



Digital and Technological Sovereignty

DIHK Position Paper 2026

DIHK

Deutsche
Industrie- und Handelskammer

 **Gemeinsam Digital**

Imprint



Editors and contact information

Arian Siefert
siefert.arian@dihk.de
Dr. Katrin Sobania
sobania.katrin@dihk.de

Contributors and contact information

Klemens Kober
kober.klemens@dihk.de
Philipp Flore
flore.phillip@dihk.de

Lorenz Kramer
kramer.lorenz@dihk.de
Susanne Gewinnus
gewinnus.susanne@dihk.de

Lukas Littmann
littmann.lukas@dihk.de
Jana Heiberger
heiberger.jana@dihk.de

Julia Flasdick
flasdict.julia@dihk.de

Publisher and Copyright

© **German Chamber of Commerce and Industry**

Department for Digital Economy, Infrastructure and Regional Policy

DIHK Berlin

postal address: 11052 Berlin | street address: Breite Straße 29 | Berlin-Mitte
Telefon: 030 20308-0 | Telefax: 030 20308-1000

DIHK Brüssel

Vertretung der Deutschen Industrie- und Handelskammer bei der Europäischen Union
19 A-D, Avenue des Arts | B-1000 Bruxelles
phone: +32-2-286-1611 | fax: +32-2-286-1605

Internet

www.dihk.de/en

Illustration

Sven Ehling, DIHK

Pictures

Getty Images

Status

June 2026

Digital and Technological Sovereignty – Harnessing Potential, Securing Prosperity, Shaping Geopolitics

Executive Summary

International competition for key digital technologies has become a central factor in geopolitical power dynamics. For Germany and Europe, this is not just a matter of innovation and growth, but of economic resilience, strategic capacity to act and geopolitical scope for influence. Digital and technological sovereignty is an essential prerequisite for this.

At present, however, Germany and Europe are heavily dependent on non-European providers in key areas of the digital ecosystem – such as cloud infrastructure, platforms, AI frameworks and parts of the public IT sector. These dependencies increase the vulnerability of the economy and the state to geopolitical tensions, regulatory conflicts and technological lock-in effects.

At the same time, Germany possesses considerable industrial, technological and scientific potential. Strong companies with in-depth domain expertise, high levels of research output, rising patent applications in key digital technologies and growing use of AI form a solid foundation for expanding digital value creation and technological leadership. The problem lies less in a lack of expertise than in inadequate conditions for scaling up and structural barriers.

A resilient and sovereign digital ecosystem therefore requires clearly defined building blocks: a streamlined, technology-neutral regulatory framework; open

standards and interoperable technologies; clear contractual and data governance; high-performance digital infrastructures and key technologies; secure access to critical raw materials; and strong digital skills.

To ensure that existing potential can be realised, policymakers must take targeted action. This requires the reduction of bureaucracy and legal uncertainty, faster approvals, competitive energy prices, prioritised investment in AI infrastructure and data centres, as well as improved access to research findings, computing power and test environments. The public sector should also consistently deploy open and interoperable technologies and, as a key strategic customer, actively drive innovation.

At the European level, digital sovereignty must be viewed as a strategic joint project. The EU must simultaneously act as a smart regulator, actively help shape international standards, reduce dependencies through diversification and open standards, and expand digital connectivity through trade and digital agreements. At the same time, the regulatory burden should be kept to a minimum in order to avoid legal uncertainty and reduce compliance costs.

Digital and technological sovereignty are achievable. Germany and Europe have the necessary companies, expertise and industrial strengths – the key now is to consistently align the political and economic framework conditions with scaling, competitiveness and resilience.



Introduction

International competition in the field of digital technologies is characterised by increasing technological, economic and geopolitical tensions. Leading economies are investing heavily in key technologies such as artificial intelligence (AI), cloud and platform infrastructures, semiconductors, cyber security and quantum technologies in order to reduce technological dependencies and set global standards. For Germany and Europe, this is not merely a matter of competing in terms of innovation and as a business location, but also of preserving value creation, data sovereignty and strategic autonomy. Digital and technological sovereignty is crucial to enabling German companies to translate their technological capabilities into scalable, internationally competitive solutions, secure value creation within the country and reduce economic dependencies in times of geopolitical uncertainty.

Digital and technological sovereignty

In this paper, digital and technological sovereignty is understood as the ability of companies and institutions – such as government bodies or research institutions – to shape digital technologies, data and infrastructure in a self-determined manner and to reduce one-sided critical dependencies in order to remain capable of acting at all times. This is intended to reduce external risks such as political influence, lock-in effects and regulatory conflicts, thereby strengthening digital and technological competitiveness and resilience. This also encompasses aspects such as cost control, freedom of contract, data portability as well as fair competitive and fiscal frameworks.

Germany and Europe possess the expertise, innovative strength and industrial power to hold their own and grow in the international competition for digital technologies. German companies, in particular, combine in-depth domain knowledge, industrial excellence and high-level engineering skills with a growing capacity for digital innovation. Germany occupies leading positions in many areas of basic research. The number of patent applications in key digital technologies has risen significantly recently – particularly for AI-related applications – and the use of AI in German companies is also growing steadily. When it comes to future technologies such as quantum technology, Europe has measurably reduced the gap with the US.

