keepit

Keepit cybersecurity factsheet

October 2024

Table of Contents

Executive summary

As businesses increasingly rely on software-as-a-service (SaaS) applications to support their critical operations, many are unaware of the shared responsibility model that governs data protection in the cloud. While SaaS providers ensure platform availability and security, the responsibility for protecting and recovering business-critical data rests squarely with the customer. This distinction creates a significant data protection gap that exposes enterprises to potential data loss and disruption.

Gartner estimates that by 2028, 75% of enterprises will prioritize backup of SaaS applications as a critical requirement — compared to 15% in 2024. And understandably so: Forrester reports that 80% of enterprise security decision-makers with network, data center, app security, or security ops responsibilities reported their sensitive data was compromised or breached at least once in the past 12 months.

Keepit addresses this challenge by offering a purpose-built, vendor-neutral SaaS data backup solution that provides organizations with the tools to secure, protect, and recover their data. Unlike other backup solutions that store backup data on the same cloud infrastructure as production data, Keepit's independent infrastructure guarantees that backup copies are always secure and restorable through immutable, air-gapped data protection.

At the core of Keepit's approach is a commitment to globally recognized standards such as ISO 27001 and ISAE 3402 type II, ensuring adherence to industry best practices. With dual active-active data centers, AES 256-bit encryption, and immutable backups, organizations can rest assured that their data is always accessible, even in the event of a major outage or cyber incident.

Keepit's solution not only ensures compliance with regulatory frameworks such as NIS2, DORA, and NIST, but also empowers organizations to meet the demands of modern security and data resilience. With over 20 years of experience in data protection, Keepit provides the reliability and expertise needed to address the evolving risks in today's cloud landscape.

Introduction to Keepit

As SaaS applications continue to enable modern businesses, critical services are migrating from the trusted confines of on-premises computing to third-party cloud providers, far removed from traditional backup solutions. This shift has introduced a shared responsibility model in which both the SaaS provider and the SaaS customer — you — each assume ownership of different aspects of data protection (Figure 1).

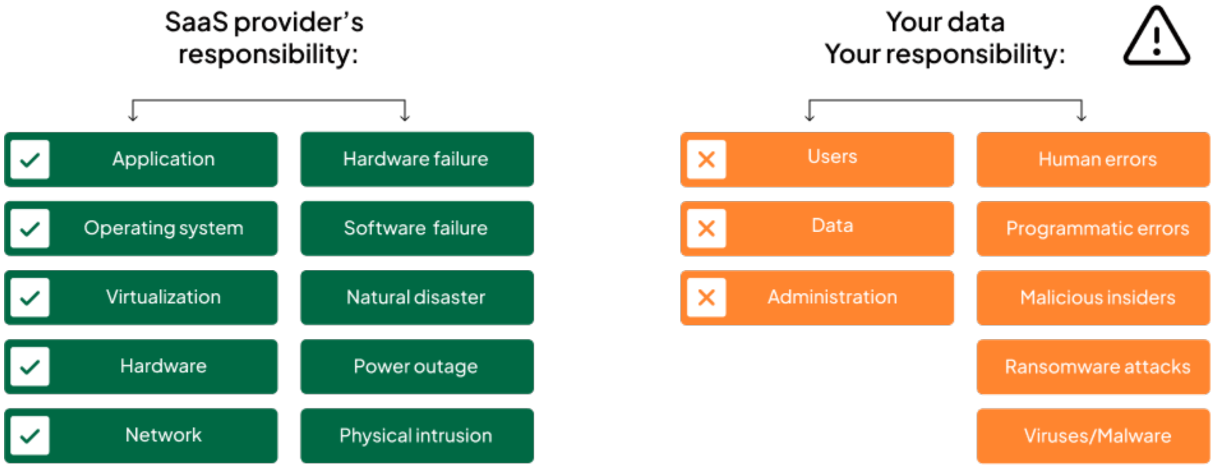


Figure 1—Division of responsibilities between the SaaS provider (left) and the SaaS customer (right)

Relying solely on the SaaS provider for data protection is a risky proposition, as their responsibility often stops short of safeguarding customer data from loss. While the adoption of cloud services has accelerated, many enterprises are only beginning to grasp the full implications of this shared responsibility. Despite widespread reliance on SaaS applications, most organizations have not yet implemented third-party backup solutions to protect their data.

Keepit bridges this gap by providing a purpose-built, vendor-neutral SaaS backup solution designed to ensure data is not only secure but also resilient and recoverable. Our solution operates independently of public cloud providers, offering separate, immutable backups that guarantee data integrity, even in the face of cyberattacks or cloud outages.

This guide outlines how Keepit's security-first approach, adherence to global security standards, and innovative backup infrastructure can empower your organization to fulfill its responsibilities under the shared responsibility model — ensuring data resilience, compliance, and business continuity in the ever-evolving cloud landscape.

