Digital Independence: Why, When and How

A Strategic Briefing for European Organizations — Understanding the legal landscape, evaluating the risks of US cloud dependency, and charting a practical path toward genuine digital sovereignty.

Meet Our Expert Speakers

Thomas Hampel

Product Manager, HCLSoftware

HCLSoftware

Wannes Rams

Cloud Architect, ISW

ISW Huddo

HCL Lifetime Ambassador

CHAPTER 1

What Is Digital Sovereignty?

> "The ability of a state, organization, or individual to control their own digital destiny."

Digital sovereignty has become a boardroom and government priority in less than a decade. It exists at three levels, and organizations that address only one remain exposed.

Data Sovereignty

Control over where data is stored and who can access it.

Technological Sovereignty

Independence from foreign-controlled platforms and infrastructure.

Regulatory Sovereignty

The ability to enforce local laws on digital actors.

THE TRIGGER EVENTS

Why Now? The Forces That Changed Everything

2013 — Snowden

Mass surveillance by US intelligence agencies exposed — the first public wake-up call.

2018 — CLOUD Act

US lawmakers formally codified and expanded compelled access to data worldwide.

2020 — Schrems II

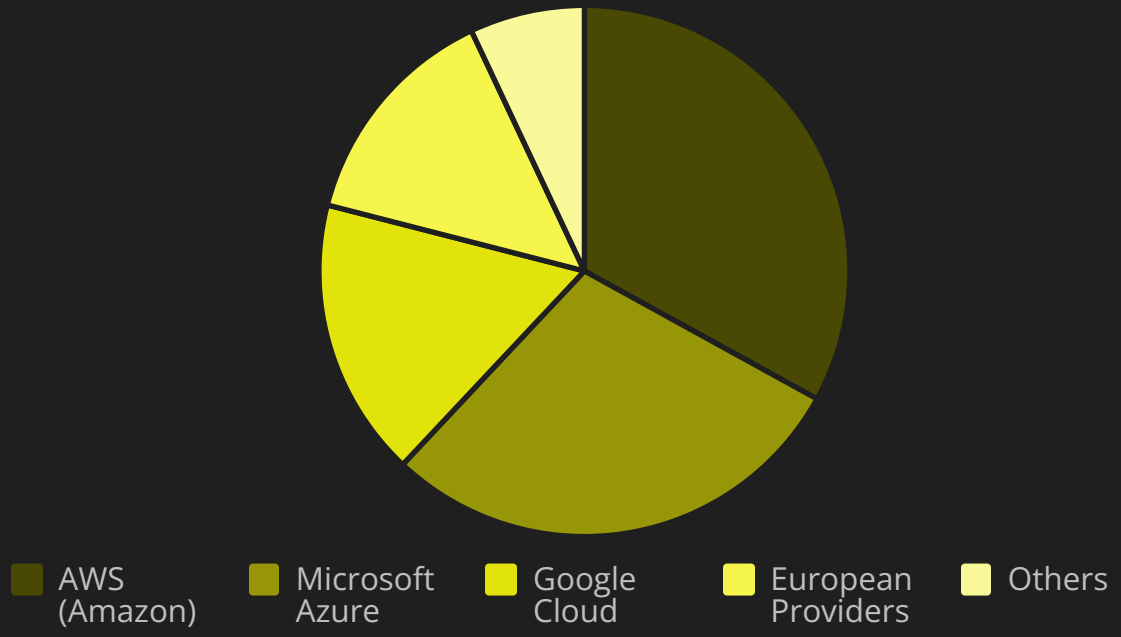
CJEU invalidated Privacy Shield. Every transatlantic transfer mechanism now under scrutiny.

2022–2025

Russia/Ukraine war, US-China tech fragmentation, NIS2, DORA, and AI Act reshape the risk landscape entirely.

The Scale of Dependency

The EU cloud market is structurally dependent on US providers. Once resellers are excluded, effective US infrastructure control likely exceeds 85%, leaving European organizations with little to no negotiating leverage.



