Towards digital autonomy

Increased control over digital dependencies

Authority for Consumers & Markets | AFM | AP | DeNederlandscheBank EUROSYSTEEM | Dutch Authority for Digital Infrastructure, Ministry of Economic Affairs

Contents

Key messages and recommendations

Key messages

- Strengthening digital autonomy goes beyond individual decision-making by firms and institutions that use IT services. Making this complex transition possible also requires coordinated and collective efforts.
- Digital autonomy means firms and institutions that use IT services have freedom of choice and self-determination with the aim of enhancing the resilience of their business processes. They must be able to move when circumstances require it.
- Digital autonomy also requires deliberate trade-offs between autonomy, cost, and functionality: not every process requires the same level of autonomy. It is particularly important to implement additional safeguards for vital processes. Having a European fallback option should, at the very least, be a prerequisite.
- Public authorities can play a key role by acting as launch customers for European digital services based on open standards, and by collaborating and pooling demand.
- Incorporating digital autonomy into tendering processes is entirely feasible within the current procurement rules. For example, compliance with specific standards can be required, and digital autonomy can be incorporated by imposing specific, verifiable requirements and award criteria that protect against undesirable dependencies and exposure to non-European legal obligations.
- We also call on firms and institutions to work together to promote digital autonomy, for example by acting as launch customers for sector-specific IT services. The Competition Act (*Mededingingswet*) provides ample scope for such initiatives.
- Equally important is that firms and institutions increase optionality and portability in their IT architecture and that they minimise vendor lock-in, for example by means of containerisation, open-source software and open standards. IT vendors should design their products and services to support switching to other vendors and facilitate integration with other (European) solutions.

Recommendations

We call on all organisations to explicitly include digital autonomy as a quality criterion in IT services tendering, procurement and contract renewal. We recommend using specific decision-making frameworks that set the appropriate level of digital autonomy for each type of process and that spells out how autonomy relates to other objectives, such as cost and functionality. The autonomy criterion must be translated into verifiable requirements in tender documents and contracts, such as requirements relating to data location, the use of open standards, interoperability, adequate exit options and vendor lock-in mitigation. Public authorities, firms and institutions can make use of the European Union's Data Act, which requires cloud providers to facilitate data portability and interoperability. It is also important to create a more level playing field by primarily using functional requirements rather than product-specific requirements as the basis for procurement and tender processes. Investing in in-house knowledge and staff ensures that crucial expertise does not rest entirely with vendors, while giving

buyers greater control. The prevailing laws and regulations provide ample scope for focusing on digital autonomy. We invite organisations to engage in early consultation and dialogue, for example if they are uncertain about interpretation of the rules.

Policymakers and legislators

- Ensure that the public authorities act as launch customers by stipulating that a certain proportion of cloud demand must meet the highest sovereignty requirements.
- Introduce legal requirements regarding the availability of a European fallback option for vital processes.
- Strengthen the investment and business environment for European IT providers, including by improving access to capital, reducing fragmentation of the single market, and targeting the limited space available for data centres towards projects that contribute to Europe's competitiveness, autonomy and resilience.
- Ensure that an effective system for screening investments is in place to protect vital sectors from takeovers that could pose risks.

Public authorities as purchasers of IT services

- Make use of the scope provided by the Public Procurement Act (*Aanbestedingswet*) to incorporate digital autonomy by imposing specific, verifiable requirements and award criteria. In doing so, explicitly capitalise on the options available to give preference to solutions that meet the highest sovereignty requirements.
- Procure jointly, for example through procurement collectives and joint framework agreements.

Businesses and institutions

- Work together within sectors to set joint requirements for IT providers and invest in European alternatives. The Competition Act provides ample scope for such initiatives.
- Create opportunities for switching by developing and testing exit and transition plans, limiting vendor lock-in and reducing short-term risks by adopting multi-vendor strategies and using open standards and interoperability as an explicit design principle in IT architecture.
- In each decision to contract for additional cloud services, explicitly consider the risk of vendor lock-in.
- Take steps to mitigate risks in the short term, such as managing encryption keys in-house, and ensure EU-based fallback options are available for data and critical software.

