E-BOOK

GDPR & UK GDPR Compliance with Wasabi

wasabi®
hot cloud storage

Table of contents

Executive Overview

Wasabi is a secure and highly performant cloud object storage service. More than 100,000 businesses and institutions use Wasabi Hot Cloud Storage for a variety of purposes, including primary storage for application data and content, secondary storage for backup or disaster recovery, and archival storage for long-term data and record retention. **The General Data Protection Regulation** (EU Regulation 2016/679) (GDPR) and the **United Kingdom Data Protection Act and the United Kingdom General Data Protection Regulation** (UK GDPR), which took effect in May 2018 and January 2021 respectively, impose strict requirements on how personal data is managed and protected. Organizations that are subject to GDPR and/or UK GDPR can use Wasabi to store and maintain personal data. Wasabi uses security best practices and technologies to ensure the physical security of its facilities and to maintain the privacy and integrity of personal data. In addition, Wasabi's **Terms of Use Agreement** ensures Wasabi customers ("data controllers" under GDPR and UK GDPR) maintain exclusive ownership of electronic records as required by GDPR. This white paper provides a brief overview of the use of the Wasabi service, considering the requirements of both GDPR and UK GDPR (references to the GDPR hereafter shall include reference to the UK GDPR).

Introduction – GDPR Overview

GDPR was enacted to strengthen and unify data protection for individuals within the European Union. The mandate is intended to provide citizens greater control over their personal data and to improve the flow of personal data within the EU and UK. GDPR regulates the export of personal data outside the EU (and specifically does not require that personal data remain within the EU or UK). GDPR supplanted the then-existing European Data Protection Directive (95/46/EC Directive) and applies to any organization that has a presence in the EU and UK or that offers goods or services in the EU or UK.

Important terminology includes:

- Data controller – an organization that collects or provides data regarding EU and UK residents (e.g. a Wasabi customer)
- Data processor – an organization that processes data on behalf of a data controller (e.g. a cloud provider such as Wasabi)
- Data subject – a person living in the European Union or the United Kingdom
- Personal data – any personally identifiable information relating to a data subject (e.g. name, identification number, location data, online identity)

Data Privacy and Security Implications

GDPR imposes strict data privacy and security rules for both data controllers and processors. The mandate requires appropriate safeguards to protect personal data and defines consent rules for use and disclosure of personal data. GDPR also grants individuals the right to examine, amend, correct, and delete personal records in certain situations.

Key data privacy and security provisions include:

- Articles 15, 16, and 17 – rights of access, rectification, and erasure – give data subjects tight control over their personal data
- Article 20 – rights to data portability – grants individuals the right to transfer personal data from one electronic processing system to another
- Article 25 – data protection by design and default – requires data controllers to implement appropriate technical and organizational measures to safeguard personal data
- Article 32 – security of processing – requires the "pseudonymization" and encryption of personal data
- Articles 33 and 34 – notice of a personal data breach – require data controllers to notify supervisory authorities and data subjects of personal data leakage.

Key UK GDPR Articles include:

- Article 5 - core article covering several aspects of data privacy, including the requirement for appropriate security of personal data
- Article 6 - Addresses the conditions under which processing personal data is lawful
- Articles 15 and 17 - Right to access and erasure
- Article 25 - Mandates that security measures are integrated into the design of systems and services from the outset
- Article 32 - Requires controllers and processors to implement technical and organizational measures to ensure security appropriate to the risk

Wasabi Hot Cloud Storage Overview

Wasabi Hot Cloud Storage is affordable, fast, and secure cloud object storage for any purpose Wasabi's technical and organizational measures, contractual terms and security features offers such as MUA and MFA, allow its customers to maintain compliance with GDPR. Unlike legacy cloud storage services with confusing storage tiers and complex pricing schemes, Wasabi Hot Cloud Storage is easy to understand and implement and cost-effective to scale. One product, with predictable and straightforward pricing, supports virtually every cloud storage application.

Businesses and institutions can use Wasabi for:

- Low-cost primary storage for on-premises or cloud-based applications
- Economical secondary storage for backup, disaster recovery in the cloud, or data migration initiatives
- Affordable and reliable archival storage for long-term data retention

GDPR Compliance With Wasabi

The Wasabi cloud storage service is designed to ensure the privacy and integrity of customers' stored content. The service is built and managed according to security best practices and standards, with GDPR standards in mind. Wasabi takes a "defense-in-depth" approach, employing multiple layers of security for ultimate protection in accordance with GDPR security guidelines. Wasabi prioritizes the physical security of its data centers; institutes strong authentication and authorization controls for all its cloud compute, storage, and networking infrastructure; and encrypts data at rest and in transit to safeguard personal data.

