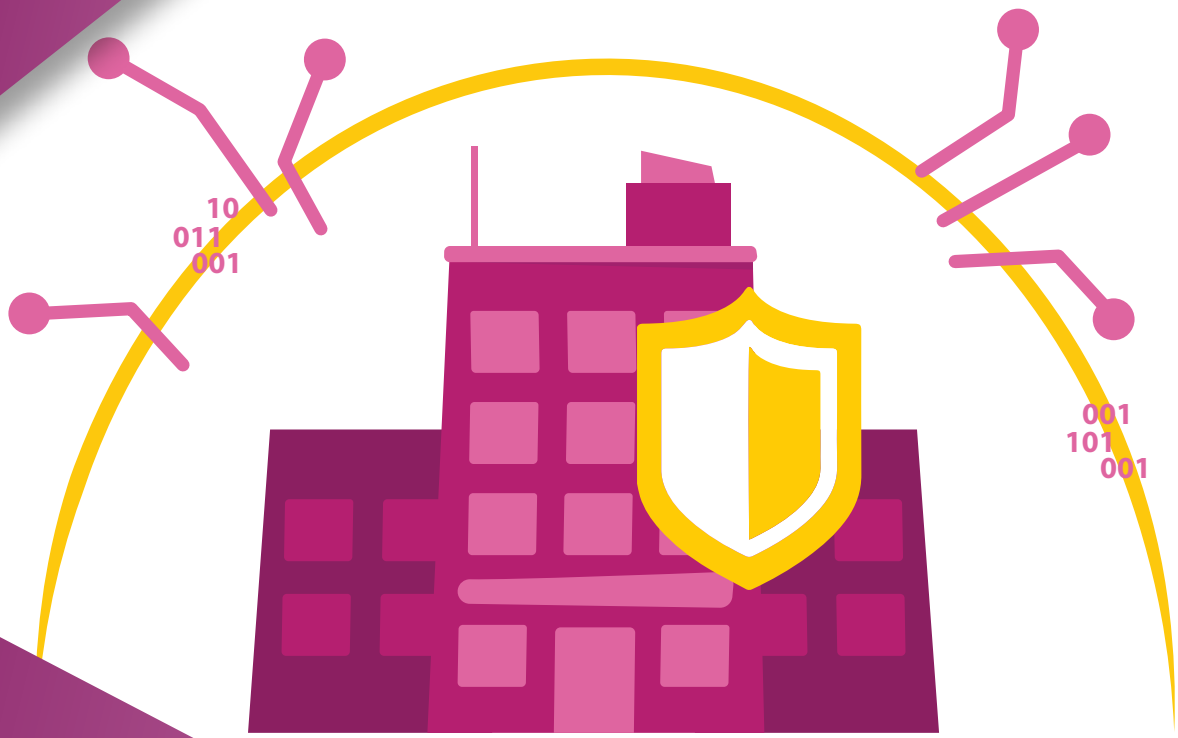
White paper:

# Digital autonomy in practice.

## From dependence to control



# Prologue

It is 2022. In the period just before Russia's invasion of Ukraine. In a meeting room in Kyiv, the Ukrainian Minister for Digital Transformation, Mykhailo Fedorov, makes a decision that would have been unthinkable in peacetime. All government data – from the tax authorities to the Ministry of Defence, from population registers to diplomatic communications – must be moved to the cloud immediately. Not in six months' time. Not after a careful migration process. Now.

Parliament amends the law in record time. President Zelensky signs the Cloud Services Act on 15 March 2022[1]. In the weeks surrounding the invasion, Microsoft transfers the data of virtually all ministries to Azure data centres across Europe. The bill runs to over 400 million dollars.

On 24 February 2022, a few hours before the first missile strikes, Microsoft's Threat Intelligence Centre detects a massive wave of cyberattacks on Ukrainian government infrastructure[2]. Thanks to the rapid warning and the scalability of the cloud, the attack is neutralised. When Russian missiles strike the physical government data centres shortly afterwards, the damage is limited to concrete and steel. The data is already gone. The Ukrainian government remains online. And operational.

It is one of the most striking lessons from the digital history of recent years. Not because Ukraine did everything right — the reliance on a single American tech giant, the CLOUD Act playing out in the background, the vendor lock-in that had become entrenched over the years — but because it makes it so painfully clear where the real vulnerability lay. Not in the cloud, but in the servers on home soil. In the illusion that physical presence equates to control.

Digital sovereignty, as that February in 2022 revealed, is not a question of where your data is stored. It is a question of who has access to it, whether you can continue to operate if a supplier drops out, and whether you hold the keys in your own hands when it really matters.

We are living in turbulent geopolitical times. The dependence of European organisations on international technology platforms is very much under discussion. In boardrooms, in The Hague, in Brussels. The tone is one of concern, sometimes of urgency, and all too often of paralysis. Because the question 'what should we do?' remains without a satisfactory answer as long as digital sovereignty is treated as a political or legal issue rather than what it really is: a security and resilience challenge.

And that is exactly what this white paper is about. It is not about leaving the US cloud. It is not about a return to servers in your own basements. Rather, it is about the question of who actually has access to the data. About the architecture that determines whether your organisation will continue to function if a supplier drops out — and that goes beyond mere recovery, towards an adaptive structure that pivots rather than collapses. About the keys — literally and figuratively — that determine whether you are in control.

For CISOs and other security advisers, now is the time to take up the gauntlet. The political and administrative urgency surrounding digital sovereignty strengthens the business case for investment in data security and resilience in a way that has rarely been so clear before. Those who now make the connection between the sovereignty debate and the security agenda will not only enhance their organisation's digital resilience, but also take the lead in a debate that has been conducted for too long without a technical voice.

This white paper explains how.

*This prologue uses publicly available information to illustrate a mechanism. Exact details regarding numbers, timing and structure may vary depending on the source and context.*

*This white paper has been drawn up to provide general information and offers guidance for organisations seeking to gain a better understanding of digital autonomy and sovereignty. With this white paper, the Digital Autonomy project group of Cyberveilig Nederland aims to contribute to a shared understanding and broad framework for action. The document is expressly not intended as legal, security or other professional advice, nor is it an exhaustive description of all applicable laws, regulations or best practices.*

*In this white paper, the term 'European' is used in several places as a shorthand for the European Union (EU) or EU-related topics, such as EU legislation and regulations and EU policy.*

*Which measures are necessary, proportionate and effective depends, among other things, on the sector and legal context, the type of organisation, risk profile, data categories, critical processes, supply chain and the specific (technical and organisational) structure of the organisation. Organisations are advised to engage appropriate expertise for further application in their own specific circumstances. This white paper helps to clarify the issues at hand.*

[1] Law of Ukraine 'On Cloud Services' [March 15 2022], No.2075-IX https://zakon.rada.gov.ua/laws/main/2075-20#Text

[2] Defending Ukraine: Early Lessons from the Cyber War

# Inhoud

# Summary

There is a growing need among Dutch organisations for insight into dependencies, risks and strategic choices relating to digital autonomy and digital sovereignty when using hardware, software and digital services. Cyberveilig Nederland has produced this white paper to provide these organisations with insight and practical guidance to help them better understand and address these issues.

Digital autonomy concerns the ability to make independent choices in the digital domain, whilst digital sovereignty focuses on legal and administrative control. Both influence an organisation's level of resilience and exist on a spectrum, with organisations needing to consciously choose a position that suits their risks and dependencies. Specifically, the following three types of threats are relevant in the context of digital autonomy and sovereignty:

- Confidentiality of data, infrastructure and services;
- Integrity of data, infrastructure and services;
- Availability of data, infrastructure and services.

At present, the geopolitical climate in particular is creating uncertainty about how states might use their influence in this area in the future. However, this does not mean that such risks are linked solely to the jurisdiction(s) in which a supplier operates. The extent to which organisations have demonstrable control over access, key management, auditability and continuity also plays an important role.

European legislation does not aim for complete independence, but rather for conscious management of digital dependencies by enforcing transparency, risk management and supply chain control. This ensures that international service provision remains legally possible, whilst appropriate control measures guarantee effective oversight. This shifts the debate from 'sovereignty' to 'demonstrable control': which technical and organisational measures make risks acceptable and demonstrably managed (verifiable)?

