Sovereignty Spotlight

EU Regulations and the Global Impact of Open Source

Sovereignty Spotlight

EU Regulations and the Global Impact of Open Source

Stefan Bergstein

Principal Chief Architect
EMEA Field CTO Org. Red Hat

stefan.bergstein@redhat.com
linkedin.com/in/stefanbergstein

David Szegedi

Principal Chief Architect
EMEA Field CTO Org. Red Hat

dszegedi@redhat.com
linkedin.com/in/david-szegedi

What we'll discuss today

- Navigating EU regulations
- Transparency and trust with Open Source
- Operational and technology sovereignty
- EU Sovereign ecosystem

Why Does Digital Sovereignty Matter ?

- **Security & Compliance** - Mitigating cyber threats, protecting sensitive data, and adhering to stringent European data protection regulations (NIS2, DORA, CRA, EUCS, etc.).
- **Operational Resilience** - Enhancing our ability to withstand global disruptions (geopolitical, economic, supply chain) by reducing dependence on external, potentially vulnerable, technologies.
- **Economic Competitiveness** - Fostering local innovation, supporting European tech industries, and retaining talent and revenue within the EU economy.
- **Trust & Transparency** - Building confidence with users, partners, and stakeholders through transparent and auditable digital processes.

Navigating EU regulations

Strengthening operational and technological Sovereignty

Cyber Resilience Act (CRA - Dec. 27)

Who is concerned:
Software vendors and manufacturers
OSS when commercial activity is involved

What is the objective:
Introduce mandatory cybersecurity requirements for hardware and software products, throughout their whole lifecycle

What it requires *:

- Cybersecurity managed and documented throughout the entire product lifecycle
- Active reporting and handling of vulnerabilities throughout the entire product lifecycle
- Security updates available throughout the entire product lifecycle

Source: https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng

* Non exhaustive list

Network and Information Security Directive (NIS2 - Oct. 24)

Who is concerned:
EU states, essential and important entities

What is the objective:
Build cybersecurity capabilities across the Union, mitigate threats to network and information systems used to provide essential services in key sectors and ensure the continuity of such services when facing incidents

What it requires *:

- Risk analysis and incident management
- Business continuity
- Network security
- Supply chain security
- Pen testing and Cybersec enablement
- Traffic Encryption
- Access control and MFA

Source: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng

* Non exhaustive list

Digital Operational Resilience Act (DORA - Jan. 25)

Who is concerned:
Financial services industry

What is the objective:
Ensure that banks, insurance companies, investment firms and other financial entities can withstand, respond to, and recover from ICT disruptions, such as cyberattacks or system failures

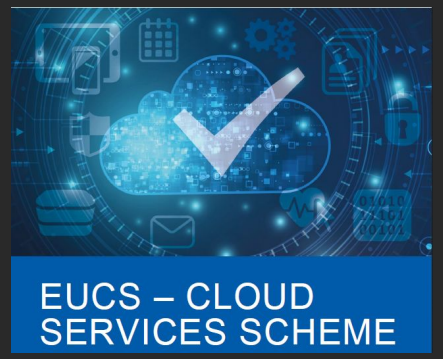
What it requires *:

- Risk management framework, including strategies, policies procedures and tools
- Third party risk management, including multi-vendor and reversibility strategy
- Digital Operational resilience testing, including DRP, risk tests and pen tests
- Incident management, including detection, logging, classification, RCA, and regulatory reporting
- Cyber-threat information sharing

Source: https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en

* Non exhaustive list

EU Cloud Services Scheme (EUCS - TBA)



Who is concerned:
Sovereign cloud service providers

What is the objective:
Harmonise the security of cloud services with EU regulations, international standards, best industrial practices, as well as with existing certifications in EU Member States

What it requires *:

- IAM, including RBAC, strong authentication, credential protection and segregation of admin/customer planes
- Key management and encryption
- SIEM and traffic observability
- Network security and tenant traffic segregation
- Secured supply chain and hardened images
- Continuous logging and monitoring
- Continuous control processes review

Source:
https://www.enisa.europa.eu/sites/default/files/publications/EUCS%20%E2%80%93%20Cloud%20Service%20candidate%20cybersecurity%20certification%20scheme.pdf

* Non exhaustive list

Artificial Intelligence Act (AI act - Aug. 27)

Who is concerned:
Providers and users or AI systems and models

What is the objective:
Promote the uptake of human-centric and trustworthy artificial intelligence (AI), while ensuring a high level of protection (...) against the harmful effects of AI systems

What it requires *:

- Risk-based classification of AI systems
- Transparency on training, validation and testing datasets
- Continuous assessment and risk management during AI system lifecycle
- Appropriate level of cybersecurity
- Compliance evidence available via technical documentation and log retention

Source: https://artificialintelligenceact.eu/

* Non exhaustive list

EU regulations: what they have in common

Resilience

Business continuity and reversibility features have to be considered.

