

Euclidia response to ARCEP consultation

Date: 12 Dec. 2024

Version: 1.0 (final)

Author: Stefane Fermigier for Euclidia (<https://www.euclidia.eu/> (<https://www.euclidia.eu/>))

Executive Summary

Euclidia welcomes Arcep's consultation on cloud computing regulation under the **SREN Act of 21 May 2024** and provides targeted recommendations to support the development of a competitive, user-focused cloud ecosystem in Europe. By emphasizing transparent pricing, harmonized technical standards and enforceable interoperability, Euclidia aims to address critical barriers to provider switching and multicloud adoption. These measures are essential for safeguarding digital sovereignty and fostering innovation.

Context and Challenges

The **SREN Act** mandates Arcep to facilitate cloud users' freedom of choice through two key initiatives:

1. **Capping data transfer and switching fees** to eliminate financial obstacles to provider migration and multicloud strategies.
2. **Defining and enforcing interoperability and portability standards** to address technical disparities that hinder seamless transitions between cloud services.

Arcep's proposal to set a zero-cost cap on data transfer fees is a bold step toward reducing vendor lock-in. However, achieving meaningful portability and interoperability also requires robust, enforceable mechanisms that ensure compliance with open standards and create measurable outcomes for users.

Euclidia's Core Recommendations

Waiving Data Transfer Fees and Ensuring Cost Transparency

Euclidia supports Arcep's proposal to cap data transfer fees at zero when switching providers. However, enforceable pricing transparency is equally crucial to eliminate hidden costs tied to migration. Providers should be required to:

- Publish detailed breakdowns of all fees associated with switching and multicloud use.
- Align pricing models with actual technical costs, eliminating financial barriers that impede data portability.

Standardization and Harmonization for Portability

To enable seamless provider migration and multicloud adoption, technical harmonization is critical:

- **Focus on ancillary services:** Identity and access management (IAM) services and SaaS data exchange formats are high-priority areas for standardization. Providers must adopt common schemas and interfaces that align with enforceable interoperability requirements.
- **Harmonize APIs and data formats:** Regulations should mandate strict adherence to royalty-free, open standards, ensuring uniformity across cloud services.
- **Open Standard diversity:** In order to stimulate innovation and smaller actors, diversity of open standards should be protected rather than prevented, as long as they meet enforceable interoperability requirements (see next item).

Enforceable Interoperability as the Foundation

Interoperability must go beyond technical standards as outlined above, and become a measurable, enforceable principle. Euclidia emphasizes that:

- **Interoperability must be outcome-driven:** Regulatory frameworks should require not only the adoption of open standards but also the demonstration of their effective implementation through testing, audits, and compliance validation.
- **Dispute resolution mechanisms should be introduced:** Users, especially SMEs, must have access to neutral, third-party processes to resolve issues related to non-compliance with interoperability requirements.
- **API interoperability must be guaranteed:** Providers should offer clear, publicly accessible, and stable APIs, with automated testing frameworks to ensure they meet interoperability benchmarks.

Enforceable interoperability ensures that cloud services function seamlessly across platforms, mitigating the risks of partial or flawed implementations of standards.

Multicloud-Ready Interoperability

Multicloud adoption offers significant resilience and flexibility but faces challenges from provider-specific implementations and interconnection agreements. Euclidia recommends:

- **Enforcing synchronization of IAM policies across platforms:** This ensures consistent access management in multicloud environments.
- **Supporting cloud-agnostic tools:** Investment in Open Source tools for provisioning, orchestration, and observability is essential to reduce dependency on proprietary solutions.

Migration Support and Documentation

Switching providers often involves indirect costs due to inadequate documentation and proprietary systems. Euclidia urges providers to:

- Offer migration tools that adhere to enforceable interoperability principles.
- Provide comprehensive and standardized guides for data export, transformation, and service reconfiguration.

