EXOSCALE

member of | A1 Digital

WHITEPAPER

Cloud under Control?

Europe's path toward digital sovereignty –
Maximum data protection, guaranteed compliance,
and full digital control

By David Furak

Content

Management Summary

Digitalisation and the use of global cloud technologies offer companies enormous opportunities. At the same time, however, the risks of foreign government access, regulatory conflicts, and loss of control over critical information are increasing.

This whitepaper explains why digital sovereignty has become a strategic necessity and how European cloud providers make the decisive difference.

- Maximum data protection in line with GDPR, the Data Act, and national security laws
- Regulatory certainty through EU-wide standards such as NIS2, DORA, and the EU Cloud Certification Scheme (EUCS)
- Digital independence through full control over data, infrastructure, and key management within Europe

Through concrete case studies, legal comparisons between the U.S. and the EU, and practical recommendations, this document provides clear guidance for choosing secure cloud strategies.

The result: long-term legal certainty, protection of sensitive information, and sustainable competitiveness through a cloud that is committed to European values.

The digitalization of business processes and applications is prompting companies worldwide to adopt cloud technology.

Executive Summary

The digitalization of business processes and applications is prompting companies worldwide to adopt cloud technology. At the same time, concerns about information security, data privacy, and sovereignty are growing. While European states and the European Union take a rule-of-law approach that prioritizes the protection of personal data and critical infrastructures, the United States relies on the global reach of major hyperscalers with an ever increasing gap on how these technologies should be regulated.

European Approach – principled based focus

- The GDPR (section 44 and subsequent sections) stipulates that personal data may only leave the EU under strict conditions. Mechanisms such as Standard Contractual Clauses (SCCs), Binding Corporate Rules (BCRs), and the Trans-Atlantic Data Privacy Framework are possible but are further restricted by the Schrems II ruling and ongoing case law.

- The upcoming Data Act, effective September 2025, extends similar protection requirements to non-personal data.

- NIS2 and DORA require harmonized security and resilience standards across Europe.

US Approach – surveillance & control based focus

- The CLOUD Act (2018) clarifies the extraterritorial access of data for US-based providers and obligates them to hand over personal data, regardless of location.

- FISA Section 702 allows the surveillance of non-US persons outside the US for foreign intelligence purposes.

- Executive Order 12333 allows the NSA to access data directly, including through clandestine means.

Central Principles

Out of this ever stronger divergence in focus, Three central principles of action arise from this divergence for European companies and organizations:

1. THOSE THAT DO "BARE MINIMUM" (CLOUD FOR EUROPE)

These cloud providers offer basic infrastructure and services, often focusing on cost-efficiency and leaving most compliance and security responsibilities to the user.

2. THOSE THAT ARE TRYING TO BYPASS REGULATORY HURDLES WITH MEASURES (CLOUD IN EUROPE)

These providers implement specific technical or contractual measures designed to mitigate regulatory challenges, such as data localization or specific encryption methods, without necessarily offering full sovereign control.

3. THOSE THAT HAVE FULL SOVEREIGNTY SPECTRUM (CLOUD BY EUROPE)

These cloud solutions are designed from the ground up to provide complete control over data, infrastructure, and operations, ensuring compliance with strict regulatory frameworks and national sovereignty requirements.

It is important to note that only in the last type of cloud offering (fully sovereignty spectrum) can confidentiality and availability be truly safeguarded.

Out of this ever stronger divergence in focus, Three central principles of action arise from this divergence for European companies and organizations.

European Initiatives

- With the Data Act and cybersecurity directives NIS2/DORA, both personal and machine-generated data are comprehensively protected.

- The European Cloud Cybersecurity Certification Scheme (EUCS), under the ENISA framework and GAIA-X, promotes interoperable and trustworthy cloud ecosystems.

- National blocking statutes in countries such as France and Switzerland effectively prevent forced data outflows and uncontrolled access.

