keepit®

Whitepaper

Keepit data protection:
GDPR compliance and readiness

April 2024, Copenhagen

Data protection with Keepit: GDPR compliance and readiness

The General Data Protection Regulation (GDPR) is the EU's data privacy and security gold standard, protecting the fundamental right for data protection of data subjects' personal data.

With its implementation in 2016, the GDPR brought new obligations for organizations to be transparent about their data collection and processing practices, to obtain clear consent for the use of personal data, and to implement appropriate technical and organizational measures to ensure the security of that data. Additionally, the GDPR established the right for individuals to request access to their personal data and the right to have it erased. These changes have led to a heightened sense of responsibility among organizations for how they handle and process data and have helped to increase trust in the digital economy.

Any organization in the EU processing personal data must comply with GDPR. Non-compliance results in significant fines as well as a damaging loss of reputation: As one of the most high-profile cases, Meta has been fined $1.3B for mishandling data, showing that there will be huge consequences for GDPR non-compliance.

Given that GDPR has significant data protection and security implications, your SaaS data protection solution must do more than check compliance boxes — it should ensure that your data is safe and help you make the process of achieving compliance simple. As a European-born and operated vendor, compliance is second nature to Keepit.

Our services are purposefully built to make compliance requirements easy to accommodate for customers. And our company is rigidly compliant with all relevant regulations in the regions we operate across the world — so much so that Forrester has recommended Keepit as the "best fit for companies that need Microsoft 365 protection and GDPR expertise."*

Curious to find out why?

This document will explain in depth how Keepit's backup and recovery solution supports and enables GDPR compliance and data protection through its key features.

* Forrester, New Wave™: SaaS Application Data Protection, 2021

1. Platform design

Keepit has designed its platform to provide leading security for any modern cloud SaaS application, which means that even if the entire infrastructure of the SaaS vendor is compromised, customers will still have a full copy of all recent data accessible. Ensuring data availability is the backbone of any data protection plan.

2. Security by design

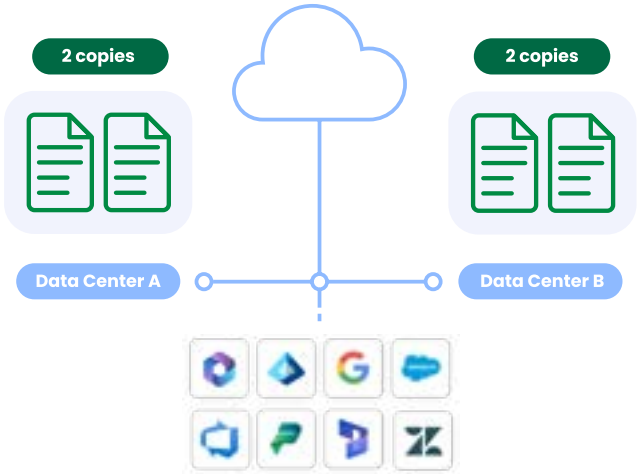
At the technical level, the Keepit solution employs blockchain technology, cryptography, purpose-built APIs, and systems and service segregation to maintain the highest level of security. Keepit employs encryption when data is in transit using HTTPS secured with modern TLS when accessing customer data through primary workload vendor APIs such as Microsoft 365, Salesforce, Google Workspace, and others.

As an additional physical layer of security, Keepit will typically exchange traffic directly with the workload providers over major internet exchanges, far from the prying eyes of the average Wi-Fi hotspot eavesdropper. Once data reaches Keepit, it is encrypted before being stored in Keepit storage systems. For this purpose, Keepit employs AES encryption directly on storage systems — this is the same encryption algorithm that is used throughout industry and government bodies to keep secret practically anything that needs to be kept secret.

As yet another additional security layer, the storage media upon which customer data resides is kept in a physically secure data center.

3. Data center security

Each of Keepit's geographic regions operates active-active from separate physical locations to protect not only against the forces of criminals seeking to compromise data, but also against the forces of nature. This means that each Keepit region employs two regional data centers, each data center being a complete mirror of the other. The two data centers operate in active-active mode, continually keeping data replicated between them. For this reason, any single system can fail without affecting the operation of the platform, and even a full site can fail without affecting the platform, as it has a separate, mirrored data center operating alongside it. This keeps customer data always accessible and available for restore, even in the unlikely event of the loss of a full data center.