Protecting European Digital Sovereignty

Reducing reliance on non-European providers is essential for safeguarding Europe's digital

sovereignty. Euclidia recommends:

- **Introducing procurement quotas for European providers:** Public procurement should prioritize cloud solutions that comply with enforceable interoperability standards and support Europe's strategic autonomy.
- **Promoting Open Source innovation:** Encouraging the adoption of free and Open Source software (FOSS) mitigates lock-in risks and fosters a competitive ecosystem.

Strategic Impact

Placing enforceable interoperability at the heart of the regulatory framework will drive significant benefits:

- **Enhanced User Freedom:** Measurable interoperability ensures users can seamlessly switch providers and adopt multicloud strategies without technical or financial constraints.
- **Strengthened Digital Sovereignty:** Supporting European cloud providers through enforceable standards reduces dependency on non-European players and enhances strategic autonomy.
- **Fair Competition and Innovation:** Robust enforcement of open standards creates a level playing field, encouraging SMEs and fostering an ecosystem of innovation.

Euclidia's recommendations align with Arcep's mandate to enable user choice and promote multicloud adoption. By prioritizing enforceable interoperability, transparency, and harmonization, these measures will create a resilient, open, and competitive cloud market in Europe, empowering users while fostering innovation and digital independence.

About Euclidia

The **European Cloud Industrial Alliance (EUCLIDIA (<https://www.euclidia.eu/>))** is an industry association uniting European SMEs in the cloud sector to promote innovation, competition, and digital sovereignty. Members are majority-owned by European shareholders and develop hardware and software solutions for Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS). EUCLIDIA's mission is to support the growth of a vibrant European cloud ecosystem by fostering collaboration, ensuring technological independence, and advocating for open and competitive markets.

EUCLIDIA recognizes the pivotal role of SMEs as drivers of innovation and R&D within Europe. However, European cloud companies often face challenges from market dynamics that favor larger, non-European providers, as well as the frequent acquisition of local innovators by foreign entities. These trends erode Europe's technological assets and hinder the development of independent cloud infrastructure. EUCLIDIA aims to reverse this trajectory by creating an environment where European SMEs can thrive and contribute to Europe's strategic autonomy.

To achieve its mission, EUCLIDIA advocates for policies that support SME growth, such as prioritizing open standards, fostering public-private partnerships, and promoting supplier diversity through procurement quotas. It also supports initiatives like distributed edge cloud platforms fully developed by European SMEs, enabling cutting-edge use cases in sectors such as Big Data, IoT, and university research.

Through its work, EUCLIDIA seeks to build a competitive, innovative, and sovereign European cloud industry, ensuring Europe remains at the forefront of technological advancement while safeguarding its digital independence.

Question 1: Observations on Pricing Practices

Pricing practices that penalize data transfers between cloud providers undermine digital sovereignty and perpetuate vendor lock-in. These practices hinder data portability—a fundamental user right based on Open Source principles and open standards. Transparent pricing aligned with actual technical costs is essential to support fair access to interoperable services and foster competition.

Question 3: Cost Determinants for Data Transfers

Costs related to non-standard formats and proprietary tools used by some providers pose significant barriers to data migration. These indirect costs contravene the principles of openness and interoperability. Euclidia advocates for the adoption of open standards to minimize obstacles and promote seamless data mobility.

Question 5: Influence of Provider Strategy on Costs

Provider strategies, such as internalizing infrastructure or leveraging exclusive interconnection agreements, should not artificially restrict users' ability to migrate or implement multi-cloud architectures. Decisions that create barriers to portability or interoperability contravene the principles of digital sovereignty.

Question 9: Data Transfers as Non-Recurring Events

Migrations related to provider changes are planned and non-recurring events. Any associated costs must be transparent and aligned with the principles of data portability, ensuring users' freedom to choose providers without financial or technical constraints.

