CISO Assurance Series

Preservica Data Residency & Access Governance Overview

About the CISO Assurance Series

The Preservica CISO Assurance Series provides concise, factual briefings intended to support customer Legal, Privacy, Information Security, and Risk stakeholders when evaluating specific aspects of the Preservica platform. Each document in the series focuses on a defined topic and is designed to complement, not replace, formal contractual documentation and due diligence materials.

These briefings are provided for informational and assurance purposes only. They describe Preservica's approach, controls, and practices as of the date of publication and do not constitute legal advice, contractual commitments, or warranties. Customers should rely on their applicable agreements with Preservica, including any data processing agreements and service terms, for binding obligations.

This document forms part of the Preservica CISO Assurance Series and may be read independently or alongside other series publications, depending on customer needs.

Preservica

Preservica

1. About this document

Preservica provides a cloud-based digital preservation platform used by customers operating in regulated, public sector, and risk-sensitive environments.

This document is designed as a **customer-facing assurance overview** that can be shared internally with Legal, Privacy, Information Security, Compliance, and Risk stakeholders when evaluating or approving the use of Preservica's SaaS platform.

It explains:

- Where customer data is stored and processed
- How access to customer data is governed
- How Preservica uses sub-processors
- How market terms such as data jurisdiction and data sovereignty map to Preservica's contractual commitments

This document is **informational in nature**. It supports customer understanding and internal assurance discussions and should be read alongside the applicable contract, Order Form, and Data Processing Agreement.

2. Preservica data handling at a glance

Across all Preservica cloud deployments, the following core principles apply:

- **Region-specific deployments** – Customer data is stored and processed only within the geographic region specified on the Order Form.
- **Contract-backed data residency** – Data location commitments are contractual and enforceable.
- **No routine human access** – Preservica does not generally have routine or day-to-day access to customer content.
- **Controlled and auditable access** – Any access, where required, is exceptional, least-privilege, logged, and subject to oversight.
- **Region-aligned sub-processors** – Approved sub-processors are used in a region-dependent manner consistent with the customer's data residency requirements.
- **Controlled and auditable access** – Any access, where required, is exceptional, least-privilege, logged, and subject to oversight.

3. Why terms like “data sovereignty” are often misunderstood and key definitions

In customer due-diligence processes, questions about “data sovereignty” typically reflect a combination of three underlying concerns:

1. Where data is stored and processed
2. Who can access data and under what conditions
3. How legal or regulatory requests for access are handled

These concerns are often described using overlapping terminology in the market. Large cloud providers (including hyperscalers) have published guidance distinguishing between **data residency** and broader notions of **data sovereignty**, particularly for regulated and public sector use cases.

Preservica addresses these concerns by focusing on **specific, auditable controls** and **explicit contractual commitments**, rather than relying on broad or ambiguous claims.

3.1 Data Residency

Data Residency describes **where customer data is stored and processed** for the service. For Preservica customers, this is the **geographic region specified in the Order Form**.

This is the primary and enforceable commitment Preservica makes regarding data location.

3.2 Data Jurisdiction

Data Jurisdiction is commonly used to describe the relationship between data location and applicable local laws.

In practice, discussions about jurisdiction are resolved by reference to:

- The contracted data residency location
- The governing law and legal provisions in the customer contract

To avoid ambiguity, Preservica aligns discussions of “jurisdiction” back to these contractual terms.

3.3 Data Sovereignty

Data Sovereignty is often used as a non-technical umbrella term to describe controls beyond data location, such as:

- How access to data is governed
- Whether access is routine or exceptional
- How legal requests for access are handled

Unless explicitly agreed otherwise, Preservica does not use “data sovereignty” to imply absolute restrictions on legal authority. Instead, it focuses on **practical, documented, and auditable controls** around residency, access, and transparency.

3.4 Access vs Processing

These terms are frequently conflated in questionnaires:

- **Processing** refers to automated system operations required to deliver the service (for example storage, backup, indexing, and rendering)
- **Access** refers to **human access** to customer content

Preservica distinguishes clearly between the two.

4. Where customer data is stored and processed

Customer data is **stored and processed only within the geographic region specified on the Order Form**, in accordance with the contract.

Preservica does not move, replicate, or process customer data outside that region except:

- Where explicitly instructed by the customer, or
- Where required by applicable law

5. Use of sub-processors

Preservica uses approved sub-processors to deliver its SaaS platform, including cloud infrastructure and security services.

Sub-processors are selected and used in a **region-dependent manner** so that customer data remains stored and processed in line with the customer's contracted data residency.

Preservica maintains contractual and governance controls over sub-processors consistent with its data protection and security obligations.

6. Human access to customer data

Preservica employees do **not** have routine or standing access to customer content.

Access may occur only in limited, controlled circumstances, such as:

- Where a customer explicitly authorises access (for example, to support a support request)
- To respond to an active or imminent security incident
- Where Preservica is legally required to do so by a competent authority

Where access is required:

- It is granted on a **least-privilege, need-to-know basis**
- All access is **logged and auditable**
- Access is subject to internal security controls and management oversight

Authorised access, where required, may be performed by Preservica personnel based in the **United Kingdom and the United States**.

7. Legal access requests and the U.S. CLOUD Act

Customers operating in regulated environments often ask whether laws such as the U.S. **CLOUD Act** could require access to data stored outside the United States.

As a general matter, cloud service providers may receive legally binding requests for data from competent authorities. The existence of such laws does not mean that data is accessed routinely or without due process.

