keepit®

The path to cloud sovereignty

A guide to understanding the EU Cloud Sovereignty Framework — and how Keepit helps



Table of contents

INTRODUCTION

The European Commission's Cloud Sovereignty Framework ... 3

From principles to practical evaluation 4

Keepit's interpretation of EU cloud sovereignty 4

The sovereignty objectives 5

SOVEREIGNTY OBJECTIVES

Objective 1: Strategic Sovereignty 6

Objective 2: Legal & Jurisdictional Sovereignty 7

Objective 3: Data & AI Sovereignty 9

Objective 4: Operational Sovereignty 10

Objective 5: Supply Chain Sovereignty 11

Objective 6: Technology Sovereignty 12

Objective 7: Security & Compliance Sovereignty 13

Objective 8: Environmental Sustainability 14

CONCLUSION

From framework to decision 15

Learn more 15

© 2026 Keepit. All rights reserved

The European Commission's Cloud Sovereignty Framework

If you are responsible for IT, security, or digital infrastructure in Europe, the concept of data sovereignty is not new. Regulations like NIS2, DORA, and GDPR already make it clear that **you are accountable for:**

Where your data resides

Who can access it

Third-party dependencies

What is often less clear is something more practical: How do you consistently evaluate whether a cloud provider meets those expectations? This is exactly the problem the EU Cloud Sovereignty Framework is designed to address.

The framework is not a regulation, and it does not introduce new legal obligations. Instead, it provides a structured model for assessing cloud providers across the areas that matter most for sovereignty and control — from legal exposure and data handling to operational independence and supply chain risk. In simple terms:

It turns the abstract idea of "sovereignty" into something you can evaluate, compare, and document.

The framework outlines eight objectives, from strategic to environmental. This guide will walk you through all eight objectives, their contributing factors, and how Keepit approaches each area of sovereignty.



Read more in our research report:
Data sovereignty: Take control of your data →

© 2026 Keepit. All rights reserved

From principles to practical evaluation

Most regulatory frameworks define what risks you need to manage, but not how to assess them consistently. The Cloud Sovereignty Framework bridges that gap by helping you to answer, in practice, a simple question: *"Can we rely on this provider from a sovereignty and control perspective?"* The framework helps you answer that question in a structured, defensible way by guiding you through three key steps, which together turn what could be a subjective assessment into a consistent, repeatable evaluation process:

1. Breaking down sovereignty into concrete areas of evaluation

Instead of treating sovereignty as a single concept, you assess it across distinct dimensions such as legal exposure, operational control, and data handling, called "sovereignty objectives" in the framework.

2. Examining the contributing factors within each area

Each dimension is supported by specific factors that help you evaluate real-world risks — for example, exposure to foreign jurisdictions, level of operational independence, or dependency on external supply chains. These are called "contributing factors" in the EU framework.

3. Assessing both minimum acceptability and overall strength

You determine whether a provider meets the minimum required level in each area ("sovereignty effectiveness") and then evaluate how strong they are overall to support comparison between vendors ("sovereignty score").

Keepit's interpretation of EU cloud sovereignty

In line with the European Commission's Cloud Sovereignty Framework, Keepit understands cloud sovereignty not as technical isolation, but as the practical ability for EU customers to retain control over their data, operations, and legal position when using cloud services. This includes:

- Control over jurisdiction, governance, and access to data
- Protection against unintended extraterritorial access
- Operational resilience and independence
- Transparency of technology and supply chain dependencies

In this guide, we will present the eight sovereignty objectives (SOV-1 to SOV-8) and summarize how Keepit addresses each of these objectives. By doing so, we want to describe how we ensure that customer data remains under effective European control, protected from undue external influence, and managed in accordance with EU law and values.



Kim Larsen
Group Chief Information Security Officer, Keepit

© 2026 Keepit. All rights reserved

The sovereignty objectives of the EU Cloud Sovereignty Framework

The framework assesses providers against eight objectives, which clearly define what sovereignty means. Each objective asks a different question about who is in control.