IT vendors

- Work with other vendors and stakeholders in the ecosystem to develop scalable European cloud and IT services, allowing alternatives to today's dominant non-European providers to emerge. The Competition Act provides sufficient scope for such initiatives.
- Develop services that explicitly meet public and private requirements regarding digital autonomy, such as interoperability, open-source solutions, open standards and data portability.
- Design products and services to support switching to other vendors, limit vendor lock-in and facilitate integration with other (European) solutions.

Introduction

This position paper has been authored jointly by the ACM, the AFM, AP, DNB and the RDI. Together, we seek to contribute to the transition towards greater digital autonomy and to reduced dependence on today's dominant non-European IT vendors, with an eye to boosting the resilience, continuity and security of business processes. The Netherlands' and Europe's digital infrastructure relies heavily on a small number of – mostly non-European – tech firms providing cloud services, software and hardware. This entails concentration and systemic risks, particularly in the current geopolitical climate. Moreover, there are risks to Europe's economic development as various scenarios could materialise. For example, services could suddenly be disrupted due to outages, a cyber incident or third-country political pressure, or third countries could demand to have access to data, for instance through legislation such as the United States' CLOUD Act. Furthermore, vendor lock-in makes switching to other providers and spreading risk difficult and costly, thereby weakening negotiating positions and potentially leading to higher prices. For public authorities, financial institutions and other vital organisations, digital dependency therefore has a direct impact on the security and continuity of service provision. In the long term, these dependencies will undermine the economy's earning capacity.

Making the Dutch economy more resilient by strengthening digital autonomy has now become a widely shared objective. The Dutch government's coalition agreement explicitly identifies digital autonomy as a guiding principle for government policy. The Dutch Digitalisation Strategy and the government's vision on digital autonomy and sovereignty also emphasise the importance of self-determination, freedom of choice and switching options in the digital domain. Nevertheless, as supervisory authorities we note that, in practice, dependencies continue to grow. The situation in the Netherlands is illustrative of the broader European trend, but effective solutions must largely be implemented at European level. Digital autonomy requires a more careful balance in terms of dependencies on regions outside Europe. This requires not only mitigating risks, but also actively bolstering the European digital ecosystem, including by further developing strategic capabilities, increasing the diversity of IT services available, enhanced pooling of organisations' purchasing power and fostering collaboration.

For all five supervisory authorities, this issue is of great importance in the context of their own mandate. The Netherlands Authority for Consumers and Markets (ACM) notes that vendor lock-in at major technology vendors restricts freedom of choice, thereby hindering the proper functioning of the market.[1] As the supervisory authority responsible for enforcing legislation such as the Telecommunications Act (*Telecommunicatiewet*), NIS2, eIDAS and CSA, the Dutch Authority for Digital Infrastructure (RDI) has observed that the Netherlands' digital resilience depends on a small number of firms, which entails systemic risks.[2] The Dutch Authority for the Financial Markets (AFM) and De Nederlandsche Bank (DNB) supervise the sound and ethical business operations of financial institutions and, more specifically, their digital resilience as required by the Digital Operational Resilience Act (DORA). The AFM and DNB note that increasing reliance on a limited number of – mostly non-European – technology providers leads to concentration and systemic

1 State of the Market 2026 | ACM
2 Monitoring the use of cloud services | RDI (available in Dutch)

risks, which could jeopardise the stability of the system and harm the interests of consumers.[3] Digital dependence also entails the risk that personal data within vital processes may become unavailable on a large scale for a prolonged period, or may be compromised. Under the GDPR, both public authorities and businesses are required to take measures to prevent this. The Dutch Data Protection Authority (AP) considers it of the utmost importance that these vital processes are better protected.[4]

It is particularly important for firms and institutions to spread their risks, rather than putting their eggs in one basket when it comes to digital infrastructure and services. At present, Europe relies on critical infrastructure from various regions outside Europe in areas such as cloud services, security and data centres. The recommendations in this position paper are therefore not directed against any particular jurisdiction or region that offers these services or infrastructure. Nor does the position paper contain any new rules or obligations for firms and institutions subject to our supervision. However, Europe is lagging behind when it comes to digital innovation, and it must catch up for both strategic and economic reasons. This ambition is also central to the European Commission's recently presented Tech Sovereignty Package, which aims to structurally strengthen Europe's digital capabilities and reduce strategic dependencies.

