CIONET SESSION REPORT

Digital Sovereignty: Moving from Illusion to Strategic Reality

A reflection on the CIONET session of 23 June 2026

AUTHOR Steven De Schrijver, Partner, Allegiance Law

OCCASION CIONET: The Sovereignty Play, 23 June 2026

AUDIENCE Chief Information Officers and the CIONET Community

CLASSIFICATION For CIONET CIO Community

ALLEGIANCE LAW

About this Article

Last Tuesday evening, I had the pleasure of joining Luc Hendrikx, CEO of CIONET, for what turned into one of the most energising conversations I have had on stage in recent memory. The questions were sharp, the room was engaged, and the topic of digital sovereignty turned out to be far more urgent and far less theoretical than many expected walking in. For those who were there, I hope this article captures and extends what we discussed. For those who could not make it, I hope it gives you something genuinely useful to take back to your organisation.

The Gap Nobody Talks About

We opened with what I consider the most underappreciated problem in enterprise IT governance: the gap between perceived control and actual control. In my experience, that gap is almost never where people expect it. CIOs feel in control because a contract has been signed, the SLA looks solid, the GDPR checkbox is ticked, and the dashboard is green. But control on paper and control in practice are two very different things.

The real exposure typically sits three layers down from the contract itself. It lives in the subcontractor chain that was never fully negotiated. It lives with the support engineer operating from another jurisdiction who holds privileged technical access to your environment for routine maintenance. And it lives inside the cloud provider's own internal architecture; a control plane you did not design and cannot fully audit. The CIO controls the relationship with the vendor. What many do not control is what that vendor's own suppliers, infrastructure, and legal obligations expose them to. That is the illusion, and it is a comfortable one precisely because the contracts are usually professionally drafted and sincerely meant.

A clause that says 'data will be hosted in the EU' may be entirely accurate and legally enforceable. But it says nothing about who can access that data, under which legal regime, and through which support or subprocessor channels. The contract provides a comfortable sense of compliance. The technical reality (access paths, encryption architecture, key management) can tell a completely different story. The conversation between legal and procurement on one side, and technical architects on the other, is almost always the missing link.

Redefining Sovereignty

I urged the room to stop using the word 'sovereignty' as a compliance term and start using it as a resilience and negotiation term. Strip away the political connotation, the notion that everything must be European or that hyperscalers must be replaced with domestic alternatives. That framing is neither accurate nor realistic for most organisations. Using a US hyperscaler is not inherently incompatible with Belgian or EU requirements. What matters is whether the overall legal environment, combined with the right contracts and technical measures, provides adequate protection for the specific data and processing activities involved.

What sovereignty actually means, in practical terms, is this: do you retain the ability to change your mind? Can you switch providers, renegotiate, move workloads, or recover from a disruption without your business grinding to a halt? Once you frame it that way, sovereignty stops being a legal checkbox and becomes a genuine business capability that can be placed in the same category as disaster recovery or business continuity. A CIO who can credibly say 'we could move thirty percent of our critical workloads within ninety days if we had to' holds a fundamentally stronger negotiating position with every vendor at the table, commands better pricing leverage, and gives a board the kind of reassurance that actually sticks. That is the strategic lever.

The US CLOUD Act: The Risk That Rarely Makes It Into the Contract

One theme that generated significant discussion after the session was the extraterritorial reach of US law, and specifically the Clarifying Lawful Overseas Use of Data Act of 2018, better known as the CLOUD Act. This is worth addressing head-on, because it illustrates precisely why data residency alone is an insufficient measure of control.

The CLOUD Act allows US authorities to compel providers under US jurisdiction to hand over data in their possession, custody, or control, regardless of where that data is physically stored. A server in Brussels, operated by a company subject to US jurisdiction, can still be reachable by US law enforcement entirely independently of where the hardware sits. We even saw a major hyperscaler acknowledge in 2025 that its own EU data boundary commitments do not fully shield data from this kind of access. That is not a conspiracy theory; it is the provider itself being transparent about the limits of geography as a control mechanism.

It is worth being precise here: the CLOUD Act primarily addresses law enforcement access. Separate frameworks, such as FISA Section 702, raise distinct questions around foreign intelligence surveillance. But the combined picture reinforces the same core message: when a vendor tells you that your data is hosted in Belgium, you should smile, say thank you, and then ask the follow-up question: who can access this data, from where, and under what legal process, regardless of where it sits? That is the question that actually matters. Residency is a location. Sovereignty is about control over access.

Following the Schrems II judgment, European regulators have been clear that Standard Contractual Clauses alone are insufficient. Organisations must carry out proper Transfer Impact Assessments and implement supplementary measures where needed. The possibility of foreign government access is one of the factors that must be considered in those assessments, and the data controller remains accountable for demonstrating that adequate protection is in place.