SOV-1
Strategic Sovereignty

Who owns and governs the provider, and could that change under pressure? Strategic Sovereignty assesses ownership stability, governance influence, and EU priority alignment.

SOV-2
Legal & Jurisdictional Sovereignty

Which laws apply to the provider, and how exposed is it to foreign authority? This objective evaluates the legal environment, exposure to foreign authority, and enforceability of rights.

SOV-3
Data & AI Sovereignty

How is data secured, where is it processed, and who controls it? This objective focuses on the protection, control, and independence of data assets and AI services.

SOV-4
Operational Sovereignty

Can EU actors run, support, and evolve the service independently? This objective measures the practical ability for EU actors to run the technology independently of foreign control.

SOV-5
Supply Chain Sovereignty

Where do critical components come from, and who can interrupt them? This objective evaluates the geographic origin, transparency, and resilience of the supply chain.

SOV-6
Technology Sovereignty

Is the technology stack open enough to audit, interoperate with, and leave? This objective evaluates the degree of openness, transparency, and independence of the tech stack.

SOV-7
Security & Compliance Sovereignty

Are security operations and compliance controlled within the EU? This objective assesses the extent to which security, compliance, and resilience measures are controlled within the EU.

SOV-8
Environmental Sustainability

How resilient is the provider in terms of energy use and raw materials? This objective evaluates autonomy and resilience in relation to energy usage and raw material dependency.

Source: European Commission, Cloud Sovereignty Framework

© 2026 Keepit. All rights reserved



OBJECTIVE 1:
Strategic Sovereignty

Ownership, control, and alignment with the EU ecosystem

Strategic Sovereignty asks a more fundamental question than where your data is stored: Who actually controls the company running your cloud service, and could that change under pressure? It looks at where decision-making authority sits, how exposed the provider is to a change of ownership or control, how much of its funding and economic footprint is EU-based, and whether it could keep operating under external pressure.

CONTRIBUTING FACTORS	HOW KEEPIT HELPS
Location of decision-making authority (EU jurisdiction)	Keepit is an EU-based company headquartered in Denmark, with strategic decision-making, security governance, and product development anchored in the European Union.
Safeguards against change of ownership or control	Keepit operates independently with full control over its infrastructure and technology stack, reducing reliance on external providers (e.g., hyperscalers) based abroad. Keepit uses colocation providers for housing hardware, while the infrastructure — computers, storage, network — is fully owned and managed by Keepit and not shared with the colocation infrastructure. Read more about this in our cybersecurity factsheet.
Reliance on EU-based funding and financial structures	Keepit is backed by European investors, such as the Export and Investment Fund of Denmark (EIFO), as well as One Peak, reflecting alignment with EU financial priorities.
Contribution to EU economy (investment, jobs, value creation)	Keepit has major operational hubs in Denmark and Poland, with additional offices across key European markets, including Germany, France, and the Netherlands.
Alignment with EU strategic initiatives and policy objectives	Keepit enables customers to store and manage data within the EU, supporting data sovereignty and control, and aligns with EU priorities for secure and energy-efficient digital infrastructure. Keepit aligns with EU regulations such as GDPR, NIS2, and DORA, and helps its customers comply with these initiatives.
Ability to maintain service continuity under external pressure (e.g., legal or vendor disruption)	Keepit's independent infrastructure reduces exposure to third-party disruption, supporting continued service availability. Keepit's operations, management, and long-term service continuity are governed under EU law and not subject to direction from non-EU authorities.