What This Means

- EU data subject to US jurisdiction by default
- European organizations hostage to foreign policy decisions
- No viable alternative means zero commercial leverage
- True US dependency likely exceeds 85% when resellers are excluded

CHAPTER 2

The EU Legal Framework

GDPR (2018)

Cross-border transfer restrictions, Arts. 44–46. Fines up to **4% of global annual turnover**.

NIS2 Directive (2024)

Supply chain security, 24h/72h incident reporting, and **personal executive liability** for cybersecurity failures.

EU AI Act (2025)

Risk-based AI governance with **extraterritorial effect** on any AI system used within the EU.

Data Act (2024)

Cloud switching rights and data portability, Arts. 23–31 — attacking vendor lock-in at law.

DORA (2025)

Financial sector digital resilience. Cloud **concentration risk rules** — regulators can require hyperscaler diversification.

Digital Markets Act (2022)

Gatekeeper obligations and interoperability mandates targeting dominant platform providers.

Case Law — The Schrems Saga

> Schrems III is coming. The Data Privacy Framework is already under legal challenge. History says it will not survive.

Schrems I — 2015

Safe Harbor invalidated. US surveillance incompatible with EU fundamental rights.

Schrems II — 2020

Privacy Shield invalidated. SCCs require case-by-case Transfer Impact Assessments.

Meta / DPC — 2023

€1.2 billion fine. SCCs alone deemed insufficient for US transfers.

DPF — 2023

Current mechanism. Already challenged by NOYB. Schrems III expected.

Regulatory Pressure Points

Threat Vectors & Regulatory Responses

→ US CLOUD Act reach

DPF challenge, national cloud mandates emerging across member states.

→ AI training on EU data

EU AI Act and GDPR Article 22 create enforceable obligations around automated processing.

→ Supply chain attacks

NIS2 and the Cyber Resilience Act impose ongoing security update obligations on vendors.

→ Critical infrastructure

DORA mandates cloud concentration risk management — regulators can compel diversification.

National Frameworks

- **BSI C5** 🇩🇪 — German cloud security catalogue. CLOUD Act risk explicitly noted.
- **SecNumCloud** 🇫🇷 — French qualification. US providers **structurally excluded** from top tier — a deliberate policy choice.
- **EUCS** — EU Cloud Certification Scheme. Sovereign tier under active political debate.
- **GAIA-X** — European federated data infrastructure. Monitor but do not wait for it.

CHAPTER 3

Organizational Risk Reality

⚖️ Legal Risk

- Transfer Impact Assessments required for every US tool
- €2.1 billion+ in GDPR fines in 2023 alone
- Personal executive liability under NIS2 — board members face individual sanctions

🔧 Operational Risk

- Vendor can terminate services with minimal notice (Russia sanctions precedent)
- Foreign government can access data without notifying you or EU authorities
- Zero commercial leverage when no viable alternative exists

🌐 Reputational Risk

- Customers and partners asking "where is my data?"
- Public sector procurement now requiring sovereignty attestation
- ESG frameworks beginning to incorporate digital sovereignty scores

The CLOUD Act — How It Actually Works

⚠ National Security Letters are issued by the FBI without court approval and routinely carry indefinite gag orders. Your DPA notification promise is legally void in precisely the most sensitive scenarios.

The Hyperscaler Response

Vendor	Offering	Status
Microsoft	EU Data Boundary + Cloud for Sovereignty	Live since 2023
Google	Sovereign Controls + Partner Model	Live since 2023
Amazon	AWS European Sovereign Cloud	Building — 2024 onwards

> "Your data stays in Europe. You maintain control." — *The Promise*

> "The parent company remains a US corporation subject to US law — regardless of where the servers are." — *The Legal Reality*

Why Sovereign Offerings Don't Fix This

Microsoft Ireland

Owned by → **Microsoft Corporation (US)** → CLOUD Act applies. A US order goes to Redmond's legal department, not to Dublin.

Google Cloud EMEA

Owned by → **Alphabet Inc (US)** → FISA 702 applies. Corporate EMEA branding does not alter the ownership chain.