Security mission and strategy

Cybersecurity has never been more important — or challenging — than it is today. In a world of evolving cyberthreats, resilience is not just a priority; it’s a necessity. Backup has become far more than a precautionary measure, and it’s now the backbone of an enterprise’s ability to recover after a data loss event. In an era of increasingly sophisticated cyberattacks, businesses must not only focus on protecting their data but also on how quickly and effectively they can restore it.

One of the most critical, yet often overlooked, challenges organizations face is the shared responsibility model inherent in SaaS applications. While SaaS providers ensure the availability and security of their platforms, the onus of data protection falls squarely on the customer. Keepit bridges this gap by providing a secure, vendor-neutral solution that ensures your SaaS data remains safe, immutable, and easily recoverable, no matter the circumstances.

Keepit offers this essential capability, providing an immutable, air-gapped backup solution that ensures organizations can quickly return to a "last known good state" in the event of data loss. Our purpose-built backup solution is designed to be the foundation upon which enterprises recover from attacks, ensuring operational continuity even in the face of a major disruption.

At Keepit, we believe that security is not just a feature — it’s the foundation of everything we do. With over 20 years of experience in data protection in the cloud, we have the expertise and vision to deliver a solution that not only meets today’s security challenges but also anticipates those of tomorrow.

Our approach extends beyond just backup storage. By leveraging our active-active data centers, organizations can work directly with their data in hot storage, ensuring it is always available and recoverable in real time. This continuous active-active setup allows seamless access to data, even during ongoing backups, so users can restore and resume operations. This architecture not only guarantees availability but also enhances business continuity, enabling enterprises to maintain productivity and minimize the impact of any cyber incident.

Keepit’s security-first approach reflects our commitment to meeting the security and compliance demands of modern enterprises, now and in the future. In a world where data is constantly under attack, traditional backup methods are no longer sufficient. This is why we designed Keepit’s infrastructure from the ground up, with an unwavering focus on security, resilience, and compliance.

Our security strategy is founded on industry-leading best practices and globally recognized standards, such as ISO 27001 and ISAE 3402 type II certifications. These frameworks guide our approach to risk management, access control, encryption, and disaster recovery, ensuring that Keepit’s customers are not only protected today but also prepared for the challenges of tomorrow. Our ongoing pursuit of SOC 2 compliance further demonstrates our commitment to exceeding industry standards and continually enhancing our security posture.

Beyond external threats, we take a holistic view of security, ensuring that our human resources, access control, and physical security measures are as robust as our technical solutions. By adhering to the principle of least privilege, we ensure that only authorized personnel can access critical systems. Additionally, our geographically diverse, dual-data center architecture guarantees redundancy and resilience, future-proofing companies for compliance with various frameworks and regulations, such as NIS2, DORA, and NIST, along with other international data protection regulations.

We believe in transparency and learning from our customers. Accordingly, we've prepared this document to proactively address the most common inquiries about our solution, explain the decisions we made in building it, and demonstrate how our solution is fundamentally different from others in the market.

Enjoy the read,

Kim Larsen
CISO
Keepit

Frameworks followed

When it comes to backup and recovery, businesses seeking solutions need to be incredibly thorough in their due diligence processes. Keepit's information security management system was formalized and implemented at Keepit based on ISO 27001 requirements.

The Keepit service holds the ISO 27001 certification and independent ISAE 3402-II report. Additionally, Keepit is currently being audited for the SOC2 framework and other certifications are in scope and planned for the coming year. More on Keepit's end-to-end ISO/IEC 27001 certification:

By achieving the ISO/IEC 27001 certification, Keepit continues to demonstrate its dedication and ability to deliver best-in-class security technology to its customers. The certificate states that:

> *"[Keepit] operates an information security management system (ISMS) which complies with the requirements of the ISO/IEC 27001 for the following scope:*
> *The ISMS scope includes development, operations, and maintenance of services that support the company's business & B2B SaaS Backup Solutions System, in accordance with the ISMS Statement of Applicability v1.1 dated 22.02.2024."*

We perform regular and independent security checks and penetration tests to ensure Keepit continues to meet the requirements of the ISO/IEC 27001 standard and complies with industry best practices. On a yearly basis, Keepit obtains an independent third-party ISAE 3402 Type II audit report concerning Keepit's organizational procedures, security, and assets. A third-party company provides penetration testing based on OWASP Top 10 on a yearly basis.

Apart from that, Keepit implements and maintains appropriate organizational and technical measures to protect the customer data stored within Keepit's backup solution (Customer Content), processed under the Agreement pursuant to GDPR Articles 28(3)(c) and 32. These measures are based on industry best practices such as ISO 27001, ISO 27002, NIST SP800-30, NIST SP800-39, and FEMA guidelines.

Keepit is highly motivated to continually improve its security infrastructure to be compliant with industry recognized security certifications and security assessments, demonstrating our commitment to industry leadership.

Data protection compliance

At Keepit, we understand the importance of staying compliant with data protection laws and regulations, especially as a provider of SaaS backup and recovery solutions. We're committed to ensuring that our services not only meet but exceed the standards required by these laws, providing our customers with confidence in their data protection practices.