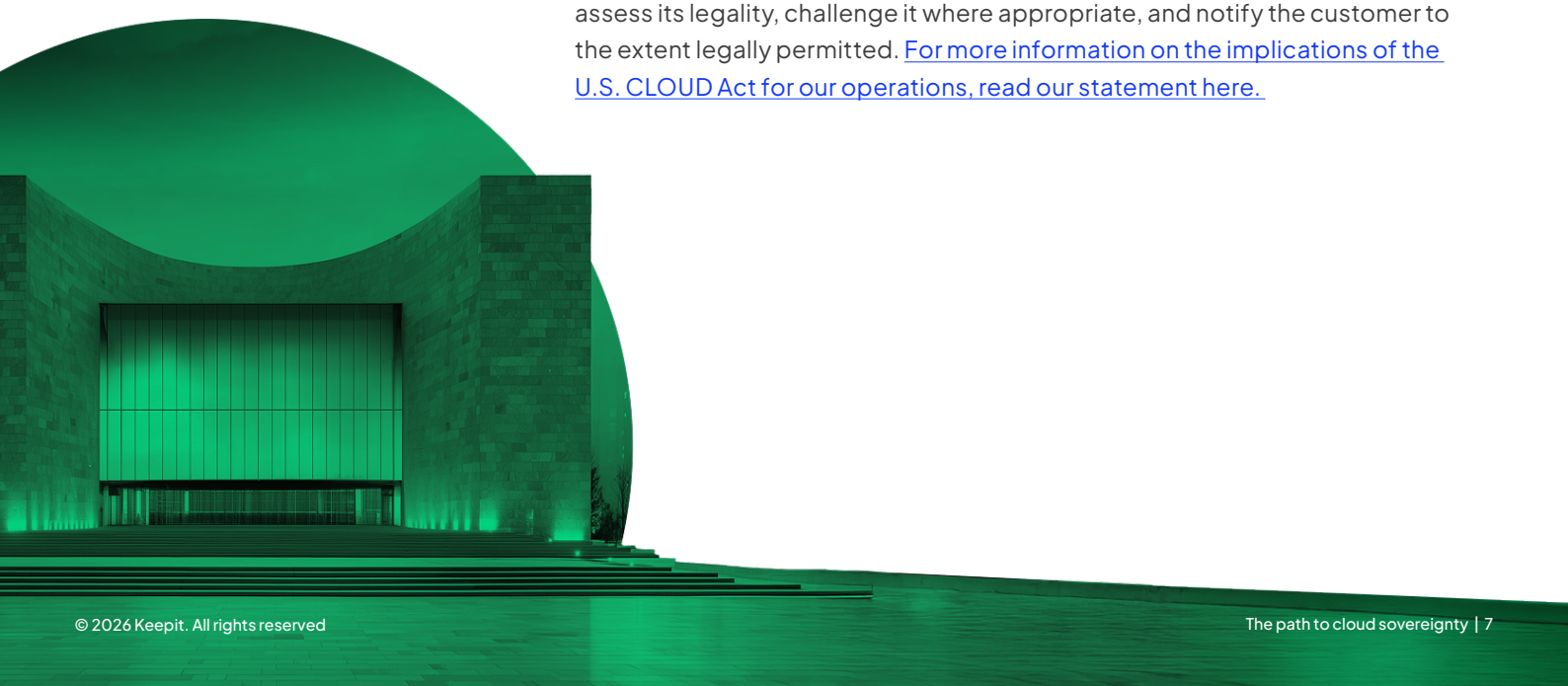
© 2026 Keepit. All rights reserved

OBJECTIVE 2:
Legal & Jurisdictional Sovereignty

Exposure to legal systems and data access risks

Every cloud contract sits inside a legal system, and that system determines who can be compelled to hand over your data and under what circumstances. This objective evaluates which country's law actually governs your provider's operations and contracts, how exposed that provider is to foreign laws with extraterritorial reach (such as the U.S. CLOUD Act), and whether legal, contractual, or technical channels exist that could let a non-EU authority access your data or systems.