Recommendations for Action:

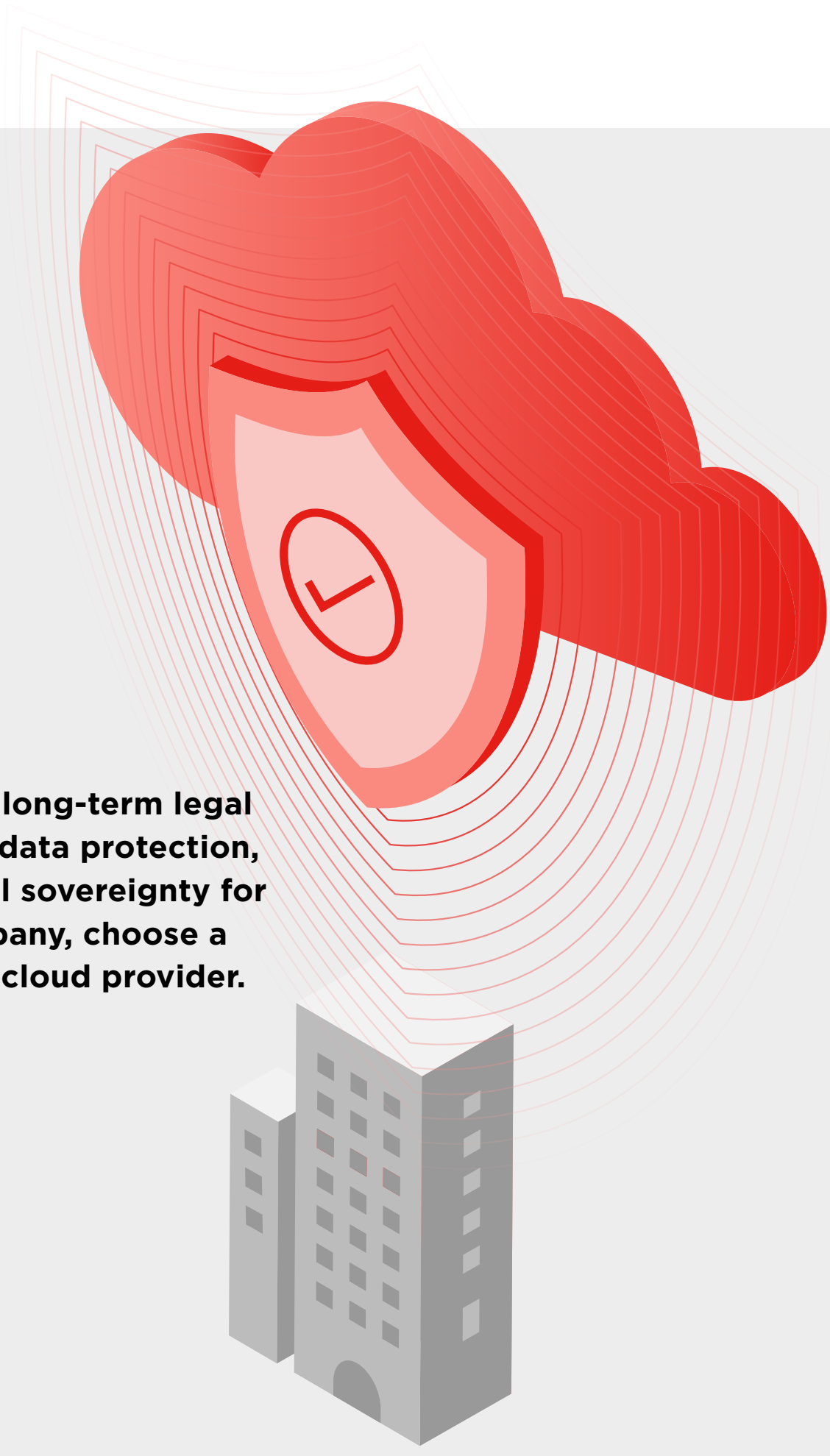
1. Prioritize the migration of sensitive workloads, from those being mission-critical to those containing sensitive data, to European cloud providers which can provide the full cloud sovereignty spectrum (cloud BY Europe).