Keepit's compliance with legal and regulatory requirements

To remain compliant with legal and regulatory obligations, Keepit takes a multifaceted approach:

- **Dedicated legal team**

- **Collaboration with external legal advisors**
- **Proactive policy updates**
- **Customer communication**

Adherence to data protection laws

Keepit fully complies with the General Data Protection Regulation (GDPR). We have implemented a comprehensive approach to ensuring that all personal data handled by our services is processed securely and transparently, with a strong focus on protecting privacy and maintaining data integrity.

Additionally, we comply with other applicable data protection laws, ensuring that our customers remain fully protected no matter where they operate. Our commitment to privacy and security ensures that our customers can rely on Keepit to meet their data protection needs.

No transfers of personal data to third countries

Keepit does not transfer Customer Content to third countries, nor do we engage sub-processors in connection with the provision of our services. Should this ever change, we will inform affected customers in advance and provide a clear explanation of the legal basis for the transfer, in accordance with the applicable Data Processing Agreement.

Read more about Keepit’s compliance with legal and regulatory requirements in the apprendix located at the end of this document,

Resilience in Keepit backup and recovery

When designing and building The Keepit Cloud, we aspired to provide a number of important fundamental features and characteristics, including:

- Vendor neutrality
- Resilience and data immutability
- Secure, reliable, and change-based long-term data storage
- Easy and fast data recovery unparalleled in the industry

The application uses a patent-pending, blockchain algorithm which makes any low-level tampering impossible and easily evident. The Keepit storage system features a proprietary immutable storage scheme, protecting data from deletion or tampering. Keepit uses advanced crypto technology (Merkle tree approach) as part of the solution architecture that identifies blocks of data to ensure storage efficiency (deduplication), redundancy, immutability, and instant access.

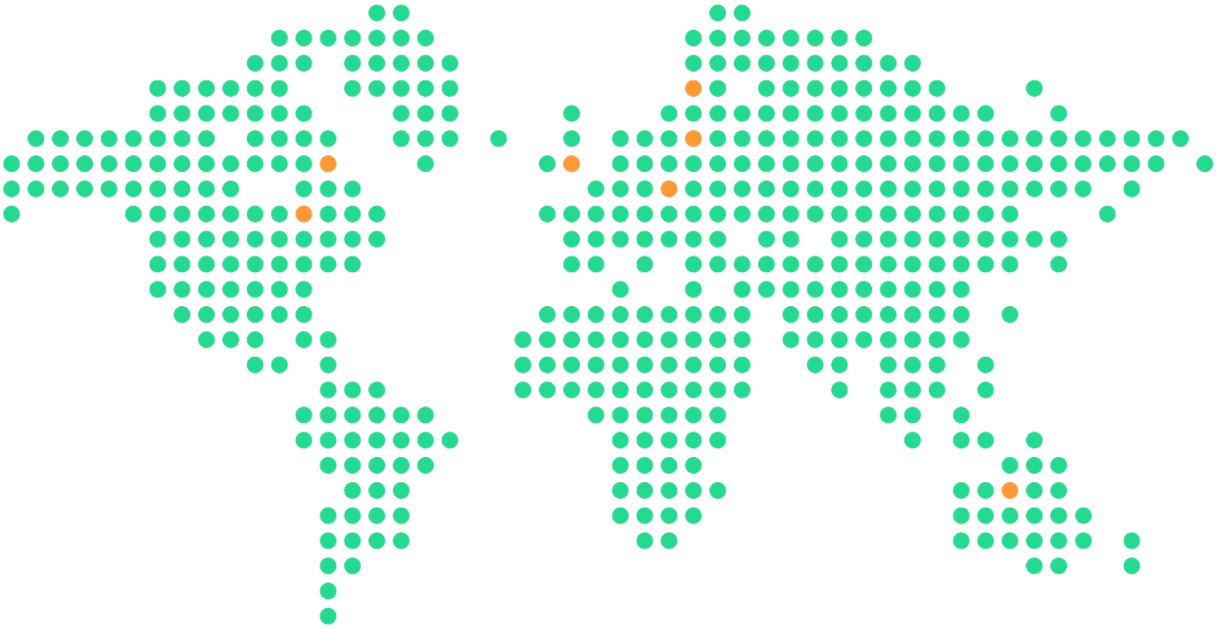
In the Keepit data model, when a backup executes, we effectively only transfer the differences in your dataset; however, when you view your data in the Keepit platform, all access is instant across time and space, and every single backup snapshot — no matter how old — appears as if it was a standalone full copy of your dataset at the time it was taken. We designed, completely from scratch, an object storage architecture for this information model, and can store backup data very efficiently on simple high-density hard drive-based storage systems, which simplifies our supply chain and lowers both the risk and the price point for our customers.