More and more solutions are being developed by major cloud providers seeking to address this. Nevertheless, digital autonomy requires more than just technological provisions. Establishing one's own technical, organisational and contractual measures remains necessary to maintain control.

Furthermore, the threats arising from our digital dependencies do not constitute a new category of risk, but rather a new manifestation of familiar security issues. What makes the situation different now is the political and administrative context, which necessitates the adoption of additional (control) measures. These include encryption with independent key management, an adaptive (network) architecture and an independent recovery environment. This does not, therefore, argue against international suppliers per se. On the contrary: international technology can fit perfectly within this approach. It is a question of technical and organisational control measures. These must be demonstrably in order, and organisations must actively manage their dependencies.

Demonstrable control – that is what digital autonomy is all about in practice.

# Introduction and background

We are increasingly migrating our on-premises IT functions to cloud-based alternatives provided by US companies. Is that still a sensible move? Should we stop doing this?





We purchase hardware and/or software from a supplier outside the EU that is currently regarded as a high-risk jurisdiction in the current geopolitical climate. Is that risky? Should we do something differently, or is there anything we need to bear in mind?

These are just a few examples of the many questions organisations in the Netherlands are asking their cybersecurity suppliers. It highlights a growing need among organisations to gain insight into their dependencies and the risks that help determine their strategic choices within the digital domain. These (strategic) dependencies, geopolitical developments and European legislation and regulations are leading to an increase in such questions. Issues such as data processing, supply chain dependencies and risks associated with outsourcing are not problems for the future, but problems that organisations are grappling with right now.

Consequently, a project group has been launched within the cybersecurity sector, coordinated by Cyberveilig Nederland, to assist organisations with the above issues. The organisations participating in the project group are: Atos, Cisco, DataExpert, Defion, Fox-IT, Northwave, Schubergphilis, Sentyron and Tesorion.

First of all, the theory will be explained so that it is clear what we mean by certain terminology. In the context of digital autonomy, three threats are relevant and will be explained in more detail. However, legal objections are also frequently raised during the design and procurement of digital services. It is therefore important to outline the legal perspective as well. We will then define the concept of a sovereign cloud and outline the steps to be taken. The appendix contains a roadmap that organisations can use when taking measures to ensure digital sovereignty and autonomy in practice.

# Digital resilience, sovereignty and autonomy

In this chapter, we outline and briefly describe the concepts of digital resilience, digital autonomy and digital sovereignty, and how they relate to one another.

**DIGITAL RESILIENCE** is the ability to prevent, detect, mitigate and recover from breaches of information confidentiality and integrity, as well as disruptions to business processes, whilst continuing to function as effectively as possible. Achieving digital resilience requires a wide range of safeguards. Frameworks such as ISO 27001, NEN 7510 and IEC 62443 provide concrete measures that organisations can implement using a risk-based approach. In addition, digital autonomy and digital sovereignty also influence the degree of an organisation's resilience.

Digital autonomy and digital sovereignty are often mentioned in the same breath, but they represent two different – yet mutually reinforcing – perspectives. See also the Government's Vision on Digital Autonomy and Sovereignty[3.], a document which, although written for the government, is also relevant to businesses.

**DIGITAL SOVEREIGNTY** focuses on legal and administrative control. The key word here is control: who ultimately determines the rules governing data, systems and infrastructure? Essentially, this is about jurisdiction: which legislation applies to systems and information? We explain this in more detail in Chapter 3. Digital sovereignty therefore influences both continuity and confidentiality issues, as we explain in Chapter 4.

**DIGITAL AUTONOMY** concerns the ability to make independent choices in the digital domain, or in other words, freedom of action. The scope to decide, change and steer without external parties restricting (or being able to restrict) that freedom. The Digital Autonomy and Sovereignty vision states that this freedom consists of three aspects:

1. technological freedom of choice;
2. knowledge autonomy;
3. mitigation of strategic dependencies.

In practice, digital autonomy, freedom of action, has a significant impact on continuity issues, as we explain in Chapter 4.

### NOT BLACK AND WHITE, BUT A SPECTRUM

None of these concepts are absolute, but exist on a spectrum ranging from less to greater resilience. Full digital resilience, sovereignty and autonomy are therefore not necessarily an end goal in themselves. It is up to organisations to consciously choose the right position on this scale, in line with the sensitivity of the data, the risk profile and strategic dependencies. For instance, having less autonomy and less sovereignty due to dependence on the cloud can, in certain circumstances, actually lead to greater resilience. Consider how cloud migration can be essential for maintaining and securing critical systems and data. Digital sovereignty and autonomy are therefore about conscious control rather than the cautious use of (cloud) technology.

[3.] https://open.overheid.nl/documenten/c49a2705-3f3d-44be-8a7d-2cecd2183604/file

# What is the threat?

Specifically, the following three types of threats are relevant in the context of digital autonomy and sovereignty:

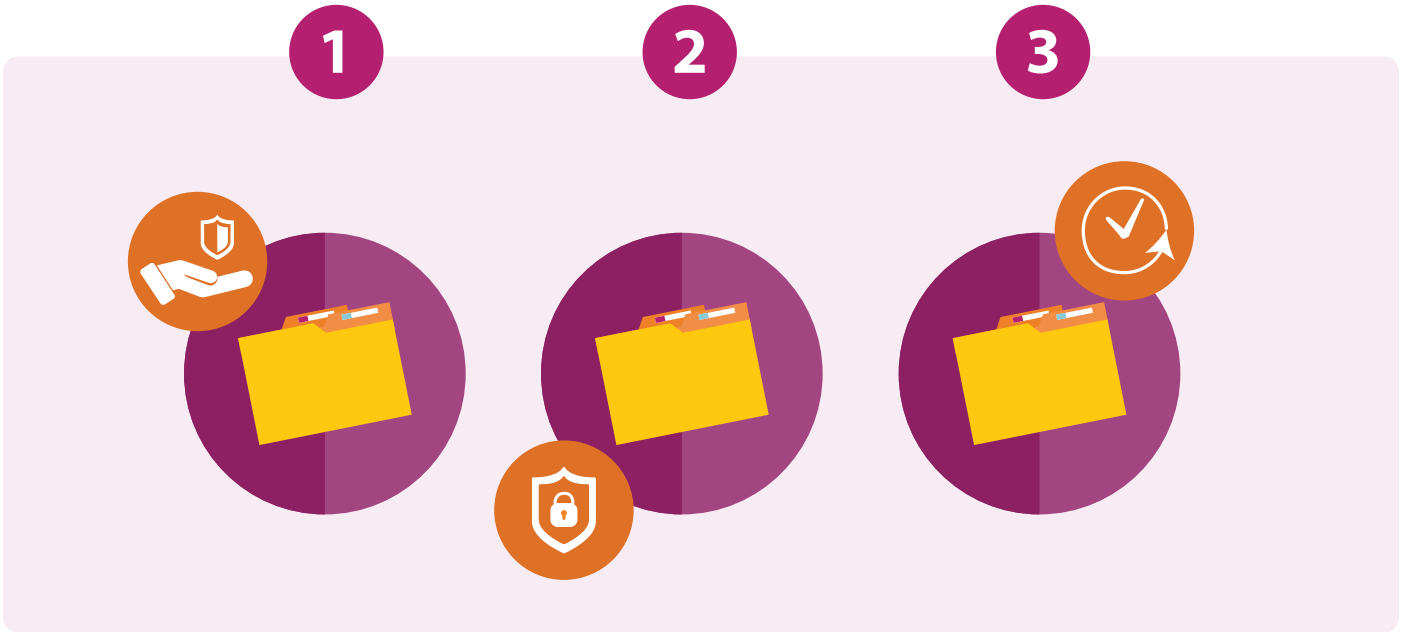
1. **CONFIDENTIALITY OF DATA, INFRASTRUCTURE AND SERVICES.**
Under certain circumstances, a cloud provider may be obliged to grant foreign authorities access to data to which it has access.

2. **INTEGRITY OF DATA, INFRASTRUCTURE AND SERVICES.**
Digital interference by a cloud provider or authority can compromise the integrity of information if data is stored incompletely or incorrectly, or if it was altered during use.