CONTRIBUTING FACTORS	HOW KEEPIT HELPS
Governing law of the provider's operations and contracts	Keepit A/S is a Danish company, and its operations are subject to Danish law and applicable EU law. This includes directly applicable EU regulations such as GDPR. Agreements for European customers are governed by the law of an EU/EEA member state — by default Danish law, or another member state's law when agreed with the customer — and are subject to the jurisdiction of that member state. Mandatory provisions of EU and national law apply irrespective of the chosen governing law.
Exposure to non-EU laws with extraterritorial reach (e.g., U.S. CLOUD Act)	Keepit A/S is established in Denmark and subject exclusively to Danish and EU law. Customer data of European customers is stored exclusively in data centers within the EEA. Keepit has a subsidiary in the United States. This subsidiary is a separate legal entity and does not have possession, custody, or control of customer data held by Keepit A/S, and no technical or operational access to that data. Consequently, Keepit's assessment is that the U.S. CLOUD Act does not provide a basis for U.S. authorities to compel disclosure of customer data from the subsidiary. In the event of any foreign authority request, Keepit will assess its legality, challenge it where appropriate, and notify the customer to the extent legally permitted. For more information on the implications of the U.S. CLOUD Act for our operations, read our statement here.



© 2026 Keepit. All rights reserved

OBJECTIVE 2:
Legal & Jurisdictional Sovereignty

CONTRIBUTING FACTORS	HOW KEEPIT HELPS
Potential for non-EU authorities to access data or systems (legal, contractual, or technical channels)	Since Keepit A/S is established in Denmark and subject only to Danish and EU law, Keepit has no legal obligation under non-EU law to disclose customer data. The U.S. subsidiary does not have possession, custody, or control of that data. Any request from a non-EU authority would need to proceed through recognized legal channels, such as mutual legal assistance or applicable international agreements. Keepit will assess any such request for legality, challenge it where appropriate, and notify the customer to the extent legally permitted. Additionally, Keepit does not use external, third-party sub-processors to handle customer data, which minimizes exposure to non-EU legal frameworks through external providers. A list of all sub-processors, including those supporting non-content functions, is available. From a technical perspective, EU customer data resides only in the customer-selected region on Keepit-owned infrastructure. Data is encrypted both in transit and at rest, using keys managed by Keepit within the EEA. Access to production systems and customer data is restricted to authorized personnel located in the EEA, with access logged and reviewed.
Applicability of international legal regimes affecting data use or transfer	Keepit enables data to be stored and managed within the EU, reducing reliance on international data transfer frameworks and associated legal complexities.
Location and jurisdiction of intellectual property creation and ownership	Keepit's platform is developed and operated by teams based within the EU, supporting alignment with EU legal jurisdiction over its technology.

In short:
Keepit A/S is a Danish company, headquartered in Denmark, and governed by EU law. Customer data resides only on Keepit-owned infrastructure in the customer-selected region and will never leave that region.

Ask your provider:

- [ ] Which country's law governs my contract?
- [ ] Which of your entities could a non-EU authority compel?
- [ ] Who else touches my data?

© 2026 Keepit. All rights reserved



OBJECTIVE 3:
Data & AI Sovereignty

Control over data, how it is used, and how it contributes to AI systems

Data sovereignty isn't just about geography — it's about who can act on your data and how verifiable that control is. This objective looks at whether the customer, not the provider, holds effective cryptographic control over their own data, and whether data access and AI model usage are auditable and deletion is verifiable. It also details whether storage and processing are strictly confined to EU jurisdictions with no silent fallback elsewhere, and how independent any AI capabilities are from non-EU technology stacks.

CONTRIBUTING FACTORS	HOW KEEPIT HELPS
Customer control over cryptographic access to their data	Keepit applies strong encryption to customer data in transit and at rest, with strict access controls governing how data can be accessed within the platform. Customers retain control over who can access their data and how it is used within the platform.
Visibility and auditability of data access and AI usage, including verifiable data deletion	Keepit ensures controlled and logged administrative access and visibility into data access through audit logs and controlled interfaces. Upon contract termination, Keepit ensures data is deleted in line with its data retention policies and GDPR obligations.
Confinement of data storage and processing to European jurisdictions	Keepit operates data centers in EU regions — including Germany and Denmark — enabling customers to store and manage data within the EU. Data never leaves the selected region, and Keepit does not process customer data using external third-party sub-processors.
EU control over AI models, data pipelines, and underlying technology	By not relying on external third-party sub-processors for processing customer data, Keepit retains full control over data pipelines and avoids dependency on external technology ecosystems.

