Tible EU Cloud Sovereignty Framework Assessment

Date: 2026-06-11 | Framework: EU Cloud Sovereignty Framework v1.2.1

88 %

SEAL-3: Digital Resilience

Leeuwenbrug 89
7411 TH Deventer

T +31 85 007 9700
E info@tible.com
W www.tible.com

KVK 27353683
BTW NL8212.30.566B01

Breakdown by Objective

Objective	Score	Weight
SOV-1 Strategic Sovereignty	94%	15%
SOV-2 Legal & Jurisdictional	88%	10%
SOV-3 Data & AI Sovereignty	88%	10%
SOV-4 Operational Sovereignty	100%	15%
SOV-5 Supply Chain Sovereignty	81%	20%
SOV-6 Technology Sovereignty	81%	15%
SOV-7 Security & Compliance	94%	10%
SOV-8 Environmental Sustainability	81%	5%

Leeuwenbrug 89
7411 TH Deventer
T +31 85 007 9700
E info@tible.com
W www.tible.com
KVK 27353683
BTW NL8212.30.566B01

Detailed Answers

Q1.1 [CRITICAL] — SEAL-4

To what extent are the bodies having decisive authority over your cloud services located within EU jurisdiction?

→ All governing bodies are EU-based with no non-EU influence on decision-making

Q1.2 — SEAL-3

What assurances exist against a change of control that could move decision-making outside the EU?

→ Significant protections exist with some residual change-of-control risk

Q1.3 — SEAL-4

To what degree does your organization rely on financing from EU sources, with EU-based investment, jobs, and value creation?

→ Financing entirely EU-sourced; majority of jobs, R&D, and value creation within EU

Q1.4 [CRITICAL] — SEAL-4

How resilient are your operations if a key vendor suspends service or withdraws support?

→ Full operational autonomy — can sustain all services independently of any single vendor

Leeuwenbrug 89
7411 TH Deventer

T +31 85 007 9700
E info@tible.com
W www.tible.com

KVK 27353683
BTW NL8212.30.566B01

Q2.1 [CRITICAL] — SEAL-4

Which legal system governs your cloud provider's operations, contracts, and service delivery?

→ Exclusively EU/EEA law governs all operations and contracts

Q2.2 [CRITICAL] — SEAL-3

What is your degree of exposure to non-EU laws with extraterritorial reach (e.g., US CLOUD Act, Chinese Cybersecurity Law)?

→ Minimal exposure — theoretical risk exists but practical enforcement is mitigated

Q2.3 — SEAL-4

Do legal, contractual, or technical channels exist through which non-EU authorities could compel access to data or systems?

→ No such channels exist — architecturally and contractually impossible

Q2.4 — SEAL-3

Where is intellectual property created, registered, and developed (EU vs. third countries)?

→ Majority of IP activity is EU-based with minor third-country involvement

Leeuwenbrug 89
7411 TH Deventer

T +31 85 007 9700
E info@tible.com
W www.tible.com

KVK 27353683
BTW NL8212.30.566B01

Q3.1 [CRITICAL] — SEAL-3

Does only the customer — not the provider — have effective control over cryptographic access to their data?

→ Customer controls keys with provider holding escrow under strict EU-governed conditions

Q3.2 — SEAL-4

What visibility do you have into when, where, and by whom data is accessed, including auditability of AI model usage?

→ Complete real-time audit trails for all data and AI access under EU-only control

Q3.3 [CRITICAL] — SEAL-4

Is storage and processing strictly confined to EU/EEA jurisdictions with no fallback to third countries?

→ All storage and processing exclusively in EU/EEA — no third-country fallback possible

Q3.4 — SEAL-3

To what extent are AI models and data pipelines developed, trained, hosted, and governed under EU control?

→ Primarily EU-controlled with non-EU dependencies in non-critical AI components

Q4.1 — SEAL-4

How easily can you migrate workloads or integrate with alternative EU-controlled solutions without vendor lock-in?

→ Fully portable — standard formats, open APIs, tested migration paths to EU alternatives

Q4.2 [CRITICAL] — SEAL-4

Can EU operators manage, maintain, and support the technology without requiring non-EU vendor involvement?

