Digital Sovereignty: Status Quo and Perspectives

Book · April 2021

CITATIONS
0

READS
726

5 authors, including:

Johannes Winter
L3S Research Center & acatech - National Academy of Science and Engineering
66 PUBLICATIONS **341** CITATIONS

SEE PROFILE

acatech IMPULSE

Digital Sovereignty

Status Quo and Perspectives

Henning Kagermann, Karl-Heinz Streibich,
Katrin Suder

acatech
NATIONAL ACADEMY OF
SCIENCE AND ENGINEERING

acatech IMPULSE

Digital Sovereignty

Status Quo and Perspectives

Henning Kagermann, Karl-Heinz Streibich, Katrin Suder

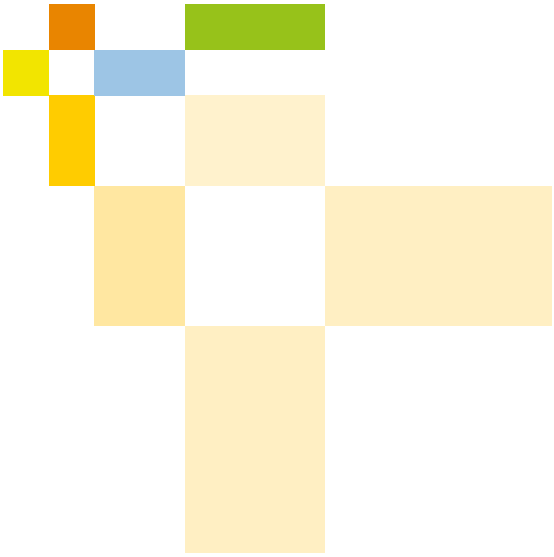
acatech
NATIONAL ACADEMY OF SCIENCE AND ENGINEERING

The acatech IMPULSE series

This series comprises contributions to debates and thought-provoking papers on strategic engineering and technology policy issues. IMPULSE publications discuss policy options and are aimed at decision-makers in government, science and industry, as well as interested members of the general public. Responsibility for the contents of IMPULSE publications lies with their authors.

All previous acatech publications are available for download from www.acatech.de/publikationen.

Contents



Foreword

Digital Sovereignty has become a key strategic policy issue. The importance of sovereignty in the use of digital platforms and applications grows with each new area of private, economic and public life that they are used in.

Digital Sovereignty is not just a question of competitiveness, but also of the political autonomy of the European Union and its member states, the innovativeness of businesses, and the freedom of research institutions and all Europeans in the digital world.

A European brand of Digital Sovereignty must aim to adopt a distinctly European approach to digitalisation. It should steer clear of both State intervention and isolationism in the mould of the Great Firewall and the use of market power to implement de facto standards in key areas. Instead, the concept of a European brand of Digital Sovereignty pursues a vision of digitalisation based on freedom of choice, observance of European legal principles and values, openness towards the rest of the world and the promotion of fair competition.

During its presidency of the Council of the European Union, Germany promoted Digital Sovereignty as the leitmotiv of the EU's digital policy. The need to address this issue strategically at European level was recently reaffirmed in a joint open letter from the German Chancellor and the Prime Ministers of Denmark, Estonia and Finland to the President of the European Commission. Europe's pioneering GAIA-X project already provides the foundation for a standardised, trusted European data infrastructure based on European values and fundamental rights.

The formulation of a concrete strategy to realise this common European vision of Digital Sovereignty will be a balancing act: practical solutions will be needed both to address technology dependencies in the digital sphere and to promote prosperity through international cooperation and the global division of labour.

In this IMPULSE publication, the authors and the many experts who shared their knowledge and viewpoints have sought to contribute to the formulation of a concrete definition of European Digital Sovereignty and the development of concrete policy options for its different technology levels.

Prof. Dr. Henning Kagermann

Karl-Heinz Streibich

Dr. Katrin Suder

Contributors

Authors

- Prof. Dr. Henning Kagermann
- Karl-Heinz Streibich
- Dr. Katrin Suder

Coordinated and edited by acatech Secretariat

- Florian Süssenguth
- Dr. Johannes Winter

Support provided by acatech Secretariat

- Juliane Abdeen
- Dr.-Ing. Patrick Bollgrün
- Alexander Grieß
- Dr. Jorg Körner
- Dr. Martina Kohlhuber
- Peter Kraemer
- Dr. Annka Liepold
- Joachim Sedlmeir
- Christoph Uhlhaas
- Sebastian Witte

Interviewees

- Adel Al-Saleh, T-Systems International GmbH
- Dr.-Ing. Michael Bolle, Robert Bosch GmbH
- Sanjay Brahmawar, Software AG
- Dr. Svend Buhl, NXP Semiconductors
- Dr. Vanessa Cann, KI Bundesverband e. V.
- Mike Cosse, SAP SE
- Martin Fassunge, SAP SE
- Peter Ganten, Univention GmbH
- Dr. Norbert Gaus, Siemens AG
- Lisa Gradow, Bundesverband Deutsche Startups e. V.
- Prof. Dietmar Harhoff, Ph. D, Max Planck Institute for Innovation and Competition
- Dr. Ralf Herbrich, Zalando SE
- Dr. Stefan Hofschen, Bundesdruckerei GmbH
- Dr.-Ing. Stefan Joeres, Robert Bosch GmbH
- Thorsten Küpper, Qualcomm Technologies Inc.
- Rafael Laguna de la Vera, Federal Agency for Disruptive Innovation
- Dr. Jürgen Müller, SAP SE
- Claudia Nemat, Deutsche Telekom AG
- Prof. Dr-Ing. Boris Otto, Fraunhofer Cluster of Excellence Cognitive Technologies and Data, Data Spaces Research Center
- Manfred Paeschke, Bundesdruckerei GmbH
- Prof. Dr. Peter Parycek, Fraunhofer Institute for Open Communication Systems FOKUS
- Dr.-Ing. Reinhard Ploss, Infineon Technologies AG
- Frank Riemensperger, Accenture GmbH
- Siim Sikkut, Ministry of Economic Affairs and Communications of the Republic of Estonia
- Dr. Peter van Staa, Robert Bosch GmbH
- Joe Sullivan, Cloudflare Inc.
- Dr. Claudia Thamm, Bundesdruckerei GmbH
- Prof. Dr. Wolfgang Wahlster, German Research Center for Artificial Intelligence (DFKI)
- Prof. Dr. Michael Waidner, Fraunhofer Institute for Secure Information Technology SIT
- Arne Weber, IMS Evolve Ltd.
- Dr. Richard Weber, Cliqz MyOffrz GmbH
- Oliver Zipse, BMW AG