3. **AVAILABILITY OF DATA, INFRASTRUCTURE AND SERVICES.**
A cloud provider may (whether under pressure or not) restrict or discontinue services. This can have immediate consequences, but also consequences that manifest themselves later, such as a provider's on-premise software for which updates are no longer provided.

In practice, these threats are often perceived as greater when there is a reliance on international cloud providers, partly due to differences in legislation and regulations, the involvement of multiple jurisdictions, and the limited influence that individual organisations can exert over them. Furthermore, the geopolitical climate creates uncertainty as to how countries might exercise their influence in the future.

The three core aspects of information security mentioned above – confidentiality, integrity and availability – are not abstract. They become apparent in situations where European governments, public services or critical infrastructure prove to be dependent on international technology. The scenarios below illustrate how these threats may manifest in practice and what risks they entail. These scenarios are illustrative and deliberately focus on situations involving international dependencies, as this is where the tension between dependence and control is often most apparent. They demonstrate how these threats may arise in practice and what risks may result from them.



# Scenarios

*The scenarios in this chapter are illustrative and describe possible mechanisms. They are not intended as factual accounts of specific events or actions by particular suppliers.*

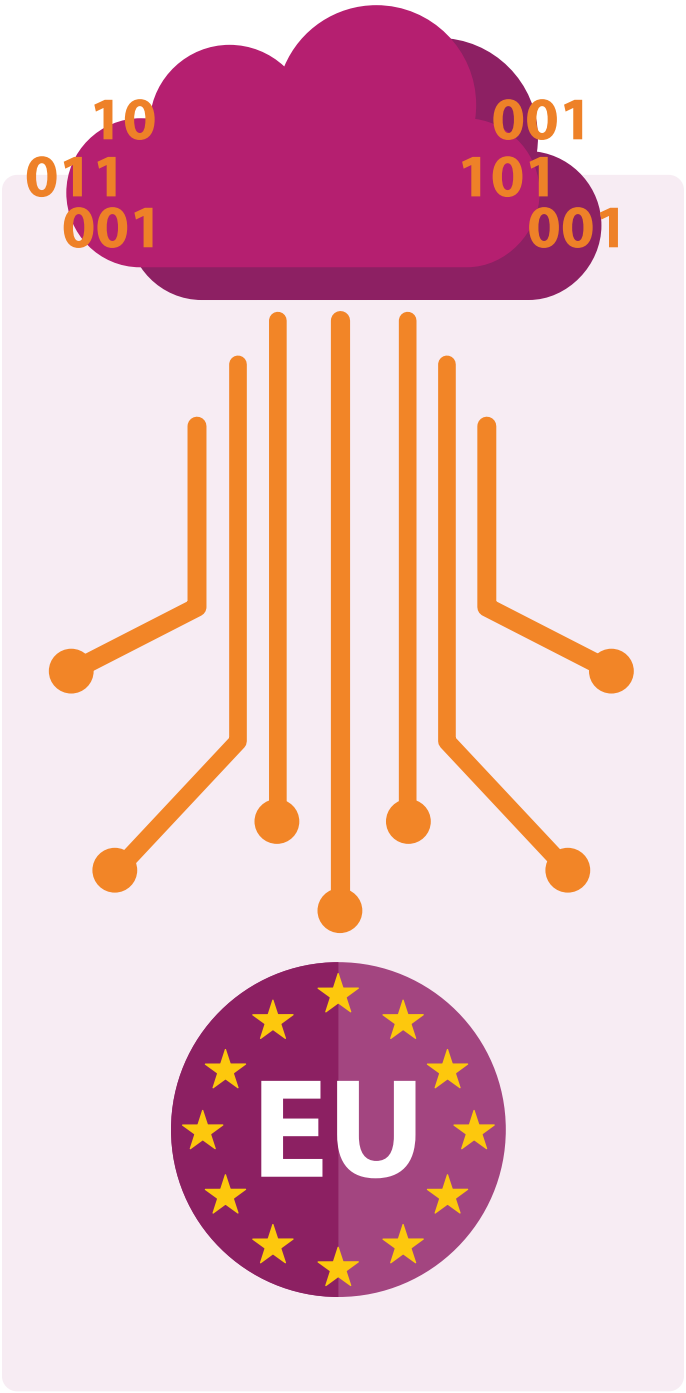
## **SCENARIO 1:** ACCESS TO EUROPEAN PERSONAL DATA VIA A US CLOUD PROVIDER

**SITUATION:** A European organisation runs a large part of its data analytics platform on a cloud environment provided by an international cloud provider. The data includes personal data and sensitive business information.

**TRIGGER:** An American law enforcement agency is investigating an organisation that appears in European datasets. It is seeking data through legal proceedings, targeting specific accounts or datasets held by the cloud provider that fall under the Stored Communications Act (SCA).

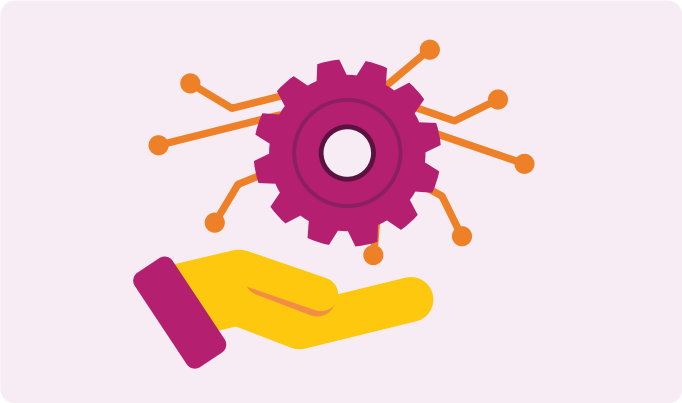
**THREAT MECHANISM:** Under the CLOUD Act, in conjunction with the SCA, a US cloud provider subject to US jurisdiction may be required, pursuant to valid legal proceedings, to retain and disclose content and/or (meta)data[4.] that is in its possession, custody or control, regardless of where that data is physically stored. Furthermore, the legal process may be accompanied by a (temporary) non-disclosure or stay order, preventing the cloud provider from informing the customer about this (immediately).

**MANIFESTATION:** The cloud provider receives a legal request that may be (temporarily) subject to confidentiality. Without the European organisation's knowledge, certain data and associated information from selected accounts are collected and passed on to the competent authority. A cloud provider may, however, under certain conditions, have such an order reviewed or challenged on the basis of a comity assessment in the event of a conflict with foreign law (such as the GDPR). In that case, a US judge must weigh up the various interests against one another.




[4.] Examples include log files, access credentials and communication patterns

## **SCENARIO 2:** A EUROPEAN GOVERNMENT'S IDENTITY SERVICE IS RUN BY AN INTERNATIONAL IT SERVICE PROVIDER



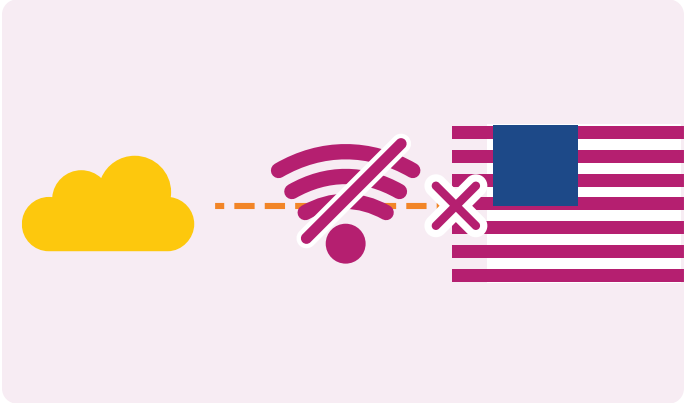
**SITUATION:** A national digital identity service, used by millions of citizens for purposes including tax returns, healthcare portals and municipal services, runs on an external platform provided by a non-European IT service provider. The supplier manages, amongst other things, the authentication servers, PKI components, logging and monitoring services, and (part of) the incident response process. The government has limited insight into the underlying infrastructure and is dependent on the supplier for recovery in the event of disruptions.