In short:
At Keepit, we are committed to providing our customers with an independent, vendor-neutral cloud that keeps a trusted copy of their data separate from production environments. As AI agents take on business-critical decisions, they need data they can trust. Keepit's AI Truth Cloud gives organizations a complete, immutable copy of their data that no third party can influence. It's designed to help you verify data before AI uses it and to recover to a known-good state when something goes wrong.

Read more in our white paper:
The principles of true SaaS data protection →

© 2026 Keepit. All rights reserved



OBJECTIVE 4:
Operational Sovereignty

Ability to operate, support, and sustain the service independently within the EU

A provider can check every legal and data-residency box and still leave you exposed. Operational Sovereignty assesses how easily you could migrate away without lock-in, whether EU-based staff can manage and support the technology without needing non-EU vendor involvement, whether there's a real EU talent pool behind it, and whether full technical documentation and operational know-how exist to sustain the service long-term.

CONTRIBUTING FACTORS	HOW KEEPIT HELPS
Ease of migrating workloads or integrating with alternative EU-controlled solutions (avoiding vendor lock-in)	The primary form of vendor lock-in for SaaS data is dependence on the SaaS provider. Keepit addresses this by storing data in its own vendor-independent cloud, fully isolated from hyperscalers, so customers retain access to their data even if the SaaS provider is unavailable. Keepit provides integrations and APIs that enable interoperability with broader IT environments, supporting flexibility and reducing dependency.
Capacity for EU-based operators to manage, maintain, and support the service without non-EU vendor involvement	Keepit's core product development and engineering are anchored in the EU, with primary teams based in Denmark and Poland. Keepit owns and operates its platform without reliance on non-EU technology providers.
Availability of EU-based expertise and talent to operate and sustain the service	Keepit has established operational and engineering teams across Europe, supporting access to EU-based expertise required to operate and sustain the platform. Operational sovereignty is also supported by documented service continuity and disaster recovery processes.
Delivery of operational support from within the EU under EU legal jurisdiction	Keepit's primary operational support is based in the EU, with teams in Denmark and Poland operating under EU legal frameworks. Global support teams outside of the EU are available for customers upon request.
Availability of technical documentation and operational know-how enabling long-term autonomy	Keepit develops and operates its platform in-house, maintaining full ownership of operational knowledge and documentation required to manage and sustain the service.
Location and legal control of critical suppliers or subcontractors involved in service delivery	Keepit does not rely on external third-party sub-processors, reducing dependency on external suppliers and maintaining control over service delivery.

© 2026 Keepit. All rights reserved

OBJECTIVE 5:
Supply Chain Sovereignty

Control of and dependency on the supply chain needed to deliver the service

Sovereignty claims tend to focus on the provider's headquarters, but risk often lives further down the chain — in hardware manufacturing, firmware, and software components sourced from elsewhere. This objective traces the geographic origin of physical components and manufacturing, how reliant the provider is on non-EU vendors or proprietary technologies, and how much visibility and how many audit rights exist across the supply chain.

CONTRIBUTING FACTORS	HOW KEEPIT HELPS
Dependence on external suppliers for critical components (hardware, software, infrastructure)	Keepit maintains transparency over its critical suppliers. Keepit owns its own hardware and software stack and operates its platform within data center facilities provided by Equinix and Cibicom. Keepit maintains full control over its data, software, and operational processes within those facilities, minimizing reliance on external providers.
Geographic origin of key suppliers (EU vs non-EU)	Keepit's core engineering and operations are EU-based. Keepit uses two colocation data center providers: Cibicom, a Danish (EU) provider, and Equinix. In both cases, the partner provides facilities (physical space and power) only, while Keepit retains full control of its own hardware, software stack, and customer data within those facilities. EU-based customers can select an EU data center region (Copenhagen or Frankfurt), and Keepit guarantees that data never leaves the selected region. Equinix is U.S.-headquartered, but the facilities Keepit uses for these customers are physically located within the EU, so customer data does not reside in the US.
Transparency and control over the supply chain	By owning and operating its hardware and software platform, Keepit maintains direct visibility and control over its technology stack and data pipelines.
Risk of disruption from third-party vendors	Keepit manages third-party risk through contractual controls, hardware ownership, and a mirrored dual-data-center architecture that ensures continuity if a single facility is affected. Keepit also engages in an ongoing review of supplier jurisdictional and operational risks.
Ability to substitute or mitigate supplier dependencies	Keepit's independent architecture reduces critical dependencies, improving its ability to manage or mitigate supplier-related risks.