2. Use multi-cloud approaches. Non-critical workloads can remain on global hyperscalers, but especially sensitive data should be stored exclusively in “Cloud by Europe”.

3. Rely on audited standards such as EUCS, SecNumCloud, and the European Cybersecurity Certification Group (ECCG).

4. As an Austrian cloud provider, A1 Digital offers you a sovereign, highly-available, high-performance, and legally compliant platform.

To ensure long-term legal certainty, data protection, and digital sovereignty for your company, choose a European cloud provider.



To ensure long-term legal certainty, data protection, and digital sovereignty for your company, choose a European cloud provider.

Introduction

Cloud Sovereignty as a Strategic Challenge

DIGITALIZATION AND CLOUD TRANSFORMATION

Migration to the cloud is now a driver for innovation, agility, and cost efficiency, not just an IT optimization measure. Studies show that companies save an average of 20 % on infrastructure costs and achieve development cycles up to 30 % shorter through cloud adoption.

However, moving to public clouds raises questions: Who controls my data? Where is it stored? Which legal framework applies to it? How can I be sure that authorities or intelligence agencies do not access it unnoticed?

DIGITAL SOVEREIGNTY AND GOVERNMENT REGULATIONS

Digital sovereignty encompasses a state, region, or company's ability to independently control digital resources, data, and infrastructures. At the European level, this term is closely linked to sovereignty, network and information security, and privacy policy.

The EU's Digital Compass 2030 strategy aims to develop a "Digital Sovereignty Cloud Infrastructure" that meets the highest standards of data protection, security, and performance. Similar approaches are pursued by national strategies in France (Cloud de Confiance), Germany ("Secure Cloud" ecosystem), and Switzerland (Swiss Cloud Strategy).

OBJECTIVE OF THIS WHITEPAPER

This whitepaper aims to provide decision-makers in business, administration, and public institutions with the following:

- An overview of the key legal and data protection differences between the US and Europe
- The significance and opportunities of European cloud providers
- Risks in cooperating with US hyperscalers, as exemplified by the Bundeswehr-Google project
- An introduction to key EU initiatives (Data Act, NIS2, DORA, and EUCS)
- Concrete recommendations for securely operating your cloud workloads.

Studies show that companies save an average of 20 % on infrastructure costs and achieve development cycles up to 30 % shorter through cloud adoption.

Different Approaches to Data Protection and Privacy in the US and Europe

US Legal Framework: Panopticon and Chokepoint

THE CLOUD ACT (CLARIFYING LAWFUL OVERSEAS USE OF DATA ACT)

Effective since March 2018, the CLOUD Act supplements the Stored Communications Act (SCA, 1986) and clarifies that every US provider must hand over data to authorities upon request, regardless of whether the data is located within or outside the US.

IMPACT (PANOPTICON)

Under court order, US authorities can access emails, chat logs, metadata, and other customer data stored exclusively in European data centers.

FISA SECTION 702

The 2008 FISA Amendments Act, especially Section 702, allows the US intelligence agency NSA to conduct targeted surveillance of non-US persons outside US territory. Providers must retrieve communication content and metadata as part of foreign intelligence surveillance.

IMPACT (CHOKEPOINT)

In extreme cases, the US government could instruct US technology companies to stop providing services to certain customer groups or entire countries.

EXECUTIVE ORDER 12333

This 1981 presidential order authorizes the NSA to collect “signals intelligence”, including through clandestine means. Unlike the CLOUD Act and FISA, this involves direct, covert (“backdoor”) access to data in the cloud.

PRACTICE AND SECRECY

Major US hyperscalers (Amazon Web Services, Microsoft Azure, and Google Cloud) claim to provide information only as legally required and rarely. However, all statistics on FISA orders are subject to secrecy orders, so neither the scope nor the specific targets are publicly traceable.

This creates a significant so called “chokepoint problem”, as these few dominant providers control vast amounts of data, making them prime targets for government surveillance requests. Consequently, the concentration of data within these hyperscalers raises concerns about the potential for widespread, untraceable access to user information.