3 Digital dependence of the financial sector | DNB, AFM
4 Letter to the Minister of Economic Affairs on digital sovereignty | AP (available in Dutch)

Digital autonomy

Digital autonomy requires freedom of choice

Digital autonomy means public authorities and organisations can make their own decisions about their IT and enjoy genuine self-determination. We do not at all mean to suggest that all technology must be developed in-house or that absolute technological independence must be achieved. The focus should be on minimising unwanted strategic dependencies and ensuring freedom of choice when switching between vendors. This also offers a framework for action should adverse scenarios materialise.

Digital autonomy requires a fundamental rethink of the design of the IT architecture. Freedom of choice can only be achieved when the IT architecture is designed to be open, based on open standards and interoperable solutions, in such a way that public authorities and organisations are not tied to a single vendor. At present, however, the dominance of cloud solutions offered by (non-European) hyperscalers is creating significant dependencies and vendor lock-in.

In the current geopolitical context, digital autonomy is also associated with legal sovereignty. Having to rely on non-European IT service providers means organisations could be subject to foreign legislation, which may limit their control over data and digital processes. As long as there are still insufficient fully-fledged alternatives available in Europe, it is conceivable that state actors might weaponise dependence on non-European service providers. Extending the range of available European IT services is key to improving resilience to scenarios of this kind. In this context, the concept of legal sovereignty is important – certain legal risks must be prevented, such as situations in which non-European authorities unilaterally demand to have access to data.

Digital autonomy requires deliberate trade-offs

Digital autonomy is not an end in itself, but a matter of making deliberate and proportionate trade-offs. Not every application requires the same level of autonomy or sovereignty, which is why it is necessary to categorise processes and services and explicitly specify what level of autonomy and control is required for each category. This distinction is already reflected in legislation. In the financial sector, DORA sets out requirements for 'critical and important'[5] functions, while in several other sectors, the NIS2 Directive sets out rules for 'essential and important'[6] entities and the services they provide. Furthermore, some of these functions and entities can also be classified as 'vital' if failure, disruption or manipulation could lead to serious social upheaval, significant economic damage or – in the worst-case scenario – a threat to national security. In the financial sector, such processes include payment and securities transactions, and balance management by banks.[7]

5 Critical or important functions are those whose disruption would materially impair a financial entity's financial performance or the soundness or continuity of its services and activities.

6 Essential and important entities are those that are critical due to the sector in which they operate or the type of services they provide, taking their size into account.

7 For a complete overview of vital processes, see Aanpak vitaal | National Coordinator for Counterterrorism and Security, and for further information on vital processes in the financial sector, see Parliamentary Document 30821, No. 323 | Overheid.nl > Official Announcements (both documents available in Dutch).

It is particularly important to implement additional safeguards for vital processes to limit dependencies and mitigate concentration risks. It is crucial to prevent sudden service disruptions due to outages, a cyber incident or third-country political pressure, or because third countries demand access to data. When national security is at stake, legislation also provides the scope to exclude service providers from a tender process on the basis of sovereignty risks.

Given the geopolitical risks, having a European fallback option specifically for vital processes should be a prerequisite to ensure continuity. We are asking European legislators to require this by law. Insofar as dependence on non-European vendors continues in the short term, it is also important for organisations in these sectors to take measures to mitigate the more immediate risks. For example, managing encryption keys in-house gives organisations greater control over their data and reduces the risk of unauthorised third-party access. Independent backups, preferably on-premise or in the European Union, provide recovery options in the event of outages or incidents in the primary cloud environment.

For all critical, important and essential functions and services, the risks associated with dependencies on IT service providers must be managed. In the financial sector specifically, DORA requires providers of IT support for critical and important functions, as well as the financial institutions themselves, to comply with requirements relating to such aspects as information security, business continuity plans and exit strategies.[8] The ECB Guide on outsourcing cloud services to cloud service providers aims to provide further clarity on the expectations under DORA and sets out best practices for meeting the various requirements. Other sectors are subject to the NIS2 Directive[9], which requires essential and important entities and the essential services they provide to meet heightened cyber resilience and duty of care requirements, including in the areas of supply chain security and dependencies on IT service providers. In a recently issued opinion[10], the RDI stated that firms and institutions need to step up their management of dependencies.