By intelligently linking software, data, AI and industrial applications, German companies can create competitive advantages, establish new business models and secure value creation within the regions. Digital and

technological sovereignty is not an end in itself, but a strategic opportunity to accelerate innovation cycles, increase resilience and expand technological leadership roles within the digitally relevant technology stack.

However, there is a significant need for action, as key layers of the digital stack – from cloud infrastructure and operating systems to AI frameworks, cybersecurity solutions and public IT – are largely controlled by non-European providers¹. This gives rise to critical dependencies and risks for the strategic capacity of companies and the state to act. Growing geopolitical tensions, particularly between the US and China, further exacerbate these risks, as German companies are increasingly caught up in global systemic conflicts and dependencies.

The German chamber network sees a key need for action, above all, in promoting open and interoperable technologies, strengthening trustworthy digital infrastructures and key technologies, and systematically building up digital and technological skills.

Key demands for digital and technological sovereignty

Reducing legal uncertainty and bureaucracy

A clear, streamlined and technology-neutral digital regulatory framework is needed. Laws and regulations



must be better coordinated and designed to be practicable in order to provide companies with planning certainty and to avoid distortions of competition and unnecessary bureaucracy.

Consistently implement open standards, interoperability and digital identities

The public sector should consistently prioritise open standards, interoperable solutions and sovereign technologies, and make the use of the Deutschland-Stack mandatory across all levels of administration. At the same time, digital identities based on the European Business Wallets and the EUDI Wallets should be established as a central foundation of sovereign digital ecosystems and actively promoted by the state. Furthermore, the European open-source ecosystem needs to be strengthened in a sustainable manner. Data, as the basis for AI, must also be made more accessible to SMEs. To this end, interoperable data spaces such as Manufacturing-X should be secured for the long term, scaled up and made accessible to SMEs.

Strengthen cyber resilience

All businesses, particularly those in the critical infrastructure sector, must identify threats at an early stage and be resilient to attacks. This requires closer cooperation between the private sector and the state, for example in the exchange of security-related information, whereby reporting obligations must be kept as free from red tape as possible and translated into concrete, actionable situational assessments for businesses. At the same time, effective European response and coordination mechanisms are needed to counter threats swiftly and effectively. For critical infrastructure, there is also a need for a clear, long-term strategy aimed at gradually reducing dependence on non-European providers.

Systematically expand and scale up key technologies

Industrial strengths should be channelled more purposefully into marketable and internationally scalable solutions. This applies above all to industrial applications involving software, data and AI, as well as the faster roll-out of successful digital and technology projects on a broad scale. This requires clearly prioritised government investment in strategic future sectors, as well as regulatory certainty. In addition, there must be clearly prioritised government investment in strategic future-oriented sectors and a significant acceleration of the transfer of research into industrial application, for example through the consistent integration of the commercialisation of research results from the outset, faster and less bureaucratic access for companies to test environments, and the increased provision of key resources such as computing power.



Accelerate infrastructure expansion and reduce energy prices

Digital infrastructures such as fibre-optic and mobile networks, as well as data centres, are crucial for the rapid development and expansion of digital innovations and business models. To ensure these can emerge and grow quickly, competitive energy prices are needed for the operation of data centres, alongside faster planning and approval procedures and the availability of suitable sites.

Strategically securing critical raw materials

Digital sovereignty requires a coordinated European approach to securing critical raw materials. This includes strategic partnerships, greater exploitation of domestic potential and the expansion of downstream processing, for example within the framework of the EU Chips Act and the Critical Raw Materials Act.

A sovereign Europe: rule-maker rather than rule-taker

The EU should proactively help shape international digital standards, norms and data protection, and expand digital cooperation through trade and digital agreements. Standardisation must be strategically strengthened and the participation of European companies, particularly SMEs, facilitated. The digital euro, should it be introduced, and European private-sector initiatives should be used to build an independent European payment infrastructure.

Systematically building digital skills

Competitiveness requires strong digital skills. This calls for an effective digital education infrastructure, targeted training for teachers, and the expansion of European learning platforms and educational data repositories.

Reducing legal uncertainty and bureaucracy

Technological progress and clear regulatory guidelines are not mutually exclusive but are interdependent: only their balanced interaction enables responsible, sustainable and sovereign development. However, regulation must not stifle innovation. If a jurisdiction imposes too many documentation and reporting requirements on digital innovations from the outset, this significantly slows down their implementation – and thus also jeopardises its technological autonomy in the long term.

Companies are also faced with a growing number of horizontal and sector-specific regulations, which are often not coordinated with one another. Overlaps, regulatory conflicts, unclear responsibilities or duplicate reporting obligations result in heavy bureaucratic burdens and legal uncertainty. This is evident, for example, in the interaction between the AI Act and sector-specific legislation such as the Medical Devices Regulation or the Radio Equipment Directive, as well as with horizontal frameworks such as the GDPR. There are more rules that fail to take sufficient account of technical differences, for example where the AI legal framework does not distinguish between general-purpose AI, consumer-facing applications and industrial assistance systems. This hinders the deployment of AI and innovation processes and creates competitive disadvantages.