The Customer can configure data retention rules for the Customer Content within the Services. Data retention refers to the amount of time Customer Content remains in the backup after being deleted from the Customer’s SaaS workload(s) backed up by the Services. Data retention can be set by the Customer to align with different deletion policies. Keepit offers up to 99-years retention, depending on the data retention included in the Agreement. Additionally, in relation to the deletion of Customer Content in connection with the termination or expiration of the Agreement, Keepit will delete Customer Content in accordance with the Data Processing Agreement.

To ensure data sovereignty, once a customer chooses a Keepit region for backup, their data never leaves that region. Not only does Keepit guarantee that backup data will always go to that region, but also that no processes exist that could transfer backup data out of that region (aside from customer initiated restores and downloads, of course). Should systems in a region ever need to be moved out of that jurisdiction, then Keepit will negotiate the moves with all affected customers prior to execution.

The full list of DC locations:

- *Copenhagen, Denmark*
- *Frankfurt, Germany*
- *London, United Kingdom*
- *Zürich, Switzerland*
- *Washington, D.C., United States*
- *Toronto, Canada*
- *Sydney, Australia*



Keepit operates two separate physical facilities in the data center region in which the customer decides to store data. All Customer Content is replicated between these two facilities and all operations run active-active from these facilities. This setup allows the customer to fully access data, as well as continue the use of Services even in the unlikely event of the total loss of one of the full physical sites.

Keepit uses co-location data center providers such as Equinix for housing Keepit's hardware. It's important to understand that Keepit's infrastructure residing in the data centers, including computer, storage and network, is fully owned and managed by Keepit. Nothing Keepit uses to deliver its services is shared or part of the co-location infrastructure.

Equinix and other co-location suppliers don't process data on behalf of Keepit and have therefore not been listed as a sub-processor of Keepit, and as such, Keepit does not rely on any sub-processors, so Customer Content is handled only by Keepit. All data center facilities employed by Keepit conform to a high physical security baseline and hold ISO 27001 certification plus complementary certifications (e.g., SOC-2, ISAE 3402, PCI/DSS, HIPAA).

Keepit has a physical and environmental security policy in place as per ISO 27001. It defines the physical access in working areas and data centers as physical entry control, electronic access cards, and a clearly defined visiting procedure. All data processing equipment containing Customer Content is in a data center (there is no customer backup data on personal devices or other devices that could reside in an office or elsewhere). The datacenters are considered physically secure areas to which only a small number of staff with certain duties have access.

In addition to the measures already presented (e.g., regional lock-in, dual data center redundancy), the Keepit platform also incorporates a number of additional security features to enhance protection of Customer Content:

Security measure	Explanation
Encryption in transit	Keepit employs encryption in transit using HTTPS secured with modern TLS v1.2. or higher when accessing your data through primary workload vendor APIs such as Microsoft 365, Salesforce, Google Workspace, and others.
Authentication to connector	To authorize access to different APIs Keepit uses Authorization Code Grant Flow (based on the OAuth 2.0 Authorization Framework). An authorization code represents the resource owner's consent to allow the application to access a resource. The application gets the authorization code from Microsoft Entra ID and then exchanges it for an access token to access the resource. The application never sees the user's credentials, and the user's agent or browser environment never sees the access token. Tokens are stored in our database, in ISO27001 accredited data centers.
Encryption at rest	For data at rest, the encryption process is done locally based on our internally developed operating system. Data at rest is encrypted with AES, with the key size up to 256 bit.
Encryption key maintenance	The key remains unchanged for the lifetime of the storage system as it’s used automatically only in isolated environments without any access to it. We store encryption keys directly on the servers and back them up on a central system. The encryption key is backed up on a separate system to reduce the impact of a corrupted key and to ensure continuous services.
Metadata security	On the Keepit NG backend, user metadata, such as name and e-mail address, are stored unencrypted in a database. User credentials are protected using a one-way hash algorithm (SHA-256 with a salt), thereby preventing theft of user credentials, should this database be compromised.
Secure Access Control	Keepit’s recommended best practice for deployment uses the customer’s existing authentication infrastructure (such as Entra ID, Okta) by means of SAML integration. This approach allows customers to leverage the identity security measures they already have in place (e.g., multi-factor authentication).

RBAC	Keepit provides a highly functional and robust role-based access control framework to allow administrators to designate granular pieces of Keepit functionality to certain Active Directory groups and users. Keepit is supplied with several template functional roles such as "Master Admin" and "Helpdesk" to help customers get started. However, these roles can be customized as well as new roles created. Keepit does provide a granular auditing function which can be interrogated via an audit viewer (supplied with the product). Out of the box, we offer eight roles, but the customer can create unlimited, customized roles to meet their needs. Specific to deletion, there are approval workflows in place to change retention. Any deletion that occurs is never immediate, as it is protected by delete retention. Users can perform the actions of their roles only on connectors they have access to. Access to data is restricted only to authorized users. Finally, an audit trail is maintained for the duration of the customer engagement. The audit log can be viewed directly in the web application by authorized administrators, and it can be accessed via the API for integration into third-party log analysis solutions.