For non-vital processes, strengthening digital autonomy can also be achieved through solutions offered by non-European vendors, provided that deliberate trade-offs are made following a careful assessment of the risks. Optionality, portability and avoiding vendor lock-in are key factors in this regard. This requires a wider range of IT services, open standards and interoperability. Furthermore, organisations that manage non-vital processes can take technical measures to mitigate the most significant risks, such as managing encryption keys in-house and ensuring independent fallback options.

8 ECB Guide on outsourcing cloud services to cloud service providers
9 The NIS2 Directive is being transposed into Dutch law as the Cyber Security Act (*Cyberbeveiligingswet – Cbw*), which will come into force in 2026.
10 Monitoring the use of cloud services | RDI (available in Dutch)

Towards digital autonomy

The road towards digital autonomy requires a joint effort from multiple parties. Reducing digital dependencies and increasing freedom of choice is not a task that can be achieved by individual organisations or the market alone. Governments, policymakers and legislators play a decisive role by setting the direction through policies, procurement and legislation. Firms and vital organisations make the practical decisions regarding their IT strategy. IT vendors, through their design choices and the degree of interoperability, ensure that migrating is actually possible. Supervisory authorities contribute by providing flexibility and clarity within existing frameworks and by removing barriers to cooperation and migration. In this chapter, we outline the steps required to work, along these lines, to achieve a more autonomous and resilient IT infrastructure.

Public authorities as launch customers

A coordinated approach led by European public authorities is needed. Organisations that are the first to migrate to a European provider incur additional costs and face greater risks. This creates a situation in which market forces and competition do not sufficiently encourage the development of alternatives. Without coordination, therefore, the necessary steps towards digital autonomy will not be taken. European alternatives can only develop if European public authorities commit themselves as buyers on a long-term basis. Thanks to their scale and continuity, public authorities can offer guaranteed demand, thereby stimulating market development and fostering a more integrated range of services offered. Furthermore, focusing on achieving tangible results in the public sector is key. Pooling knowledge and expertise to achieve a successful migration in one or more organisations will produce a concrete and replicable model for others to follow. Subsequently, lessons learned can be used to accelerate the transition to a more autonomous IT stack.

Cooperation is both necessary and possible

Cooperation across public authorities and within sectors offers opportunities to stand stronger together. A group of customers can jointly set requirements for cloud and software service providers. By pooling demand and setting joint requirements (for example, focusing on autonomy, limiting vendor lock-in, increasing transparency and ensuring continuity), the group can exert greater influence over the range of services provided. Organisations can jointly invest in the development of existing and new (European) cloud services or infrastructure, including open-source alternatives. This reduces the risks for individual organisations and speeds up the availability of alternatives.

Scale is needed to create a European range of services that can compete with major players from outside Europe; pooling both supply and demand can help achieve this. Consider, for example, agreements between financial institutions to purchase cloud services from a European provider that does not yet have sufficient scale. Pooling demand enables this provider to scale up quickly, thereby reducing costs and investing in quality and functionality. Pooling supply can also help in achieving the necessary scale. Agreements on pooling supply and demand may therefore ultimately lead to greater competition.

As supervisory authorities, we often see that firms are reluctant to cooperate, but the Competition Act permits cooperation in many cases. Many forms of joint procurement, investment and the setting of technical requirements do not restrict competition and may, in fact, contribute to a more diverse and autonomous range of products and services. Collectives can also broaden the options available to buyers, for example by setting requirements regarding interoperability, data portability and compliance with regulatory requirements. On the supply side, reaching agreements on the use of open standards, for example, can facilitate switching to a different service provider, which in fact strengthens the potential for competition.

Ensure options for switching

Deliberate architectural and procurement decisions must be made to extend options for switching between providers, such as the use of open standards, drawn up jointly. Open standards and open-source software increase the degree of control, improve interoperability and extend options for switching to different providers. When systems are based on open standards, it is be easier to replace components, bring in new providers and switch services, thereby limiting vendor lock-in. While the use of open standards helps to facilitate switching, it does not in itself offer a full guarantee of independence or digital autonomy. That is why it is important that open standards are developed jointly wherever possible. Customer collectives can play a role in this context by setting requirements regarding interoperability, data and application portability.