What the Regulatory Landscape Is Actually Telling Us

We then worked through the regulatory alphabet (NIS2, DORA, the Data Act, the AI Act, and the newly proposed CADA) and I tried to cut through the complexity to isolate the single message they collectively send: you can no longer outsource accountability.

NIS2, which has been in force in Belgium since October 2024, extends well beyond traditional critical sectors and explicitly brings the supply chain into scope. Organisations are now expected to assess and manage the cyber risk of the vendors they depend on, not merely their own internal systems. DORA, fully applicable since January 2025, changed sourcing fundamentally for financial institutions by requiring concrete exit strategies, concentration risk analysis, and active board-level oversight of ICT risk, none of which can be delegated away. The Data Act, in force since September 2025 and

probably the most underrated of the frameworks for CIOs, directly attacks vendor lock-in by mandating real cloud-switching rights and interoperable export formats. And CADA, the Cloud and AI Development Act proposed by the Commission in June 2026, adds a tiered sovereignty assurance framework on top, with four levels of assurance for cloud and AI services that place progressively stronger demands on interoperability, migration planning, supply chain transparency, and exit readiness. It is not yet binding law, but it signals clearly where European public procurement, and by extension the whole market, is heading.

The shared implication of all these frameworks is equally clear: when a major provider suffers an outage or a security failure, the regulator does not accept 'our cloud provider had a problem' as a defence. Regulatory accountability for the service, for the data, and for the continuity of business operations stays with the organisation and ultimately with the board. Contractual remedies against the provider may help with financial recovery. They do not transfer regulatory liability. The question 'who is responsible if this goes down?' must be answered before the contract is signed, and the answer must describe what your organisation will do, not merely what the vendor has promised.

Where Sovereignty Actually Lives: Encryption and Access Control

The most substantive part of our conversation concerned the practical architecture of real control, and the audience questions after the session pushed even deeper into the technical dimensions. So let me be specific.

Strong encryption is one of the most effective safeguards available, but only when properly implemented. Encryption that the provider manages end-to-end is good security hygiene. It is not sovereignty, because the provider holds both the lock and the key. What you need is a setup where the cryptographic keys are controlled by you or by a trusted third party in your jurisdiction, so that even if someone gains access to the storage layer, the data is unreadable without your key.

Two models are worth understanding clearly. Bring Your Own Key, or BYOK, allows organisations to generate and manage their encryption keys while still leveraging the provider's key management infrastructure. It delivers greater control and governance without sacrificing too much operational convenience, though depending on the implementation the provider may still participate in certain key operations. Hold Your Own Key, or HYOK, offers stronger separation by keeping keys entirely outside the provider's environment, typically in customer-managed hardware security modules. The cloud service can request cryptographic operations without ever possessing the keys. This provides meaningfully better protection for highly sensitive workloads, though it introduces additional complexity and integration requirements. The marketing language between these two models is often blurred, so it is worth pressing your provider directly on which one they actually offer and what the technical boundaries are.

It is equally important to recognise what encryption does not cover. Even with strong key management, providers may still process metadata, logs, identity information, configuration data, and operational telemetry. Encryption delivers the best results when combined with robust access controls, identity management, zero-trust principles, continuous monitoring, and data minimisation. It is a powerful layer in a broader strategy, not a complete solution on its own.

Second, privileged access management: full visibility into who on the provider's side can technically reach your environment, real-time notifications when that access is used, and ideally the ability to approve or deny it. This is the access path that is invisible in most contracts but very real in practice.

Third, and this is the one most often forgotten, ensure that these technical guarantees are explicitly reflected in the contract, with audit rights that allow you to verify them. A technical capability that exists but is not contractually guaranteed can be quietly downgraded in a future service update, leaving you with no recourse.

Exit Clauses: From Legal Boilerplate to Strategic Instrument

The audience questions after the session also touched on a topic that deserves considerably more attention than it typically receives: exit clauses, and what it actually takes to make them work.

Exit provisions (sometimes called termination assistance, reversibility clauses, or migration provisions) have moved from being a contractual nicety to an essential safeguard. They spell out how an organisation can end a relationship, retrieve its data, transition workloads, and keep the business running. A well-crafted exit framework is one of the most direct contractual expressions of digital sovereignty, because it determines whether your technology choices are genuinely reversible or merely theoretical.

In practice, exit plans fall apart in three predictable ways. The clause exists on paper but was never tested, so the ninety-day exit window in the contract turns out to be wildly unrealistic given the actual data volumes and integration dependencies. The data is technically exportable but returned in a format that is practically unusable since you get a pile of data, not a working system. And the applications and integrations built on top of the platform are themselves the lock-in, even when the underlying data is portable. Proprietary SaaS features, deeply coupled workflows, and custom development built on platform-specific services can trap an organisation far more effectively than the data itself.