Question 13: Zero Transfer Cost Cap

Setting transfer costs to zero aligns with the principle of data portability as a fundamental user right and prevents vendor lock-in. This approach supports competition and protects SMEs from excessive fees. Providers must integrate transfer-related costs into their overall pricing strategies without resorting to hidden fees.

Question 19: Additional Services for Provider Change

Providers should offer tools that facilitate data export and transformation, alongside comprehensive technical documentation. Support for a seamless transition to multi-cloud environments must prioritize transparency and openness to prevent undue dependence on proprietary solutions.

Question 22: Definitions and Typologies of Cloud Services

The proposed IaaS, PaaS, and SaaS definitions are pertinent but must emphasize the role of

open standards and interoperable solutions. These are particularly critical for PaaS and SaaS, where the risk of vendor lock-in is high. A clearer distinction between open and proprietary services will empower users to make informed choices.

Question 24: Coverage of Needs by Cloud-Agnostic Tools

Cloud-agnostic tools address key user needs for provisioning, orchestration, and observability. However, additional efforts are required to extend these tools to more complex functionalities and standardize APIs for proprietary services. Open Source solutions are essential to bridge gaps and ensure interoperability.

Question 30: Migration Challenges for PaaS Services

Migration challenges often stem from reliance on provider-specific DevOps tools, integrated APIs, and serverless services. Euclidia emphasizes the need for open standards and comprehensive provider documentation to mitigate these issues and promote seamless transitions.

Question 31: Services Hindering Migration and Recommendations

Key barriers include proprietary databases, AI/ML services, DevOps tools, and serverless functions. Recommendations include:

1. **Promote Open Standards:** Encourage databases like PostgreSQL over proprietary solutions.
2. **Document APIs:** Provide clear migration guides to alternative services.
3. **Support Cloud-Agnostic Tools:** Invest in open solutions.

Databases should be a priority for harmonization, as they are critical for operational continuity.

Question 39: Interoperability in Integrated Multi-Cloud Architectures

Interoperability in multi-cloud architectures is critical for resilience, cost optimization, and regulatory compliance. Challenges include non-standard APIs and complex IAM synchronization. Euclidia recommends developing European standards and supporting cloud-agnostic tools to address these issues.

Question 41: Interoperability via Open, Documented APIs

Interoperability relies on APIs that are:

1. **Accessible and Open:** Allow integration with third-party systems.
2. **Well-Documented:** Facilitate efficient implementation and migration.
3. **Stable:** Minimize costs from unforeseen changes.

APIs must adhere to open standards to ensure competition and avoid lock-in.

Question 52: Standardization of SaaS Data Structures

Standardizing SaaS data formats is essential for portability and interoperability. Priority areas include ERP, CRM, and collaborative tools. Euclidia advocates for:

1. **Common Export Formats:** Standard schemas for critical data types (e.g., financial transactions, customer data).
2. **Use of Open Standards:** Ensure compatibility with tools independent of any specific provider.
3. **Standardization:** Establish a European SaaS standardization framework to guide providers and users.

Question 53: Additional comments on the issues raised in the consultation

Avoid falling into the trap of vague or biased definitions of open standards

An **open standard**, as defined in the **European Interoperability Framework (EIFv1, 2005)**, refers to a technical specification that is formalized, independent, and accessible for implementation **without legal, operational, or financial restrictions**. This strict definition ensures that all actors—large or small—can adopt and implement such standards equitably, fostering a competitive and innovative digital ecosystem.

It is crucial to align regulatory approaches, especially for cloud services, with the principles of **open standards in their strictest sense**. This includes fully open interfaces, data formats, and communication protocols that enable true interoperability and portability, reducing the risk of vendor lock-in and supporting Europe's digital sovereignty.