AWS EU

Owned by → **Amazon.com Inc (US)** → NSL applies. The European Sovereign Cloud is still a wholly-owned US subsidiary.

⊗ No subsidiary arrangement breaks the legal chain. No EU data center changes corporate jurisdiction. No contractual promise overrides a US court order.

CHAPTER 4

Hyperscaler Sovereign Offerings — Reality Check

Microsoft EU Data Boundary

✅ EU data at rest and in transit
✅ Improved GDPR operational posture
❌ CLOUD Act immunity — not provided
❌ FISA 702 immunity — not provided
❌ Non-EU staff (UK, India, Australia, US) retain access pathways

"Microsoft remains a US company subject to US law." — Microsoft Privacy & Compliance, 2023

Google Sovereign Controls

✅ Encryption key management
✅ Region restriction
✅ Access transparency logging
❌ Google controls the key management interface — CLOUD Act can target the interface
❌ Non-EU staff retain potential access pathways

AWS European Sovereign Cloud

✅ EU-only data storage claimed
✅ EU-based operational staff claimed
❌ Wholly-owned subsidiary of Amazon.com Inc — CLOUD Act, FISA 702, NSLs all apply
❌ **Not yet operational** — cannot be relied on for decisions made today
❌ EUCS sovereign tier qualification unresolved

The FISA Section 702 Problem

CLOUD Act vs. FISA 702

Dimension	CLOUD Act	FISA 702
Purpose	Law enforcement	Intelligence gathering
Targets	Known suspects	Foreign nationals — your staff and customers
Court	Federal court	Secret FISC
Notification	Sometimes	Never

Why This Is Critical

- Schrems II was **specifically about FISA 702** — CJEU found it incompatible with EU fundamental rights
- DPF did not reform or limit FISA 702 — it only created a redress mechanism
- No hyperscaler sovereign offering addresses FISA 702 exposure
- DPF is the only current mitigation — and it is already legally challenged

The Contractual Promise Gap

> "We will notify you if we receive a government request for your data **unless prohibited by law.**"

What Actually Happens

1. Warrant plus gag order served on US headquarters
2. Gag order legally prohibits disclosure of the warrant's existence
3. Company **cannot** notify you — even if they want to
4. Data is produced to US authorities
5. You never know it happened

⊗ **The critical flaw:** "Unless prohibited by law" — gag orders ARE prohibited by law. The notification promise is void in precisely the most sensitive cases. Ask your compliance team: does your current TIA for Microsoft 365 account for this?

What Regulators Actually Say

ANSSI / SecNumCloud 🇫🇷

US-controlled providers **cannot** achieve the highest qualification tier. Explicit policy — not ambiguity. Deliberately excludes non-EU-jurisdiction providers.

BSI C5 🇩🇪

CLOUD Act risk explicitly noted. Not mitigated by BSI certification. Microsoft 365 restricted for certain German government data categories.

French Council of State (2022)

Azure suspended for national health data. CLOUD Act specifically cited as the **disqualifying factor** — the most significant sovereignty precedent in EU case law.

EDPB Position

Transfer Impact Assessments must explicitly account for law enforcement access rights in the destination country — including CLOUD Act and FISA 702.

The Sovereign Cloud Verdict

✅ What It Gives You

- EU data residency
- Improved GDPR operational compliance
- Reduced — not zero — external staff access
- Better audit logging
- A more defensible procurement narrative

❌ What It Does NOT Give You

- CLOUD Act immunity
- FISA 702 immunity
- Guaranteed breach notification — gag orders void this
- SecNumCloud qualification
- True jurisdictional independence
- Legal certainty for Transfer Impact Assessments
- Protection if DPF is invalidated

> **Sovereign cloud from US hyperscalers is a compliance improvement. It is not a sovereignty solution.**

Introducing

The Sovereign Cloud News Channel

Your Host: Thomas

Last year at Engage we had this...