Physical Security

The Wasabi service is hosted in premier top-tier data center facilities that are highly secure and certified for SOC 2 and ISO 27001 compliance. Wasabi's services are also certified for ISO 27001 compliance, providing further assurance of the quality and security of Wasabi's data centers and offerings. Each site is staffed 24/7/365 with on-site security personnel to protect against unauthorized entry. Security cameras continuously monitor the entire facility—both indoors and outdoors. Biometric readers and two-factor or greater authentication mechanisms secure access to the building. Each facility is unmarked so as not to draw attention from the outside.

Secure Network Architecture

Wasabi employs advanced network security elements, including firewalls and other boundary protection devices, to monitor and control communications at internal and external network borders. These border security devices segregate customers and regulate the flow of communications between networks to prevent unauthorized access to Wasabi infrastructure and services.

Data Privacy and Security

Wasabi supports a comprehensive set of data privacy and security capabilities to prevent unauthorized disclosure of personal data. Strong user authentication features tightly control access to stored data. Access control lists (ACLs) and administratively defined policies selectively grant permissions to users or groups of users. Wasabi encrypts data at rest and data in transit to prevent record leakage. All data stored on Wasabi is encrypted by default to protect data at rest and all communications with Wasabi are transmitted using HTTPS to protect data in transit.

Access Logging

Wasabi supports detailed storage access logs for audit purposes. Log records contain information about each access request, such as the request type, accessed resources, and the date and time the request was processed. Administrative logging tracks notable activities and exports console events such as logins, MFA changes, password resets, and more. Bucket logging is another feature that provides a readable format to understand actions performed against a bucket, such as HTTP status codes, request Id, time and IP address for valuable updates on bucket access patterns

Data Durability and Protection

Wasabi Hot Cloud Storage is engineered for extreme data durability and integrity. Wasabi provides eleven 9s object durability, protecting data against hardware failures and media errors.

Data Portability and Deletion

Wasabi customers can easily export data to another storage platform or delete personal data to comply with GDPR and UK GDPR data portability and right-to-erasure requirements.

Data Ownership and Disclosure

The Wasabi Storage Platform **Terms of Use Agreement** and **Data processing Agreement** grants the data controller exclusive ownership and control of stored data. Under the terms of the agreement, the subscriber (the data controller) maintains ownership of all subscriber data. All data stored on Wasabi remains the exclusive property of the subscriber.

Customer Responsibilities

Even though Wasabi's environments and service offerings are designed to be highly secure, privacy and security are a team sport. Wasabi customers typically interface with the Wasabi service using **third-party file management applications and backup tools**. To ensure GDPR compliance, IT personnel must ensure the storage management tools and applications they use are configured to take advantage of Wasabi's security features. For example, HTTPS must be enabled to encrypt data in transit; MUA and MFA can be enabled to prevent unauthorized account access. In addition, customers should encrypt and "pseudonymize" all content and data prior to uploading it to Wasabi. IT organizations must also ensure they have strong security systems and practices in place to safeguard other elements of their on-premises and cloud-based infrastructure, including their Wasabi access credentials. The Wasabi storage service is typically employed as part of a larger public or hybrid cloud IT implementation that includes multiple compute, storage, and networking components.

Conclusion

GDPR and UK GDPR introduced robust data privacy and security requirements for organizations doing business in the European Union. IT planners, InfoSec teams, and compliance officers must ensure their systems and practices conform to applicable regulations. Wasabi's cloud storage service is designed to ensure the privacy and integrity of personal data in accordance with GDPR and UK GDPR guidelines. Wasabi stringently vets the physical security of its data centers, employs strong authentication and authorization controls to safeguard infrastructure and services, and encrypts data at rest and in transit to prevent unauthorized record disclosure. Wasabi is typically used in conjunction with other compute, storage, and networking platforms and services. IT organizations must implement strong security systems and practices across all on-premises and cloud-based infrastructure to fully protect personal data.

Additional Information

For additional information about GDPR and UK GDPR, and Wasabi, consult the following resources:

- **European Commission Data Protection web page**
- **EU GDPR complete text**
- **United Kingdom Data Protection web page**
- **UK GDPR complete text**

For additional information about Wasabi's Data Processing Agreement, please visit the webpage **here**.

For more information around Wasabi's security, privacy, and compliance practices, please visit Wasabi's Trust Center **here**.

About Wasabi

Wasabi provides simple, predictable and affordable hot cloud storage for businesses all over the world. It enables organizations to store and instantly access an unlimited amount of data at 1/5th the price of the competition with no complex tiers or unpredictable egress fees. Trusted by tens of thousands of customers worldwide, Wasabi has been recognized as one of technology's fastest-growing and most visionary companies. Created by Carbonite co-founders and cloud storage pioneers David Friend and Jeff Flowers, Wasabi is a privately held company based in Boston.

Follow and connect with Wasabi
on Linkedin, X, Facebook, Instagram, and The Bucket.

wasabi®
hot cloud storage