European Legal Framework: General Data Protection Regulation (GDPR) and EU Data Protection Agreements

THE GDPR (REGULATION (EU) 2016/679)

The GDPR protects personal data in several ways:

- Principles such as purpose limitation, data minimization, and storage limitation (section 5).
- Data Subject Rights: Access, Deletion, and Portability (section 15 and subsequent sections)
- Strict rules for third-country transfers (section 44 and subsequent sections) — especially SCCs, BCRs, or an adequacy decision.

SCHREMS II AND THE TRANS-ATLANTIC DATA PRIVACY FRAMEWORK (DPF)

In July 2020, the ECJ declared the EU-US Privacy Shield invalid (Case C-311/18) because US laws, such as the CLOUD Act, do not provide "essential European guarantees". The executive order implementing the DPF was signed in October 2022, and the EU Commission's adequacy decision legally enacted the DPF in July 2023.

DATA SOVEREIGNTY OF EUROPEAN PROVIDERS

"Cloud by Europe" means: service, operation, and owner jurisdiction are entirely within the EU/EEA or in third countries with an adequacy decision (e.g., Switzerland).

Comparison: US vs. Europe

POINT	US	EUROPE
Legal Sources	CLOUD Act, FISA Section 702, E.O. 12333	GDPR, Data Act, NIS2, DORA
Authority Access	Extraterritorial compulsion with high secrecy	Strict transparency and complaint mechanisms
Data Transfers	Free global transfer, subject to US orders	Allowed only with SCC/BCR/ DPF or adequacy decision
Sanctions for Violation	Criminal and administrative proceedings, possible export bans	Fines up to €20 million or 4 % of global turnover
Technical Solutions	Confidential Computing, Data Trust Models, EU partnerships	Geo-locked data centers, BYOK, EUCS certification

Why European Cloud Services are Essential for Companies and Organizations

Three Levels of Cloud Sovereignty

Research by Michels et al. (2023) distinguishes three levels:

- **Cloud for Europe (Compliance Sovereignty):** Focuses on certifications such as ISO 27001, Code of Conduct, and EUCS, as well as EU compliance with GDPR and NIS2.
- **Cloud in Europe (Data Location):** Physical storage and processing of data within the EU/EEA, with transfers only under regulatory requirements.
- **Cloud by Europe (Provider Nationality)** Complete European control: ownership, operation, support, and key management remain in EU hands.

The higher you climb the sovereignty ladder, the lower the risk of government access and service interruptions by third countries.

This results in several legal and regulatory advantages

- Avoidance of US legal conflicts (CLOUD Act, FISA Section 702)
- Compliance with GDPR transfer mechanisms (SCC, DPF, BCR)
- Fulfillment of future Data Act requirements for non-personal data
- Compliance with NIS2 and DORA security requirements
- Protection from “blocking statutes” (e.g., Swiss banking secrecy and the French Cloud de Confiance framework).

Technical and operational advantages

- Transparent key management models (BYOK)
- Encryption at rest, in transit, and “in use” (confidential computing)
- Multi-regional data center distribution within the EU (resilience and latency optimization)
- Dedicated service level agreements (latency, availability, and data protection clauses)
- Independence from US infrastructure provider backbones.

Main reasons for switching to European clouds

- Legal certainty and compliance
- Highest data protection standards under GDPR and Data Act
- Protection of sensitive business and customer data
- Avoidance of hidden sovereign access
- Long-term independence and control.

CASE STUDY

The Bundeswehr's Cooperation with Google Cloud Data Protection Risks and Political Criticism

In 2025, the German Armed Forces (Bundeswehr) has decided to use Google Cloud as part of a comprehensive IT modernization initiative. The contracting party is Google Cloud EMEA Ltd., which is based in Ireland and is a subsidiary of the US-based Google LLC. The plan is to use data centers in Frankfurt am Main, the Netherlands, and Finland. The goal is to standardize and increase the efficiency of the military's IT infrastructure nationwide.