Security

Access controls, network and supply chain security have to be enforced.

Software components security and lifecycle have to be managed.

Reporting

All controls and security processes have to be documented, traceable and continuously monitored.

Transparency and trust with Open Source

Advantages of Open-Source Solutions for Data Sovereignty (1/2)

Flexibility and Independence	• Customize and further develop cloud infrastructure without being dependent on providers. • By using open standards, the risk of vendor lock-in is minimized. • Increases long-term planning security.
Transparency and Security	• A key advantage of open-source solutions is complete transparency. • Open-source technologies allow for independent audits ->increases trustworthiness. • Transparency supports requirements of the General Data Protection Regulation (GDPR)
Economic Independence and Cost-Efficiency	• Reduced costs by eliminating licensing fees and proprietary technologies • Use of open-source solutions promotes the development of technological expertise. • Economic independence and strengthens regional innovation.

Advantages of Open-Source Solutions for Data Sovereignty (2/2)

Criteria for Sovereignty and Security	• A sovereign cloud needs to meet specific criteria beyond technology. • Data sovereignty, GDPR compliance, protection from third-party access, and EU-based data processing. • Open-source solutions supports for independent control and adaptability.
Sustainability and Future-Proofing	• Open standards lead into sustainability. • Future-proof and adaptable to new technologies and requirements. • Long-term evolution of infrastructures without the need for migration processes.

Operational and technology sovereignty

The Dimensions of Digital Sovereignty

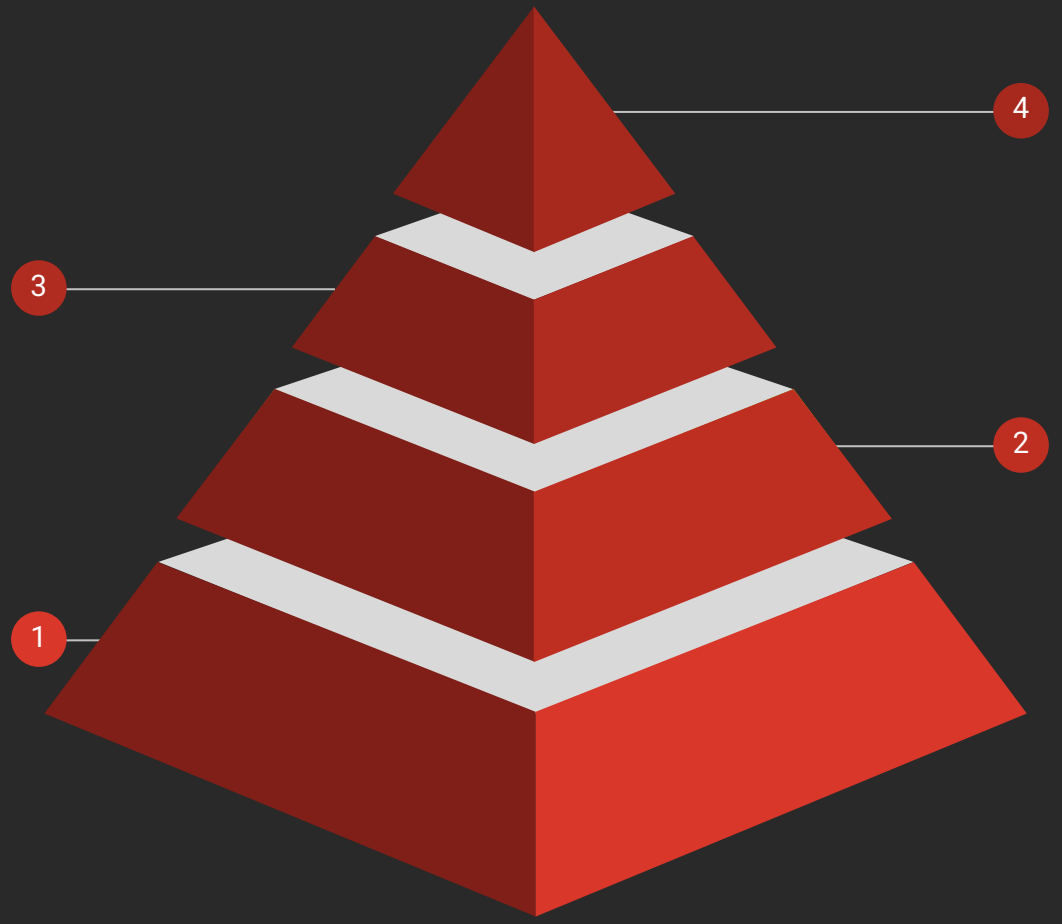
Digital Sovereignty is a continuum, reflecting a range of practices and policies that nations adopt to manage and control their digital assets, data, and technology infrastructure