**TRIGGER:** In the country where the supplier is based, new export, sanctions or compliance regulations have been introduced (for example, relating to cryptographic technology). As a result, certain aspects of the service must be reviewed, (re)certified or temporarily suspended.

**THREAT MECHANISM:** Due to legal or regulatory requirements, the supplier may suspend certain security features, delay updates or restrict the service until the necessary rules and certifications have been met. The supplier may only be able to provide limited information on this matter due to legal restrictions.

**MANIFESTATION:** Within a short space of time, authentication servers go down, citizens are unable to log in to government services, or certificates are revoked or not renewed. This triggers a chain reaction in systems that rely on identity verification. The government cannot restore the service independently if crucial components fall outside its control.

## **SCENARIO 3:** SUSPENSION OF SERVICES UNDER PRESSURE FROM THE US GOVERNMENT



**SITUATION:** An international organization based in the Netherlands uses a major US cloud provider for the storage and processing of sensitive research data. This includes witness statements, supporting documents, internal analyses and communications between staff members. This data is essential to the international organisation's operations and is processed and stored in Europe. However, the cloud provider is subject to US laws and regulations.

**TRIGGER:** The international organisation is launching an investigation into possible war crimes, which also involves US military personnel due to the location of the conflict. Political pressure in Washington is mounting.

**THREAT MECHANISM:**
The threat is twofold:

**Data access:** Under the CLOUD Act/SCA, a cloud provider may be compelled, through legal proceedings, to retain and/or disclose data that is in its possession, custody or control, regardless of where that data is physically stored.

**Service continuity:** Geopolitical pressure may lead to services being restricted, support being suspended, accounts being blocked or other measures being taken. There may also be a (temporary) delay in notifying the customer within the aforementioned SCA framework in the event of a legal request for data access.

**MANIFESTATION:** The cloud provider receives a legal request and/or internal instructions that are not immediately public or fully transparent. For the international organisation, this means in practice that certain data or accounts are no longer available, that backups are less effective, or that important administrative tasks are delayed. This makes it more difficult to access important information and can cause investigations to be delayed or even come to a standstill. This has direct consequences for the organisation's independent operation.

**POTENTIAL IMPACT:** COMMON THREAD

The threats outlined in the scenarios above could affect the three key aspects of information security: confidentiality, integrity and availability.

Confidentiality: unauthorized parties may gain access to sensitive data, such as personal data or government information. This can lead to privacy issues and risks of espionage, for example in the fields of policy, defense or diplomacy.

Integrity: data, settings or access rights may be altered, either deliberately or accidentally, rendering the information unreliable.

Availability: systems or services may fail, rendering key processes and public services — such as healthcare, benefits or education — unavailable.

When such disruptions are prolonged or widespread, they can lead to social problems and disruption. The crux of these scenarios is that the risk does not depend solely on the country in which a supplier is based. What is more important is the extent to which an organisation understands its dependencies, can influence them and, if necessary, can adjust them. Digital sovereignty and autonomy can help in this regard, but do not guarantee the confidentiality, integrity and availability of data, systems and services.

In practice, digital autonomy is primarily about effective control measures, such as technical security, clear contractual agreements and good governance, tailored to the risks an organisation is prepared to accept.

The scenarios highlight the risks. The following chapter describes the legal rules and the scope that exists within them. On this basis, it becomes clear what measures are needed to use international services responsibly.

# Digital autonomy: the legal perspective

The previous section of this white paper focused primarily on cyber threats. However, legal concerns are also frequently raised when designing and procuring digital services. These often refer to the requirements of autonomy and sovereignty in European laws and regulations. This is understandable, as geopolitics, supply chain risks, and oversight make it more complicated to blindly trust technology that is not fully under one's own control. At the same time, these terms often lead to requirements that sound more absolute than what is actually required under existing laws and regulations. Digital autonomy within the European Union therefore does not aim for complete independence, but rather for conscious management of digital dependencies and risks. European legislation does not aim to exclude international technology, but increasingly focuses on enforcing transparency, risk management, and supply chain governance.

This chapter briefly explains the key legal frameworks and outlines the requirements for organisations regarding digital autonomy when using (international) digital services.[5.]

A common requirement is: "Data must remain within the EU." While this may serve as a useful rule of thumb, legally it is often a means rather than an end. The goal is to know who has access to the data, under what conditions, and how you monitor that access. Location can help with this, but it does not automatically guarantee that access, logging, key management, or exit are properly managed. That is why it is useful to distinguish between:

- data residency (where the data is hosted);
- access and jurisdiction risk (who can access it, both legally and technically);
- exit/portability (how quickly and securely you can migrate in the event of changing risks or conditions).

In other words: in practice, digital autonomy is not so much about strict legal requirements but rather about a set of control measures to assess, audit, and enforce contractually.

### NIS2 (REGULATION (EU) 2022/2555)

NIS2 is an important European framework for cybersecurity. The directive does not focus on the origin of technology, but on managing cyber risks. Organisations required to comply with NIS2 legislation must implement appropriate security measures, clearly assign responsibilities, report incidents and manage, identify, assess, and monitor risks among suppliers and other supply chain partners. In doing so, they must be able to demonstrate which risks they accept, how they mitigate risks, and how they verify that this is done properly.

### DATA ACT (REGULATION (EU) 2023/2854, ALSO KNOWN AS "DATAVERORDENING")

While NIS2 focuses on cybersecurity, the Data Act mostly concerns the control organisations have over their data and their dependence on suppliers. The regulation is intended to make it easier to switch cloud providers or data service providers and to exchange data between systems. This gives organisations greater control over their data and enables them to reduce their dependence on a single supplier. In addition, the Data Act requires providers of data processing services to resist unlawful requests from foreign governments for access to non-personal data stored in the EU. While this does not provide complete protection, it does offer additional legal safeguards and greater transparency. The Data Act thus contributes to digital autonomy by giving organisations more options to manage their data, move it, and switch providers.

[5.] This is a non-exhaustive list of relevant laws and regulations. Other examples include DORA, the CER Directive, the EU Cybersecurity Act, etc. In this white paper, we have sought to address what we believe to be the most common legal concerns.

## GENERAL DATA PROTECTION REGULATION (ALSO KNOWN AS "GDPR" OR "AVG")

The GDPR stipulates that personal data may only be transferred to third countries (outside the EEA) if the conditions for international transfer have been met, for example on the basis of an adequacy decision, appropriate safeguards or an applicable exception. In other words, the level of protection for data subjects must not be undermined by the transfer of data to third countries.

- The European Commission has adopted adequacy decisions for a number of countries. This means that these countries are presumed to offer an appropriate level of data protection. For transfers between the EU and the United States, the EU-US Data Privacy Framework applies.[6] U.S. organisations that have obtained certification from the U.S. Department of Commerce are deemed to offer an adequate level of protection, thereby permitting transfers to these parties under the GDPR. However, this does not eliminate all concerns regarding potential access by foreign authorities. For this reason, organisations often implement additional measures to strengthen actual control over data.

- Appropriate safeguards are available when no such adequacy decision exists. For example, the European Commission has published Standard Contractual Clauses (SCCs).[7] These can be used when an adequacy decision is lacking. In such cases, it must be assessed whether additional technical and organisational measures are necessary to ensure an effectively equivalent level of protection.

The GDPR does not prohibit international data transfers, but it does require a thorough risk assessment and appropriate contractual, technical, and organizational measures. The GDPR also stipulates that, under certain conditions, organisations must make contractual agreements regarding this.

## LIMITATIONS OF THE CLOUD ACT

Discussions about digital sovereignty often refer to the CLOUD Act. This U.S. law can require certain U.S. service providers to hand over data, even when it is stored outside the United States. It is important to note that the CLOUD Act does not grant unlimited access to data. Requests must follow legal procedures and target specific accounts or datasets. The CLOUD Act therefore does not simply provide for generic, mass, or automatic access to data. Additionally, U.S. service providers may challenge a request based on a comity consideration if it conflicts with the laws of another country, such as the GDPR. In that case, a U.S. judge must weigh the various interests against one another. Furthermore, a service provider can only be required to disclose data that it actually possesses or to which it has access. If services are designed in such a way that the provider does not have access to readable customer data, this may in practice restrict access to readable content under the CLOUD Act, although the provision of encrypted data or metadata may still be required depending on the actual configuration. Technical measures such as end-to-end encryption, customer-managed encryption keys (Hold Your Own Key), and zero-access architectures can play an important role in this regard.