However, jurisdictional challenges arose during the design of the contract. Although data processing takes place in European data centers, Google Cloud EMEA Ltd. is ultimately subject to US law, including the CLOUD Act and the Foreign Intelligence Surveillance Act (FISA Section 702). Additionally, Executive Order 12333 allows US intelligence agencies to access network and steward data.

Since the Bundeswehr processes classified military inventory, situation, and personnel data, there is a significant risk of uncontrolled access. This risk is further compounded by the absence of a BYOK option, which prevents the Bundeswehr from protecting sensitive live workloads with its own encryption keys.

Controversial Debate

A controversial debate has erupted in politics and the media between transparency advocates and those in favor of secrecy. Critics in the Bundestag and investigative journalists complain that only Google can provide information about official requests from the US and that no external audits are planned. They also criticize the lack of clear statements about whether and to what extent “secrecy orders” have been requested and issued.

Overall, skeptics see a potential conflict between the European General Data Protection Regulation (GDPR) and US supremacy rules, such as the CLOUD Act. Proponents, on the other hand, point to Google's high technical security standards, its regulation by the US Federal Trade Commission (FTC), and the fact that Google Cloud is already used successfully in many sensitive industries.

In summary, the Bundeswehr's cooperation with Google Cloud raises central questions about the compatibility of national data sovereignty, international law, and IT security. A final solution will only be possible through transparent auditing mechanisms and clear contractual guarantees against uncontrolled access.

A controversial debate has erupted in politics and the media between transparency advocates and those in favor of secrecy.

European Initiatives and Standards for Sovereign Cloud Architectures

Data Act: Extension to Non-Personal Data

Effective September 2025, Regulation (EU) 2023/2854 extends protection obligations to machine- or sensor-generated data.

European and national cybersecurity and digital data protection regulations provide clear requirements to prevent unfair contract clauses and exclude uncontrolled access by third-country authorities. Cloud and ICT providers must ensure through their contracts that they take all necessary technical and organizational measures to minimize the risk of unauthorized access and guarantee the integrity, confidentiality, and availability of data at all times.

Clauses that allow for further data disclosure are expressly prohibited, as are any contractual provisions that enable third-country authorities to access sensitive information without judicial oversight or transparency.

NIS2 and DORA

The NIS2 Directive (EU) 2022/2555 and the DORA Regulation (EU) 2022/2550 establish binding cybersecurity and operational resilience standards throughout the European Union. These directives address operators of critical infrastructures and the financial sector, requiring these companies to establish comprehensive risk management processes and report incidents within 24 hours.

They also require governance structures, employee awareness measures, and regular audits. Particular importance is placed on contractual arrangements with third-party ICT providers. Location requirements, access restrictions, and concepts for failure and emergency management must be established in the contract.

