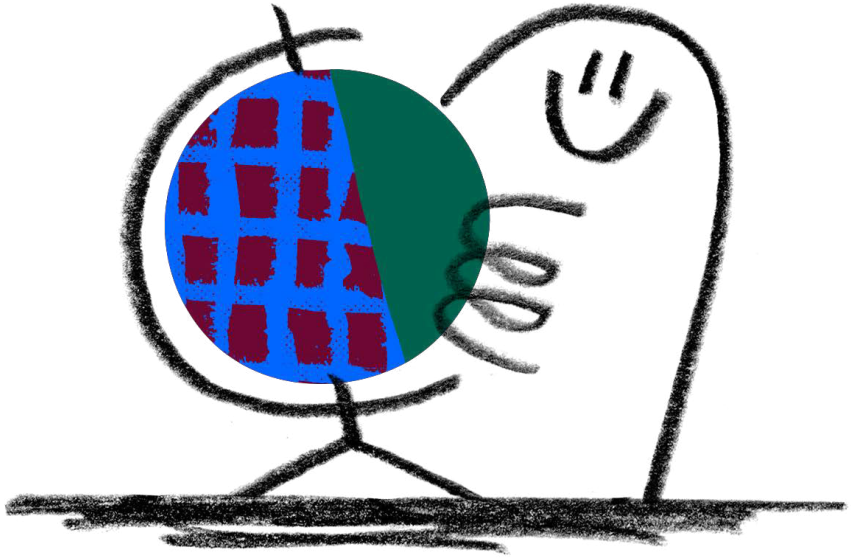
Europe's General Data Protection Regulation (GDPR), a European Union regulation that updates and harmonises the framework for processing personal data in the EU, went into effect on 25th May 2018.

Since the regulation went into effect, our customers have been increasingly focused on the real-world implications of the new European data protection framework.

At Dropbox, we are prepared for GDPR. Based on customer feedback, we've decided to share a bit of our journey with you.

What the GDPR means to 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 information seriously.

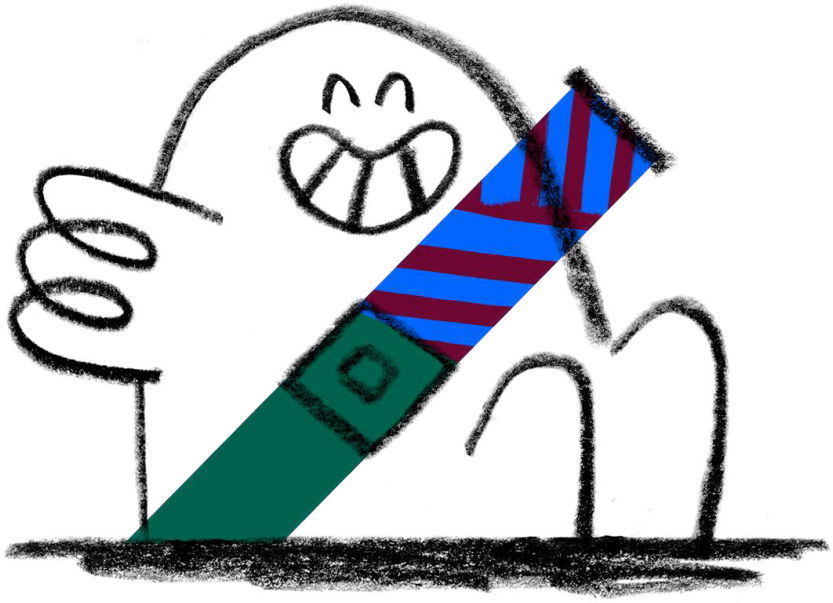


At Dropbox, the security and privacy of your data are our highest priorities:

- We have a dedicated security team using specialist tools and engineering practices available to build and maintain Dropbox, and we've implemented multiple levels of security to protect and back up your files.
- Our security practices comply with the most widely accepted standards and regulations like ISO 27001, ISO 27017, ISO 27018, HIPPA/HITECH, Germany BSI C5 and SOC 1, 2 and 3. Independent third-party auditors test our controls and provide their reports and opinions.
- More information on the standards that we comply with and how we verify our security practices is available on our www.dropbox.com/business/trust/compliance web page.
- Our Dropbox Business Security White Paper sets out in detail all aspects of our approach to security (infrastructure, network, application, physical, information, etc.).