Further uncertainty arises when legally required guidelines or technical standards are made available too late, even

though the relevant obligations are already in force. The situation is further complicated by additional regulations from related areas such as supply chains or corporate social responsibility.

Overall, this undermines Europe's competitiveness as a business location. Germany is particularly affected by this, as the high proportion of SMEs and medium-sized global market leaders means that new European regulatory initiatives place a disproportionate burden on the German Mittelstand. This is particularly evident in heavily regulated sectors, where complex verification, approval and documentation requirements are often out of proportion to the achievable market and scaling opportunities. For small and medium-sized enterprises in particular, this can give rise to significant economic risks that delay or prevent innovation.

DIHK recommendations:

Design a digital regulatory framework that is consistent, streamlined and technology-neutral

Companies are empowered to develop and deploy their own digital solutions autonomously if the rules are understandable, predictable and legally certain.

European and national digital regulations should be well coordinated to avoid unnecessary bureaucracy, duplicate obligations and conflicting requirements. Key general regulatory frameworks such as the AI Act, the Data Act, the GDPR, NIS2, the Cyber Resilience Act, the Industrial Accelerator Act, the planned reform of public procurement law, as well as more sector-specific regulations such as the Machinery Regulation, the Medical Devices Regulation, the European Health Data Space and regulations in the financial investment sector, must be better integrated and implemented as practical and as easy as possible.

Regulation will only be effective and accepted if it is not perceived as a competitive disadvantage. A 'level playing field' should be guaranteed, and rules should be consistently enforced, including in relation to companies from third countries. To this end, supervisory and regulatory authorities must be adequately resourced and cooperate effectively. In the area of certification and conformity assessment, faster procedures and lower costs are needed. At the same time, close international cooperation is required to avoid conflicting obligations for companies operating internationally. In this respect, new regulatory approaches are also needed within the EU.

Overall, regulation should remain technology-neutral, avoid unnecessary documentation and reporting requirements, and help strengthen innovation, international cooperation and competitiveness. Complexity



and competitiveness checks could actively drive down red tape, particularly for SMEs.

Ensuring implementation through guidelines, standards and transition periods

Legal requirements should be as streamlined and practical as possible to ensure that regulations are understandable and applicable. Businesses should be able to understand and implement requirements independently. Where guidelines, implementing acts or technical standards are required, these should be published at an early stage. Sufficiently long transition periods are important to ensure that businesses have enough time to adapt to the new requirements and implement the necessary measures.

This gives them greater control over their digital processes and enables them to drive innovation in a targeted manner.

Businesses should receive appropriate support well in advance of new obligations coming into force. This includes, for example, self-assessments to determine, in a legally compliant manner, the extent to which they are affected, as well as reliable guidance and model contracts – such as for AI and data collaborations – which should be developed in close consultation with the business community and made available by the relevant government bodies and supervisory authorities.

Consistently implementing open standards, interoperability and digital identities

A lack of interoperability, proprietary interfaces and a shortage of open standards are holding back the digital transformation and increasing dependence on individual manufacturers. Particularly against the backdrop of current geopolitical developments, this poses a threat to digital sovereignty and, consequently, to the resilience of businesses.

According to the DIHK Digitalisation Survey 2026, German companies largely consider themselves to be digitally self-sufficient, particularly in the field of industrial software. In other areas – ranging from office software, hardware and cloud to AI and platforms – the majority consider themselves to be largely or entirely dependent on applications and technologies from non-EU countries. The data required for digital AI-powered applications often remains untapped within businesses and the political sphere.

Digital identities that can be used across different sectors are a key building block for digital sovereignty and resilience. So far, however, there have mostly been only isolated solutions for individual sectors, for example within data rooms. Solutions from the public administration, such as the business account for dealing with official procedures, are also not yet designed to be integrated into a common European trust framework.

The state's ability to act also depends on the public administration itself using sovereign, secure and trustworthy digital solutions and simplifying processes before they are digitised. In some areas, such as specialist applications, sovereign digital solutions are already in use, but this is not the case in the field of desktop solutions. Furthermore, the lack of uniform technical standards and interoperable interfaces too often prevents digital solutions from small and medium-sized enterprises and

start-ups from being widely adopted within the public sector.

The federal and state governments have taken steps, including through the Deutschland-Stack, the Digital Ministers' Conference and the IT Planning Council, to make greater use of the innovation potential offered by private-sector providers of digitally sovereign solutions for the digitalisation of public administration.

Nevertheless, the implementation of new digital technologies in public administration is often too slow and poorly coordinated. This is due, amongst other things, to complex governance structures and a legal framework that is not sufficiently adapted to the digital age. There is a need for expertise to be pooled more and for clear central steering to enable solutions to be deployed more quickly and on a larger scale. To achieve this, the legal and financial prerequisites must first be put in place, and effective steering structures must be established.