Additional input

- BASF SE
- micro resist technology GmbH

This acatech IMPULSE presents an overview of the views and conclusions expressed in the interviews. However, individual interviewees may have had different opinions on some of the questions.

1 Digital Sovereignty for Germany and Europe

1.1 The definition and significance of Digital Sovereignty

Digitalisation is transforming entire industries, and digital technologies and services are creating completely new markets. While the US and China have built up a clear lead in the consumer platform economy, the race is still on for global **leadership in the industrial sector**.

It is vital for Germany and Europe to discuss Digital Sovereignty in critical technology fields in order to maintain their industrial **innovativeness** and protect their **freedom of choice** in the face of simmering international **trade disputes**. **Europe** must pursue **its own, new path** based on a coherent strategy.

Digital Sovereignty refers to the ability of individuals, businesses and government to freely choose how they implement the digital transformation and their priorities in doing so. There are **three** key **enablers** in this context:

1. **The relevant technologies and data must be available**, either directly from within Europe or through guaranteed access, even in times of crisis.

2. **Businesses, public institutions and a sufficient number of professionals must possess the skills** needed to evaluate, test and use digital technologies.

3. **The European Union's Digital Single Market** must allow companies to successfully scale up business models, products and services that are based on digital technology. This will also call for regulatory and industrial policy support, for example to compensate for systemic disadvantages such as the limited availability of venture capital compared to the US and the restrictions on access to the Chinese market.

All measures should be geared towards strengthening the **digitalisation of European industry** as a basis for the **global scaling** of the relevant technologies and new value creation. This approach can also help to overcome **Europe's** renowned **weakness at translating** its first-class research into value-added applications.

Coordinating the goals and activities of the relevant sectors will ensure that, in the future, **key** digital **technologies receive the necessary support right up to the highest Technology Readiness Level**.

It is important to stress that Europe's regulatory framework should not seek to exclude non-European actors such as the American and Chinese hyperscalers. Instead, it should promote the **involvement of** global **technology companies, provided that they meet European standards** on matters such as cybersecurity, data protection and personality rights.

1.2 Focus of this paper: the technology and data enablers

While this IMPULSE publication focuses on **the technology and data enablers**, **all three enablers are vital** to the accomplishment of Digital Sovereignty. A technology or group of technologies cannot achieve global success on its own. Global success also relies on the relevant assessment and application skills and on strategic regulatory and industrial policy support that compensates for the disadvantages currently faced by European players wishing to scale up their business.

In order to clarify the different dimensions of Digital Sovereignty and reflect the **increased importance of digital ecosystems**, the paper proposes an **updated technology layer model** (see Figure 1). This model provides a more detailed breakdown than the usual distinction between microchips, hardware and software, and shows where various other levels that are relevant in today's environment fit into the overall context.

The degree of Digital Sovereignty of individual technologies is **assessed and discussed for each of the model's eight levels**. The authors **identified the technology fields that** – in keeping with the chosen definition of Digital Sovereignty – **are most relevant** and feasible and currently have the **greatest need for policy action**. The **examples of existing regulatory sandboxes and institutions** cited in the layer model can provide a **starting point** for further initiatives.

1.3 Overarching recommendations

By proposing a framework for action in the shape of the layer model and examining **one initial focus area per level**, this IMPULSE publication seeks to provide a **starting point for a broad-based discussion of Digital Sovereignty**.

However, a comprehensive discussion of Digital Sovereignty in Germany and Europe will **require a systematic, in-depth analysis** of **the individual levels** and the **other two drivers** identified above.

In addition, technology **foresight processes** should be used to ensure that **fields** that could be relevant to Digital Sovereignty in the future are **identified** as soon as possible. This will allow the corresponding targeted **measures** to be implemented in good time.

Competence monitoring underpinned by a levels-based analysis **is also recommended for those fields** that involve **interactions between multiple technologies** at different, superposed levels. The following are some of the many examples of such fields from recent years:

- the **US hyperscalers' strategy** in the B2C sector: The supremacy of the US hyperscalers in the cloud infrastructure market (Level 3) explains why they are also dominant in the platform and data sectors and to some extent the software market (Levels 4, 5 and 6) – they are able to create lock-in effects at the lower level that tie users in to their ecosystem across all the other levels.
- the **GAIA-X European data infrastructure**: In order to reduce these lock-in effects and become less dependent on US and Chinese hyperscalers, GAIA-X aims to create an open, federated, secure and trusted digital data infrastructure for Europe, based on European values. It seeks to do this by establishing binding standards for European and non-European providers and by guaranteeing interoperability and portability. This infrastructure can provide the basis for a digital ecosystem.
- **Artificial intelligence and autonomous systems**: In order to add new value in the industrial sector, it will be necessary to control the entire AI production chain, from specialised hardware and microchips and the generation and preparation of data, to algorithms, software, sensors and actuators.
- **Quantum computing**: Maintaining a strong component base and establishing European quantum computer hardware capacity are vital to guaranteeing future value creation through software and algorithms.[1, 2]

These examples illustrate the importance of **analysing the current strengths and weaknesses** for each level. It is essential to do this before engaging in strategic regulation and formulating **industrial policy on strategic issues**. In order to minimise unilateral overdependence on individual markets, the Digital Sovereignty project must also encompass the formation of broad **strategic alliances** with other countries that are significant players in the layer model technologies.