Operational Sovereignty

Visibility and control over provider operations from provisioning and performance management, to monitoring of physical and digital access, to the infrastructure.

Data Sovereignty

Maintaining control over how data is collected, classified, processed and stored to ensure that data regulations are met



Assurance Sovereignty

Ability to independently verify and assure the integrity, security, and reliability of digital systems and processes including resilience of critical services.

Technical Sovereignty

Running workloads without dependence on a provider's infrastructure or software, and protected from all extra-territorial interference and scrutiny.

Sources:
"Sovereign Clouds and the Digital Sovereignty Imperative: Europe's Quest for Digital Independence" (IDC #EUR149098122, December 2022)
The Evolution of Digital Sovereignty: Moving Beyond Data and Cloud" (Rahiel Nasir, IDC, January 13, 2023)

Digital sovereignty refers to the ability to have control over your own digital destiny – the data, hardware and software that you rely on and create.

Source:
"What is digital sovereignty and why is Europe so interested in it?" (Sean Fleming, World Economic Forum, March 15, 2021)

Definitions according to the Dutch Government

(1) **Digital autonomy** refers to the ability of the central government to operate independently and self-sufficiently in the digital domain. A digitally autonomous government has control over its own digital infrastructures, systems and data without excessive dependence on external parties, in particular foreign entities

Digital Autonomy

(1) **Digital sovereignty,** According to the authors of the report, digital sovereignty goes one step further. It refers to the complete independence and enforceable jurisdiction of the central government over its digital domain, without the possibility for foreign entities to exercise control or influence.

Digital Sovereignty

Source: (1) Digital autonomy is not yet sovereign (Google Translate)

Technology : Information Security for traceability

- **CVE - Common Vulnerabilities and Exposures**
  - Public dictionary of unique CVE-IDs for each disclosed cybersecurity vulnerability.
  - Managed by MITRE and CVE Numbering Authorities (CNAs).
- **CVSS - Common Vulnerability Scoring System**
  - Maps vulnerabilities to severity score (0.0-10.0) and patch priority (None to Critical).
  - Part of risk assessment; Requires context, including threat sources and vectors.
- **SBOM - Software Bill of Materials**
  - List of the components of a software product, available in formats such as CycloneDX and SPDX.
  - Does not indicate whether any component is vulnerable or safe.
- **VEX - Vulnerability Exploitability eXchange**
  - Machine-readable advisory that asserts the status of specific vulnerabilities in a given product.
  - Complements SBOM by providing security relevance of listed components.

https://www.cve.org/
https://www.first.org/cvss/
https://www.cisa.gov/sites/default/files/2023-01/VEX_Use_Cases_Aprill2022.pdf
https://www.oasis-open.org/2022/11/28/common-security-advisory-framework-version-2-0-oasis-standard-is-now-published/
https://cyclonedx.org/
https://spdx.dev/

Technology: Sigstore for security lifecycle

- Sigstore empowers software developers and consumers to **securely sign and verify software artifacts** - source code, release files, container images, binaries, SBOM, playbook, and more to enhance software supply chain security.
- Signing metadata are stored in a tamper-resistant log for **transparency & verification**.

