keepit®

Whitepaper

Keepit Data Protection Compliance & Readiness

November 2021
Copenhagen

Keepit Data Protection Compliance & Readiness

Any company or organization processing personal data must comply with relevant Data Protection regulation. Non-compliance can result in significant fines as well as damaging loss of reputation.

Keepit backup and recovery solution supports and enables Data Protection compliance and readiness through implementation of the following key features:

1. Platform Design:

Keepit has designed its platform to provide security for any modern cloud workload which means that even if the entire infrastructure is compromised, customers will still have a full copy of all recent data which is the backbone of any data Protection plan.

2. Security by Design:

At the technical level, the Keepit solution employs blockchain technology, cryptography, and purpose-built APIs, 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 governments to keep secret practically anything that needs to be kept secret. As an additional physical layer, the storage media upon which customer data resides is kept in a physically secure data center.

3. Data Center Security:

Each of Keepit 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 data centers. 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 reachable 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 owned and run by Keepit. Our systems, our people, our standards. Keepit can therefore guarantee that the backup data Keepit is storing is fully isolated from customer SaaS vendors cloud, no matter if that may be Azure, AWS, G Cloud or something

else. Keepit does not share infrastructure with any public cloud, period. Keepit believe this to be a fundamental requirement for any backup solution. 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 since it is backed up on Keepit's private cloud. An independent, third-party: this is data protection best practice.

5. Data Sovereignty:

To meet customer data sovereignty requirements, Keepit operates separate clouds in multiple regions - currently Americas, Europe and Asia-Pacific. Each cloud is run from data center locations provided by the Keepit data center partners Equinix, Cibicom. Each of the data center regions are completely isolated from each other.

6. Data Processing Agreement:

Is the fundamental legally binding agreement that Keepit enters into with each of its customers and 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. Customer is 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 regulation generally requires that systems must 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. 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. 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 hijacker who takes on a user identity will face similar restrictions as the user. In other words, customers are practically invulnerable to ransomware.

10. Data Integrity:

Keepit has been built to be tamper-proof by being an inherently immutable data store; once data is in, it cannot change. The application does not expose any APIs or other means that would allow data overwrites. Furthermore, the blockchain-like structure allows all layers in the platform to verify that a given requested data object is unaltered from its original form.

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 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 the 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 client platform facilitating customized data clean up.

12. Security of Processing:

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 Organization Measures paper. The purpose of these measures which among other things includes encryption of data 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 hence our long time focus of not deviating from data immutability and protection against deletion.

13. Right to be forgotten:

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 the personal data. Several 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 with the initial request and erase the data again as you restore data to protect the rights of the data subject. We recommend to 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. Keepit will closely monitor the legal development relating to Art 17 and Art 32 and how they apply to our backup services.

14. Keepit Compliance:

Keepit meets demanding regulatory requirements. Keepit is annually audited by third party (currently Deloitte) who prepares an ISAE 3402 II audit report. Moreover Keepit is in the in the process of implementing ISO 27001. 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.

15. Data Protection Officer (DPO):

Keepit employs its own dedicated DPO to assist and monitor internal compliance, as well as inform and advise on Data Protection obligations.

While there is no single standard or certification for compliance with regulation on protection of Personal Data; Keepit ensures that organizations are well equipped to comply with today's challenges, as well as future regulations and contractual demands, involving the governance and safekeeping of Personal Data.

Dedicated SaaS Data Protection

About Keepit

The world's only independent vendor-neutral cloud dedicated to SaaS data protection, Keepit is trusted by thousands of companies worldwide to protect and manage their cloud data.

Leading analysts agree Keepit is the fastest and most secure enterprise-class SaaS backup and recovery service.

Keepit – Dedicated to SaaS data protection, loved by customers.

Visit: Keepit.com