Although the CLOUD Act primarily concerns access to data, broader legal and geopolitical circumstances can also affect the availability of services. For example, when sanctions, compliance requirements, or internal risk assessments lead to restrictions or the suspension of service provision.

To the best of our knowledge, requests based on the CLOUD Act are currently used only to a limited extent. In addition, the providers themselves may have an interest in challenging such requests, for example due to reputation, costs, or the potential to set a precedent. Despite these legal safeguards, some uncertainty remains in practice. Therefore, it is prudent to implement additional technical and organisational measures to further mitigate the risks.

[6] Adopted by the European Commission via Implementing Decision (EU) 2023/1795)

[7] See also: EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data

## IN SUMMARY: LEGAL FRAMEWORKS ENABLE THE PROVISION OF INTERNATIONAL SERVICES, BUT COMPLIANCE DEPENDS ON CONTROL MEASURES

These rules demonstrate that providing international digital services is legally feasible, as long as organisations have a clear understanding of their dependencies and take appropriate measures, such as through governance, contracts, and risk management.

At the same time, there is a significant difference between what is legally permitted and what is effectively managed in practice. Laws and regulations may set conditions, but they do not automatically guarantee the security and availability of systems and data. This requires effective technical and organisational measures.

As a result, the discussion shifts from "sovereignty" to "demonstrable control": which measures ensure that risks are acceptable and demonstrably managed? An international supplier can, when agreements and infrastructure are properly arranged, sometimes even offer better security than a smaller European provider.

This white paper demonstrates how organisations can continue to operate securely and with demonstrable control within the applicable legal frameworks, even if full digital autonomy is not always feasible in the current geopolitical situation.

Legislation provides the framework, but the details are worked out in practice. In response to this development, hyperscalers (large international cloud providers with global infrastructure and economies of scale, such as Microsoft, Google, and Amazon) have developed "sovereign" versions of their services. In the next chapter, we will examine how these solutions contribute to digital autonomy and where their limitations lie.

# Sovereign cloud: building blocks, but not a final solution

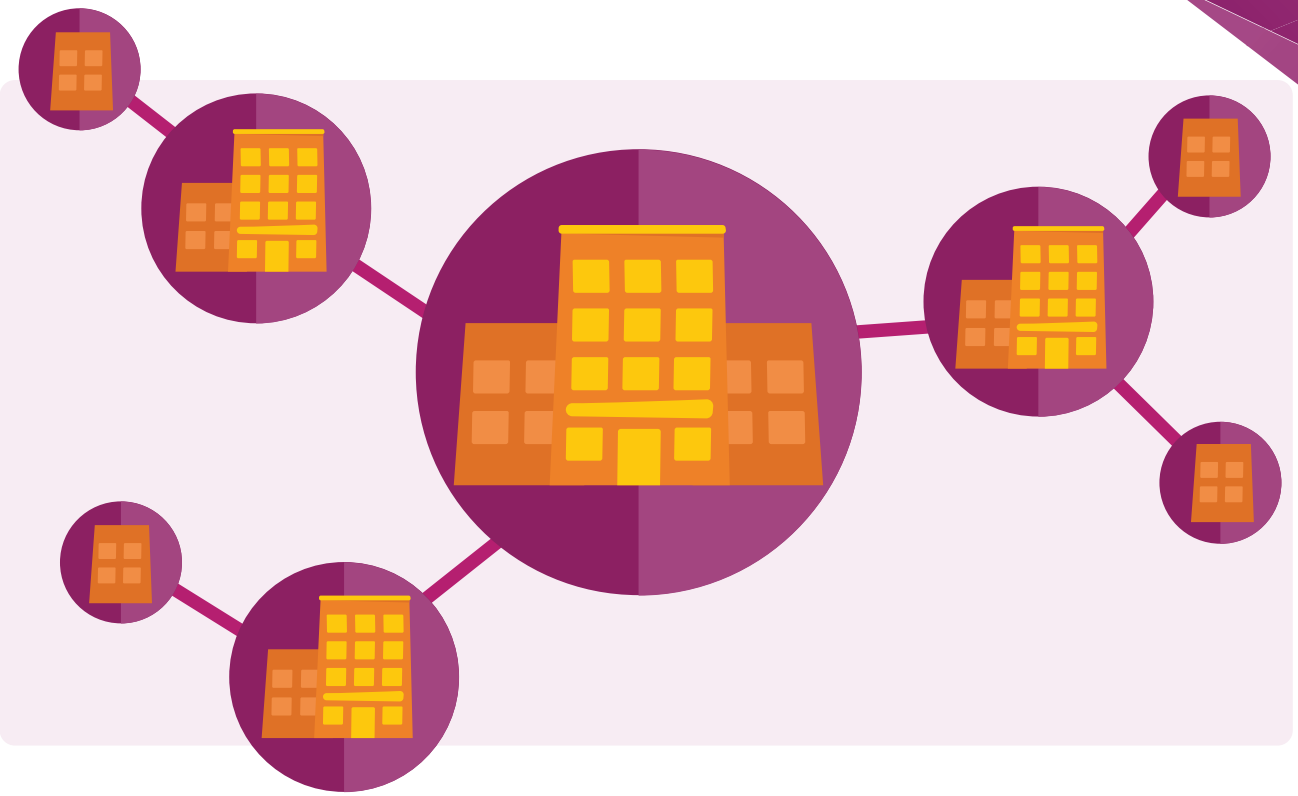
In response to the debate on digital sovereignty and autonomy, and growing concerns among European organisations, major international cloud providers have generally developed a “sovereign” version of their cloud services. These solutions are designed to address concerns regarding confidentiality, integrity, and availability, and combine legal, organisational, and technical measures.

In practice, the sovereign alternatives offered by these cloud providers increase control and transparency, but do not eliminate the underlying dependency. For example, establishing an EU entity and employing EU staff may raise legal barriers to accessing data, but this offers no guarantee against influence exerted through the foreign parent company. Additional measures are also being taken on the technical front. Mechanisms such as end-to-end encryption and trusted computing can strengthen the confidentiality and integrity of the data. At the same time, these solutions warrant a nuanced view. With end-to-end encryption using customer-controlled keys, the provider remains responsible for the software layer where encryption and decryption take place. In situations where that same provider is part of the threat model, this can limit the effectiveness of this measure. End-to-end encryption thus remains valuable, but especially in scenarios where the infrastructure is not trusted and the application layer is, for example when data is stored in the cloud but processed via proprietary software. In addition, the major international cloud providers are only transparent to a certain extent about how they handle access requests from foreign authorities. As a result, uncertainty remains regarding the extent to which the measures taken can actually limit or prevent such requests.

Taken together, these developments show that cloud providers are increasingly supporting digital sovereignty, but that none of the solutions offered achieve full autonomy.

The European Cloud Sovereignty Framework (SEAL) can help provide a clearer understanding of these developments. The Framework provides a practical assessment framework with so-called Sovereignty Effective Assurance Levels (SEAL), which helps organisations assess the extent to which they have control over their data, access, security, and dependencies. The levels range from SEAL-0 (no specific sovereignty measures) to SEAL-4 (full digital sovereignty under exclusively European law). The levels are based on various aspects of sovereignty, such as legal independence, technological control, and supply chain dependencies. This enables organisations to better assess and compare the degree of digital sovereignty. In practice, this classification looks as follows:

| SEAL LEVEL | DESCRIPTION |
|---|---|
| SEAL-0 | No measures to assert sovereignty; complete dependence on external parties |
| SEAL-1 | Formal legal agreements, but limited technical oversight |
| SEAL-2 | Data remains within EU borders; basic safeguards for access and management |
| SEAL-3 | Digital resilience under EU oversight; operational independence of non-EU parties |
| SEAL-4 | Full sovereignty; all components fall exclusively under EU jurisdiction and administration |



Although the Cloud Sovereignty Framework is primarily relevant for cloud providers who wish to assess safeguards of sovereignty, it may also be relevant for other organisations in the supply chain. When cloud platforms are used to provide services to (semi-)governmental entities, providers and partners can demonstrate that they comply with the relevant sovereignty requirements. This is often done through contracts, tenders, and audits. The SEAL framework thus offers a way to assess digital sovereignty and make it a topic of discussion, even outside the immediate context of tenders.