EU Cloud Certification

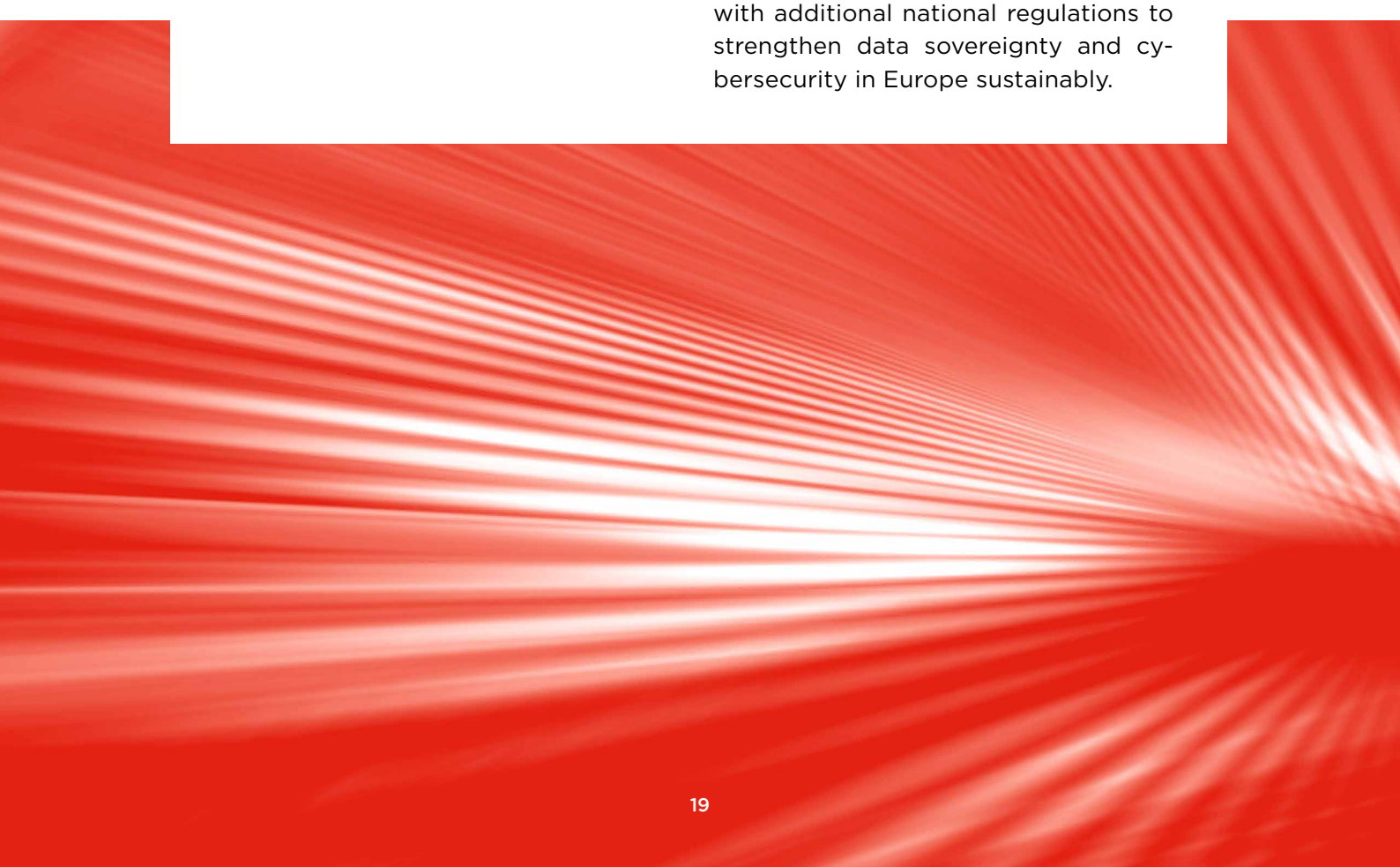
The European Union is advancing the EU Cloud Certification Scheme (EUCS), developed by the European Union Agency for Cybersecurity (ENISA), as a unified framework for cybersecurity certificates for cloud services. Based on international ISO/IEC standards, the EUCS aims to build trust by providing consumers and public authorities with clear evidence of cloud providers' security levels.

Additionally, the GAIA-X initiative aims to establish a federated European cloud ecosystem combining common interfaces, data sovereignty principles, and a shared trust framework. Over 300 companies, research institutions, and government bodies are collaborating to develop a privacy-friendly infrastructure that reinforces European values in the digital landscape.

Regional Regulations

In addition to these EU-wide instruments, several member states have enacted their own blocking statutes to prevent official data outflows. Switzerland, a non-EU country, protects banking secrecy with Article 47 of the Banking Act, which imposes criminal sanctions for the unlawful disclosure of customer data. France has introduced the "Cloud de Confiance" certification, which has security-critical requirements for cloud services, especially for sensitive government applications.

Germany is planning stricter rules to secure state data in a so called "TRUST Cloud" and further restrict the use of foreign cloud providers that may be accessed by authorities in other countries. Overall, this regulatory framework takes a multi-level approach, combining EU-wide minimum standards with additional national regulations to strengthen data sovereignty and cybersecurity in Europe sustainably.