→ Full EU operational autonomy — all maintenance performed by EU personnel

Leeuwenbrug 89
7411 TH Deventer

T +31 85 007 9700
E info@tible.com
W www.tible.com

KVK 27353683
BTW NL8212.30.566B01

Q4.3 — SEAL-4

Does an EU-based talent pool exist with the expertise to operate and sustain the service long-term?

→ Deep EU talent pool with full documentation and training programs

Q4.4 — SEAL-4

Is full technical documentation, source code, and operational know-how available to enable long-term autonomy?

→ Complete documentation, source code, and run-books available under EU control

Q5.1 [CRITICAL] — SEAL-3

Where are your critical hardware components manufactured or assembled, and what is their geographic provenance?

→ Majority EU-sourced with documented non-EU components from allied jurisdictions

Q5.2 — SEAL-3

What is the jurisdiction and provenance of firmware and embedded code controlling your hardware?

→ Primarily EU-controlled firmware with documented non-EU components

Q5.3 — SEAL-3

Where and by whom is your software architected, developed, packaged, and distributed?

→ Primarily EU-developed with open-source components under EU-governed distributions

Q5.4 — SEAL-4

What visibility do you have into the entire supplier and sub-supplier chain, including audit rights?

→ Full transparency with contractual audit rights across all supply chain tiers

Leeuwenbrug 89
7411 TH Deventer
T +31 85 007 9700
E info@tible.com
W www.tible.com
KVK 27353683
BTW NL8212.30.566B01

Q6.1 — SEAL-3

To what extent does your solution use well-documented, non-proprietary APIs and open standards?

→ Primarily open standards with minor proprietary extensions documented

Q6.2 — SEAL-3

Is the software accessible under open licenses with rights to audit, modify, and redistribute?

→ Core components open-source; some proprietary add-ons with source available

Q6.3 — SEAL-4

What level of architectural transparency exists, including documentation of data flows and dependencies?

→ Full architectural transparency with published docs, data flows, and dependency maps

Q6.4 — SEAL-3

What is the degree of EU independence in HPC capabilities (processors, accelerators, software ecosystems)?

→ Primarily EU-controlled with some non-EU components under acceptable terms

Q7.1 — SEAL-4

What EU and internationally recognized certifications has your organization attained (ISO 27001, ENISA schemes)?

→ Full certification portfolio including EU-specific schemes (ENISA, C5, SecNumCloud)

Q7.2 [CRITICAL] — SEAL-3

Are your Security Operations Centers and incident response teams operating exclusively under EU jurisdiction?

→ Primary SOC in EU with follow-the-sun handled by EU-allied jurisdictions

Leeuwenbrug 89
7411 TH Deventer

T +31 85 007 9700
E info@tible.com
W www.tible.com

KVK 27353683
BTW NL8212.30.566B01

Q7.3 — SEAL-4

Can security patches be developed and applied independently of non-EU vendors?

→ Full ability to develop and apply patches autonomously with transparent reporting

Q7.4 — SEAL-4

Can EU entities perform independent security and compliance audits with full access?

→ Full audit access granted to EU entities at any time, including source code

Q8.1 — SEAL-4

What energy efficiency measures and targets are in place for your infrastructure (e.g., PUE levels)?

→ Industry-leading PUE (<1.2) with published improvement targets and EU energy audits

Q8.2 — SEAL-3

What circular economy practices do you follow for hardware (reuse, refurbishment, end-of-life)?

→ Active refurbishment and recycling programs for most hardware

Q8.3 — SEAL-3

How transparently do you measure and disclose carbon emissions, water usage, and sustainability indicators?

→ Scope 1/2 reporting with scope 3 in progress; annual sustainability disclosures

Q8.4 — SEAL-3

To what extent is your infrastructure powered by renewable or low-carbon energy sources?

→ Majority renewable (>75%) with credible path to 100%

Leeuwenbrug 89
7411 TH Deventer

T +31 85 007 9700
E info@tible.com
W www.tible.com

KVK 27353683
BTW NL8212.30.566B01