For most organizations, however, SEAL-4 is not a realistic or necessary goal. The strength of the SEAL levels lies primarily in the ability to make an informed assessment for each service, data domain, or use case and to determine an appropriate level based on risks and dependencies. The framework can help organizations implement targeted improvement measures without requiring full digital sovereignty as a starting point. Practical application is still limited because cloud providers do not always provide sufficient insight into their approach. As a result, it is often unclear how the major cloud providers relate to the various SEAL levels and what commitments they are willing to make in this regard. Consequently, it is difficult for organisations to determine whether a specific SEAL level is being met and to demonstrate this. This does not mean that cloud providers are not taking steps toward higher SEAL levels, but rather that these steps are currently difficult to compare and verify.

For cybersecurity and IT service providers, this means that, in practice, they remain heavily dependent on the implementation choices made by cloud providers. Although the framework helps structure requirements and expectations, the actual safeguarding of digital sovereignty depends on additional technical, organizational, and contractual measures. Digital autonomy is therefore ultimately not determined by the choice of a specific cloud variant, but by the extent to which organisations themselves retain control over access to data, keys, architecture, and continuity.

In short, the current solutions offered by cloud providers provide valuable building blocks, but not a complete solution. Digital autonomy only exists when organisations combine these capabilities with their own technical, organisational, and contractual measures. In the next chapter, we translate this into concrete courses of action.

# Digital autonomy in practice: from debate to control

## This is not a threat — it is an opportunity

The preceding chapters have identified the threats: the geopolitical vulnerability of our digital dependencies, the legal complexities of cross-border data processing, and the specific scenarios in which those dependencies can result in operational and strategic harm. The question that remains is not whether organisations should act, but how they can do so most effectively.

The answer lies closer to home than the political debate sometimes suggests. For anyone who carefully analyses the threats to digital sovereignty will recognize an issue that security professionals have been addressing for years: how do you protect sensitive data from unauthorized access, and how do you ensure that critical business processes continue to function when a supplier or environment fails? The geopolitical context adds a new dimension to this issue but does not fundamentally change its nature.

What is changing, however, is the priority that executives assign to this issue. Discussion about digital sovereignty is making its way into the boardroom more often than traditional technical or cybersecurity arguments, because the sovereignty issue directly impacts strategic interests and business continuity. This creates a unique situation: the strategic agenda of executives and the operational agenda of security professionals are now aligned.
The strategic value of security investments increases significantly when those same investments simultaneously strengthen the organisation's digital sovereignty and autonomy. In fact, measures that make organisations resilient to geopolitical risks also arm them against cyber threats.

For security professionals and Dutch security providers, this is therefore not a time to wait and see, but to take a clear stance. This chapter offers practical guidance on how to translate the sovereignty discussion into concrete measures that align with your organisation's risk profile and can be implemented using existing security expertise supported by sovereign Dutch and European solutions.

## Risk as a guide

The tendency to approach digital sovereignty as a broad organisational issue is understandable, but it leads to difficulties in practice. Not every application, system, or dataset requires the same level of protection. The first and most fundamental step, therefore, is not to define a sovereignty strategy, but to identify what is truly at stake.

Two questions are central to this:

1. What data is so sensitive that access by foreign authorities — whether or not through legal mechanisms such as the CLOUD Act — poses unacceptable risks?

2. Which business processes are so critical that (partial) disruption or restriction of service delivery — for example, due to sanctions, export restrictions, or geopolitical pressure — directly jeopardizes the organisation's continuity?

In the current geopolitical context, it is virtually impossible to answer the question of how likely it is that a foreign government will actually demand access, or that a supplier will cease providing its services under political pressure.

Organizations cannot always determine whether a threat exists, but they can assess how vulnerable they are to it, how quickly a threat could have consequences, and what the impact of those consequences would be. These factors help in determining which measures should be prioritized.

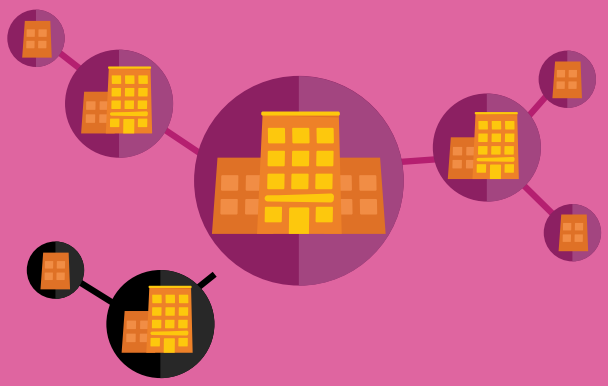
The SEAL framework can serve as a reference in this regard. A higher SEAL classification indicates how the infrastructure is structured from a legal and organisational perspective but says nothing about how it is used in practice. Organisations therefore remain responsible for implementing additional measures. Even the "sovereign" cloud solutions offered by major cloud providers do not eliminate that responsibility. Those seeking to strengthen digital sovereignty and autonomy must implement measures that are not dependent on a single specific provider. Ultimately, it is not about a fully sovereign solution, but about demonstrable risk management: measures that reduce risks and whose effectiveness can be verified, regardless of the chosen provider.

# Two threats, one discipline

Despite their geopolitical context, the threats described in the preceding chapters can be boiled down to two fundamental issues that every security professional recognizes.

### 1. DATA SOVEREIGNTY

The threat that sensitive data could become accessible to foreign governments based on legal requests (for example, under the CLOUD Act) is essentially a confidentiality issue. An important measure is: encrypt the data and manage the encryption keys yourself, for example using a Dutch or European key management solution. This makes it much more difficult for foreign parties to access the content of the data. The infrastructure on which data is stored may be located abroad — what matters is that key management does not rest with the provider. Whoever manages the key largely determines who has access to the data.



### 2. OPERATIONAL AUTONOMY

The likelihood that critical business processes will fail because a supplier ceases its services due to geopolitical pressure or sanctions is primarily a risk to service availability. This raises the question of how well an organisation can continue to function if a supplier, system, or environment becomes unavailable. The measures organisations take against ransomware, data breaches, or data center outages often also help mitigate these types of geopolitical disruptions.

That is the crux of this white paper. Digital sovereignty and autonomy are not entirely new topics that require new solutions. They are well-known security and resilience issues that have received greater attention. International infrastructure can be used effectively, if the organisation itself demonstrably retains control over the security and continuity of its systems and services.

## From resilient to adaptive

Resilience has become a familiar concept for most organisations. The ability to recover after an incident — whether it's a ransomware attack, a data center outage, or the loss of a supplier — is essential to any mature security strategy. In the context of digital autonomy, however, resilience takes on an additional dimension.

The geopolitical threats described in this paper often resemble "traditional cyber threats" in their consequences: they can emerge gradually but also strike suddenly and decisively. A supplier subject to sanctions does not merely suspend operations temporarily but may cease them permanently. Once data has been disclosed, it is often irreversible in practice. That is why it is important to restrict access through technical measures. Those who are prepared solely for recovery are missing a crucial step in their preparedness.

A mature approach to resilience therefore starts with graceful degradation: the principle whereby systems are designed so that if one component fails, the remaining functions continue to operate. This prevents a complete operational shutdown. Critical processes can continue to run while less essential functions are temporarily suspended. This requires deliberate architectural choices when designing systems and processes or a reevaluation of previously made architectural choices. Applying graceful degradation significantly reduces the risk of total failure.

The next step beyond resilience is adaptive architecture. Whereas resilience focuses on returning to the original situation, an adaptive architecture is designed for continuity under changing circumstances. This means that critical business processes can continue to run when a primary supplier fails. You achieve this by having an alternative environment ready in advance — for example, a private cloud or an environment with a European supplier — that can be activated at the right moment.