4. The Keepit cloud

The Keepit cloud is fully owned and run by Keepit. Our systems, our people, our standards.Keepit can therefore guarantee that the backup data we are storing is fully isolated fromcustomer SaaS vendors cloud, no matter if that may be Azure, AWS, G Cloud or somethingelse. Keepit does not share infrastructure with any public cloud, period. We believe this to be a fundamental requirement for any backup solution, in line with the well-known 3–2–1 backup principle.

Customers would not store backup data on the server they are backing up — so how could customer cloud backup data reside in the same cloud they are backing up? That would not make sense, of course. Why not? In the event that the SaaS provider's cloud is down, data would be inaccessible. With Keepit, data will still be accessible in this case since it is backed up on Keepit's private cloud. An independent, third-party cloud for always-on availability: that is data protection best practice.

5. Data sovereignty

To comply with GDPR, companies with operations in the EU are required to store all their customer data within the EU. To meet such customer data sovereignty requirements, Keepit operates separate data centers in multiple regions — currently America, Europe, and Asia-Pacific. Each cloud is run from data center locations provided by the Keepit data center partners Equinix and Cibicom. Each of the data center regions are completely isolated from each other. Keepit offers a no-transmission guarantee — a promise that data will never leave the selected data region.

6. Data processing agreement

The DPA is the fundamental legally binding agreement that Keepit enters into with each of its customers which states the rights and obligations of each party concerning data protection. The agreement includes a number of guarantees to customers that entrust Keepit with its personal data on how this data is processed and protected when stored with Keepit.

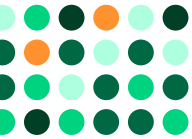
Keepit is a European-born and operated company, which means we comply with all relevant data protection regulations in the EU and do not rely on any data sub-processors globally who would be able to access data. Next to these guarantees in the DPA, our customers are further entitled to receive annual third-party audit reports.

7. Data processor

According to personal data regulation, Keepit is defined as data processor, acting solely on instructions of the customer being the data controller. Keepit does not collect, nor store, data that is not specifically directed by its customers. Further, Keepit does nothing without the clear instruction from its customers.

8. System restore

Data protection regulations such as GDPR, but also cybersecurity regulations such as NIS2, generally require that businesses have the ability to restore availability and access to personal data in a timely manner in the event of a physical or technical incident. Keepit provides for this, as in case of an incident, data can rapidly be located, verified, and restored in-place — usually in a matter of minutes.



9. Deletion impossible

Keepit customers will notice that — just like a tape in a vault — it is not possible to alter backup datasets. Because of our unique architecture and object storage, data is undeletable and unchangeable.

Users cannot re-write history. Users cannot even delete a user account without going through a holding period. What this means to customers is that a potential malicious hijacker who takes on a user identity will face similar restrictions as the user. In other words, customers are practically invulnerable to ransomware and data loss.

10. Data integrity

Keepit has been built to be completely tamperproof by being an inherently immutable data store: once data is in, it cannot be changed. This means Keepit is immutable by design.

The application does not expose any APIs or other means that would allow data overwrites. Furthermore, the blockchain-like structure used, called Merkle Tree, allows all layers in the platform to verify that a given requested data object is unaltered from its original form through unique identifiable hashes. The result is guaranteed data integrity.

11. Data retention

Within the Keepit solution, customers can determine the amount of time any given data object remains in the backup after being deleted from customer's cloud solutions backed up by Keepit. In addition to the various regulatory frameworks that customers are already tasked with, customers may also have contractual and business requirements that dictate implementation of a customized data retention policy.

In order to draft and implement an accurate data retention policy, customers need to know what kind of data the organization holds, the purpose of having this data, and in which systems the data resides. However, holding onto data longer than required by law or longer than needed for use can have various adverse consequences which include:

- **Increasing risk of experiencing a data breach or security incident;**
- **Placing client data at greater risk of being breached;**

- **Contributing to cluttered hardware and/or software, making it difficult to find data that is actually needed; and**
- **Expanding the regulatory compliance burden related to data access.**

Ultimately, in order for an organization to implement an effective data retention policy, data that no longer serves a purpose to the organization or data that has been held for the required retention period should be deleted.

Keepit enables customers through its unique platform connector model to build and maintain an effective and compliant data retention plan. Thus, the customer can configure its own unique and individual data retention rules within the Keepit platform, facilitating customized data clean up.

12. Processing security

GDPR Article 32 requires data controllers and data processors to implement technical and organizational measures that ensure a level of data security appropriate for the level of risk presented by processing personal data. Keepit has implemented such measures, which are described in the "Keepit technical and organizational measures" paper.

The purpose of these measures, which, includes data encryption, is to ensure the ongoing confidentiality, integrity, availability, and resiliency of your data backup with Keepit.