Key characteristics of an open standard

The minimal criteria for a true open standard, which should underpin any cloud service regulation, include:

1. **Publicly accessible and freely available specifications:** The documentation must be public, without financial or legal barriers, ensuring equal access for all stakeholders, including SMEs, public administrations, and individual developers.
2. **Compatibility with competing implementations:** Open standards should enable multiple implementations, including Open Source solutions, to foster diversity and competition in the market.
3. **Technical neutrality and absence of blocking patents:** Essential patents within the standard must be available on a **royalty-free (RF)** basis. Licensing models such as RAND (*Reasonable And Non-Discriminatory*) or FRAND (*Fair, Reasonable And Non-Discriminatory*) should be excluded as they introduce barriers for free software implementations.
4. **Independent and transparent governance:** The development and maintenance of the standard should be overseen by an open, non-profit organization where all stakeholders have equal influence, with decisions based on consensus or majority voting.
5. **Interoperability as a core goal:** Open standards should prioritize enabling seamless interaction between different systems, whether proprietary or Open Source.

Addressing the shortcomings of current definitions

The definition of open standards under existing French law, particularly the **LCEN (2004)**, lacks precision. While it defines an open standard as a protocol or data format with public specifications and no implementation restrictions, it fails to:

- Define “restrictions” clearly, leaving room for ambiguity that could allow proprietary practices, such as RAND licensing.
- Include explicit obligations for **verifiable and enforceable interoperability**.

To strengthen this framework, the definition should be revised to ensure that open standards are truly inclusive and practical. A suggested revision could be:

“An open standard is a protocol or data format with publicly available specifications, free from royalties or discriminatory conditions, ensuring its unrestricted adoption. The standard must include comprehensive documentation and mechanisms for guaranteeing and verifying enforceable interoperability.”

Interoperability as a concrete, enforceable principle

Enforceable interoperability is a pragmatic response to the challenges posed by the current fragmented landscape of standards. It shifts the focus from rigid technical prescriptions to **measurable outcomes** that guarantee effective interaction between systems. This approach addresses:

1. **Real-world implementation gaps:** Many standards, even when formally open, suffer from partial or flawed implementations due to bugs, proprietary extensions, or divergent interpretations. Enforceable interoperability imposes measurable outcomes and validation mechanisms to ensure compliance.
2. **Vendor accountability:** Enforceable interoperability provides tools for stakeholders—especially smaller actors—to compel providers to correct non-compliant implementations. This includes testing frameworks, audits, and legal recourse mechanisms.
3. **Neutrality and flexibility:** Rather than mandating a specific technology stack, enforceable interoperability focuses on outcomes, allowing for diverse technological approaches and innovation.

Examples of enforceable interoperability in cloud services

In the context of cloud services, enforceable interoperability include:

- **Data interoperability:** Requiring providers to offer open APIs for exporting data in standardized, vendor-neutral formats.
- **Service portability:** Ensuring users can migrate workloads or applications between providers without significant modification or additional costs.
- **API interoperability:** Mandating clear, publicly documented APIs with automated testing to verify compliance.

- **Dispute resolution frameworks:** Establishing third-party mechanisms to resolve technical disputes over non-compliance.

Protecting smaller actors

By emphasizing enforceable interoperability, smaller actors can compete on an equal footing with dominant providers. This approach prevents large vendors from exploiting ambiguities in standards to lock users into their ecosystems or create barriers to competition. It also fosters an innovative and diverse ecosystem where smaller players can thrive by adopting simpler, more innovative standards.

Conclusion

To support the goals of interoperability, portability, and vendor neutrality, the regulation of cloud services must be built upon strict, enforceable open standards as outlined in the EIFv1. Furthermore, introducing enforceable interoperability as a core principle would ensure that these standards translate into practical and measurable outcomes, reducing the risks of fragmentation and lock-in while promoting innovation and competition across the European digital landscape.

Question 54: Regulatory Recommendations for Cloud Services

Promoting European cloud solutions

To strengthen European digital sovereignty, it is essential to support the growth and competitiveness of European cloud providers, particularly small and medium enterprises (SMEs). Measures to achieve this include:

- **Market access quotas for European providers:** Reserving a minimum percentage of public procurement contracts for European cloud providers, especially SMEs, to foster innovation and stimulate the local ecosystem.
- **Preference for open standards and F/OSS technologies:** Mandating the use of solutions that adhere to strict open standards and free/open source technologies in public tenders, reducing the risk of vendor lock-in and reinforcing Europe's technological independence.