1.4 Summary

The **most important element** of sovereignty is **freedom**. In the digital world, this means **the freedom to choose** whether or not to use a particular technology.

The ability to choose **between different suppliers** is key. **Protectionism is not the answer** – the best way to ensure Digital Sovereignty is through access to the widest possible range of flourishing suppliers.

The following general strategies are **recommended in cases where freedom of choice does not exist**:

- Rather than simply copying a technology, it is important to invest in developing and becoming a market leader in the technology's **next generation**.
- Lock-in effects with regard to individual technologies should be avoided through **open standards**, **interoperability**, **portability** and **commodification**.
- The **strategic assets** of Germany and Europe in global value networks should be protected through global growth rather than through isolationism.

The strengthening of Digital Sovereignty will thus often form an integral part of strategies for promoting **innovation and prosperity** in Europe **and ensuring the future viability of European industry**.

1 | See. Kagermann et al. 2020.
2 | See. Buchenau et al. 2021.

2 The technology layer model

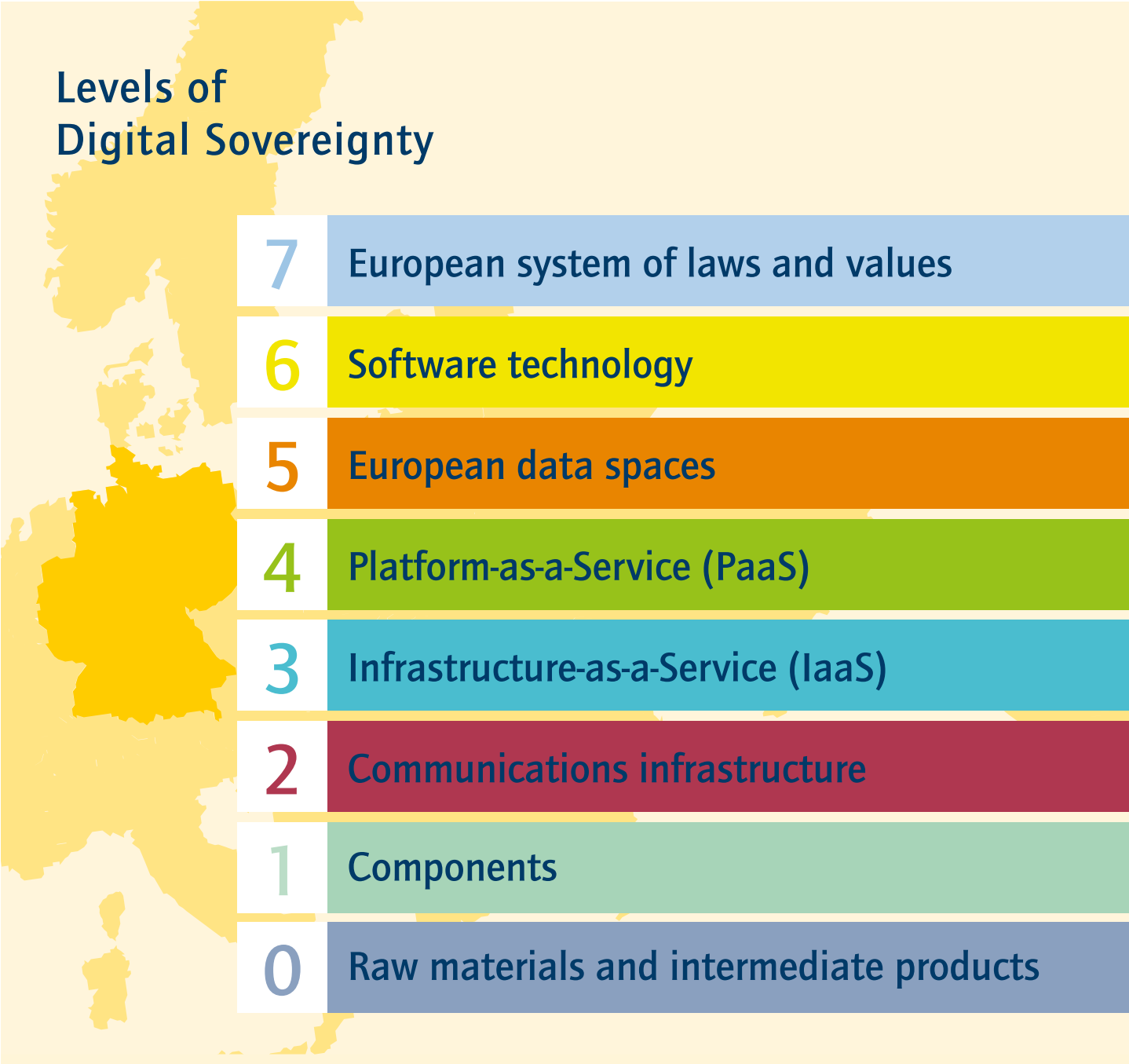


Figure 1: Layer model showing how the different levels of Digital Sovereignty build on each other (source: authors' own illustration)