© 2026 Keepit. All rights reserved

OBJECTIVE 6:
Technology Sovereignty

Control of core technologies, architecture, and reliance on external tech ecosystems

This objective is about whether you're locked into one vendor's technology stack or free to move. It evaluates whether the platform integrates through open, well-documented APIs and widely adopted standards rather than proprietary protocols; whether the underlying software is open enough to audit, modify, or redistribute; how much visibility you have into the system's architecture, data flows, and dependencies; and how independent the provider is from non-EU high-performance computing infrastructure.

CONTRIBUTING FACTORS	HOW KEEPIT HELPS
Ability to integrate with other technologies through open and well-documented APIs and standards	Keepit is committed to avoiding vendor lock-in and technology dependencies. Keepit provides integrations and APIs that connect the platform with customers' broader IT environment, including SaaS applications. This supports interoperability and reduces dependency on a single vendor ecosystem.
Use of open or auditable software, enabling transparency and adaptability	Keepit's platform is proprietary, fully developed and operated in-house, giving Keepit full control over its technology and enabling transparency into how the service is built and managed. Architectural documentation and APIs are published.
Visibility into system design, architecture, and data flows	Keepit provides transparency into where data is stored and processed through its regionally isolated data centers and no-transfer guarantee, giving customers clear visibility into data residency and data flow.
Degree of independence from non-EU high-performance computing and advanced infrastructure	Keepit owns its own hardware and software stack and does not rely on hyperscalers such as AWS or Azure, reducing dependency on major non-EU cloud ecosystems.

In short:
Sovereignty is a cornerstone of Keepit's architecture. Unlike traditional SaaS data protection vendors, we built our platform from the ground up and control our own infrastructure, independent of the public cloud. This removes hidden dependencies and indirect access paths. We built our platform this way because true data protection requires separate physical and logical infrastructure. If you want to know more about our architecture, read our white paper on how we raise the bar for data protection in the cloud.

Read more in our white paper:
Leading SaaS data security →

© 2026 Keepit. All rights reserved



OBJECTIVE 7:
Security & Compliance Sovereignty

Ability to ensure security, show compliance, and align with EU regulatory requirements

Security certifications tell you a provider takes security seriously. This objective covers recognized certifications (e.g., ISO schemes), alignment with GDPR, NIS2, and DORA regulations, whether security operations and monitoring run exclusively under EU jurisdiction, how transparent and timely breach reporting is, and whether EU entities can independently audit security and compliance controls.

CONTRIBUTING FACTORS	HOW KEEPIT HELPS
Attainment of EU and internationally recognized security certifications (e.g., ISO, ENISA schemes)	Keepit operates a mature security and compliance program aligned with EU and international standards. Keepit holds ISO 27001 certification and an independent SOC 2 Type II audit report, delivering regulatory-ready SaaS data protection to organizations worldwide.
Adherence to EU regulatory frameworks (e.g., GDPR, NIS2, DORA)	Keepit is designed to support its customers' compliance efforts under EU regulations such as NIS2 and DORA, most importantly helping its customers separate backup data logically and physically from production data, thus reducing the risk surface. Keepit also supports GDPR compliance by design and default through its unique architecture, helping organizations maintain control over data protection, access, and residency.
Operation of security monitoring and response (SOC) under EU jurisdiction, with visibility into logs and alerts	Keepit operates its platform within the EU, and its security operations center is operating exclusively under EU jurisdiction. This means that security monitoring, incident response, and compliance oversight are all performed under EU jurisdiction.
Transparent and EU-compliant incident reporting, and autonomy in applying security updates and patches	Keepit manages incident response and applies security updates within its own platform, enabling timely response and reducing reliance on external vendors. This includes the ability to develop, test, and apply security patches independently of non-EU vendors. Keepit follows EU-compliant incident notification timelines according to NIS2.
Ability for EU entities to audit and verify security and compliance controls	Keepit provides documentation and audit capabilities that support verification of security controls by relevant authorities. Multiple sovereign external auditors regularly check Keepit's security posture.