According to Article 32, you are not only required to protect your data from unauthorized access and outages but also from any form of modification or deletion.

In a recent decision from a European data protection authority, the authority held that backups being read, modified, and deleted in connection with a ransomware attack was a breach of Article 32 and led to the organization being heavily fined for not securing the availability of data. To help our customers avoid such a scenario, we offer true data immutability and absolute protection against deletion.

13. Right to be forgotten (RTBF)

Under GDPR Article 17, personal data must be erased without undue delay, if you as a data controller do not have a legal basis for keeping personal data. A common question that arises from this is how we comply with this article, as due to our unique architecture, the backup history cannot be modified and data is undeletable.

Data protection authorities hold the position that if deletion in the backup is not technically possible, you cannot be required to delete data, but instead, have to ensure that the data is not restored from the backup to your live environment. This entails that if personal data needs to be restored from backups, you, as the data controller, will have to take the necessary steps to comply and ensure the data is not restored to protect the rights of the data subject.

To help our customers stay compliant, we have developed a dedicated feature. The RBTF label allows customers to tag those records which, in accordance with GDPR, are not allowed to be recovered in any way, shape or form — be it through restoring to the source organization or a download. Once assigned, the record will become inaccessible, and if it is ever part of a larger restore job, it will not be restored either. This makes us the only backup provider globally with a full implementation of the GDPR "Right to be forgotten" (RTBF) legislation of Article 17 and Article 32.

We recommend you, as our customers, to maintain transparency with the data subjects and clearly describe in your data privacy policies how you handle your obligations under Article 17 and Article 32 in connection with backups and immutability of data.

14. Keepit compliance

Keepit meets demanding regulatory requirements. As a European vendor, compliance is second nature to Keepit: Our services are built to make compliance requirements easy to accommodate for customers. And our company is rigidly compliant with all relevant regulations in the regions we operate in. Plus, Keepit employs its own dedicated DPO to assist and monitor internal compliance, as well as inform and advise on Data Protection obligations.

As your trusted cloud backup vendor, we're serious about the security of your data. Keepit and our data centers are therefore certified by both ISO/IEC 27001:2013 and the ISAE 3402–II (audited by Deloitte annually). Further information about data security in Keepit, compliance certifications of Keepit, as well as our data center partners can be found in the Keepit Security Guide available at our website.

Because of this functionality, we believe that Keepit is an essential tool in helping you achieve GDPR compliance and ensure solid data protection.

With the highest security standards and by running our own infrastructure with data centers across the world offering a no-transmission guarantee, Keepit allows you to store your data in a specific region and guarantees that your data will never be moved outside of that region — vital for businesses that have regulations or concerns around data sovereignty, privacy, or data residency.

Further, our dedicated feature set makes us the only backup provider globally with a full implementation of the GDPR "Right to be forgotten" (RTBF) legislation of Article 17 and Article 32. With our ongoing commitment to compliance, we ensure that organizations are well equipped to comply with today's challenges, as well as future regulations and contractual demands for data protection involving the governance and safekeeping of personal data.

Keepit has been recognized by Forrester as a leader in SaaS application data protection due to its "significant experience with data privacy and compliance needs." The analysts confirm that Keepit offers strong core SaaS application data protection support in regard to privacy regulation compliance and recommend it as "the best fit for companies that need Microsoft 365 protection and GDPR expertise." Learn more about this in the Forrester New Wave Report.

Take the next step toward protecting your Saas data

Request a demo

keepit®

Keepit provides next-level SaaS data protection for key business applications, ensuring business continuity and access to data. Keepit is the world's only independent backup and recovery solution and keeps data resilient to cyberattacks and human error. Headquartered in Copenhagen with offices and data centers globally, Keepit is trusted by companies worldwide.

HQ - Copenhagen
Denmark
Keepit A/S
Per Henrik Lings Allé 4, 7.
2100 København, Denmark
CVR: 30806883
+45 8987 7792
sales@keepit.com

Dallas, Texas
United States
Keepit USA Inc.
3232 McKinney Avenue Suite 820
Dallas TX 75204, USA
TIN: 85-358 6335
+1 469-461-4892
sales@keepit.com

London
United Kingdom
Keepit Technologies UK, LTD.
Warnford Court
29, Throgmorton Street
London EC2N 2AT, UK
Company reg. no.: 13785045
sales@keepit.com

Munich
Germany
Keepit Germany GmbH
Maximiliansplatz 22
380639 München
Amtsgericht München,
HRB 270094
Geschäftsführer Morten Felsvang
sales@keepit.com

www.keepit.com