Components/Focus area	Regulatory sandboxes and institutions
Cybersecurity, cryptography, **e-identity,** EU certification (consumer protection) and standards	Regulatory sandbox: cybersecurity centre Institution: BSI + network of cyberregions in Germany
App development, Office, ERP, AI, middleware, robotics software, blockchain, algorithms, **EU open source,** VR/AR, QC	Regulatory sandbox: n/a Institution: Federal Agency for Disruptive Innovation, AI network
E.g. for **mobility**, health, public sector, digital public space	Regulatory sandbox: Data Space Mobility Institution: GAIA-X, German and European strategies for data
Application and development ecosystems B2B and B2C (abstraction layer, container technology) QC, AI, **IoT**	Regulatory sandbox: n/a Institution: GAIA-X/completion of EU single market
Virtual, distributed cloud ecosystems, edge technology, QC, AI-HPC centres	Regulatory sandbox: **Gardener** (Deutsche Telekom, SAP, Bosch, ...) Institution: GAIA-X
Broadband infrastructure, mobile networks **(Open RAN),** Galileo navigation	Regulatory sandbox: **Open RAN** Institution: O-RAN Alliance
Microchips, sensors, actuators, production and enabling technologies, 3D printing, QC, AI	Institution: IPCEI on microelectronics
Rare earth elements, ...	Institution: German Mineral Resources Agency

0 Raw materials and intermediate products

Rare earth elements, ...

Institution: German Mineral Resources Agency

What is included in this level?

This level encompasses the extremely **heterogeneous field of raw materials and intermediate products** required to produce electronic components such as microchips and batteries. **Rare earth elements** are the best-known example of resources that are essential for modern devices. However, other resources such as the high-purity, high-quality **process chemicals** used in the production process are equally important.

Demand is also growing for new, **high-tech raw materials**, for example **functionalised materials** such as quantum dots. The absorption and emission properties of quantum dots can be precisely adjusted by selecting the size of the particles and manipulating their surface.

Status quo

In recent decades, the **value networks** for many raw materials and intermediate products have been **relocated to Asia**. As well as the **cost benefits**, the reasons for this trend include **proximity to major customers**, which makes it easier to work on joint innovations, and the environmental benefits of reduced transport.

As a result, European producers **are in general becoming increasingly dependent** on US and Asian raw material and intermediate product suppliers. This poses **major challenges, especially for SMEs**, whose limited market power means that they have very little influence over the general market conditions.

Proposals

It is not possible to achieve autonomy at this level. However, the existing **dependencies** can be addressed through a range of measures that could be brought together under an **updated raw material strategy**. These include:

- **Continuous monitoring** of raw material requirements and availability by the **German Mineral Resources Agency**; monitoring could potentially be extended to more complex intermediate products.
- **Policy initiatives** to guarantee access to raw materials and intermediate products for which there is only one supplier and to reduce dependence, for instance by gaining access to a second raw material source or promoting the development of process chemical production capacity.
- A stronger emphasis on **circular economy** principles in order to **reduce import volumes** of some raw materials, accompanied by the **promotion of research into potential alternatives** for scarce raw materials.

Summary

The European economy will continue to rely on raw material imports for the foreseeable future. Continuous **monitoring**, **proactive policy measures** and the **development of alternatives** are key to preventing critical dependencies. It may also be possible to create mutual dependencies in the case of high-tech raw materials.

1 Components

Microchips, sensors, actuators, production and enabling technologies, 3D printing, QC, AI

Institution: IPCEI on microelectronics

What is included in this level?

The component level encompasses **microchips, sensors and actuators**. As the foundation of all other infrastructures, these **components**, their **enabling and production technologies** and to some extent also the relevant development software tools are particularly important, not least because they are increasingly becoming **a focus of geopolitical disputes**, primarily between the US and China.

With numerous established companies, Germany is strongly positioned in the **sensor, actuator and production technology** markets. It also has several start-ups such as Q.Ant (quantum sensors) and Franka Emika (robotics), and has established and expanded research centres focusing on the technological principles of human-machine interaction. In the interests of Digital Sovereignty, it is important to **maintain these strengths**.

Focus on microchips – the status quo

	Importance for Digital Sovereignty	Degree of dependence on non-EU countries	Resulting degree of vulnerability
Functional level (*product as a functional item in its own right, before assembly*)			
Processors for AI, data processing, communication (4G/5G)			
Memory			
Sensors			
Power electronics			
Design level (*ability to develop the functional level products*)			
Basic design software tools (CAD) for circuit design			
Additional development software			
Production and enabling technologies (*required to produce the functional level products*)			
Chip production – highly-integrated products			
Chip production – sensors and power electronics			
Packaging and testing			
Production equipment (*specialist systems, machines*)			
Equipment for chip production			
Equipment for packaging			
Testing equipment			

Significance of colour values

Low — High

Figure 2: Heatmap for microchip technology field: priority areas in terms of Digital Sovereignty, existing dependencies in these areas, and vulnerabilities arising from the current structure of each area (source: authors' own illustration)

At this level, the area where policy action is mostly urgently required is the **microchip** market.

This field presents a **very mixed picture**. Many of its elements are characterised by complex international supply chains, and are thus highly **dependent on non-EU markets**. As a result, some of these elements are particularly **vulnerable** (see Figure 2). These vulnerabilities were highlighted when several industries suffered shortages during the first quarter of 2021.

Europe is unlikely to be able to close the gap on the market leaders in every area, and it would in any case be economically inefficient to do so. It is therefore necessary to identify the particular areas where Europe should focus on **building and expanding its expertise and capacity**. These should strengthen the **Digital Sovereignty of European industry** and also serve as a **bargaining chip in the global market**.

