FAST LTA

COMEX

Whitepaper

Digital sovereignty can now truly be measured.

The discussion about digital sovereignty has been going on for quite a few months now. In policy documents, in European strategies and in countless panels at IT conferences. Yet one question often remained unanswered: how do you actually measure whether an IT environment is truly sovereign?

The Dienst ICT Uitvoering (DICTU) has now provided a concrete answer to this. With the new Sovereignty Assessment Tool for cloud services, organizations can systematically assess their digital dependencies. Not only legally, but also technically, operationally and organizationally.

That is important. Because digital sovereignty has long since stopped being only about where data is located. The core question is, as we have been saying for many months: **who ultimately has control?**

Since: March 2026

Why this assessment tool had to be created

The reason is clear. A large part of the European cloud market is currently controlled by a small number of international hyperscalers. According to various analyses, that share is around seventy percent. This creates a dependency that goes beyond technology alone.

An important point of concern is the extraterritorial effect of legislation such as the American CLOUD Act. Because for many technology companies jurisdiction follows ownership, foreign authorities can under certain circumstances demand access to data, even when that data is physically stored in Europe.

For government organizations and critical sectors, this raises a fundamental question: how much control do we actually still have over our own digital infrastructure?

The DICTU assessment tool tries to provide an objective framework for this. Let's take a look at what that looks like.

Five dimensions of digital autonomy

The tool does not look at a combination of just a few factors. In total, five dimensions are assessed:

- **Legal** – under which legislation does a service provider fall and where is the parent company located?
- **Data & AI** – where is data stored, who has technical access to it and how are algorithms managed?
- **Technology** – to what extent are systems interoperable and how great is the risk of vendor lock-in?
- **Operational** – how dependent is an organization on suppliers or external infrastructure?
- **People** – who manages the systems and how transparent are the support and management chains?

This broad approach immediately makes it clear that sovereignty is an architectural issue with a wide range of factors.

Measure and improve.
The new assessment tool makes digital sovereignty concrete by allowing organizations to measure where they stand across five areas: legal, data and AI, technology, operational and people. By systematically assessing these dimensions, it becomes visible where dependencies exist and where targeted improvements are possible.

From cloud strategy to data control

In many organizations, the issue starts with data. Where is it stored, and under what conditions?

That is why a hybrid model is emerging more and more often. Cloud remains an important part of the IT strategy, but for certain datasets organizations consciously choose an environment where control remains fully in their own hands. Sensitive data therefore remains under their own management.

European on-prem storage is playing an increasingly important role.

An example of this is the storage solutions of **FAST LTA**, a German manufacturer for which Comex is the exclusive distributor in the Benelux. The technology was specifically developed with data storage control and long-term availability in mind. Let's take a look at how these systems can contribute to increasing the DICTU score.

Sovereign off-cloud AI application

Silent AI

Ransomware-proof backup and recovery with air gap

Silent Bricks

Compliant long-term archiving without data loss

Silent Cubes

Sovereignty starts with jurisdiction

One of the first questions in the DICTU assessment is legal in nature: under which legislation does a supplier fall?

FAST LTA is based in Munich and operates fully under European jurisdiction. This means that the infrastructure does not fall under extraterritorial legislation such as the American CLOUD Act. For organizations that want to retain control over their data, this can make an important difference.

Data that truly remains onder your own control

n addition to legal control, the DICTU tool also looks at the technical protection of data.

FAST LTA's storage architecture is designed entirely on-premise. Data is stored locally and therefore physically remains within the organization's infrastructure. This supports scenarios in which data residency and direct control are hard requirements.

In addition, there are functions such as hardware-based WORM sealing and physical air gaps, which means data can no longer be modified or encrypted once it has been stored. Such mechanisms are increasingly being used to protect backups against ransomware and manipulation.

These are exactly the kinds of technical measures that contribute to a higher sovereignty score in the DICTU model.

Technology without lock-in

Another important criterion in the assessment tool is technological independence.

When data can only be accessed through proprietary protocols, switching to another supplier often becomes complex and expensive. That is why DICTU explicitly looks at support for open standards.

FAST LTA's storage platforms support, among other things, S3-compatible object storage, SMB/NFS and VTL emulation. This makes it possible to integrate systems into existing environments while also offering flexibility for future migrations.

Technology that is based on standards reduces the risk of vendor lock-in and increases strategic room for manoeuvre.

Continuity as part of sovereignty

One aspect that often remains underexposed in discussions about sovereignty is operational continuity.

The DICTU model therefore also looks at factors such as system lifetime, supply chains and maintenance contracts. Hardware that is designed for long-term use and can be maintained locally reduces dependency on global supply chains.

FAST LTA, for example, positions its systems with a minimum lifetime of ten years and long-term service contracts. These kinds of choices can contribute to stability in environments where infrastructure must remain available for a long period of time. In addition, this helps prevent unforeseen costs because the TCO is clear from the moment of purchase.

Digital sovereignty as an architectural choice

The most important insight from the DICTU tool may be that digital sovereignty is not an all-or-nothing choice. It is not about cloud versus on-premise. It is about **conscious architectural choices**.

Many organizations will continue to use a hybrid model, in which different types of infrastructure exist alongside each other. But precisely within that architecture, it becomes important to think about where the core of your data foundation lies.

European storage solutions can play a role in this as a kind of sovereign anchor point within the infrastructure.

From discussion to measurability

Perhaps that is the greatest value of the new DICTU tool. It brings a discussion that often remained abstract back to something concrete: digital sovereignty becomes measurable.

And as soon as something becomes measurable, you can also steer it in a targeted way.

For IT architects and policymakers, this means that the question of **how to realize digital sovereignty in practice has suddenly become tangible**. Curious about how FAST LTA's systems fit within your infrastructure? Take a look at our website or contact @Axel Booltink or @Roel Lenssen.

Hello.

COMEX | Vogt 21 | NL-6422 RK Heerlen | office@comex.eu | **www.comex.eu**

FAST LTA | Ruedesheimer Str. 11 | 80686 Munich, Germany | info@fast-lta.de | **www.fast-lta.com**