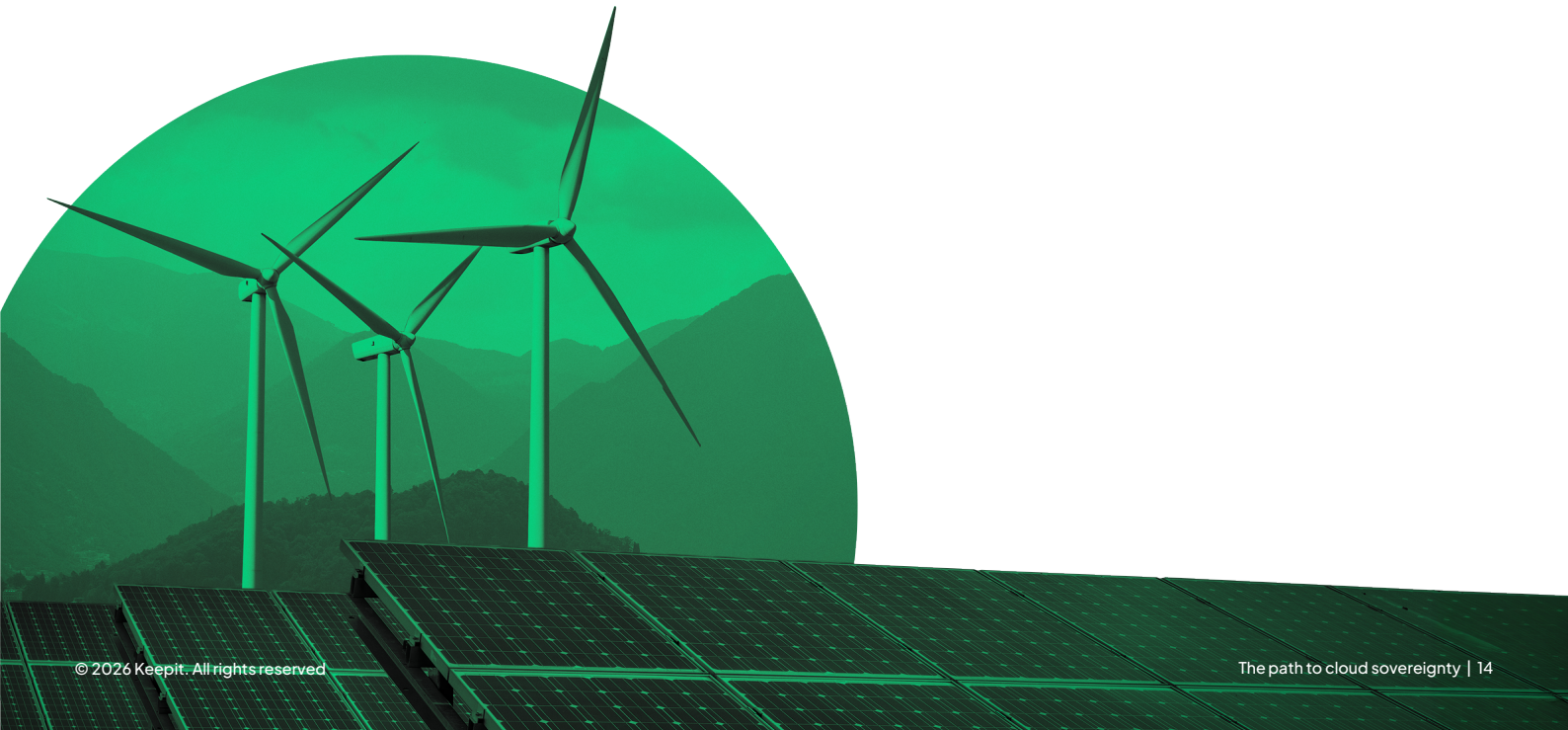
© 2026 Keepit. All rights reserved

OBJECTIVE 8:
Environmental Sustainability

Environmental impact of infrastructure and alignment with EU sustainability objectives