The German Federal Government's 2025 coalition agreement contains a clear commitment to digital sovereignty as a key political objective. Open source is explicitly recognised as a strategic foundation for building a sovereign digital ecosystem. However, concrete, verifiable targets or binding implementation requirements have so far remained largely undefined.

DIHK recommendations:

Prioritise open standards and interoperable solutions in public administration

The public sector should place greater emphasis on open standards, interoperable architectures and sovereign technologies. This helps to avoid dependencies, promote



fair competition and safeguard its own capacity to act. The aim should be a high-performing, end-to-end digital ecosystem for Germany.

The state can benefit particularly from innovative solutions provided by the private sector, especially in the areas of administrative digitalisation, IT security, data infrastructures, AI applications and digital identities. The Deutschland-Stack has laid an important foundation for this. It is now crucial that these structures are used on a mandatory basis throughout the entire public administration – from the federal government through the federal states down to the local authorities. Only in this way can efficiency and innovation potential be fully realised and the public administration as a whole be made more future-proof, resilient and sovereign. This requires appropriate legal and organisational frameworks, such as an amendment to the division of powers under the Basic Law and concrete support measures for local authorities.

However, the Deutschland-Stack must not be limited to the modernisation of public administration alone. It should become a shared digital infrastructure for the state and the economy.

Establishing digital identities as the foundation for sovereign digital ecosystems

Secure digital identities are a key success factor for sovereign digital ecosystems. They are essential for reducing costs within businesses and enabling secure data exchange with customers, business partners and the public sector.

What is required is a functional ecosystem of digitally sovereign corporate identities based on the European Business Wallets, in conjunction with the voluntary use of digital identities for natural persons, such as the EUDI Wallets, insofar as they are engaged in business activities. The development of this ecosystem should be actively supported by the public sector. As a major user of the trust services contained in the wallets and as an issuing authority for certificates, the public sector should

therefore play a key catalytic role. The aim must be to ensure that digital identities, certificates, administrative data, corporate data spaces and industrial data ecosystems do not exist in isolation, but can interact in an interoperable manner.

Providing sustainable support for the European open-source ecosystem

Open-source software forms the foundation of almost all modern software development. At the same time, the underlying open digital infrastructure is often underfunded and inadequately supported – a structural problem with far-reaching consequences. Yet Europe's existing strengths in open source provide an important basis for expanding digital sovereignty.

Open digital infrastructures and European open-source communities should be strengthened in a targeted and sustainable manner. They make it possible to identify vulnerabilities at an early stage and to develop our own, sovereign digital solutions. Where the state itself uses open-source software, it must also take responsibility for its ongoing maintenance and further development. Only in this way can these solutions remain secure, high-performing and reliable in the long term.

Ensuring the sovereignty of data spaces

Interoperable data spaces such as Manufacturing-X facilitate efficient data flows between companies and can thus strengthen European technology stacks. They contribute to the data readiness of many companies and should be secured and scaled financially, legally and organisationally, going beyond project-based funding models. This includes, in particular, the establishment of implementation and testing environments that serve as stable platforms for building and maintaining communities comprising industry, technology providers and users. Efforts should be made to involve small and medium-sized enterprises in particular more closely in these ecosystems centred on future-oriented digital and technological topics.

Strengthening cyber resilience

European legislation addresses key aspects such as supply chain risks, operator responsibility, cybersecurity, data sovereignty and dependencies on third countries through, amongst others, NIS2, the Cyber Resilience Act, the Data Act and the GDPR.

As a result, businesses are faced with a multitude of reporting, documentation and evidence-provision obligations. These are often complex, difficult to understand or overlap. To date, reporting obligations have too rarely delivered direct added value for businesses. There is a lack of easily accessible, up-to-date situational assessments and concrete recommendations for action. The exchange between public authorities and the business community remains too fragmented.

DIHK recommendations:

Design security requirements to be practicable and low on bureaucracy

The legislator should harmonise and simplify requirements more effectively and consistently gear them towards practical applicability. The aim must be: less bureaucracy, more actual security gains.

Strengthen cyber resilience through cooperation

Digital sovereignty in the areas of cybercrime and industrial espionage requires a coordinated approach across several levels. This includes closer cooperation between the private sector and the state, for example in the exchange of information. The additional burdens – such as reporting obligations on companies – must be designed to minimise red tape as far as possible. The reports must be used to

compile practical information on current threats and risks, which must then be made available to companies in a targeted manner. In doing so, cyber and analogue risks should be considered holistically.

Expanding support services for SMEs

Many small and medium-sized enterprises are overwhelmed by cyber requirements. The government needs to take action to provide low-threshold advice, standardised security solutions and concrete implementation services based on the 'cyber resilience-as-a-service' model.

Cyber resilience is often understood in technical terms, but this is too narrow a view. Businesses also need support with business continuity management, contingency planning and recovery processes. The government should provide appropriate standards and guidelines.