A multi-vendor strategy increases flexibility, as organisations are not dependent on a single provider in their IT stack. By using multiple (partially overlapping) vendors for vital processes, genuine optionality and portability are created, and the barrier to migrating is lowered. This does, however, require investment in interoperability, the use of open standards and portable architectures, for example through containerisation. Also, a multi-vendor strategy can entail additional costs, complexity, administrative burdens and potential security risks, making careful trade-offs essential. It is important that the supply chain risks associated with the various vendors are identified. Public authorities could act as role models in this respect: by systematically incorporating multi-vendor, modular architectures and open standards into their tender requirements, they can actively drive change in the market.

In addition, organisations can set explicit requirements for IT vendors, for example, that they design their solutions in such a way that these can be deployed in different environments. By ensuring that applications and services can run both across different cloud platforms and on-premise, customers retain the ability to reconsider their choices when risks, costs or strategic circumstances change. This requires IT vendors to design their solutions with portability and interoperability in mind, and not to create unnecessary technical or contractual dependencies.

Realistic exit and transition plans increase flexibility and allow the practical execution of migration. Under DORA, financial institutions are already required to draw up exit and migration plans, but even beyond that, it is essential to

consider in advance scenarios in which switching to a different service provider is necessary. For example, NIS2 also sets out requirements for effective vendor management. In order to develop realistic exit and transition plans, investment is needed to ensure the quality and feasibility of these plans, including regular testing.

Include digital autonomy in tendering and procurement

We call on organisations and public authorities to explicitly include digital autonomy as a quality criterion in their procurement decisions, thereby creating a level playing field for European open-source solutions. This means, for example, imposing requirements on legal sovereignty, such as being subject solely to European legislation. Autonomy should be treated as a fully-fledged quality criterion in its own right, alongside price and functionality. Specifically for vital infrastructure and services, autonomy should be a prerequisite. A government-wide framework for digital autonomy could provide support in this regard.

Strengthening digital autonomy may involve making temporary concessions in terms of quality or cost. During a period of transition, it may be necessary to accept higher costs or make do with less comprehensive features. This is justifiable if it results in a greater degree of control and less dependence, while creating a stronger digital foundation in the long term. Given the importance of digital autonomy for vital processes, this criterion carries greater weight in such processes than in non-vital ones.

Incorporating digital autonomy into tendering and procurement processes need not stand in the way of deploying innovative solutions. Particularly in the case of non-vital processes, considerations regarding functionality, stability and efficiency can carry comparatively significant weight. However, even in such cases, realistic exit plans would need to be drawn up, and the IT service provider would also be required to facilitate them.

In practice, there is reluctance to include autonomy as a quality criterion, due to uncertainty surrounding its legal admissibility. Within the parameters of the Public Procurement Act, there is certainly scope to include digital autonomy as a quality criterion. To make this feasible in practice, organisations must be able to defend themselves against legal proceedings in the context of a tender process. The central government can provide the necessary expertise and resources to this end. We call on organisations that encounter difficulties in incorporating autonomy into a tender to contact the supervisory authorities.[11]

Strengthen expertise and raise awareness

It is important to strengthen expertise in procurement and IT teams. Expertise is needed in the areas of 1) sovereignty and autonomy, and the opportunities and requirements in legislation when incorporating these; and 2) technology, the vulnerability of certain workloads, and alternatives. This expertise is essential for making well-informed decisions.

11 Organisations can seek support from ACM and/or PIANOo. ACM can provide input from a competition perspective, while PIANOo can offer guidance on the application of and possibilities within public procurement law.

Many financial institutions already have this expertise, given the prevailing risk management and supervisory requirements. At the same time, this expertise must be kept up to date and deepened where necessary, particularly in light of new technological and geopolitical developments. It is also important that procurement officers draft tenders in a way that is functionally and technologically neutral, so that European vendors can also meet the requirements.