Trump's sanctions on ICC prosecutor have halted tribunal's work

1 of 5 | Karim Khan, Prosecutor of the International Criminal Court looks up prior to a press conference in The Hague, Netherlands, July 3, 2023. (AP Photo/Peter Dejong, File)

BY MOLLY QUELL

Updated 11:26 AM GMT+2, May 15, 2025

Leer en español

Add AP News on Google | Share

THE HAGUE, Netherlands (AP) — The International Criminal Court 's chief prosecutor has lost access to his email, and his bank accounts have been frozen.

This year it continues...

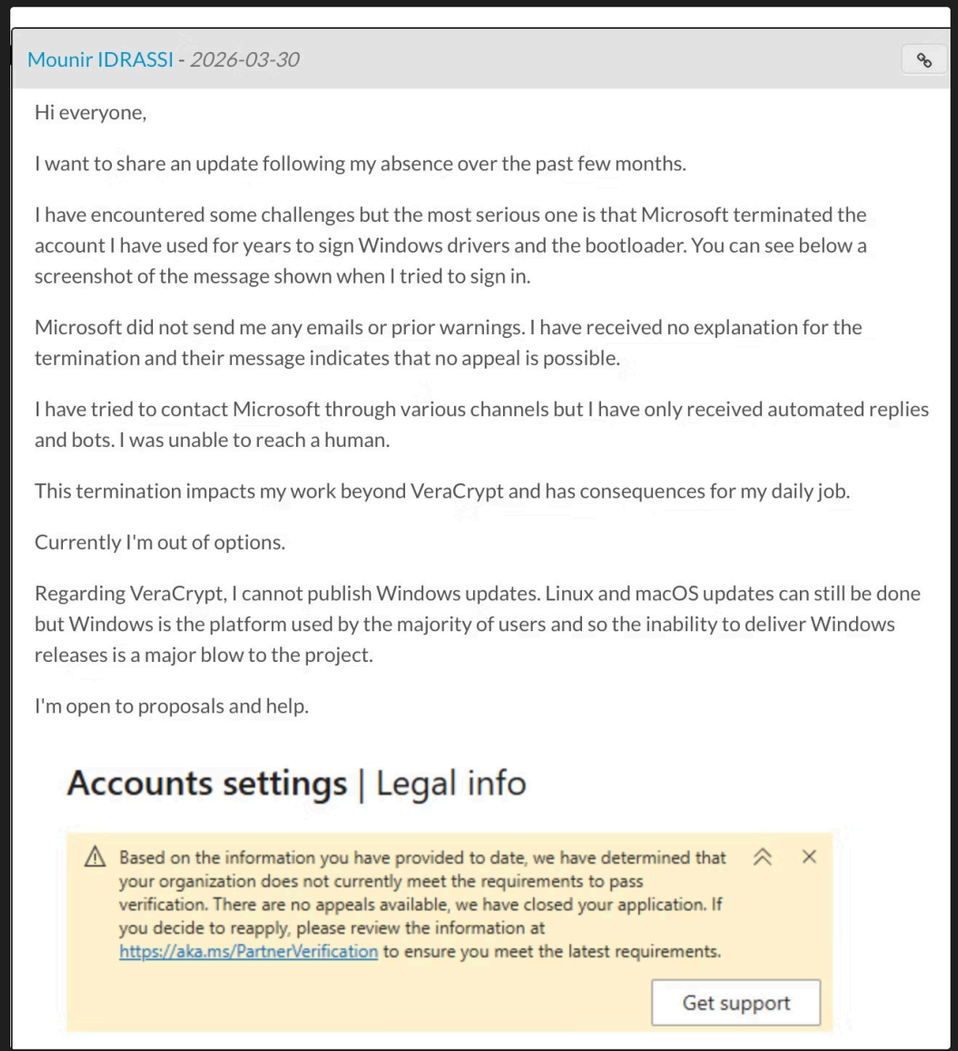
Luz del Carmen Ibáñez, the Peruvian ICC judge sanctioned by Donald Trump's government

Programa Especial - Luz del Carmen Ibáñez, la jueza peruana de la CPI sancionada por el gobierno de Donald Trump

Digital Kill Switch

Digital Kill Switch – also works great for businesses

Locked out, can't provide updates anymore



Mounir IDRASSI - *2026-03-30*

Hi everyone,

I want to share an update following my absence over the past few months.