The "ultimate recovery site" — a concept that has long been part of traditional business continuity planning — takes on new strategic significance in this context. It is no longer simply a matter of storing a copy of data at an independent location, but rather of building an environment that can be put into operational use when the primary environment is no longer available or reliable.

## What does this mean in practice

This chapter outlines the specific steps organisations can take to achieve data sovereignty and operational autonomy. The success of these measures depends on effective leadership within the organisation and clear agreements with suppliers.


### KNOW WHAT YOU HAVE TO LOSE

The foundation of everything is insight. Which business processes are essential within the organisation? Which data is so sensitive that access by third parties is unacceptable? Which other parties do you depend on, and what happens if one of those parties fails? How vulnerable are you, how quickly would you notice this, and what would be the impact on the organisation?

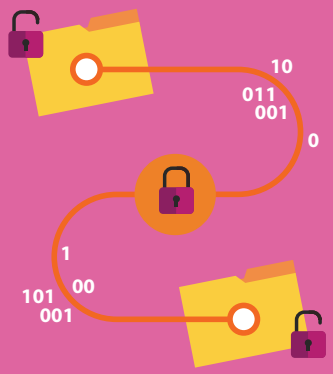
This forms the core of the organisation and serves as the starting point for all further measures to protect systems and processes. Not every system or process requires the same level of protection. A CRM system containing marketing data poses different risks than software that is essential for day-to-day operations. That is why it is important to consciously determine which systems and processes are the most critical. This is not a limitation, but rather a prerequisite for effective protection.

*Question for the executive: if our three most important services were to go down or be blocked tomorrow, which ones would they be, how long could we continue to operate, and who would be the first to call us?*


## ENCRYPTION AND KEY MANAGEMENT

For data that must under no circumstances be accessible to foreign authorities, encryption with independent key management is one of the most important measures. Proper key management means that the organisation — or a European party appointed by it — retains control over the keys. When the encryption keys are held by the same party as the data itself, encryption offers only limited additional protection in that scenario. “Bring Your Own Key” or “Hold Your Own Key” arrangements, supported by Dutch or European encryption management solutions, make the security layer independent of the infrastructure provider.

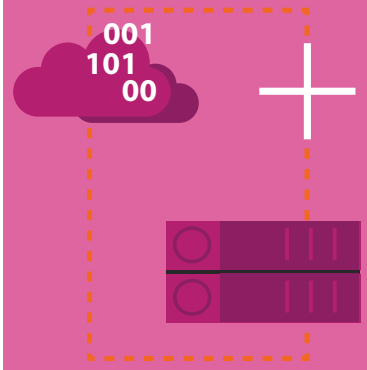
*The question for the CISO: Who can access our critical data without our permission—technically, legally, or contractually?*




## PORTABILITY AND EXIT

Vendor lock-in is rarely confined to contracts alone — it stems primarily from a vendor’s technical integration into digital architecture. A modular architecture — based on open standards wherever possible — increases the technical flexibility to migrate when necessary. An exit strategy is only a true exit strategy if it is practically feasible: is the data actually exportable, has a migration ever been tested, and has an alternative environment been developed and (periodically) tested?

*Question for the CIO: When was the last time we successfully exported our own data or tested a migration?*




## RESILIENCE AND RECOVERY

Backups located in the same environment as the production environment — whether with the same provider or accessible via the same account — offer insufficient protection if that environment goes down or is blocked. An independent recovery environment — with a separate provider or on a separate account — is the minimum requirement for true business continuity. Combined with graceful degradation and adaptive architecture as described in the previous section, this creates resilience that goes beyond recovery alone.

*Question for the CIO: If our primary cloud provider were to become unavailable tomorrow, who would take the lead internally, and do we have sufficient in-house expertise to handle that situation?*

### ECOSYSTEM AND COLLABORATION

Digital autonomy is not a solo endeavor. The challenges surrounding dependency, jurisdiction, and resilience are broad enough to warrant a collaborative approach. Organisations that actively participate in sector-specific networks and public-private partnerships not only increase their own risk awareness but also collectively influence market standards, procurement requirements, and laws and regulations.

*Question for the executive: Are we affiliated with relevant sectoral networks focused on digital resilience, and do we actively contribute to knowledge sharing that also strengthens our own position?*

*Note that the measures mentioned work best in combination: technology, organisation/governance, people, and contracts reinforce one another.*

## Conclusion

In recent years, the discussion on digital sovereignty has shifted from academic debate to administrative urgency. That is a positive development, but translating political urgency into operational action remains a challenge for many organisations. This paper has attempted to make that translation.

The central conclusion is as simple as it is far-reaching. The threats arising from our digital dependencies — unauthorized access to sensitive data, disruption of critical processes due to geopolitical pressure — are not a new category of risk. They are a new manifestation of issues that the security field has been familiar with for decades. Confidentiality, availability, integrity, resilience: the concepts are well-known, the solutions are available, and the expertise is in place.

What sets this apart is the political and administrative context that currently reinforces the priority of these measures. The strategic rationale for encryption with independent key management, for an adaptive architecture, and for an independent recovery environment (preferably within a legal and operational framework that the organisation deems verifiable) has grown stronger. Not because technology has changed, but because the world around it has.

This is not an argument against international suppliers: international technology can fit perfectly within this approach, as long as the technical and organisational controls are demonstrably in place and dependencies remain manageable.

For security professionals, now is the time to capitalize on this strengthened business case. For executives, now is the time to translate the sovereignty discussion into concrete investment decisions. And for Dutch and European security providers, now is the time to demonstrate what sovereign security means in practice: not an alternative infrastructure, but an independent security layer that complements and strengthens the organisation’s infrastructure choice.

At its core, this is not a political debate. This is business continuity.

# Appendix: From risk analysis to action

The measures required to ensure digital sovereignty and autonomy in practice vary from organisation to organisation. Which measures should be prioritized depends on the organisation's risk profile. The decision tree below helps determine where the focus should lie based on two key questions.

## Step 1: Determine your starting point

Answer the following two questions:

**QUESTION A:** Does the organisation possess data that must under no circumstances be accessible to foreign authorities?

**QUESTION B:** Does the organisation have critical business processes that must not be disrupted if a supplier fails, ceases operations, or is subject to sanctions?

Both questions may apply simultaneously. For each question answered with "yes," follow the corresponding path.

## Step 2: Determine the urgency by rail

For each applicable track, answer three follow-up questions that determine the priority of the measures:

| QUESTION | LOW | MEDIUM | HIGH |
|---|---|---|---|
| How vulnerable are you? | The organisation processes little sensitive data and has limited reliance on non-sovereign IT* | The organisation processes sensitive data and relies in part on non-sovereign IT systems for its management or storage | The organisation processes highly sensitive data and relies heavily on non-sovereign IT infrastructure or services |
| How quickly could the threat materialize? | The threat gives plenty of advance warning, so there is time to respond | The threat is partly foreseeable, but the time pressure is real | A threat can arise suddenly or persist over time without warning |
| What would be the impact if this scenario were to occur? | Limited operational or reputational damage | Significant damage, but recovery is possible | Existential harm to the organisation or its customers (e.g., prolonged disruption of critical services, jeopardy to statutory duties, significant societal impact). |

* The term "non-sovereign IT" refers to IT services or components over which the organisation lacks sufficient demonstrable control regarding rules governing access, key management, auditability/transparency, and exit/continuity, resulting in unmanageable dependencies (regardless of the supplier's origin). In other words, "outside the organisation's control."