Many companies are heavily dependent on third-party providers. In addition to existing legal requirements, the government should provide support in assessing IT supply chain risks and in developing trustworthy European alternatives.

Promoting innovation and security solutions

There is a lack of scale in innovative security solutions 'Made in Europe'. The government should specifically promote the research, development and market launch of cybersecurity technologies and support their widespread adoption. Developing cyber resilience requires not only technical security solutions, but also skilled staff who can identify risks at an early stage and respond appropriately.

Improving European response capabilities

Cyberattacks are cross-border in nature, yet response structures are often still fragmented at national level. Effective European coordination and intervention mechanisms are needed, along with clearly defined responsibilities in the event of a crisis.

Strategically prioritising critical infrastructure

Germany also needs a clear, long-term strategic direction for critical infrastructure. The aim must be to gradually reduce dependence on non-European providers for key software, platforms and control systems, whilst at the same time maintaining the international competitiveness of the companies concerned. In particularly sensitive areas, the focus should be on European or German solutions in the long term. Digital sovereignty should be treated with the same strategic priority as energy supply or defence capability.



Systematically expanding and scaling up key technologies

Germany ranks among the world's leading nations in terms of patent applications filed with the European Patent Office, second only to the USA. However, this strength in research and the invention of new technologies is increasingly failing to translate into economic growth in the market for innovation-driven future technologies. It is precisely at this interface between technological excellence and market-effective implementation that start-ups and spin-offs, as central elements of high-performing innovation ecosystems, play a decisive role.

Yet, when it comes to scaling up, highly innovative deep-tech companies² in Germany and Europe reach their limits. Whilst Europe is competitive in research thanks to its diverse landscape of universities and research institutes, and increasingly so in the early stages of start-up development, there is often a lack of capital markets capable of supporting scaling, reliable public anchor clients and fast, implementation-focused structures. Companies and start-ups also require quick and easy access to resources such as computing capacity. Added to this are fragmented regulatory and funding landscapes within Europe, as well as complex IP- and licensing regimes that delay growth. As a result, Germany and Europe too rarely succeed in fully realising the economic potential of their own key technologies – and technological value creation shifts to where capital and speed of implementation converge.

Strategic investments and government support measures in future technologies must be capable of generating long-term leverage. The Federal Government's High-

Tech Agenda, launched in 2025, is already focused on supporting six key technologies and five strategic research fields in order to establish Germany as a leading hub for new technologies.

DIHK recommendations:

Targeted strengthening of key technologies

Crucial to the success of key technologies in Germany are the early involvement of industry in collaboration with academia, clearly defined milestones and effective levers for innovation transfer, such as those set out in the roadmaps developed for the key technologies. Strong technology sectors – for example those where existing industrial expertise is systematically combined with key digital technologies – can thus be developed and expanded. Furthermore, attention should be directed towards areas in which Europe is well positioned – such as embedded systems, sensor technology, industrial technology and software, as well as automation and connected production, or medical technology. AI will also fundamentally transform key industrial sectors such as manufacturing, mechanical engineering, the automotive industry and industrial process control.

In these areas, Europe has a strong industrial base, a high level of systems expertise and globally competitive companies. A forward-looking strategy for technological and digital sovereignty should build consistently on these strengths, whilst also remaining open to new technological developments rather than simply replicating



other models of success. This will also enhance Europe's appeal as a destination for foreign investment.

A unified European venture capital market for start-ups and scale-ups

Capital markets are essential for rapid growth. Radical innovations and rapid scaling can only be financed through venture capital. To prevent a further exodus of successful start-ups and scale-ups to the US and to be able to offer larger funding rounds in Europe, a unified European venture capital market is needed. Particularly in the areas of capital mobilisation, exit opportunities and regulatory frameworks, initial reform proposals aimed at reducing intra-European fragmentation are emerging in the political debate; these should be discussed constructively and adopted and implemented swiftly.

Strengthening European technology infrastructure and securing access to key resources

High-performance digital infrastructures are indispensable. This requires both: large AI data centres, such as the EU-funded AI gigafactories for particularly computationally intensive applications – and, at the same time, well-developed regional data centres that ensure comprehensive and reliable coverage.

The path from research to practical application should be improved by involving the private sector more closely in development and implementation. Companies and start-ups must therefore have simple and fair access to key resources such as large-scale computing power. This also includes low-threshold and unbureaucratic access to research infrastructures. Barriers should therefore be removed so that knowledge from the scientific community can be transferred to the private sector quickly and easily.

The state as a key customer for innovation and sovereignty

As one of the largest buyers, the public sector can help bring digital and technological innovations to market maturity, enable scaling up, and retain technological

expertise within the country and in Europe. Innovation-oriented procurement can send demand signals to companies, start-ups and SMEs.