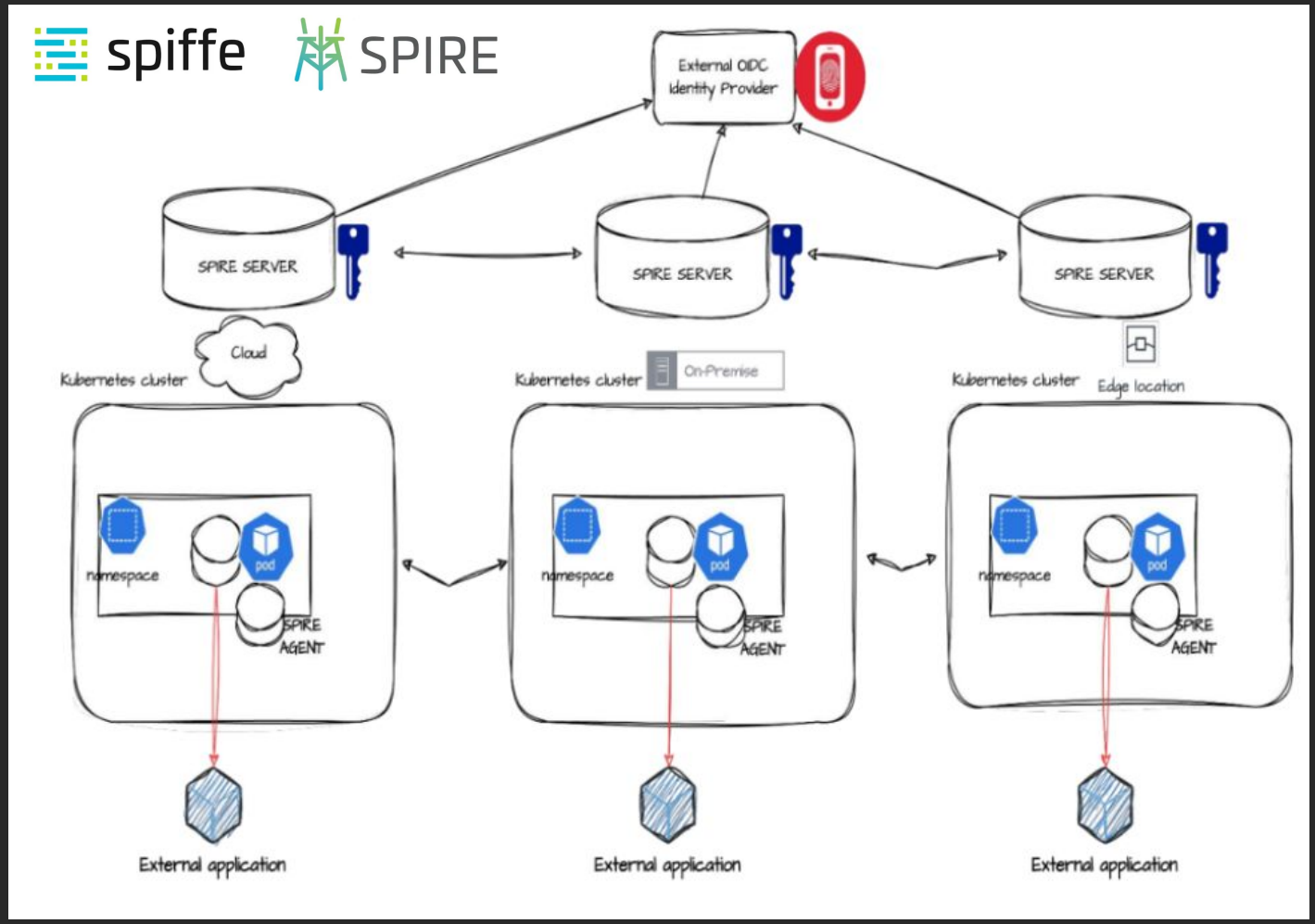
https://www.sigstore.dev/

Key Capabilities:

- Tamper-proof software artifacts with a keyless signing solution
- Sign Git commits with a valid OpenID Connect identity
- Verify authenticity and origin from an immutable ledger
- Build provenance is cryptographically signed
- Establish a non-repudiable chain of custody

Technology: Universal workload identity with SPIFFE/SPIRE

- SPIFFE - Secure Production Identity Framework For Everyone :
  - Defines how cloud native workloads obtain and present short-lived, cryptographically-verifiable identities.
- SPIRE - SPIFFE Runtime Environment:
  - Production-ready implementation of the SPIFFE standards.
  - Agent / server architecture that manages both node and workload attestation for secure SVID issuance.
- CNCF graduated project
- Works on Kubernetes, VMs, serverless, and multi-cloud deployments
- SPIFFE ID (URI) and SVID (certificate) provide a trusted way to identify applications - compared to traditional methods (IP, hostnames, secrets, ...)



https://spiffe.io/

Technology: hybrid cloud reversibility

How long does it take you to move critical applications from one cloud to another?

Key considerations:

- Architect for workload mobility
- Avoid vendor lock-in
- Define your standards:
  - Containerization and Orchestration
  - Open-Source Data Layer
  - Unified Observability and Monitoring
- Hybrid Cloud Connectivity and Identity Management

Technology: upstream reversibility

Can you switch from your open source enterprise infrastructure platform to upstream?