Security in Keepit internally

Physical security

All data centers have 24/7 monitoring (CCTV, security guards), multi-factor authentication (access to the building and room), limited access to the server room with pre-agreements, remote systems monitoring, and the data centers provide us with mandatory documentation to prove backup and emergency plans and certifications.

Backup power systems, cooling systems, fire alarm systems, early fire detection systems are all fully covered by the co-location providers. Power, fire extinguishers and detectors and other subsystems are designed in Keepit’s offices.

Customer data is classified as secret in Keepit's internal policies and is securely sanitized using NATO approved wipe products or physically destroyed. Storage media containing Confidential or Secret information are securely erased before reuse — or if they cannot be sanitized, they are destroyed before disposal. Storage media used for Customer Content storage are collected for disposal in the datacenter in which they are used; when sufficient media is collected, media is physically destroyed by mechanical shredding. Customer backup data written is also encrypted at rest and therefore the physical destruction of media is a second significant layer of protection.

Human resources security

Keepit employees and consultants are contractually bound by non-disclosure obligations and go through data privacy training on a regular basis (at least once every year).

Furthermore, employees and consultants are contractually bound and legally required to adhere to the Keepit employee handbook and policies, including the Information Security Policy. On a regular basis, employees and consultants are trained in how to comply with the Information Security Policy. Current employees are required to pass it once per year as a mandatory action. Newly joined members are required to complete it on day one of their work at Keepit as part of their onboarding process.

In the awareness training, Keepers (what we call all Keepit employees) learn about information security, why it's important, how to protect themselves and the company from security incidents, who the Keepit InfoSec team is and what they're responsible for, when to report an incident, and what they should be aware of to stay cyber secure including: passwords security, phishing, and cybersecurity basic rules while working in the office, at home, and while travelling.

Access control

Keepit has documented all internal processes and internal statements, which are accounted for in Keepit's policies. The principle of least privilege is followed within Keepit: If an employee requires access to systems, a formal procedure is in place.

Access to administrative accounts for all critical elements have only certain employees based on their duties. In addition, environments are separated, controlled with specific accesses, and several types of VPN certificates are utilized as per the duties of the respective employee/contractor.

Testing or development activities are conducted only in a testing/development environment with test data. Each environment is an autonomous independent unit: There is no data exchange between them. Keepit’s infrastructure and security measures are continually evaluated by the operations team and our InfoSec department.

The Services are fully automated and provisioned based on the Customers instructions, i.e., the Agreement and the configuration of the Services. Therefore, no human operators outside of the Customer’s own organization are involved in accessing, reviewing, and/or otherwise processing actual Customer Content, unless otherwise specifically instructed by the Customer.

Security of operations and communications

To ensure reliable around-the-clock operation, we closely monitor our production systems' physical operational health and software stack health.

System and data center performance is continuously compared to baseline thresholds, while our health monitoring system monitors the physical equipment (e.g., environmental, network, hardware, operating systems, and services) with 30-second granularity, alerting on a range of unwanted situations (e.g., high temperatures in our data centers, failing disks in storage systems, congested network connections that threaten to impede ingress and egress, etc.).

Our real-time high-frequency event monitoring (RTHFEM) system provides platform-specific deep stack insights on software components and their operational health. Our operations team has different dashboards and areas of interest they follow and monitor, and live metrics can even be shared across organizational groups to provide developers with real-world insights into how their code performs in production.

The RTHFEM system provides insights into data ingress rates from different SaaS vendors and quickly identifies problems, should they arise within the software stack. Our backend engineers also use this system to troubleshoot specific customer-related situations based on anonymized views of the interoperability of each customer's connectors, data estate, and index.

Keepit uses an advanced logging system to track all activity. We have significant logging internally, as well as a security operations center which collects security events from across the systems. Keepit hosts its own SOC (Security Operation Center) and sets the monitoring in SIEM (Security Incident and event management system) based on actual events, needs, and best practices.

Additionally, detailed insights into software processes can assist with determining if an SLA is at risk or if an anomaly might be an indicator of malicious activity.

Risk management

Keepit information security management focuses on identifying appropriate and sufficient risk and risk management practices. It outlines Keepit's strategy for identifying, mitigating, and managing potential risks that could impact its operations or financial stability.

We have a mature and defined risk management process that assures risks are mitigated in a proportional and cost-effective manner. However, there is a low-risk appetite for specific risks, such as unauthorized access to sensitive data, noncompliance with industry and statutory regulations, and lack of resilience against cybersecurity threats.

Regular risk assessments are conducted at least once every 12 months, or when significant changes occur. Risks are identified and assessed for processing, storing, or transmitting restricted/confidential data, third-party suppliers handling sensitive data, new systems or environments, and significant changes to the environment. Identified risks are recorded and stored in the risk register. The senior management team is regularly updated on new risks that exceed the company's risk appetite, as well as the progress of remediate efforts.