Digital autonomy can also be strengthened through services offered by non-European providers, but this requires organisations to carefully assess to what extent these effectively add to digital autonomy and resilience. Increasingly, non-European providers are offering sovereign cloud solutions for the European market. While these can help mitigate certain risks, it is important to carefully assess to what extent they meet specific needs and requirements in terms of digital autonomy. Such needs and requirements differ from organisation to organisation and from process to process, and depend on each organisation's own risk appetite. For example, an organisation requiring an IT solution to be completely shielded from non-EU legislation will most likely find the services available from a non-European hyperscaler inadequate.

Strengthening policy, legislation and regulations

An effective system for screening investments is needed to protect vital sectors from takeovers that could pose risks. In the Netherlands, the Investment Screening Authority (BTI) is tasked with assessing mergers, investments and acquisitions governed by this system for potential risks to national security and the public interest.[12] The aim is to protect the Netherlands against, for example, the disruption of vital processes and the leakage of sensitive technology should a third party gain control of a firm. If investments or acquisitions pose risks, it is important that sufficient alternatives are available that have a lower risk profile. The availability of such alternatives requires that particular attention continues to be devoted to the functioning of the European Capital Markets Union.

Introducing legislation and regulations promoting autonomy can heighten the sense of urgency by actively discouraging lock-ins and explicitly facilitating and, where proportionate, enforcing switching. The European Union's Data Act and DORA, and possibly in the future the Digital Markets Act, already facilitate significant progress in this regard by establishing standards for data portability, exit strategies and operational resilience. The Data Act sets out requirements for interoperability and data portability to facilitate switching and multi-vendor strategies. In addition, the European Commission is currently exploring the designation of two major cloud providers as gatekeepers under the Digital Markets Act. This would entail additional requirements that further facilitate migrating and combining services.

12 The BTI is part of the Ministry of Economic Affairs and Climate Policy's TEVEA Directorate.

Promoting a competitive European range of services, and thereby strengthening digital autonomy, is only possible if the underlying causes of digital dependency are also addressed. As highlighted in the Draghi and Letta reports, this requires achieving structural improvements in the investment climate and boosting market appeal to scale-ups and strategic technology firms. This will give them enhanced access to capital, reduce fragmentation of the single market, create scope for the construction of data centres and, where relevant, provide revenue guarantees to innovative market players. In mobilising sufficient capital, the 'savings and investment union' plays a crucial role. In this context, access to finance with a view to scaling up innovative firms is a key focus. If these preconditions are not met, the services offered will remain fragmented and insufficiently competitive, thereby perpetuating dependencies.

The role of the ACM, the AFM, AP, DNB and RDI

We aim to provide organisations with clarity and possibilities, including through targeted guidance on when and how forms of collaboration, such as joint procurement, joint investment, pooling of supply, are permissible. We acknowledge that there are questions regarding the scope for collaboration on digital autonomy. The ACM,, the AFM, AP, DNB and RDI believe it is important that these issues do not hinder the development of a more autonomous IT stack. There are often more possibilities than people realise.

We expressly invite organisations to engage in early consultation and dialogue, for example if they are uncertain about interpretation of the rules. If you have any doubts about interpretation of the regulations or supervisory requirements, please contact us at an early stage.

We are working together to reduce barriers to switching and using European alternatives, and to jointly address issues identified in practice, such as bottlenecks and market failures. We identify bottlenecks and intervene where laws and regulations are breached, paying particular attention to practices that unnecessarily hinder the development of an autonomous IT stack.

We identify our own dependencies and make deliberate decisions to reduce them if possible. Digital autonomy also requires efforts from supervisory authorities in their capacity as IT users. For example, DNB recently signed a contract with a European cloud service provider. Making such choices allows us to gain first-hand experience of the trade-offs, opportunities and limitations associated with the use of European alternatives. This helps to make the dialogue with the sector more concrete and realistic, and to ensure that policy and supervision are better aligned with practical feasibility.

We are committed to actively raising the profile of digital autonomy among our European regulatory counterparts, such as the ECB, ESMA, EIOPA and ENISA. We will actively promote digital autonomy within European consultative bodies, with the aim of contributing to a consistent and forward-looking policy framework. At the same time, we believe the Dutch government has an important role to play in steering efforts at European level to strengthen strategic coordination regarding the provision and development of European IT services. This will collaboration to build a robust, competitive and resilient European digital ecosystem.