We have a strong track record on data protection:

- Dropbox places the utmost importance on data protection and has a track record of staying ahead of the compliance curve – for example, we were one of the first cloud service providers to achieve ISO 27018 – the internationally recognised standard for leading practices in cloud privacy and data protection.
- We have dedicated privacy experts designing and maintaining our privacy program and policies to help safeguard your data in line with the requirements of the GDPR.
- Dropbox includes strong contractual commitments in its agreements with our business customers. Our business customer agreements incorporate the EU model contract clauses and we are certified under the EU-US Privacy Shield Framework. This means there are additional legal protections and external monitoring regarding the collection, use and retention of personal data transferred from the European Union to the United States.



How Dropbox Prepared for GDPR

Given this strong foundation, Dropbox views GDPR compliance as an incremental build on top of our existing practices and controls, rather than a revolution in the way we process personal data.

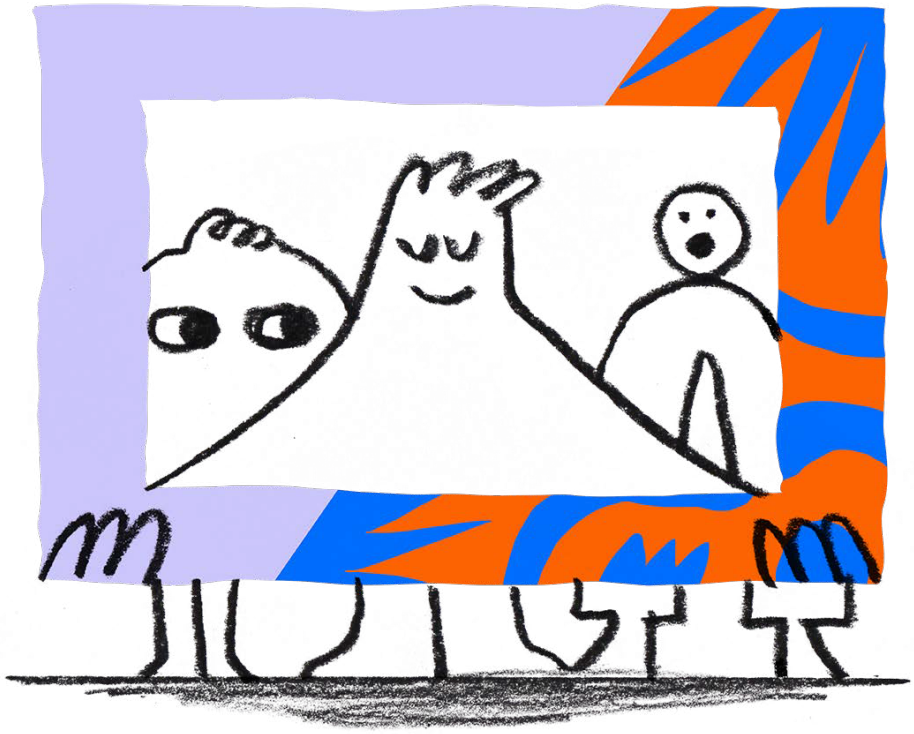
Dropbox's journey to compliance began as soon as the regulation was adopted in 2016. Our first step was to **form a cross-functional team of data protection specialists** consisting of legal counsel, security and compliance professionals, product and infrastructure engineers, from both sides of the Atlantic to specifically analyse and address the new requirements of GDPR.

The next step was to **evaluate our current security and data protection practices and GDPR readiness levels**. This involved performing a complete and detailed gap assessment of the GDPR and most recent accompanying guidance, determining what areas were applicable to Dropbox and then assessing if our current practices either met the requirements as described or needed iteration in order to fully meet the requirements.

Our next step was to **perform a complete and detailed evaluation of our personal data processing activities**. This exercise is sometimes referred to as "Data Mapping". In effect, this data mapping traces the lifecycle of personal data through our systems, from initial collection from the user all the way to deletion and disposal.

We **built 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.

With our expert team established and with a GDPR gap assessment and data mapping completed, Dropbox implemented steps and process developments to ensure we can comply fully with GDPR by May 2018.



Dropbox