Business continuity and disaster recovery plans

The Business Continuity Management Policy is aimed at preparing Keepit in the event of disaster caused by factors beyond our control (e.g., natural disasters, manmade events, cyber-attacks, etc.), and restoring operations to the widest extent possible in a minimum timeframe.

For specific DR (disaster recovery) scenarios, such as loss of site, backup and restore tests are regularly rehearsed to be effective when needed.

Incident management

Our formal Incident Management Policy defines criteria for incident urgency, impact classification, incident priority, and recommended timeframes for incident response and resolution. The process was established based on NIST (National Institute of Standards and Technology) recommendations. All incidents are assessed according to this policy and process.

Information security incidents are handled by the Incident Response Team (IRT). The IRT consists of the Legal team, Internal IT, SOC team, and the Information Security team according to their direct team responsibilities or all together as a part IRT. If necessary, other employees of Keepit and representatives from the management team may be involved in the process of incident investigation and response. The crisis committee was established and consists of the senior management level to oversee and manage large-scale crises that could affect the entire organization.

The operational status of the infrastructure and incident reports are available at https://status.keepit.com/.

Keepit maintains a data breach policy, which, among other things, accounts for the notifications provided to the Customer after a known or reasonably suspected data breach or other security incident. Such notifications will be provided without undue delay in accordance with GDPR art. 33(2) and the applicable Data Processing Agreement. There have yet to be any security incidents or data breaches related to the Keepit platform which required the notification of affected data subjects.

Conclusion

As the shared responsibility model gains wider recognition, it's become clear that resilience — the ability to recover from serious data loss — is a joint responsibility between SaaS customers and their SaaS providers. Keepit's purpose-built infrastructure, designed specifically for cloud SaaS data protection, positions us as a leader in mitigating the risks that come with migrating business-critical operations to the cloud. Our solution ensures that organizations can meet their obligations under this shared responsibility model by providing the necessary tools to secure, recover, and safeguard their SaaS data.

Keepit's infrastructure is entirely independent from public cloud environments, ensuring that SaaS data backups are stored separately from the production data. Backup copies remain secure, resilient, and immutable to potential data loss. This level of resilience is critical in the modern cloud landscape, where the ability to recover from disruptions is as important as protecting the data itself. By managing our own infrastructure across geographically diverse regions, we offer unparalleled data sovereignty, availability, and integrity, ensuring your data is always accessible, even in the event of a major cloud service outage.

At the core of Keepit's solution is our commitment to globally recognized security standards, including ISO 27001 and ISAE 3402 type II certifications, reflecting our adherence to best practices in data protection and operational security. Our pursuit of SOC 2 compliance and ongoing efforts to enhance our security posture is proactive to evolving threats and recovery scenarios.

Keepit's solution employs advanced data protection features, including AES 256-bit encryption for data at rest and in transit, immutable and air-gapped backups, and a proprietary blockchain-based system that guarantees the integrity of backup data. With dual active-active data centers, organizations can access their "always hot" backup data in real time, ensuring business continuity and minimizing downtime even during disruptions.

Resilience extends beyond technology — it involves people, processes, and proactive planning. Keepit emphasizes a comprehensive approach to security, integrating human resources security, access control, and physical security into our strategy. By adhering to the principle of least privilege and maintaining stringent access controls, we ensure that your data is handled only by authorized personnel, in line with GDPR and other regulatory requirements.

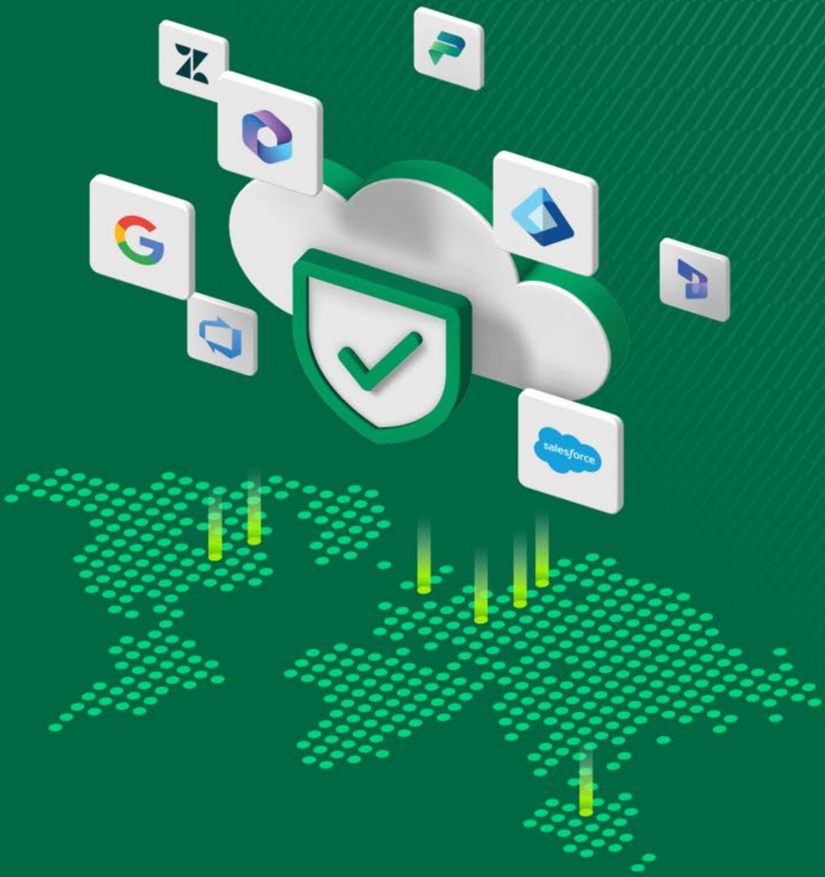
Keepit is built in the cloud, for the cloud, on a foundation of more than 20 years of security excellence. Our solution not only meets today's security and compliance challenges but also anticipates future risks, ensuring your organization can confidently address the joint responsibility of protecting and recovering SaaS data. Keepit empowers businesses to maintain data resilience, safeguard their operations, and innovate with confidence, knowing their most valuable digital assets are protected.