The regulatory environment is now directly addressing this. The Data Act creates real obligations around standardised, interoperable export formats and explicitly prohibits contractual, technical, or commercial barriers designed to prevent switching. DORA requires financial entities to maintain concrete, demonstrable exit strategies for services supporting critical functions. Not paper exercises, but plans that can be shown to work. And CADA, once adopted, will place further emphasis on documented migration plans and exit readiness, particularly for public procurement and regulated sectors.

The three contractual provisions I find most consistently absent from sourcing agreements are a genuinely tested exit plan with realistic timelines, full subprocessor transparency with the right to approve or object to changes in the subprocessor chain, and audit rights that survive contract modifications. I would add two more that I increasingly advocate for: material change notification clauses with re-audit and possible termination rights when the provider makes significant changes to architecture, ownership, or jurisdiction; and stronger liability alignment, including higher or uncapped liability caps for data breaches, flowing down to critical subprocessors.

On the technical side, contractual protections can only go so far. The most effective exit strategies pair strong clauses with thoughtful architecture from the outset, including containerisation, open standards, infrastructure as code, API-first design, and multi-cloud or hybrid approaches for critical workloads. No contract can fully compensate for a deeply proprietary system. And exit planning deserves the same discipline as business continuity: documented, tested, and regularly updated. A tabletop exercise that walks your team through a simulated provider exit will teach you more than any audit report, and should be run at least annually for your most critical dependencies.

The Audit Question: Paper Compliance Versus Real Oversight

One of the sharper questions from the audience concerned audits, specifically, how to tell the difference between an audit that provides genuine assurance and one that merely looks good on a spreadsheet.

The answer is in the question being asked. A spreadsheet audit asks: did the vendor tick the box for ISO 27001, SOC 2, NIS2, GDPR? And the answer is almost always yes, because vendors are very good at producing certificates. That tells you they passed someone's audit, at some point, against general criteria.

An effective audit asks a different question: does this specific contractual promise match what is technically happening in our instance of the service, right now? That requires actual audit rights. Not merely the right to receive a report, but the right to request evidence, ask technical questions, and bring in an independent third party to verify. It requires surviving audit rights that trigger on material changes to the service, not just at the moment of signing. And it requires treating governance as an ongoing operational function rather than a document in a binder, with continuous monitoring, subprocessor oversight, and board-level visibility into ICT risk.

ALLEGIANCE LAW

Changing the Boardroom Conversation

The final theme we explored was how to shift the internal narrative. Sovereignty and compliance are persistently framed as cost centres and legal obstacles. The reframe I advocate is simple: stop talking about sovereignty and start talking about optionality. Boards understand optionality; it is a concept from finance and risk management, and it maps precisely onto what we are building.

The conversation shifts from 'we need to spend money to comply with NIS2 and DORA' to 'we have built the ability to switch providers, recover faster from an outage, and negotiate better commercial terms because we are not trapped, and as a side effect, we are also compliant.' The financial angle reinforces this directly: penalties under NIS2 and DORA can reach two percent of turnover. That is not abstract risk; it is a number the CFO recognises immediately. And resilience that prevents a major outage, or delivers meaningful leverage in a cloud renegotiation, pays for itself many times over. Framed correctly, digital sovereignty is one of the few compliance investments that can show up as a genuine line-item benefit rather than a pure cost.

Six Things to Do Before the Month Is Out

I closed the session with a short action list, and the follow-up questions only reinforced how practical and immediate these steps are. So I will repeat them here, and mean them to be used.

First, go back to your top three or four critical vendor contracts and ask the access question, not the residency question. Who can access your data, under what legal authority, and through which channels? If you do not know the answer, that is your starting point.

Second, check whether you actually hold or control your encryption keys, and understand the difference between BYOK and HYOK in your specific provider arrangement. Also verify whether privileged access by provider staff is logged, visible to you, and subject to meaningful controls.

Third, run a real, time-boxed exit exercise on at least one critical system this year. Not a theoretical discussion but an actual simulation of what it would take to move, including realistic timelines, data volumes, format compatibility, and cost. You will learn more from that exercise than from any certification audit.

Fourth, rewrite your next board compliance update in terms of optionality and resilience rather than obligations. That single shift in language changes how sourcing decisions get prioritised and funded.

Fifth, map your real data gravity and dependencies, particularly around AI workloads, where lock-in is deepening rapidly and often without full visibility.

Sixth, start including clear sovereignty requirements in new contracts from day one: explicit rights to export your models and training data, guarantees that your data will not be used for provider-side model training, and portability commitments that cover not just data but configurations, metadata, and integration documentation.

Do those six things and you will be in a genuinely stronger position than most of your peers. Be ready for whatever comes next, whether that is the finalisation of CADA, the next iteration of the AI Act, or simply the next time a major provider has a difficult day.

