CO-CREATE & SCALE DATA-DRIVEN INNOVATION

Digital sovereignty for Europe's critical industries

Why chemicals and pharmaceuticals need trusted European cloud, AI and data infrastructures

A whitepaper on Europe's digital dependency, regulatory pressure, sovereign infrastructure and practical paths to resilient industry platforms.

coac Whitepaper | By Niklas von Tschirnhaus | August 2025

1 Introduction

The digital transformation of industry is accelerating rapidly. At the same time, Europe's technological dependence on non-European providers is becoming an increasing geopolitical and economic risk. The establishment of sovereign digital systems has therefore become a fundamental strategic issue, especially for critical infrastructures such as the chemical and pharmaceutical industries.

Cloud infrastructures, AI systems and data platforms form the foundation of industrial innovation, productivity and sustainability. They must therefore be trustworthy, legally compliant and remain in European hands in the long term.

According to an analysis by Synergy Research, the market share of European cloud providers is currently below 5%, while US hyperscalers such as Amazon Web Services, Microsoft Azure and Google Cloud together account for more than 70% of the global cloud market. These figures illustrate Europe's structural dependence in one of the most strategically important technology fields.

This dominance creates not only economic but also political risk. The US CLOUD Act allows US authorities to access data processed by US companies, even when that data is stored outside the United States. For European companies, particularly in regulated sectors, this creates significant legal uncertainty.

In addition, concerns are growing over political influence resulting from the close integration of business, politics and security interests in the United States. Examples often cited include influence on social media platforms, control over access to critical infrastructure data and economic agreements with security-policy implications.

This whitepaper highlights the urgency and strategic relevance of digital sovereignty for the chemical-pharmaceutical industry, outlines current legislative and technological developments and presents practical solutions that pave the way toward a self-determined digital future.

2 Europe's digital dependency: facts, figures and risks

Europe is currently heavily dependent on non-European providers in key digital sectors. According to the "Digital Dependence Index" published by the Konrad-Adenauer-Stiftung, Germany's score is 0.82 on a scale from 0 for no dependence to 1 for maximum dependence. This dependency is visible across cloud computing, AI infrastructure, software platforms and the control of digital standards.

This situation is not only problematic from a data protection perspective, but also creates geopolitical risks. Extraterritorial laws such as the US CLOUD Act can make European data accessible without European law applying in the expected way. At the same time, trade conflicts or cyberattacks can lead to outages that threaten system-critical industrial processes.

The European Commission is responding through initiatives such as Gaia-X, the Digital Compass 2030 and IPCEI-CIS. The aim is to create a European cloud and data infrastructure that strengthens technological independence while accelerating innovation.

According to the Commission's targets, 75% of companies should be using cloud technologies by 2030, 10,000 edge nodes should be created and 100% of critical public services should be digitized. These ambitions underline how central sovereign digital infrastructure has become to Europe's economic future.

3 Critical infrastructures under digital pressure: focus on chemicals and pharmaceuticals

Hardly any other sector is as dependent on security, availability and regulatory compliance as the chemical-pharmaceutical industry. At the same time, it falls within the KRITIS category and is therefore subject to heightened protection requirements and increased scrutiny. The digitalization of product development, approval, production and supply chains is advancing rapidly.

According to the German Federal Office for Information Security (BSI), the number of security-related incidents in the KRITIS environment continues to rise. More than 20,000 reports were counted in 2022 alone. The attack surface is growing continuously due to connected systems, IoT devices and globally distributed data streams.

At the same time, regulatory requirements are expanding. The AI Act, the NIS2 Directive, the Corporate Sustainability Reporting Directive (CSRD), the EU Taxonomy, the European Sustainable Products Regulation (ESPR) and the Data Act all move in the same direction: more transparency, more traceability and more sovereignty over data, systems and AI applications.

In order to meet these requirements, chemical and pharmaceutical companies must:

- process sensitive data in secure, legally compliant data spaces,
- operate AI models in a traceable and auditable manner,
- combine industry-specific workflows with regulatory documentation,
- and do all of this within an IT infrastructure that is subject to European jurisdiction and control.