This objective looks at how energy-efficient a provider's infrastructure is, how transparently carbon emissions and resource use are measured and disclosed, and how much of the provider's energy comes from renewable or low-carbon sources.

CONTRIBUTING FACTORS	HOW KEEPIT HELPS
Energy efficiency of infrastructure and data center operations	Keepit has built its platform from the ground up as a purpose-built architecture for data protection, optimizing performance while minimizing energy consumption and infrastructure overhead.
Use of renewable or low-carbon energy sources	Keepit's EU-based data centers are powered by renewable energy, supporting reduced carbon impact of cloud operations. Data centers are supplied by energy sources that fall under local renewable energy guarantee schemes, such as the GoOs (guarantees of origin) in the EU.
Transparency in environmental impact and sustainability practices	Keepit's efficient technology stack reduces storage, processing power, and operational resource needs through design choices such as streamlined architecture and optimized data handling.
Alignment with EU environmental and sustainability objectives	Keepit's approach focuses on responsible resource consumption and efficient infrastructure, aligning with EU priorities around sustainable and energy-efficient digital services. Keepit's sustainability practices are independently assessed through an annual EcoVadis sustainability rating, providing third-party validation of its environmental and operational efforts.



© 2026 Keepit. All rights reserved

From framework to decision

As European organizations place increasing emphasis on sovereignty, many are reassessing their reliance on global cloud ecosystems. Moving toward a more EU-anchored technology stack can help reduce legal and operational exposure — but it also introduces trade-offs. Shifting to regional providers may require upfront investment and careful consideration of resilience, innovation, and long-term flexibility.

This is where the EU Cloud Sovereignty Framework becomes valuable. It provides a structured way to evaluate providers across legal, operational, and technical dimensions — helping organizations not only meet regulatory expectations, but also demonstrate control over data, infrastructure, and third-party risk.

The challenge, however, remains identifying providers that strengthen sovereignty without compromising performance or scalability.

Keepit addresses this challenge by combining:

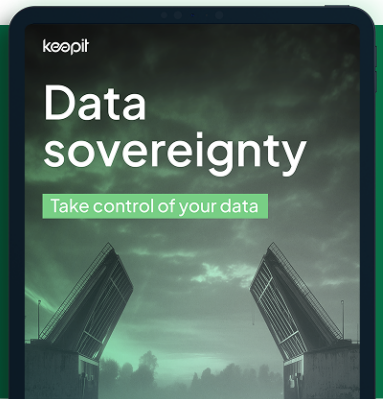
- **A fully independent and EU-controlled platform**
- **Strong legal and jurisdictional positioning**
- **Architecture that minimizes external dependencies**

Across the sovereignty objectives outlined in this guide, Keepit consistently aligns with key criteria, enabling organizations to reduce risk while maintaining resilience and operational continuity.

In an era where sovereignty risks are growing, Keepit stands as a beacon of control and reliability.
By partnering with us, your organization can confidently navigate the complexities of today's evolving challenges and regulatory requirements with a modern solution that ensures data is secure, compliant, and ready to support innovative business initiatives.

Learn more

Our report on data sovereignty offers guidance for IT and business leaders on navigating compliance, risk, and control. Learn how to build resilience, strengthen governance, and take control of your data across international operations.
Download the report →



keepit® Your data. Here today. Here tomorrow.

Keepit provides a true SaaS data protection platform 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.
For more information visit keepit.com or follow Keepit on LinkedIn.

bsi ISO/IEC 27001 Information Security Management CERTIFIED
IS 759831

© 2026 Keepit. All rights reserved