To a certain extent, the state can facilitate pilot markets and showcase projects, as well as accelerate the transition from development to widespread deployment. Competition must always be safeguarded in this process, for example by taking potential cross-subsidisation into account. Investments in future cross-cutting technologies should be long-term in nature and aligned with clear priorities, milestones and measurable leverage effects. In this context, the funding logic in the field of innovation should be more agile and promote disruptive innovations and innovation sprints. At the same time, strategic objectives based on the EU's 'Think small first' principle must not lead to procurement procedures becoming more complex or, in practice, exclude SMEs from procurement procedures due to the bureaucratic burden.

Making research knowledge accessible and designing intellectual property (IP) rules to be innovation-friendly

A modern, transfer-oriented IPR regime³ must ensure low-threshold access to publicly funded research across the EU, so that start-ups and SMEs in particular can access exploitable knowledge, data and intellectual property at an early stage. IP restrictions in EU programmes should be avoided wherever possible: geographical and temporal limitations should be removed, and transfer bans – for example in the European Competitiveness Fund or the 10th EU Framework Programme for Research and Innovation – should be restricted to clearly and exhaustively defined exceptions relating to security strategy.

Instead, qualitative criteria and resilience-oriented assessments for European IP should be strengthened. Furthermore, the use of intellectual property rights as collateral should be permitted in order to facilitate access to innovation funding and EU funding programmes, particularly for capital-constrained, research-intensive companies, even though the valuation of intangible assets remains challenging.

Accelerating infrastructure expansion and reducing energy prices

A high-performance digital infrastructure is a key prerequisite for competitiveness, technological sovereignty and resilience. It forms the basis for cloud and edge computing, AI, data ecosystems, networked industrial processes, as well as digital supply chain infrastructures and logistics platforms. As digitalisation progresses, the demand for high-performance networks, data centres and computing capacity is rising significantly. Similarly,

the successful transition from research into quantum technology to practical application will only be possible with a high-performance digital infrastructure.

Thanks to its central location and the excellent infrastructure surrounding the DE-CIX internet exchange, Frankfurt am Main has a clear advantage for data centres: data can be transferred particularly quickly there because



the connections involve short distances and low latency. German companies thus benefit from faster and more stable data connections, for example in cloud services, digital business processes or data-intensive applications such as AI. At the same time, other regions also offer favourable conditions for data centres and represent important locations, for instance due to the availability of renewable energy.

However, these are offset by structural locational disadvantages in Germany, which are holding back the expansion of data centres and other digital infrastructure. High electricity prices can limit the cost-effective use

of AI and data-driven applications. Added to this are a lack of suitable sites for data centres or mobile phone masts, a lack of electricity grid connections, as well as lengthy and complex planning and approval procedures. Local authorities are often not sufficiently equipped to implement such projects swiftly. Among other things, limited capacity in energy network areas makes it considerably more difficult to find suitable sites for new data centres in the first place. These factors delay investment and prevent rapid scaling.

DIHK recommendations:

Ensure competitive prices for data centres

Sovereign computing and AI capacities require internationally competitive electricity costs. The Federal Government should absorb levies into the federal budget, reduce the electricity tax to the EU minimum and facilitate green direct power purchase agreements (PPAs). Workable framework conditions should enable the sensible use of waste heat, rather than forcing uneconomical grid connections.

Significantly speed up planning and approval procedures for digital infrastructure

The expansion of data centres and energy grids, as well as fibre-optic and mobile networks, is often held back by lengthy approval processes. Procedures should be standardised, digitised and accelerated nationwide. Sufficient suitable land should be made available, for example for data centre sites or mobile phone masts. This requires a fundamental reform of the planning and approval system rather than selective prioritisation legislation. Public land, where topographical conditions permit, should be systematically utilised for mobile phone sites, and national coordination of data centre locations is required.

Strategically securing critical raw materials

A secure and resilient supply of raw materials is a fundamental prerequisite for digital sovereignty. All technical innovations and critical technologies, such as AI, quantum computing and the cloud, require physical infrastructure, e.g. semiconductors for data centres. This infrastructure relies on the availability of critical raw materials, such as gallium, germanium, rare earths and silicon. Germany and Europe are heavily dependent on a small number of third countries, particularly in these areas. This also applies to components such as modern, high-performance chips. With increasing geopolitical tensions, these economic dependencies are being exploited by third countries as a means of exerting pressure. Conflicts, such as the recent one in the Middle

East and its impact on the supply of helium, demonstrate just how vulnerable key supply chains in semiconductor manufacturing are. A more resilient European electronics and components base is an essential component of digital sovereignty.

DIHK recommendations:

Pursue a strategic approach to raw material partnerships

Critical dependencies can only be resolved internationally through partnerships. Germany should act less on a national basis and more at a European or multilateral

level, and participate more actively in EU initiatives or international raw materials alliances. In agreements with raw material-rich countries, the business community should be involved from the outset to ensure that economic needs, including those relating to critical future technologies, are taken into account. It is important that such partnerships are underpinned by concrete projects involving industry.

Improving the framework conditions for raw materials extraction, processing and recovery in the EU

Germany and Europe are not lacking mineral resources, but these are scarcely explored, mined or exploited. Better framework conditions, faster approval procedures, more accessible financing options and an improved public perception of projects are needed.