Data governance is a fundamental necessity for a good cyber resilience plan, which begins with ensuring critical data and systems are categorized and defined. Cybersecurity is a journey, not a destination.

Keepit future proof

Take the next step toward protecting your SaaS data

Request a demo



Keepit provides next-level SaaS data protection purpose-built for the cloud, by securing data in a vendor-independent cloud to safeguard essential business applications, boost cyber resilience and future-proof data protection.

Headquartered in Copenhagen with offices and data centers worldwide, over ten thousand companies trust Keepit for its ease of use and effortless backup and recovery of cloud data.

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
D-80333 München
Amtsgericht München
HRB 270094
Geschäftsführer Morten Felsvang
sales@keepit.com

www.keepit.com

Appendix: Keepit's compliance with legal and regulatory requirements

At Keepit we understand the importance of staying compliant with legal and regulatory requirements, especially as a provider of SaaS backup and recovery solutions. This is reflected in Keepit's Terms of Service, where it is established that Keepit will comply with all relevant laws and regulations applicable to the Services (cf. section 18.1). To ensure that Keepit remains up to date with any changes that could impact our service, Keepit employs a multifaceted approach:

- **Dedicated legal team:** Keepit has a dedicated legal team composed of experienced professionals who specialize in the regulatory landscape relevant to our industry. This team continuously monitors legislative developments and regulatory updates at both national and international levels, in compliance with Keepit's Legal and Regulatory Compliance Policy subject to ISO 27001. Keepit's legal team regularly attend industry conferences and participate in legal seminars to stay informed about upcoming changes and new requirements.
- **Collaboration with external legal advisors:** In addition to our in-house legal team, the legal team collaborates with external legal advisors and law firms with specialized knowledge in specific jurisdictions. This ensures that Keepit has access to the latest insights and expert opinions on complex regulatory matters.
- **Proactive policy updates:** Upon identifying relevant legal and regulatory changes, Keepit's legal team works closely with the Infosec team and product development to update internal policies and procedures.
- **Customer communication:** Keepit maintains transparent communication with its Customers regarding any regulatory updates/guidelines that may affect their use of Keepit's solution and how our Customers remain compliant with such regulations. This e.g. includes conversations around additional requirements that a Customer may be subject to under e.g., EBA/EIOPA/DORA guidelines, where Keepit's Outsourcing Addendum for Critical Outsourcing can be discussed and entered.

By combining the expertise of its dedicated legal team with external legal support, Keepit ensures that it remains at the forefront of regulatory compliance, allowing it to provide a reliable and compliant SaaS solution to its Customers.

Data protection compliance

Keepit will comply with data protection legislation applicable to the Services. Keepit adheres to the General Data Protection Regulation (GDPR), which represents the highest standard of data protection globally. This comprehensive and progressive legislation sets the benchmark for privacy rights and data handling practices.

In this section, Keepit aims to offer further insights into its GDPR compliance and address other relevant data protection laws that Customers frequently inquire about. This ensures that Customers have a clear understanding of how Keepit meets their data protection needs and upholds the highest standards of privacy and security.

Keepit's compliance with GDPR and UK GDPR

Keepit operates an independent private cloud with data centers in seven locations, including within the EU and the UK, making it subject to the General Data Protection Regulation (GDPR) and UK GDPR. Therefore, Keepit processes data in accordance with these regulations and has appointed a Data Protection Officer (DPO) to oversee the company's compliance efforts and ensure best practices in data management.

Under Keepit's Data Processing Agreement the parties agree that in relation to the GDPR, the Customer acts as the 'data controller' and Keepit as the 'data processor' except for situations where the Customer act as the 'data processor' and Keepit as the 'sub-processor'. Keepit's most recent Data Processing Agreement is available at https://www.keepit.com/data-processing-agreement/. Additionally, Keepit offers its customers the possibility of entering into Keepit's Data Processing Agreement based on the EU Commissions Data Processing Agreement[1]. This approach streamlines the contracting process, ensuring compliance with GDPR requirements while simplifying the negotiation and legal review, making easier for Customers to formalize their data protection arrangements effectively.