- **High-end microchips: There is no easy way to address the technology dependence that currently exists** with regard to high-end microchips made using the five nanometre process and beyond (More Moore). The only companies capable of producing these high-end chips are Taiwan's TSMC and South Korea's Samsung. Nevertheless, when it comes to using these chips, a certain degree of sovereignty can be achieved through testing and the encryption of the processed data.
  Businesses also currently rely mainly on Taiwan and South Korea **to produce the chips for highly-integrated products**. Germany only has **partial expertise in the enabling technologies**, and **very little expertise with regard to the relevant production technology**.
  However, the leading **chip manufacturers** are themselves actually **dependent on a European company**. With a market share of two thirds, Dutch company ASML is the world's largest supplier of the lithography systems that play an essential part in the chip manufacturing process. Moreover, Zeiss and Trumpf are two of ASML's most important suppliers. These European companies provide a certain degree of leverage and **protection in the global supply chain system** for high-end chips.
- **Specialised microchips**: **High-end chips** optimised purely for performance **are actually not necessary** for many projects in **leading-edge** industrial value creation **fields** in Germany, such as IoT and edge computing, mobile base stations, and sectors like the automotive and pharmaceutical industries.
  Other factors are often **more important**, for example **low costs** and properties such as **low energy consumption, a long service life** or **specialised functionality**. These can be achieved with **"good enough" production processes** in the 12-28 nanometre range. The same even applies to highly innovative solutions such as silicon-based photonic chips for quantum computing.
  However, **Europe cannot claim to have sovereignty in this field either**, since there is **not enough** European-owned **production capacity**. **GlobalFoundries** in Dresden can produce chips down to twenty nanometres. In recent years, however, the **Abu Dhabi-owned** company's production has **failed to meet the demand of European industry**.
  The planned **acquisition of ARM Limited** by America's NVIDIA Corporation poses a **threat to Europe's Digital Sovereignty**. Consequently, if Europe's supervisory authorities decide to approve the takeover plans, they should stipulate a clear requirement for continued access to important **intellectual property** and **chip segment know-how** relevant to **embedded systems and connected devices**.

So although it is not really worth investing in efforts to close the gap in the More Moore domain itself, **it may be worth** providing policy support **to build capacity** for the design and production of **specialised chips** (**More than Moore**) and novel chips using innovative materials, architectures, 3D structures or manufacturing technologies (**Beyond Moore**).

In this context, it will also be important to establish standards and **define innovative product categories**, provided that there is **demand from leading industries**. While the starting position is good in the mobile communications (Nokia, Ericsson) and automotive industries, the mechanical engineering industry typically still uses products that were defined in other parts of the world.

Proposals

Additional policy action is required to strengthen microchip manufacturing, which is becoming increasingly important in several strategic industrial and digital sectors in Germany and Europe. If the **current level** of production remains unchanged, it is likely that there will be a further **deterioration in** Germany's and Europe's **position** within the web of mutual interdependencies.

The following **three proposals** are aimed at strengthening policy action in this area:

- **Market measures**: European semiconductor and microchip manufacturers should be encouraged to identify **relevant** future **microchip and production technologies** and **enter the corresponding markets as soon as possible** so that they

can build a strong position in them. This will only be possible if there is more **active engagement** from other **leading industries** apart from the automotive and mobile communications industries.

While the detailed decisions about which directions are pursued should in principle be left up to the market, breakthroughs can nonetheless be facilitated by **support from industrial policy instruments**.

A **strategically oriented public procurement policy** could generate significant momentum in this context. **Other relevant measures** include protection against foreign takeovers, increased consolidation within Europe, the targeted promotion of breakthrough innovations and the involvement of ministries and public agencies in standardisation bodies.

In the future, the **strategic frame of reference** for decisions relating to the deployment of aid instruments should be the **global market** and not the European Single Market as has hitherto been the case.

- **IPCEI on microelectronics**: The IPCEI's **next phase** should be **strengthened** by ensuring that it is adequately **resourced** and by significantly **accelerating** the decision-making process.
- **New foundry for chips in the 20-60 nanometre range**: The establishment of a **European-owned** foundry for chips of this size should be investigated, for example through an **additional IPCEI**. This would support the ecosystem's development by guaranteeing a **targeted supply** of the **most important chip types** for German and European industry.

A project of this nature could build on the experience of **existing initiatives** and the companies that participated in the first IPCEI. Following a phase of public support delivered through the EU or through a consortium of individual EU member states, the medium-term **objective** should be to establish a business-driven, **globally competitive custom-built chip** production capability.

Summary

Instead of investing large sums of money in efforts to close the gap in the More Moore domain, the focus should be on building and growing a strong position in specialised **More than Moore chips**, and on gaining a **competitive advantage** in **innovative Beyond Moore chip technologies**. In a microchip market characterised by strong mutual international interdependencies, this can provide Europe with a **bargaining chip** that could be used in an escalation scenario to safeguard access to other types of chip that are not produced in Europe.

2 Communications infrastructure

Broadband infrastructure, mobile networks (**Open RAN**), Galileo navigation

Regulatory sandbox: **Open RAN**
Institution: O-RAN Alliance

What is included in this level?

The critical areas identified for the communications infrastructure level are **broadband infrastructure** (fixed and terrestrial mobile networks) and **satellite-based navigation**.

The **mobile network** is made up of the **access network** (antennae and their control systems) and the **transport**, **aggregation** and **core network**. While the access network accounts for over 70 % of investment, it is the **core network** that is the **most security-critical**. This is because it is via the core network that the overall **network is controlled** and its **traffic and metadata are managed**.

All areas of today's networks are based on **technology components** made by a variety of European, US and Chinese/Asian manufacturers (e. g. Ericsson, Nokia, Cisco, Juniper, Microsoft, Huawei and Samsung). While there are well over a hundred mobile providers in Europe, the **number** of **technology providers** that exist worldwide for each **category** is very **low**, especially for the **radio access network**, where Huawei, Ericsson and Nokia hold over 75 % of the total market share. The resulting **technology dependencies** are not easy to address, despite the fact that the individual components are largely installed, managed and controlled in a sovereign manner by the major telecommunications providers.