The processing of critical raw materials into final products, such as state-of-the-art semiconductors, must also be strengthened. In addition to extraction and processing, Europe should consistently promote the recovery of critical raw materials. Improved processes are envisaged for this purpose, for example under the Critical Raw Materials Act, RESourceEU or the EU Chips Act. These must be implemented without delay.

Strategic reserves

The stockpiling envisaged by the European Commission as part of its stockpiling strategy, to be carried out by the Critical Raw Materials Centre established in 2026, should be viewed critically. Although strategic stockpiling can offer added value for businesses and enhance resilience, state-run stockpiling would primarily lead to further price spikes without significantly improving the supply situation for the economy. Furthermore, determining demand for critical raw materials is already difficult, as parts lists provide little information about the processed state required by companies.

Instead, consideration should be given to the extent to which the EU can organise purchasing consortia in certain sectors to pool demand, in collaboration with partners such as the G7 countries. To minimise the impact of supply shortages, many companies have already expanded their stockpiling. The Federal Government should examine what is preventing or restricting companies from building up their own stockpiles. For example, the change to the taxation of duty-free warehouses, which was decided by the Federal Ministry of Finance and is due to be introduced in April 2026, makes stockpiling more difficult.

A sovereign Europe: rule-maker rather than rule-taker

Digital policy is increasingly a matter of power politics. In a global order characterised by geopolitical rivalries and technological dependencies, the ability to set rules, norms and standards determines economic scope for action

and political influence. For the European Union, digital sovereignty is therefore not merely a technological issue, but a key prerequisite for acting as an independent and effective player within the international digital order.

The ongoing fragmentation of the digital space further increases the strategic importance of norms and standards. International standards shape technological development pathways, define market requirements and, in the long term, influence value chains and competitiveness. While European standards are often regarded worldwide as a benchmark for quality and trust, international competition to set these standards is intensifying, particularly in future-oriented fields such as AI, the connected industry and digital infrastructure. Cooperation through trade and digital agreements is a key instrument for disseminating European rules and ensuring open, rules-based digital spaces.

DIHK recommendations:

EU commitment to global digital connectivity and diversification

Data-driven innovations depend on functioning, cross-border data flows. Digital discrimination and market barriers for European goods and services should be curbed worldwide.



Reinstating the WTO moratorium on tariffs on digital transmissions should restore planning certainty for businesses worldwide. Plurilateral and bilateral agreements are viable alternatives in the absence of international consensus. To this end, the EU should expand its network of trade agreements containing digital chapters, as well as digital agreements, with relevant trading partners worldwide. It is important that these agreements promote global, interoperable and open standards in order to prevent strategic digital dependencies.

The EU as a 'rule maker' rather than a 'rule taker' for tomorrow's global standards

It is important for the EU, together with its partners, to help shape international digital standards and to promote its own approaches internationally. The issue of data protection is of great importance in this context. Data protection must be developed, implemented and enforced at an international level. To this end, the Federal Government should advocate for the Europeanisation of supervisory structures, so that the EU can secure a stronger position in international negotiations through a harmonised, efficient data protection area. The Federal Government should also promote EU adequacy decisions for trusted partners.

Germany should also expand its involvement in international forums and organisations such as the Internet Governance Forum (IGF) and the International Telecommunication Union (ITU).

Accelerate the European standardisation system without jeopardising its strengths

The revision of the EU Standardisation Regulation should be used to make the European standardisation system faster and more responsive. In doing so, the tried-and-tested fundamental principles – broad

participation, high quality, and transparent, consensus-based procedures – must be preserved. In particular, the adoption of standardisation mandates, the publication of harmonised standards and the review process carried out by HAS-Consultants⁴ should be made more efficient and predictable; digital tools should be used consistently to speed up these processes.

Targeted strengthening of international standardisation work by German and European companies

To secure Europe's influence in international standardisation bodies, the involvement of companies – particularly SMEs – should be supported both financially and organisationally. This is the only way to ensure that European technological strengths and market interests are adequately reflected in global standards and are not sidelined by other actors.

Combating industrial espionage and cybercrime at an international level

The Federal Government should provide companies with recommendations for action and advocate for the fight against cybercrime and industrial espionage both globally and within international UN bodies. To combat international cybercrime more effectively, a system of rules is needed in the international cyberspace, with as many states as possible participating. It is essential to strengthen cooperation with international security authorities and to devote greater attention to the UN Cybercrime Treaty.

Upholding market principles, reducing dependencies in a targeted manner

The business community is generally critical of government directives such as 'Buy European', as



decisions on technologies and suppliers should, where possible, be made on a competitive basis. Additional requirements, bureaucratic proofs of origin or evidence of ownership structure, as well as potential backlash from trading partners, place a particular burden on small and medium-sized enterprises. At the same time, in light of geopolitical risks, many companies are increasingly willing to prioritise European suppliers and technologies in order to reduce dependencies – particularly in the case of critical infrastructure and aspects relating to digital resilience, such as sensitive data, cloud services and security-relevant IT components. A similar picture emerges in digital payments, where many eurozone countries rely on non-European companies for the technical execution and processing of digital payments. The digital euro, should it be introduced, and European private-sector initiatives should be utilised to build an independent European payment infrastructure.