Embedding cyber-resilience as a foundational principle

Cyber-resilience must be treated as a cornerstone of cloud service design, going beyond basic regulatory compliance to ensure the robustness and continuity of services in the face of cyberattacks or operational failures. This requires a systemic and proactive approach, including:

1. **Holistic incident detection and response:** Providers should implement mechanisms to detect, isolate, and respond to incidents swiftly, minimizing the risk of cascading failures across interconnected services.
2. **Multi-cloud-specific security standards:** Establishing security frameworks tailored to multi-cloud environments, including the synchronization of identity and access management (IAM) policies and secure data flow management between providers.

3. **Transparency in cybersecurity practices:** Providers should demonstrate their capacity to handle crisis scenarios, including transparent disclosures of their security measures.
4. **Support for local cybersecurity innovation:** European SMEs specializing in cybersecurity should be prioritized in public procurement to develop tailored solutions for the European cloud ecosystem.

Addressing economic lock-in through fair pricing practices

The pricing models of cloud providers, particularly fees for data transfers, are a significant source of economic lock-in for users. Regulatory measures should address these concerns by:

1. **Capping data egress fees:** Imposing limits on data transfer costs to prevent providers from using excessive fees as a means of locking users into their platforms.
2. **Ensuring transparent pricing:** Requiring providers to publish clear and detailed pricing models, including direct and indirect costs for data transfers, storage, and auxiliary services.
3. **Monitoring and evaluating pricing practices:** Establishing an independent observatory to track and evaluate provider pricing models, identifying and addressing anti-competitive behavior or practices favoring non-European providers.

Encouraging portability and interoperability through open standards

Regulation must ensure that cloud services are designed to prioritize portability and interoperability. Key actions include:

1. **Enforcing the use of strict open standards:** Mandating that all APIs, data formats, and protocols used in cloud services comply with the principles of the EIFv1 to ensure vendor-neutral interoperability.
2. **Facilitating seamless data and service migration:** Requiring providers to offer mechanisms that allow users to transfer their data and applications between providers easily and at minimal cost, including across multi-cloud environments.
3. **Open Standard diversity:** In order to stimulate innovation and smaller actors, diversity of open standards should be protected rather than prevented, as long as they meet enforceable interoperability requirements.

Promoting European cloud solutions for strategic sectors

Certain sectors, such as healthcare, education, and public services, are critical to European sovereignty. Regulations should prioritize the use of European cloud solutions in these areas by:

- Setting specific **quotas** or **preferences** for local providers in strategic domains.
- Supporting targeted **innovation initiatives** to develop sector-specific cloud solutions tailored to European needs.

Recommendations for the regulation of cloud services

1. **Strengthen support for European cloud providers:** Introduce quotas in public procurement and prioritize solutions that adhere to open standards and free technologies.
2. **Embed cyber-resilience into regulatory frameworks:** Ensure providers implement robust, transparent, and multi-cloud-specific security measures while fostering local innovation in cybersecurity.
3. **Ensure fair pricing and prevent economic lock-in:** Cap data transfer fees, enforce transparent pricing models, and establish mechanisms to monitor and address abusive practices.
4. **Guarantee interoperability and portability:** Mandate the use of strict open standards and require mechanisms for seamless data and application migration.
5. **Prioritize local solutions in strategic sectors:** Promote European cloud providers in areas critical to public welfare and sovereignty, fostering a resilient and independent digital ecosystem.

With these additional initiatives, cloud service regulation can become a powerful tool for fostering innovation, ensuring fairness, and strengthening Europe's digital sovereignty while creating a competitive and open cloud ecosystem on the continent.