Recommendations for Action

When selecting a reliable cloud provider, consider the following criteria and check it:

- Operates all data processing centers in the EU/EEA
- Has a legally independent European corporate structure
- Offers “Bring Your Own Key” via HSM within the territory
- Is certified according to SecNum-Cloud EUCS, ISO 27001/27017/2701
- Guarantees binding SLAs for data protection, availability, and incident reporting.

In addition, we would like to offer a few useful tips for your cloud strategy and migration.

- Classify your workloads. Identify mission-critical wordloads as well as identify “high-risk” data (e.g., personnel, health, and control data)
- Use a hybrid approach. Keep sensitive workloads on “Cloud by Europe” and standard workloads in global public clouds
- Technical measures: Use encryption “at rest”, “in transit”, and “in use” (confidential computing)
- Establish clear processes for third-party service providers, audits, and regular compliance reviews.

When selecting a reliable cloud provider, consider the following criteria and check it.

Why A1 Digital?

The issues of digital sovereignty and legally binding data protection are becoming increasingly important in an interconnected world. European regulations, such as NIS2 and DORA, already establish binding cybersecurity and resilience standards for critical infrastructures and the financial sector. Meanwhile, the ENISA-led EU Cloud Certification Scheme (EUCS) establishes a unified framework for evaluating cloud services based on international ISO/IEC standards. The GAIA-X initiative complements these efforts by developing a federated, pan-European cloud ecosystem with jointly defined interfaces, data sovereignty, and trust rules.

National blocking statutes, such as the Swiss Banking Act and the French “Cloud de Confiance”, protect sensitive data from uncontrolled foreign transfers, underscoring the need for sovereign infrastructure.

A European cloud offers clear advantages. It guarantees compliance with the GDPR, establishes clear responsibilities to create legal certainty, and minimizes the risk of third-country authorities accessing confidential information unnoticed. Embedding technical and organizational protective measures within the territory avoids data leaks as well as unfair contract clauses that could force companies to make significant concessions.

And that is exactly what we offer!

As a strong partner for your cloud sovereignty, A1 Digital relies on European solutions. We operate the "A1 Cloud Souverän" platform in Austrian data centers with TÜV-certified data protection and 100% GDPR compliance. This platform uses bring your own key, full-stack encryption, and integrated key management — all within national borders.

Our EUCS roadmap and comprehensive NIS2/DORA compliance framework ensure that you always remain up to date with regulations, as does our preparation for the upcoming Data Act. We also offer professional services, including migration, DevOps, and security assessments, as well as 24/7 German-speaking support.

Another cornerstone of our strategy is our consistent use of open-source technologies. By avoiding proprietary dependencies, we protect our customers from vendor lock-in and ensure maximum flexibility in further developing their cloud environments. Open standards and transparent source codes enable quick implementation of individual adjustments and step-by-step integration of new components – without long-term commitment to a single provider.

Choose a European cloud provider like A1 Digital to enjoy data protection, legal certainty, and true digital sovereignty. This way, you maintain control of your data – today and in the future.

We hope this whitepaper provides a solid foundation for your cloud strategy and demonstrates why choosing a European cloud provider like A1 Digital is a strategic investment in your digital independence, not just a matter of data protection.

A European cloud offers clear advantages. It guarantees compliance with the GDPR, establishes clear responsibilities to create legal certainty, and minimizes the risk of third-country authorities accessing confidential information unnoticed.

Glossary

CLOUD Act
The Clarifying Lawful Overseas Use of Data Act (2018) is a US federal law that ensures US providers comply with government orders to release data, even if it is stored abroad.

DORA (Regulation
(EU) 2022/2550)
Digital Operational Resilience Act for the financial sector, which includes ICT resilience requirements.

DPF
The Trans-Atlantic Data Privacy Framework (2022), an EU-US data agreement post-Schrems II that is currently pending before the ECJ.

GDPR
General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679): European regulation for the protection of personal data.