I have encountered some challenges but the most serious one is that Microsoft terminated the account I have used for years to sign Windows drivers and the bootloader. You can see below a screenshot of the message shown when I tried to sign in.

Microsoft did not send me any emails or prior warnings. I have received no explanation for the termination and their message indicates that no appeal is possible.

I have tried to contact Microsoft through various channels but I have only received automated replies and bots. I was unable to reach a human.

This termination impacts my work beyond VeraCrypt and has consequences for my daily job.

Currently I'm out of options.

Regarding VeraCrypt, I cannot publish Windows updates. Linux and macOS updates can still be done but Windows is the platform used by the majority of users and so the inability to deliver Windows releases is a major blow to the project.

I'm open to proposals and help.

Digital Kill Switch – also works great for businesses

WireGuard VPN developer can’t ship software updates after Microsoft locks account

[WireGuard VPN developer can't ship software updates after Microsoft locks account | TechCrunch]

LinkedIn Is Illegally Searching Your Computer

Microsoft is running one of the largest corporate espionage operations in modern history.

https://browsergate.eu

California Privacy Audit

A Legal Minefield that Puts Users at Risk

webXray California Privacy Audit | A Legal Minefield that Puts Users at Risk

Ex-Microsoft engineer believes Azure problems stem from talent exodus

The cloud service's woes reflect a crisis made worse by AI – under-investment in people

https://www.theregister.com/2026/04/04/azure_talent_exodus/

German implementation of eIDAS will require an Apple/Google account to function

Sovereignty - Some do it Right...

France's plan: Away from Windows, towards Linux

By autumn 2026, each ministry – including subordinate authorities – must present its own roadmap

numerique.gouv.fr

16. September 2025 - Armed Forces ditching Microsoft Office

- **Austrian Armed forces ditching Microsoft Office in favour of LibreOffice**
- 16.000 Workstations
- *It was very important for us to show that we are doing this primarily (...) to strengthen our digital sovereignty, to maintain our independence in terms of ICT infrastructure and (...) to ensure that data is only processed in-house*"
- More than five man-years of coding have been given back to the LibreOffice community.

https://oe1.orf.at/programm/20250916/807304/Freie-Software-fuer-das-Bundesheer

2. October 2025 – Schleswig-Holstein

German State is ditching Microsoft

Schleswig-Holstein
Der echte Norden

- Projects
  - Exchange -> OpenXChange
  - Outlook -> Thunderbird
  - MS Office -> LibreOffice
  - Windows -> Linux
  - Telekom Flexport -> OSKAR
  - Active Directory -> OpenSource (t.b.d)

- Admiting there are some Problems:

  https://www.heise.de/en/news/Open-source-migration-Schleswig-Holstein-s-digital-minister-admits-problems-10667872.html

Perception

- ***We need Microsoft Office because of Macros … and Pivot Tables“***
  - Really?
  - Excel 4.0 Macros still actively used by current malware **https://blog.reversinglabs.com/blog/excel-4.0-macros**
  - You dont need MS Office for Pivot Tables: Ref.: **https://books.libreoffice.org/en/CG71/CG7108-PivotTables.html**
    - **https://www.youtube.com/watch?v=nH7J4Wr3nVs**

„OpenXChange is Open Source version of Microsoft Exchange“

- Don‘t be fooled by the Name!
- It‘s not free of charge
- It‘s not (fully) open source
- Itneeds (a lot!) moreresourcesthan Domino

OpenXchange	Domino
200 User	2000 User
10 vCPU	8 vCPU
58 GB RAM	16 GB RAM
660 GB Storage	much less (DAOS)

17. October 2025 – Go Sovereign and Save 75%

Just moving out of AWS Infrastructure...