If European providers are to be given preference in security-critical digital infrastructures – for example, by excluding providers from third countries or through data processing requirements – clear, narrowly defined criteria should be established. Such interventions should be well-justified and limited to genuinely sensitive areas. To develop alternative in-house technologies, targeted funding programmes or initiatives such as IPCEI⁵ are often more effective than rigid requirements. Efforts to avoid vendor lock-in should be supported by the creation of alternative models or providers. Where entire sectors are classified as strategic, regulation should be limited to clearly defined, sensitive components and closely coordinated with economic and security experts in order to avoid competitive disadvantages along the value chains. Ways in which SMEs can participate even more actively in EU programmes such as IPCEI should be explored.

Systematically building digital skills

The DIHK Digitalisation Survey has once again shown that digital skills are a key prerequisite for competitiveness and digital sovereignty. Vocational education and training form a cornerstone of digital sovereignty, as they impart digital skills in a practical, labour-market-oriented and technology-neutral manner, thereby strengthening the resilience and innovative capacity of the economy and the workforce. In addition, schools and higher education institutions play a key role in institutionally embedding digital sovereignty and integrating digital and AI skills across the board into their curricula.

To date, the digital education infrastructure has been heavily dominated by providers from third countries, whilst there is a lack of trustworthy European solutions for educational data, learning systems, as well as identity and payment services. Modern, interoperable and secure infrastructures, as well as qualified staff – supported in the long term by a European education data space – are therefore crucial to strengthening the mobility of skilled workers and digital sovereignty in the long term.

DIHK recommendations:

Systematically embed digital skills and AI expertise in education

Digital sovereignty requires that AI skills be systematically embedded across the board in the curricula of schools, vocational colleges and universities. This should be done in coordination with European partners so that digital skills can be utilised more effectively across borders and successful models can be more easily applied in other Member States. Federal and state governments should specifically strengthen the initial and continuing training of teachers in the areas of digitalisation and AI.

This includes, in particular, practical training in the use of specific AI tools (e.g. for lesson preparation, legally compliant assessment and individual support), as well as systematic access to and the pedagogical use of suitable AI tools in everyday teaching, so that technological developments can be taught in a pedagogically sound manner and on a par with industry practice. In this way, our education system remains aligned with the digital transformation of the economy.

Strengthening AI competence in the business world

The growth and competitiveness of the European economy will also depend on how quickly AI competence can be disseminated and professionalised amongst the working population. Continuing vocational training and SME consultancy play a key role here in focusing AI skills on specific business needs, thereby achieving productivity gains and developing new business models.



To this end, the implementation of the legal obligation on organisations to provide adequate training and raise awareness amongst staff involved in the use of AI systems (Article 4 of the AI Act) must meet a minimum standard that enables all employees to use AI applications successfully and to make well-informed human decisions as a final step. Such a minimum standard must always remain open to further technological developments.

Ensuring comprehensive, up-to-date digital education infrastructure

The federal and state governments must provide all vocational schools with sufficient funding for a modern, secure and high-performance digital infrastructure. This includes high-performance and stable broadband internet connections, industry-standard and interoperable software, technical devices specific to the relevant professions, and qualified staff to operate and further

develop this infrastructure. Only with such resources can digital sovereignty in the education sector be put into practice.

Strengthening European learning platforms and AI applications

Dependence on non-European providers in the education sector should be reduced by specifically strengthening alternative, interoperable European learning platforms, trust-worthy solutions for educational data, digital learning systems and identity services. At the same time, the Federal Government should work to ensure that small and medium-sized training organisations, in particular, are supported in the use and adaptation of AI applications developed and trained within the EU. AI should be utilised – also in light of the EU AI Act – as a strategic area of development for European providers and users in order to remain internationally competitive.

¹ See, for example, [the 2026 Digitalisation Survey: Trends and Insights for Businesses](#)

² The term 'deep tech' refers to fundamental, science- and research-based cutting-edge technologies such as AI, quantum technologies, biotechnology and robotics, which enable far-reaching industrial transformations. They are regarded as key drivers of future value creation, competitiveness and technological sovereignty.

³ An IPR regime refers to the legal and institutional framework governing the protection, use and enforcement of intellectual property rights such as patents, trade marks and copyright. In innovation and economic contexts, the term often describes the entirety of national and international regulations that influence technology transfer, scaling and the commercialisation of innovations.

⁴ HAS Consultants (Harmonised Standards Consultants) are independent experts commissioned by the European Commission to assess whether European standards comply with the requirements of EU legislation and the relevant standardisation mandates. Their assessments are a key prerequisite for harmonised standards to be published in the Official Journal of the EU and to take legal effect.

⁵ IPCEI (Important Projects of Common European Interest) are pan-European cooperation projects in key strategic technologies that create clear European added value and are designed to strengthen the EU's capacity for innovation and competitiveness in the long term.