EUCS
EU Cloud Certification Scheme: An upcoming EU certification framework for cloud security under ENISA.

FISA Section 702
Part of the 2008 US Foreign Intelligence Surveillance Act, it allows for the targeted surveillance of non-US persons outside the US.

GAIA-X
A pan-European project for a federated, sovereign data network and cloud ecosystem.

NIS2
Directive (EU) 2022/2555 — an EU directive on cybersecurity in critical sectors that imposes stricter risk and reporting obligations.

Schrems II
The ECJ's July 2020 ruling (C-311/18) that invalidated the EU-US Privacy Shield and tightened requirements for third-country transfers.

Standard Contractual Clauses (SCC)
Contract templates provided by the EU Commission for legally secure transfers of personal data to third countries.

Transparency Report
An annual publication by major cloud providers on government access requests, which are often limited by "secrecy orders" for US Government requests.

References / External Links (SELECTION)

European Commission, "Digital Compass 2030: the European way for the Digital Decade"
https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en

Regulation (EU) 2016/679 (DSGVO)
https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679

Clarifying Lawful Overseas Use of Data Act, Pub.L. 115–141
https://www.congress.gov/bill/115th-congress/house-bill/4943

FISA Amendments Act 2008, Pub.L. 110–261
https://www.congress.gov/bill/110th-congress/house-bill/6304

Executive Order 12333
https://www.archives.gov/federal-register/codification/executive-order/12333.html

ECJ, Judgment C-311/18 (Schrems II)
https://www.bfdi.bund.de/DE/Fachthemen/Inhalte/Europa-Internationales/Auswirkungen-Schrems-II-Urteil.html

Joint Statement on Trans-Atlantic Data Privacy Framework
https://ec.europa.eu/commission/presscorner/detail/en/statement_22_2043

Directive (EU) 2022/2555 (NIS2)
https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022L2555

Regulation (EU) 2022/2550 (DORA)
https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022R2554

Regulation (EU) 2023/2854 (Data Act)
https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202302854

ENISA, „EU Cloud Certification Scheme"
https://certification.enisa.europa.eu/index_en

GAIA-X AISBL
https://gaia-x.eu/

CNIL, „Cloud : les risques d'une certification européenne permettant l'accès des autorités étrangères aux données sensibles"
https://www.cnil.fr/fr/cloud-les-risques-dune-certification-europeenne-permettant-lacces-des-autorites-etrangeres

EDPS, „European Commission's use of Microsoft 365 infringes data protection law for EU institutions and bodies"
https://www.edps.europa.eu/press-publications/press-news/press-releases/2024/european-commissions-use-microsoft-365-infringes-data-protection-law-eu-institutions-and-bodies_en

Bundeswehr, Pressemitteilung zur Google Cloud-Kooperation
https://www.bundeswehr.de/de/meldungen/partnerschaft-bwi-google-bundeswehr-eigene-cloud-5952950

About the author

David Furak,

MANAGER OF STRATEGIC ENGAGEMENTS AT EXOSCALE

David Furak is Manager of Strategic Engagements at Exoscale, with a background in cybersecurity, digital infrastructure and data analytics. He holds a Bachelor's degree in International Relations from the University of Szeged and a Master's degree in EU Law from the University of Essex.

EXOSCALE
member of | A1 Digital

Contact

Boulevard de Grancy 19A
1006 – Lausanne, Switzerland

sales@exoscale.com
+41 58 255 00 66
exoscale.com

EXOSCALE

member of A1 Digital

About Exoscale

Exoscale was founded in 2011, is headquartered in Switzerland, and is member of A1 Digital – part of the A1 Group. The cloud provider empowers businesses and engineers to run their workloads and applications securely in the cloud. The user-friendly, reliable, and high-performing platform makes Exoscale an ideal partner for cloud-native deployments. With the rigorous focus on security and data protection, Exoscale ensures safe, GDPR-compliant cloud usage at every step.

More info at EXOSCALE.COM

10/2025_v1