- AWS è Hetzner
- Save 75%
- While increasing capacity // getting more

https://biggo.com/news/202510171914_Startups-Ditch-AWS-for-Hetzner-Save-75-Percent

20. October 2025 – Nuclear Weapon Manufacturer Hacked

Actually 22. July 2025, but just now in the news

- US nuclear weapons manufacturer..
  ... hacked via **SharePoint** flaws
- Critical (Non-Nuclear parts) production site affected

https://www.csoonline.com/article/4074962/foreign-hackers-breached-a-us-nuclear-weapons-plant-via-sharepoint-flaws.html


DO NOT BLEACH
DO NOT MACHINE DRY
DO NOT IRON
LAVER A LA MAIN A L'EAU TIEDE
SAVON DOUX
ETENDRE POUR SECHER
NE PAS JAVELLISER
NE PAS SECHER A LA MACHINE
NE PAS REPASSER
NOUS SOMMES DESOLES QUE
NOTRE PRESIDENT SOIT UN IDIOT.
NOUS N'AVONS PAS VOTE POUR LUI
This is a clothing label from a small American company that sells their product in France. Here's the translation of the French part of the label.
Wash with warm water.
Use mild soap.
Dry flat.
Do not use bleach.
Do not dry in the dryer.
Do not iron.
We are sorry that our president is an idiot.
We did not vote for him.

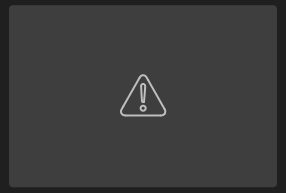
And now, the

Sovereign Cloud Weather Forecast

With Wannes

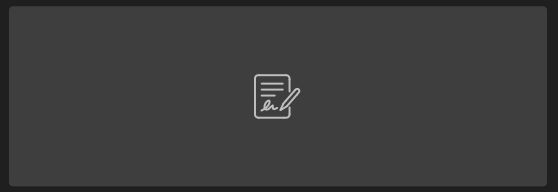
CHAPTER 5 — THE PATH FORWARD

Your Strategic Options



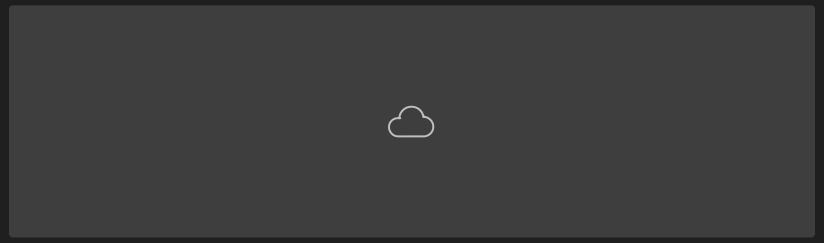
Status Quo

US cloud as-is. High legal risk. Increasing enforcement exposure. No strategic defensibility.



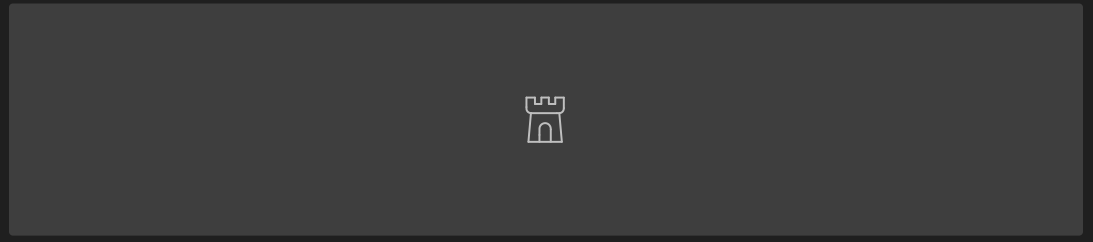
Contractual

SCCs and TIAs updated. Medium legal risk. Vulnerable to Schrems III invalidation overnight.



Operational Sovereignty

EU-region deployment plus EU cloud providers. Improving compliance. **Minimum viable target** for regulated organizations.



Architectural Sovereignty

EU-controlled infrastructure end-to-end. Strong sovereignty. Target for public sector, healthcare, finance, and defense.