Europe's **Galileo** is a global **navigation satellite** system that provides an **independent**, **civilian alternative** to America's NAVSTAR GPS, Russia's GLONASS system and China's BeiDou system. It is vital to ensure Galileo's **operational capability** in order to maintain technology sovereignty in this area.

The following section focuses on how **supplier diversity** can be increased in order to accelerate **radio access network innovation**.

Focus on radio access networks – the status quo

Radio access networks comprise the following **technology components**: a) radio cell and antenna, b) radio unit, c) baseband unit. Typically, each of these components is integrated by just **one of a handful of leading network suppliers** and contains **proprietary, non-interoperable technology**.

Huawei is currently the **global market** leader, while **Ericsson** and **Nokia** offer a European **alternative**. However, each of these three companies uses **proprietary standards**. This generates undesirable **lock-in effects**, **holds back innovation** and **reduces flexibility** in terms of switching to current and future mobile standards (5G, 6G).

Proposals

The **O-RAN** (Open Radio Access Network) concept offers a **standardised open network architecture** for the radio access network in order to address the potential negative impacts on technology sovereignty of lock-in effects associated with the limited number of manufacturers.

If antennae, radio units and baseband units made by different manufacturers complied with a **common O-RAN standard** and communicated via **open interfaces**, it would be possible to achieve significantly greater flexibility, reduce dependence on a handful of dominant network suppliers, and **facilitate market entry** for new and potentially **smaller European suppliers**. This would in turn drive **innovation** and strengthen network **security** due to greater transparency and control (see Figure 3).

Several **leading global network operators** have come together in the global **O-RAN Alliance** to work on the necessary **specifications**. The major European network suppliers are also involved, together with several – often smaller – tech companies. However, even this project still has significant dependencies on individual suppliers such as Intel.

In any case, with around 30,000 current antenna sites owned by Deutsche Telekom alone, it will only be possible to **implement** Open RAN compatible network components very **gradually**. Moreover, **open access** will need to be provided to the currently installed **interfaces** and **protocols** to enable continued use of **existing components** in an **Open RAN architecture**.

Since this will require the **cooperation** of the manufacturers who currently dominate the market, and given the **complexity** of the networks, it is likely that any **transition** will take **several years** to accomplish. **Completely open implementations** of the three

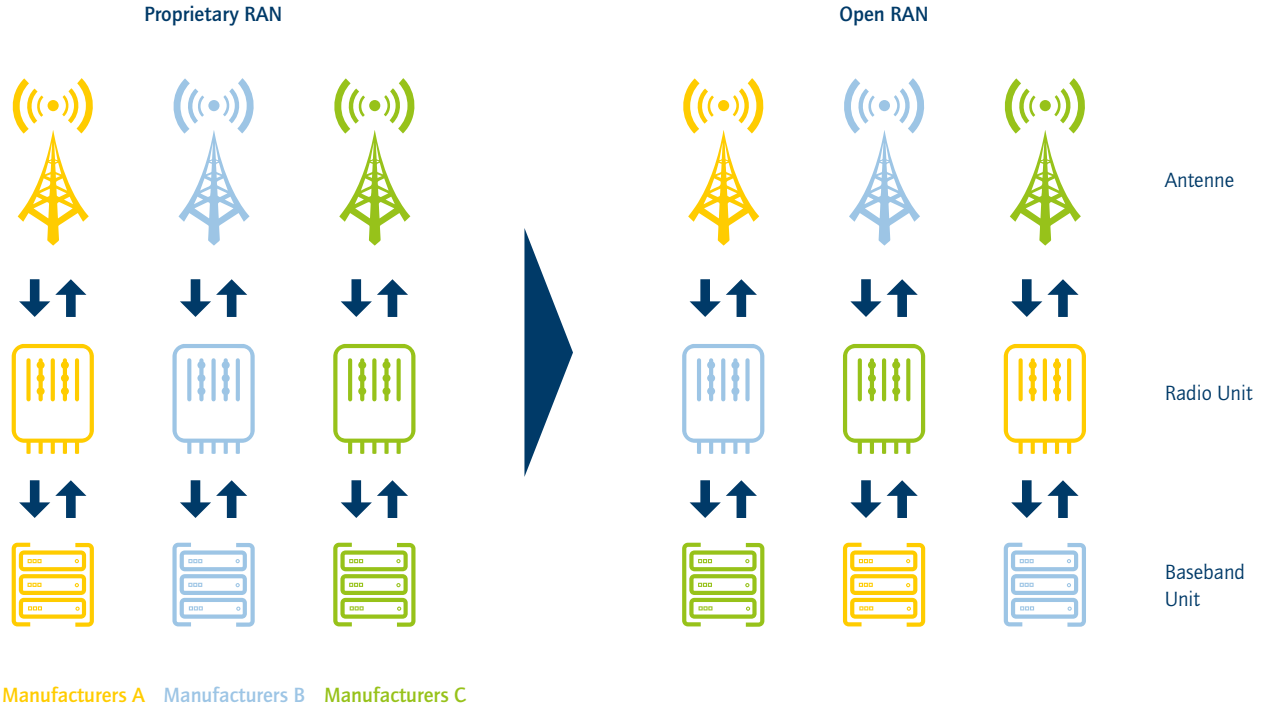


Figure 3: Transition from status quo to the standardised open network architecture of the O-RAN concept (source: authors' own illustration based on Telefónica Deutschland 2020)

layers should be promoted in order to accelerate this process. This step was recently taken by DARPA and the Linux Foundation, while Germany's Federal Agency for Disruptive Innovation (SprinD) presented a similar proposal in November 2020.