# Step 3: Prioritize measures by track

### TRACK A — DATA SOVEREIGNTY

| Priority | Measure |
|---|---|
| **Direct** | Identify what sensitive data is stored on foreign infrastructure and who is responsible for managing the keys |
| **Short term** | Implement independent key management under European oversight (e.g., BYOK, HYOK, or external key management) |
| **Medium term** | Contractually review who can have technical and legal access to critical data and adjust where necessary |
| **Structural** | Incorporate encryption and key management as a design principle in new systems and applications |

### TRACK B – OPERATIONAL AUTONOMY

| Priority | Measure |
|---|---|
| **Direct** | Identify which critical processes depend on a single supplier and what the impact would be in the event of failure |
| **Short term** | Set up an independent recovery environment with an independent vendor or in a separate environment (preferably under a framework that the organisation deems auditable) and test it periodically (e.g., semi-annually) |
| **Medium term** | Adapt architectural choices to the principle of graceful degradation so that sub-functions continue to operate in the event of failure |
| **Structural** | Build an adaptive architecture that makes switching to an alternative environment operationally possible |

### BOTH TRACKS

| Priority | Measure |
|---|---|
| **Direct** | Join sectoral networks and public-private partnerships regarding digital resilience |
| **Structural** | Actively contribute to knowledge sharing and influencing market standards and procurement requirements |

# Abbreviations and glossary (in alphabetical order)

## A

### ADAPTIVE ARCHITECTURE
An IT architecture that focuses not only on recovery after a disruption, but also on maintaining operational functionality under changing circumstances.

### ADEQUACY DECISION
A decision by the European Commission determining that a country outside the EU provides an adequate level of protection for personal data. This allows personal data to be transferred to that country under certain conditions.

### AUDITABILITY
The extent to which access, changes, and actions within systems are controllable and verifiable. An audit is an investigation used to assess how reality within a defined area relates to a specific (established) standard.

### AZURE
Microsoft's cloud platform on which organisations can run infrastructure, storage, applications, and digital services.

## B

### BACKUP
A copy of data or digital systems. This allows data or systems to be restored if the original is damaged or lost..

### BEST PRACTICES
Proven effective working methods and security measures that are commonly applied within an industry or field.

### BRING YOUR OWN KEY (BYOK)
A form of key management in which an organisation provides its own encryption keys for data in a cloud environment. This allows the organisation to maintain greater control over access to data.

### BUSINESS CONTINUITY PLANNING
Preparing processes, systems, and organisational structures so that critical services can continue to function during disruptions or crises.

## C

### CISO (CHIEF INFORMATION SECURITY OFFICER)
The employee responsible for cybersecurity within an organization. A strategic-level role.

### CLOUD
Making IT services, such as hardware and software, accessible via a network, usually the Internet. Examples of cloud services include Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS).

### CLOUD ACT
U.S. legislation that, under certain conditions, can require service providers that fall under American jurisdiction to make data available to U.S. authorities, even when that data is stored outside the United States.

### CLOUD SOVEREIGNTY FRAMEWORK
A European framework that enables organisations to assess the level of digital sovereignty in cloud environments.

### COMPLIANCE
The activities undertaken by an individual or organisation to meet specific requirements. These may include laws, industry standards, or internal organisational policies.

### CONFIDENTIALITY
The assurance that information and/or digital services, processes, or systems are accessible only to authorized individuals or software.

## D

### DATA ACT / DATA REGULATION
A European regulation aimed, among other things, at improving data portability and interoperability and reducing vendor lock-in in cloud and data services.

### DATA RESIDENCY
The physical location where data is stored.

### DATA BREACH
A common term for a breach in relation to personal data. In the context of the General Data Protection Regulation, a data breach is a layman's term for a "personal data breach," meaning an incident that compromises the integrity, availability, and/or confidentiality of personal data. Examples include ransomware attacks or an email with all recipients listed in the "To" field.

### DATACENTER
A physical location where servers, storage, and network equipment are managed.

### DIGITAL AUTONOMY
An organisation's ability to make independent decisions in the digital domain, without undesirable dependencies that limit that freedom of action.

### DIGITAL SOVEREIGNTY
The extent to which an organisation or government retains control over data, infrastructure, systems, and digital dependencies, including legal and administrative oversight thereof.

### DIGITAL RESILIENCE
The ability to prevent, detect, mitigate, and recover from breaches of the confidentiality and integrity of information, as well as disruptions to business processes, while continuing to function as effectively as possible.

## E

### ENCRYPTION
Converting information into a code so that others cannot read it. This is done when sensitive information needs to be stored or transmitted securely.

### END-TO-END ENCRYPTION
A form of encryption in which data is readable only by the sender and recipient, and not by the infrastructure provider or any intermediaries.

### EXIT STRATEGY
A practical, actionable plan to migrate data, systems, and processes in a controlled manner to another provider or environment.

## G

### GDPR (GENERAL DATA PROTECTION REGULATION)
The GDPR (AVG in Dutch) is directly applicable European regulation for the protection of personal data. In the Netherlands, the AVG is supplemented by the Implementation Act of the General Data Protection Regulation and is the successor to the Personal Data Protection Act.

### GEOPOLITICS
International political and economic power dynamics that influence technology, trade, legislation, and digital dependencies.

### GOVERNANCE
The structure of responsibilities, decision-making, oversight, and control within an organisation.

### GRACEFUL DEGRADATION
An architectural principle whereby systems continue to function partially during disruptions rather than failing completely.

## H

### HOLD YOUR OWN KEY (HYOK)
A form of key management in which an organisation retains full control over encryption keys, independent of the cloud provider.

## I

### IEC62443
International standard for cybersecurity in industrial automation and operational technology.

### INCIDENT RESPONSE
Responding to a cyber incident. It is a (structured) approach at all levels: operational, tactical, and strategic. Incident response can be viewed as a kind of fire department for cyber incidents.

### INTEGRITY (INFORMATION SECURITY)
1. Regarding data: accurate and complete information, and the processing of information. 2. Regarding individuals: a person's reliability. 3. Regarding digital services, processes, or systems: their proper functioning.

### INTEROPERABILITY
The ability of systems, applications, and services to exchange data and work together.

### ISO27001
International standard for establishing and managing information security.

## J

### JURISDICTION
The legal jurisdiction and laws governing an organisation, supplier, or infrastructure.

## K

### KEY MANAGEMENT
The management of encryption keys that determine who has access to encrypted data.

## L

### LOGGING
The recording of events, access, and system activities to enable control, monitoring, and investigation.

## N

### NEN7510
Dutch standard for information security in the healthcare sector.

### NIS2 DIRECTIVE
European directive that requires certain essential and important entities to demonstrably manage cyber risks and supply chain dependencies.

## O

### ON-PREMISES IT
IT systems that run on infrastructure managed in-house, such as in a company-owned data center.

## P

### PORTABILITY
The ability to easily move data, applications, or systems to a different environment or provider.

### PRIVATE CLOUD
A cloud environment used exclusively by a single organisation.

## R

### RANSOMWARE
Malicious software in which a victim is extorted after their digital system or the files on it have been locked with a code. The attacker offers the code in exchange for payment, so the victim can regain access. But even that is not guaranteed. Ransomware is a combination of the words “ransom” and “software.” These days, the actual software is just a small step in the overall attack that takes place. All these steps together form the Ransomware Killchain.

### RECOVERY SITE / ULTIMATE RECOVERY SITE
An independent environment that can be deployed when the primary IT environment fails or is no longer available.

### RESILIENCE
An organisation’s ability to withstand disruptions and continue to function effectively.

### RISK-BASED APPROACH
An approach in which security measures are tailored to the sensitivity of data, critical processes, and dependencies.

## S

### SCA (STORED COMMUNICATIONS ACT)
U.S. legislation that forms part of the legal framework under which access to stored digital communications may be sought.

### SEAL (SOVEREIGNTY EFFECTIVE ASSURANCE LEVELS)
A classification model within the European Cloud Sovereignty Framework that allows for the assessment of the degree of digital sovereignty. The levels range from complete dependence on external parties (SEAL-0) to full digital sovereignty under exclusive EU jurisdiction (SEAL-4).

### SUPPLY CHAIN
The network of suppliers, service providers, and technology partners on which an organisation depends.

## T

### THREAT INTELLIGENCE CENTER
A dedicated organisational function that collects, analyses, and uses threat intelligence to detect and respond to cyber threats at an early stage.

### TRUSTED COMPUTING
Technology designed to ensure that systems and hardware operate in a secure, controlled, and trustworthy manner.

## V

### VENDOR LOCK-IN
A situation in which switching to another supplier becomes technically, organisationally, or contractually difficult or costly.

## Z

### ZERO-ACCESS ARCHITECTURE
An architecture in which a vendor has no technical access to customer data, even when the infrastructure is managed by that vendor.