Vendor Sovereignty Checklist

- [ ] **Is the vendor's parent company subject to CLOUD Act?**
  Jurisdiction follows the parent, not the subsidiary or data center location.

- [ ] **Where is operational control — not just where data is stored?**
  Data residency and operational control are different things. Both matter.

- [ ] **Who holds the encryption keys — and on whose infrastructure?**
  External key management only helps if the interface itself is not subject to US orders.

- [ ] **Are sub-processors EU-based or adequately protected?**
  A sovereign primary vendor can be undermined by a non-sovereign sub-processor.

- [ ] **Is the infrastructure hosted on an EU-headquartered cloud provider?**
  Application-layer sovereignty with hyperscaler infrastructure is a significant residual gap.

CHAPTER 6 — THE SOLUTION

Enter HCLSoftware

Dimension	US Hyperscalers	HCLSoftware
Data jurisdiction	US — CLOUD Act applies	HCLSoftware doesn't have your data
FISA 702	Applicable	Not applicable
Business Model	Data is the product	Software is the product
Deployment	Cloud-first, own infrastructure	On-prem / Private / EU cloud / Hybrid
Lock-in	High — proprietary formats	Lower — open standards
Staff Access	Global including UK, AU, IN, US	EU-deployable with EU-only operations
Data Use	AI training and service improvement	Minimal by design

HCLSoftware — The Sovereign Stack

Collaboration & Productivity

HCL Notes / Domino | HCL Domino Workspace | HCL Verse | HCL Sametime Chat & Meetings | HCL Connections

Content & Application Layer

HCL DX | HCL Leap | HCL Volt MX — low-code development fully under customer control

Security & Endpoint Layer

HCL AppScan | HCL BigFix — EU-deployable endpoint management closing the frequently overlooked sovereignty gap

Infrastructure Layer

Your EU data center or EU-headquartered cloud provider — OVHcloud, Deutsche Telekom, Hetzner, IONOS, Scaleway

CHAPTER 7

Focusing In — collab.cloud

The Full Product Set

- Notes / Domino
- Domino Workspace — modern browser-based interface
- Sametime Chat & Meetings
- HCL Verse — Email
- HCL Connections
- HCL Leap — Low-code forms and apps
- IdP as a Service — sovereign authentication
- Nomad Web

The Proposition

Hosted. Managed. Subscription-based.

> Operational sovereignty + EU-only operations + no CLOUD Act + managed simplicity + complete stack from identity to collaboration.

For organizations running on-premises Lotus, IBM, or HCL Domino looking to modernize without migrating to M365 — this is the natural path that preserves existing applications, workflows, and institutional knowledge.

collab.cloud vs. Hyperscalers

Feature	Microsoft 365	Google Workspace	collab.cloud
CLOUD Act exposure	⚠️ Yes	⚠️ Yes	✅ No
FISA 702 exposure	⚠️ Yes	⚠️ Yes	✅ No
EU data residency	⚠️ Premium add-on	⚠️ Limited	✅ Standard
EU-only staff access	⚠️ Not guaranteed	⚠️ Not guaranteed	✅ Committed
Vendor AI data use	⚠️ Yes	⚠️ Yes	✅ Minimal
On-prem migration path	❌ No	❌ No	✅ Yes
Air-gap capable	❌ No	❌ No	✅ Yes (on-prem)
Sovereign IdP included	⚠️ US-controlled	⚠️ US-controlled	✅ Included
SecNumCloud-compatible path	❌ Excluded	❌ Excluded	✅ Possible

CHAPTER 8 — THE BUSINESS CASE

The Business Case for Digital Independence

Cost of Non-Compliance

Risk Event	Potential Impact
GDPR major breach fine	€20M or 4% of global annual turnover
DPA enforcement order	Immediate suspension of data flows
Schrems III invalidation	Loss of transfer mechanism overnight
Public sector disqualification	Lost procurement opportunities
Executive NIS2 liability	Individual fines and personal sanctions

Cost of Sovereignty with collab.cloud

- Predictable SaaS subscription — competitive with M365 for many profiles
- Reduces TIA and legal review overhead
- Eliminates ongoing CLOUD Act remediation project costs
- Removes non-EU staff access audit burden

> Digital independence is a competitive differentiator, not just a compliance cost.