Digital sovereignty is not about replacing hyperscalers with European alternatives. It is about preserving strategic freedom of choice. The question for every CIO is not who their cloud provider is today; it is how much autonomy their organisation will still have if that relationship were to change fundamentally tomorrow.

Steven De Schrijver — Partner, Allegiance Law

ALLEGIANCE LAW

ABOUT STEVEN DE SCHRIJVER

"The only way to do great work is to love what you do"

Steven is a partner at Allegiance Law and specializes in M&A, corporate law, IT and media, data protection and privacy and outsourcing.

Steven has more than 30 years of experience in advising Belgian and foreign companies on corporate transactions and has been involved in numerous national and cross-border transactions in the IT, media, telecoms and life sciences sectors.

Steven also advises some of the largest Belgian and foreign technology companies, as well as innovative entrepreneurs on complex commercial agreements and projects dealing with new technologies, most of the time with a cross-border element.

Steven has been involved in many IT, outsourcing, software and cloud application development, digital transformation, telecom/media projects (establishment of first mobile telephone operator in Belgium, acquisition of Flemish broadband cable operator, joint venture to launch video-on-demand services), outsourcing applicatinos, Software-As-A-Service, and cloud agreements on the customer side, and data protection (now: GDPR) compliance projects. He has a passion for artificial intelligence, robotics and drones.

He is also is active in the IBA Corporate and M&A Law Committee and the IBA Technology Law Committee and in ITechLaw. He is past-President of IFCLA and a member of the Tech M&A Committee of ITechLaw. He is Honorary member of AIJA and the Belgian member of EuroITCounsel.

Steven De Schrijver received in 20226 the Lexology Information Technology Lawyer of the Year, in 2023 (for the eight time) the Who's Who Legal award as Global Data Protection Lawyer of the Year and is considered a "Global Elite Thought Leader" in Data by Who's Who Legal (https://whoswholegal.com/steven-de-schrijver). Steven received in 2023 and 2024 also the Lexology Client Choice award for data protection and in 2012 the Lexology Client Choice Award for Corporate Law. Steven is recommended for corporate & M&A in Chambers, Legal 500 and IFLR and for IT law in Chambers, Legal 500 and Who's Who Legal.

Steven is known by his clients to go all the way to get the job done. He is pro-active, responsive, extremely available and pragmatic. Steven has an extensive international network of foreign lawyers with whom he closely cooperates on inbound and outbound cross-border transactions.

Let's connect on LinkedIn! https://www.linkedin.com/in/stevendeschrijver/

Recent transactions:

- Acquisition by Namsa of Medanex
- Acquisition by Archimed of Xpress Biologics
- Acquisition by Pixid, the French vendor management system-specialist, of TheMatchBox, a specialized text-mining company focused on the HR sector, primarily serving staffing agencies with AI search and matching services.
- Assistance of Pixid, with the acquisition of Connecting-Expertise, from the HR-group USG People Belgium.
- Acquisition by HypnoVR of Oncomfort
- Acquisition by NYSE-listed HubSpot of PieSync.
- DoubleVerify on its acquisition of Zentrick.
- Alpina Capital Partners on its acquisition of Objective International.
- Horizon Ventures on investment in Cloudalize.
- LivaNova on Belgian aspects of several global transactions.

Relevant work IT:

- DPG Media with the launch of streaming platform Streamz and the set-up, in this respect, of their joint-venture with Telenet.
- Radius Payment Solutions with launch of telecom activities in Belgium.
- ISS Facility Services, Mazda Logistics Europe on IT infrastructure and services outsourcing projects.
- Microsoft on its day-to-day commercial matters.

ABOUT ALLEGIANCE LAW

Allegiance Law is a Belgian independent law firm with offices in Brussels, boasting a strong team of lawyers with specialisations in areas including corporate, commercial, IT/IP/privacy, and EU regulatory (*e.g.,* artificial intelligence). Whether facing complex mergers, restructuring, or seeking to professionalise business operations, Allegiance Law tailors solutions by assembling specialised teams.

The firm supports national and international clients strategically by helping them to choose the best legal and financial structure for their business operations and transactions, transcending traditional methods and thinking outside the box. Allegiance Law's focus lies on IP and data-driven deals, of which the majority have a cross-border character. The firm operates regularly alongside among US, UK, French, Dutch, German and Swiss law firms, working seamlessly together. The team is specifically well equipped in the areas of technology, life sciences, media, advertising and entertainment, chemicals, transportation, and retail.

Our Areas of Expertise:

- Corporate Law and M&A
- Technology Law
- Commercial Law
- Privacy, Data Protection and Cybersecurity Law
- E-commerce and Digitalization Services
- Media, Gaming & Esports Law
- EU Regulatory
- Artificial Intelligence and Web3
- Life sciences
- Telecommunications
- Dispute Resolution and Mediation

ALLEGIANCE LAW