Preservica's approach is aligned with widely accepted industry practice:

- Preservica does **not** provide governments with direct or unfettered access to customer data.
- Any request for access must be **legally valid and binding**.
- Requests are **assessed and handled on a case-by-case basis**.
- Where legally permitted, Preservica seeks to **notify the affected customer**.
- Disclosures, if required, are **limited to the specific data identified in the valid legal order**.

The CLOUD Act does not change Preservica's contractual commitments around **data residency**, nor does it result in routine access to customer content. Data remains stored and processed in the contracted region, and access controls continue to apply.

8. Assurance and oversight

Preservica's approach to data residency and access governance is supported by its broader information security and compliance programme.

Independent assurance materials, certifications, and audit reports are made available to customers through Preservica's Trust Center as part of standard due-diligence processes.

9. Frequently asked questions (FAQ)

The following FAQs are based on common questions raised by customer Legal, Privacy, Information Security, and Compliance teams during due-diligence and procurement reviews.

9.1 Where is our data stored and processed?

Customer data is stored and processed in the geographic region specified in the **Data Residency section of your Order Form**.

9.2 Do your sub-processors process data outside that region?

No. Sub-processors are used in a region-dependent manner to support in-region storage and processing consistent with the contracted data residency.

9.3 Do Preservica staff have access to our data?

Not routinely. Access is exceptional and occurs only under controlled circumstances, such as customer-approved support, incident response, or legal obligation.

9.4 From which countries might access occur from Preservica?

Where access to customer data is required, it may be performed by authorised Preservica personnel based in the **United Kingdom and the United States**. Such access is not routine and is governed by strict access controls, logging, and oversight.

9.5 Where can we find independent assurance?

Preservica makes security certifications and assurance materials available through its Trust Center: https://preservica.com/trust-center

9.6 Do customers retain ownership and control of their data?

Yes. Customers retain ownership and control of their data at all times. Preservica processes customer data only to provide the contracted services and in accordance with customer instructions and applicable law.

Preservica's platform includes functionality that allows customers to **export some or all of their data at any time**, and for **up to 30 days following contract termination**, in a **common, machine-readable format**. Preservica supports the Open Preservation Exchange (OPEX) standard for structured export of preservation content and metadata. More information on the export format is available here: https://developers.preservica.com/documentation/open-preservation-exchange-opex

9.7 What types of customer data does Preservica process?

Preservica does not prescribe or restrict the types of data that customers choose to store in the platform. Customers are responsible for determining the classification, sensitivity, and appropriateness of data stored in Preservica, and for ensuring it is used in line with their own legal and regulatory obligations.

9.8 How is customer data protected (encryption and keys)?

Customer data is encrypted in transit and at rest using industry-standard encryption, in line with Preservica's security and compliance programme. Encryption, key management, and access controls are operated as part of Preservica's standard platform controls and are subject to independent assurance through Preservica's certifications and audits.

Further detail on Preservica's security controls, certifications, and compliance framework is available via the Trust Center: https://preservica.com/trust-center

9.9 How are backup, disaster recovery, and resilience handled?

Preservica operates defined **Recovery Time Objective (RTO)** and **Recovery Point Objective (RPO)** commitments appropriate to a SaaS digital preservation platform. Preservica's standard obligations are:

- **RTO**: 4 hours
- **RPO**: 24 hours

These obligations are set out in Preservica's **standard contractual terms**.

Preservica **tests its RTO and RPO controls on a semi-annual basis**, and the effectiveness of these controls is **independently audited as part of Preservica's SOC 2 Type II report**.

Preservica uses a combination of technical and operational measures to meet its RTO and RPO obligations. Detailed backup implementation methods are not publicly disclosed; however, all resilience and recovery measures are designed to ensure that **customer data remains within the contracted data residency region** and does not result in cross-region data movement outside agreed jurisdictional boundaries.

9.10 What is the shared responsibility model?

Preservica operates under a shared responsibility model common to SaaS platforms. Preservica is responsible for the security of the platform and underlying infrastructure, while customers are responsible for user access management, data classification, and appropriate use of the service. Additional detail is available through Preservica's Trust Center (https://preservica.com/trust-center) and supporting documentation.

9.11 Will Preservica sign a customer Data Processing Agreement (DPA)?

Yes. Preservica is willing to engage with customer-provided Data Processing Agreements (DPAs), subject to legal review and negotiation.

Customers should note that Preservica does not determine or control the specific categories of personal data that customers choose to store or process within the platform. As such, Preservica is often **unable to unilaterally complete DPA sections** that require details such as the exact categories of data, data subjects, or processing activities.

In practice, completing a DPA is typically a **collaborative exercise** between Preservica and the customer, ensuring that the agreement accurately reflects how the customer intends to use the platform and the types of data they choose to process.

10. Next steps

Customers with additional legal, privacy, or security questions are encouraged to raise them through their usual Preservica contact or formal due-diligence process.

Preservica is committed to supporting customers with clear, accurate information to enable confident adoption of its cloud platform.

About Preservica

Preservica is transforming the way organizations around the world protect and future-proof critical long-term digital information. Available in the cloud (SaaS) or on-premise, our award-winning Active Digital Preservation™ archiving software has been designed from the ground up to tackle the unique challenges of ensuring digital information remains accessible and trustworthy over decades.

It's a proven solution that's trusted by thousands of businesses, archives, libraries, museums and government organizations around the world, including the UK National Archives, Texas State Library and Archives, MoMA, Yale and HSBC.

preservica.com/about