CHAPTER 9 — NEXT STEPS

Call to Action

1

🔴 0–30 Days

Audit all US-based SaaS tools processing personal data. Map non-EU staff access. Review whether TIAs are current. Identify three highest-risk workloads.

2

🟡 30–90 Days

Pilot one team or workload. Compare DPA terms. Assess your IdP sovereignty gap — are you using Azure AD or Google Identity for SSO?

3

🟢 90–180 Days

Define organizational digital independence policy. Build migration roadmap for highest-risk workloads. Align sovereignty programme with NIS2. Select EU cloud provider for infrastructure layer.

APPENDIX A

Legal References

Reference	Summary
GDPR (EU) 2016/679	Core EU data protection law — cross-border transfer restrictions, fines up to 4% global turnover
EU Data Act 2023/2854	Data sharing, cloud switching rights and portability obligations
NIS2 Directive 2022/2555	Cybersecurity obligations, supply chain security, executive personal liability
EU AI Act 2024/1689	Risk-based AI governance with extraterritorial reach into EU market
DORA (EU) 2022/2554	Financial sector digital resilience — cloud concentration risk rules
US CLOUD Act 2018 — 18 U.S.C. § 2713	US compelled data access — location of data irrelevant by statute
FISA Section 702 — 50 U.S.C. § 1881a	US intelligence collection targeting foreign nationals via US companies
CJEU C-362/14 — Schrems I — 2015	Safe Harbor invalidated — US surveillance incompatible with EU rights
CJEU C-311/18 — Schrems II — 2020	Privacy Shield invalidated — SCCs require case-by-case TIA
Meta DPC Decision 2023	€1.2 billion fine — SCCs alone deemed insufficient for US transfers
Google Analytics DPA Decisions 2022	US analytics transfers ruled illegal by AT/FR/IT data protection authorities
French Council of State No. 452668 — 2022	Azure suspended for health data — CLOUD Act explicitly cited as disqualifying factor

APPENDIX B

Glossary of Key Terms

CLOUD Act

US law compelling US companies to produce data regardless of where it is stored. 18 U.S.C. § 2713.

FISA 702

US intelligence law authorizing collection targeting foreign nationals via US companies. Secret court proceedings.

Five Eyes

Intelligence-sharing alliance: US, UK, Canada, Australia, New Zealand. Staff access from any member state creates exposure pathways.

DPF

EU-US Data Privacy Framework — current adequacy decision from 2023. Under legal challenge by NOYB.

SCC

Standard Contractual Clauses — GDPR-approved mechanism for international data transfers. Requires Transfer Impact Assessment post-Schrems II.

TIA

Transfer Impact Assessment — required analysis before transferring personal data outside the EEA. Must account for CLOUD Act and FISA 702.

DPA

Data Processing Agreement required by GDPR Article 28 — or Data Protection Authority (the supervisory body).

IdP

Identity Provider — the system managing authentication, SSO, MFA, and directory services. A commonly overlooked sovereignty gap.

BigFix

HCLSoftware endpoint management platform. EU-deployable. NIS2-relevant. Closes the endpoint sovereignty gap.

Domino Workspace

Modern browser-based interface layer for HCL Domino environments. Modernizes user experience without compromising sovereignty.

SecNumCloud

French ANSSI cloud security qualification. US-jurisdiction providers structurally excluded from highest tier — deliberate policy choice.

BSI C5

German Federal Office for Information Security cloud security catalogue. CLOUD Act risk explicitly noted — not mitigated by certification.

EUCS

EU Cloud Certification Scheme — sovereign tier under active political debate. Whether EU-control requirement is retained has major downstream implications.

GAIA-X

European initiative for federated, interoperable data infrastructure. Monitor development but do not defer sovereignty decisions waiting for it.