4 Technological responses to regulatory and strategic challenges

The good news is that practical European solutions already exist. They show that digital sovereignty for KRITIS sectors is not merely a political vision, but something that can be implemented today through the right combination of hosting architecture, AI capability and regulatory expertise.

4.1 SAIFTY

SAIFTY is a platform that uses AI to unlock unstructured data sources such as safety data sheets, regulatory texts and technical documentation and transform them into structured, analyzable information. The platform offers ready-made reporting formats for CSRD and ESPR and can be integrated directly into existing company processes.

SAIFTY is operated on European cloud infrastructure, for example IONOS Cloud, helping ensure data sovereignty in accordance with GDPR and European law. This enables companies not only to comply with regulatory requirements, but also to build intelligent, industry-specific AI applications within a sovereign data space.

> *"With SAIFTY, we are demonstrating how regulatory compliance, sustainability and technological innovation can work together. The platform is our contribution to the intelligent digitalization of critical processes in the industry."*
>
> *— Martin Prinz, CEO of coac*

4.2 SEP (Smart Equipment Passport)

SEP is a digitally hosted solution for managing industrial assets. It combines technical documentation, material tracking, digital twins and maintenance management in one central platform.

Its hosting architecture is based on European cloud infrastructure and supports compliance with the European Sustainable Products Regulation (ESPR). SEP helps companies realize sustainable supply chains, simplify complex approval processes and manage technical data with high quality, transparency and security.

> *"SEP enables a new quality of transparency and sustainability for Industry 4.0 — on a sovereign, European infrastructure. This makes digital product responsibility tangible and feasible."*
>
> *— Martin Prinz, CEO of coac*

4.3 What both solutions demonstrate

Both solutions demonstrate the same principle: when European cloud infrastructure is combined with industry-specific technology and regulatory expertise, the result is a platform for resilience, sustainability and efficiency.

Cooperation with European hosting partners helps companies realize digital sovereignty not merely as an ideal, but as a concrete competitive advantage. Data remains controllable, workflows become auditable and innovation can scale without creating new strategic dependencies.

Solution	Primary focus	Contribution to sovereignty
SAIFTY	Regulatory intelligence, sustainability reporting and unstructured data processing	Structured analysis, compliant reporting and AI-enabled workflows on European infrastructure
SEP	Asset transparency, lifecycle management and industrial technical data	Centralized equipment intelligence, traceable workflows and secure lifecycle control on European infrastructure

> *"For us, digital sovereignty is not a buzzword, but a prerequisite for sustainable industrial development in Europe. It starts with data sovereignty — and with the right technology, it becomes a driver of transformation."*
>
> *— Martin Prinz, CEO of coac*

5 Conclusion: Digital sovereignty is not a luxury, but the basis of European competitiveness

The coming years will determine whether Europe remains a digital creator or becomes primarily a digital consumer. Particularly in critical industries such as chemicals and pharmaceuticals, digital sovereignty is not just a matter of IT, but also of location, supply security and innovation capability.

Now is the time to invest boldly in European cloud technologies, AI solutions and data spaces in order not only to comply with regulation, but to actively shape it. Digital autonomy means control over our own future — technologically, economically and politically.

Sources & references

1. Synergy Research Group, market analysis on cloud infrastructure market shares, 2023.
2. Konrad-Adenauer-Stiftung, *Digital Dependence Index*, 2023.
3. European Commission, Digital Compass 2030 and IPCEI-CIS policy framework.
4. German Federal Office for Information Security (BSI), KRITIS-related incident reporting, 2022.
5. Regulation and policy references: AI Act, NIS2 Directive, CSRD, EU Taxonomy, ESPR and Data Act.

About SAIFTY and SEP

SAIFTY and SEP are AI-enabled platforms by COAC designed to support regulated industrial environments with sovereign data architectures, structured workflows and trustworthy digital operations. Together, they help transform compliance, sustainability and asset intelligence into measurable business value.