Key considerations:

- Minimal Vendor Lock-in and Community Reliance
- Standardized APIs and Interfaces
- Abstracted Storage and Networking
- Test it - Make it part of you regressions tests

EU Sovereign ecosystem

Why Sovereignty matters: A French Cloud Services Provider Perspective

- **Regulatory compliance:**
  Adherence to European standards (GDPR, NIS2, ..) ensures appropriate data protection and security, while minimizing the risk of sanctions.
- **Risk reduction:**
  Implementation of advanced protections and continuous monitoring reduces the threat of cyber attacks.
- **Guaranteed data sovereignty:**
  Local hosting and compliance with European laws ensure controlled data management and prevent confidentiality risks from foreign regulations.
- **Transparency and control:**
  EU and local certifications ensure cloud service security, transparency, and compliance.
- **Secure local alternatives:**
  Compared to global providers, European cloud providers offer greater autonomy and security while remaining compliant with EU standards.
- **Trust reinforcement:**
  Offering a certified and secure cloud helps build strong, trust-based relationships with clients.

Cloud Sovereignty in Practice: Requirements for French Providers

- In anticipation of the forthcoming EUCS framework, the French CyberSecurity agency (ANSSI) has published the SecNumCloud security standard, which broadly align with the highest assurance level defined under the EUCS.
- Below are some requirements:
  - **Infrastructure security:** Hosting in certified data centers with physical access control and system redundancy.
  - **Data protection:** Encryption of data both in transit and at rest.
  - **System and application security:** Securing containers and orchestrators, management of updates and configurations.
  - **Access and identity management:** Role-based access controls (RBAC) and multi-factor authentication (MFA).
  - I**ncident and risk management:** Security incident response plan. Regular penetration testing and vulnerability assessments.
  - **Regulatory compliance:** Compliance with GDPR, NIS2, and other European regulations. Data hosted in France to ensure sovereignty.
  - **Continuous improvement:** Ongoing monitoring and reassessment of security practices.

As of today, 17 cloud providers based in France (combining IaaS, PaaS and Saas) are compliant

Sovereign Cloud criteria: Example from Germany

A position paper from the Data Protection Conference of the Federal and State Governments outlines "must-have" and "should-have" criteria for sovereign cloud offerings.

Must-have criteria:

- Documentation before contract conclusion and interface documentation
- Transparency regarding future viability
- Processing by providers only on instruction
- Separation by processing
- No risk of third-country access to providers
- Effective legal enforceability
- Provider location and processing in the European Economic Area
- Interchangeability
- Notification in case of a threat to sovereignty
- Possibilities for influence and choice in the offer design
- Transparent product life cycle
- Verifiable quality
- Verification of the software used
- Support for verifications

Should-have criteria:

- Transparency through Open Source and open standards
- Inclusion of sub-processors
- Combinability and modularity
- Feature parity with non-sovereign cloud offerings
- Transparent financing model of the offer
- Certification

DSK
DATENSCHUTZKONFERENZ

Sources:
- Kriterien für Souveräne Clouds

Sovereign Cloud Stack based Cloud offerings

An OSS example - SysEleven

- SysEleven is certified for and utilizes the Sovereign Cloud Stack (SCS)
- Solutions are exclusively hosted in German data centers certified under ISO27001, ensuring compliance with GDPR.
- SysEleven is a member of the Cloud Native Computing Foundation (CNCF) and a certified Kubernetes provider.
- Collaboration with companies like secunet and Bundesdruckerei to provide sovereign cloud solutions for the public sector.
- SysEleven is a new Red Hat Validated Cloud Service Provider (VCSP)
- Ideal for the public sector, system integrators, and operators of critical infrastructure
- Certifications ensure compliance in tenders for the public sector

Wrap up

EU Regulations as a Strategic Imperative:
The EU's new regulations like NIS2, DORA, EUCS, and CRA are not just compliance hurdles but a strategic framework to enhance digital sovereignty, security, and operational resilience across Europe.

The Role of Open Source in Sovereignty:
Open source is a foundational pillar of digital sovereignty, providing transparency, flexibility, and independence from vendor lock-in. This enables organizations to meet regulatory requirements and build trust.

A Holistic Approach to Sovereignty:
Digital sovereignty is a multidimensional concept that goes beyond just data. It encompasses technical, data, operational, and assurance aspects that must be considered together for a truly sovereign cloud ecosystem.

Thank you


linkedin.com/company/red-hat


youtube.com/user/RedHatVideos


facebook.com/redhatinc


twitter.com/RedHat