More generally, it is also necessary to investigate how **industrial policy** and **regulatory measures** and **mechanisms** can be used to achieve systemic structural improvements in the **European telecommunications market**. The focus should be on **strategically** and **sustainably strengthening** the **competitive position** of the **European providers** (Nokia, Ericsson, et al.), especially in relation to US and Asian competitors.

Summary

Radio access networks are dependent on a handful of manufacturers due to the **lack of vertical compatibility** between their different components. The **O-RAN Alliance** aims to address this situation by establishing **open interfaces**. A fully open-source approach would foster **innovation** (e. g. 6G), **competition**, **resilience** and **transparency** in the mobile communications sector.

Within the **European telecoms market**, it is important to use **industrial policy** and **regulatory measures** to **strengthen** the position of **European suppliers**.

3 Infrastructure-as-a-Service (IaaS)

Virtual, distributed cloud ecosystems, edge technology, QC, AI-HPC centres

Regulatory sandbox: **Gardener** (Deutsche Telekom, SAP, Bosch, ...)
Institution: GAIA-X

What is included in this level?

This level encompasses hardware and system software, providing the technological basis for connectivity (**connect**), computational capacity (**compute**) and the storage of data on servers (**store**).

In traditional contexts such as data centres, hardware is a readily available, standardised commodity. The users of enterprise software and other similar types of software can **freely choose** which hardware (e. g. PCs and notebooks) they use, and are thus able to **avoid dependence** on individual manufacturers. As long as **hardware and software are decoupled**, it doesn't matter that there are no German hardware suppliers of note in the private and commercial markets. However, the advent of the cloud is **depriving** user companies of this **sovereignty**, turning them into **consumers** of technical cloud services that are operated and provided **as a service** by specialist providers. This leads to the development of **network effects and economies of scale that favour the providers of cloud services** as the underlying platform. The huge investments required due to the need for a global presence mean that there is a **tendency for** a handful of market-leading **cloud infrastructure providers** (**hyperscalers**) such as Microsoft, AWS and Google **to form oligopolies** and try to **lock** users **in** to their platforms. These lock-in effects result from the **coercive coupling** of the rather undifferentiated cloud infrastructure with the application platforms (see Level 4, PaaS).

This makes it possible for the cloud companies to build huge **global data spaces** (Level 5), which provide them with a global competitive advantage when it comes to innovative applications and in particular **AI and machine learning**.

For the time being, the **hyperscalers** cannot be rapidly replaced in Europe, even if GAIA-X is successfully implemented. However, the fact that the American hyperscalers are governed by the **US CLOUD Act threatens the security** of **data** stored **in Europe**. Consequently, **cooperation based on European law** should be established with the hyperscalers **in Europe**, while Europe should also develop its own capabilities and services in parallel.

This is exactly the goal being pursued by **the Sovereign Cloud Stack (SCS) project** in GAIA-X, which aims to build a **network of providers** who develop and provide federated infrastructure services (IaaS/CaaS/PaaS) using **precisely defined common standards**, free software and documented operating processes. The **diversity of providers** (and the option for companies to run their own environments) will create a **highly interoperable virtual cloud**.

Focus on priority areas for development in Europe: Portability and standardisation, virtual high performance computing (HPC) networks and next generation technologies

- **Portability and standardisation**: Many modern workloads operate at the container level, and can be implemented and run independently of the underlying IaaS layer with the assistance of multi-cloud container frameworks such as Rancher, Kubermatic and Gardener. This abstraction layer **decouples the application platforms** from the cloud infrastructure, **circumventing the hyperscalers' lock-in strategy** and making application platforms portable. For example, it is possible to move container workloads between hyperscalers and SCS-based, sovereign clouds.Based on the GAIA-X concept, SAP and Deutsche Telekom have established the **Gardener Cloud Foundation (GCF)**, a promising commercial open-source project aimed at creating a digital ecosystem that uses **open standards with distributed systems** (see Figure 4). This **application platform portability** allows the **hyperscalers' lock-in strategy** to be **circumvented** in the interests of fair competition, potentially making it possible to **re-commoditise Infrastructure-as-a-Service**. Various users are already employing GCF as part of their multi-cloud strategy.
- **Virtual AI high performance computing (AI-HPC) centres** are an important resource for the development of leading AI solutions. HPC enabled by virtual cooperation between European companies puts unlimited computing resources at the disposal of the companies in question. Policy support is required in this context, especially with regard to antitrust restrictions. The first cooperation initiatives are currently in preparation. Through the federation of infrastructure services, GAIA-X can offer a modular portfolio of HPC applications for a wide range of users.
- **The development of next generation technologies and architectures** such as the edge computing cloud architecture is a promising strategy that is being actively pursued by German industry. German providers are strongly placed in this sector. In the medium to long term, there are high hopes