Processing of Customer Content

Customer Content may consist of any type of personal data about data subjects. It is entirely dependent of the Customer's type of data and its use of the Services. Customer Content stored by Keepit may contain for example, non-sensitive personal data (such as contact information, bank information, names, addresses, e-mail addresses, information relating to criminal convictions and offences, national identification numbers) or special categories of personal data (such as health data, data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data etc.) as defined in GDPR Article 9.

Given that Keepit does not access Customer Content unless required by the Customer and cannot assess the type of data contained therein, Keepit implements and maintains a level of security that takes into account that the processing may involve a large volume of personal data, including personal data subject to GDPR Article 9. This is why a 'high' level of security, and robust technical and organizational measures have been established.

The Services are fully automated and provisioned based on the Customers instructions, i.e., the Agreement and the configuration of the Services. Therefore, no human operators outside of the Customer's own organization are involved in accessing, reviewing and/or otherwise processing actual Customer Content, unless otherwise specifically instructed by the Customer.

Keepit implements and maintains appropriate organizational and technical measures to protect the Customer Content processed under the agreement pursuant to GDPR Articles 28(3)(c) and 32. These measures are based on industry best practices such as ISO 27001, ISO27002, NIST SP800-30, NIST SP800-39 and FEMA guidelines. Additionally, Keepit's current technical and organizational measures are described in a separate document, "Keepit Technical and Organizational Measures."

[1] Standard contractual clauses for controllers and processors in the EU/EEA | European Commission (europa.eu)

Location of processing

Keepit manages an independent private cloud on Keepit operated data centers. Upon onboarding the Keepit Services, the Customer decides where the Customer Content shall be stored and the data will exclusively be stored in the data center location chosen by the Customer, cf. section 9.2. and 9.3. of Keepit's Terms of Service. Keepit offers seven data center locations, including two locations within the EU: Copenhagen, Denmark, and Frankfurt, Germany, and a location in London, United Kingdom. Each region operates independently, and Customer Content cannot be transferred from one region to another.

Keepit's support organization may occasionally, as part of an ongoing support issue with the Customer, be requested by the Customer to access Customer Content, which may contain personal data. The request and the granting of access will be logged in the audit log provided within the Keepit Services. Technical and organizational measures are in place to restrict access to Customer Content, and in the unlikely event that Keepit' support require access to Customer Content all support activities will be performed by designated personnel located within the EU in accordance with Keepit's Data Processing Agreement.

Processing of Customer Content under the Data Processing Agreement cannot be performed at other locations than the location chosen by the Customer without the Customer's written authorization.

No transfers of personal data to third countries

Keepit does not currently transfer Customer Content to third countries, nor does It have any sub-processors in connection with the provision of the Keepit Services. In case of transfer of Customer Content to a third country will be initiated or Keepit engages sub-processors all affected customers will be advised accordingly and will be clearly informed about the intended changes, including the legal basis for transferring data, in accordance with the applicable Data Processing Agreement.

Compliance with California Consumer Privacy Act of 2018 (CCPA)

If Customer is subject to CPPA, Keepit complies with the CCPA by ensuring that Customer Content is handled with the highest regard for privacy and security. Keepit does not sell any Customer Content under any circumstances. Additionally, Keepit only retains or uses Customer Content for the specific purpose of providing the Services. This means that Keepit does not use Customer Content for any commercial purpose outside of delivering the agreed-upon Services to the Customer.

Keepit also ensures that personal information is used strictly within the scope of its direct business relationship with the Customer. In cases where Customer Content has been or will be de-identified, Keepit takes several important steps to protect privacy. These include implementing reasonable measures to ensure the content cannot be linked back to any individual or household, publicly committing to keeping the data deidentified, refraining from reidentifying the data, and requiring any third parties receiving the deidentified data to follow similar practices.

In doing so, Keepit remains committed to meeting its CCPA obligations and takes steps to ensure that Customer Content is handled responsibly and transparently.

Compliance with the HIPAA and HITECH Act

If the Customer is subject to the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH Act), Keepit is committed to adhering to the requirements set forth in these laws.

Keepit follows all necessary safeguards to protect Protected Health Information (PHI) within Customer Content by employing robust administrative, technical, and physical safeguards that are appropriate to the size and complexity of its operations. Keepit upholds the confidentiality and integrity of Customer Content as outlined in the Terms of Service. Keepit will only use or disclose PHI to fulfill our obligations under the Agreement and will not use or disclose PHI beyond what is permitted or required by law.

To further support compliance, Keepit offers its Customers the option to sign a Business Associate Agreement (BAA). This agreement outlines Keepit's responsibilities and commitments as a business associate, ensuring Keepit meets all HIPAA and HITECH Act requirements when handling PHI on behalf of our Customers.