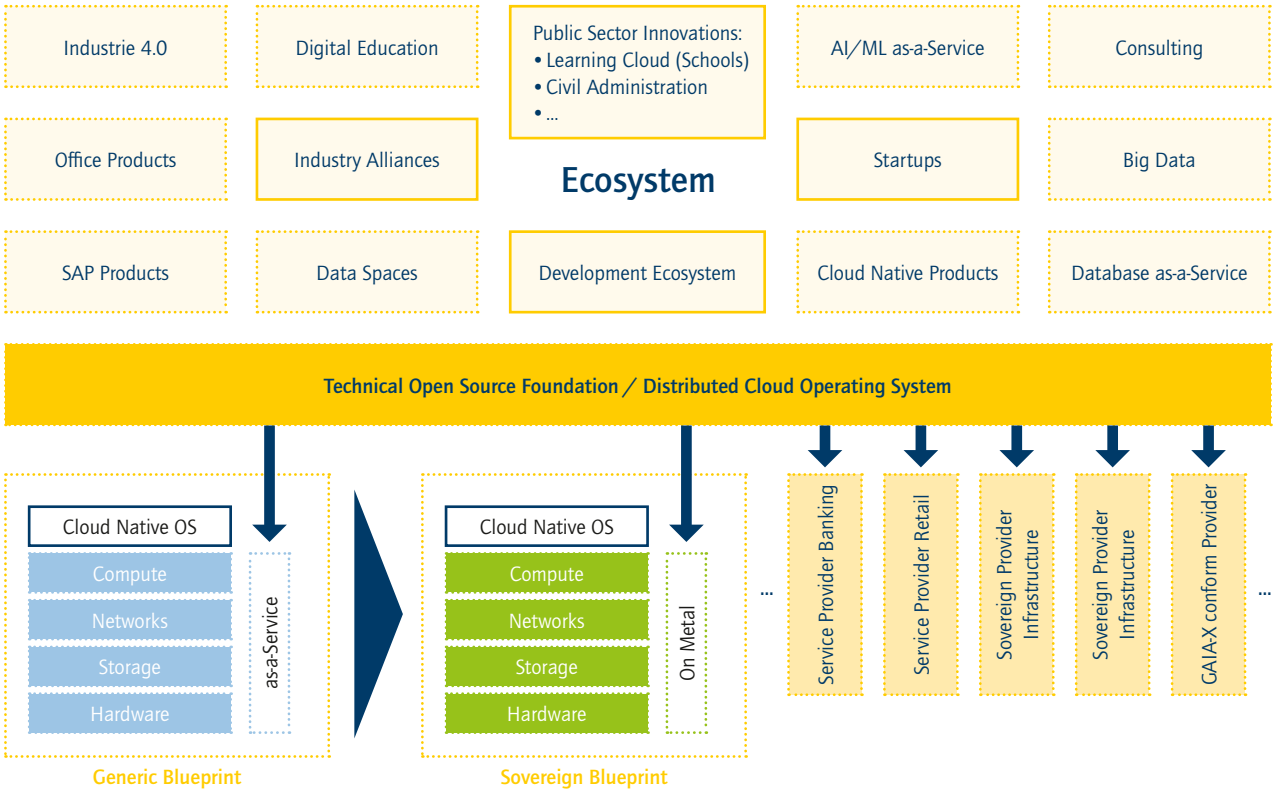


Figure 4: Gardener – an open, coherent and extensible standard (source: authors' own illustration based on SAP 2021)

that quantum computing will offer a means of closing the cloud services technology gap. Urgent action is required by decision-makers in government and industry to ensure that Germany and Europe can position themselves as leaders in this technology field.

Summary

In order to overcome dependence on global providers, the long-term aim should be to **commoditise** the services provided by the **hyperscalers**. **European projects** such as the **Gardener Cloud Foundation** can make an important contribution to enabling cross-platform **data portability**. This will allow Germany and Europe to maintain their **ability to innovate** in this field.

4 Platform-as-a-Service (PaaS)

Application and development ecosystems B2B and B2C (abstraction layer, container technology) QC, AI, **IoT**

Regulatory sandbox: n/a
Institution: GAIA-X/completion of EU single market

What is included in this level?

The **Platform-as-a-Service (PaaS)** level encompasses application and development ecosystems in the B2B and B2C sectors.

Thanks to their industrial **domain expertise, German and European providers** offer market-leading solutions in the **B2B sector**. Examples include SAP, the global market leader for ERP systems, Dassault, the market leader for PLM systems, and Siemens, although its MindSphere IoT operating system still has a relatively small market share. However, the value of these European companies is only around 10% of their American counterparts. One of the reasons for this is the **lack of scaling opportunities due to the fragmented, heterogeneous nature of the European market**.

In the **B2C sector**, there is already a high level of **dependence** on US platform providers such as Amazon, Facebook, Microsoft and Google. European providers will not be able to challenge the **market dominance** of these B2C hyperscalers in the foreseeable future. It will be a major challenge to find the best way of **regulating** these platforms, since some of them hold a monopoly-like position that potentially gives them the ability to influence political **(decision-making) processes**.

Since the relevant skills are key to maintaining Digital Sovereignty, **education, science and media** platforms are of paramount importance. Some proposals for education platforms have already been tabled and should be actively pursued. Here too, the watchwords must be agility and user focus – it will be vital to leverage the private sector's strength in innovation.

The advantage of PaaS for businesses is that they don't have to **budget** for development infrastructure and can use ready-made software modules (microservices). This creates **opportunities** for **start-ups** to enter the market, and also strengthens the competitiveness of established companies by allowing them to reduce costs and become more agile. However, the use of PaaS solutions also entails risks, such as a greater danger of **information leakage** and greater **dependence** on the PaaS provider.

Tighter regulation means that European providers have to comply with stricter standards than hyperscalers from other parts of the world. A **level playing field** should be established for European and non-European providers.

Accelerating the establishment of a **European economic and legal area and the completion of the Digital Single Market** will provide a basis for European providers to scale up their businesses (in both the B2C and B2B sectors). In order to develop technology sovereignty at **Level 4** (PaaS), it will first be **necessary** to achieve **sovereignty** at **Level 2** (O-RAN initiative) and **Level 3** (GAIA-X initiative). Consequently, these initiatives enjoy **widespread support from industry**.

An industrial IoT/I 4.0 regulatory sandbox: an EU pilot for the digitalisation of European industry

In order to harmonise Europe's heterogeneous B2B sector and in doing so help to drive the digitalisation of European industry, industry working groups have proposed the establishment of a cross-manufacturer, federated IIoT/I 4.0 platform based on **standardised interfaces**. This should build on and strengthen existing initiatives, including but not limited to *GAIA-X* (industry domain), the *Plattform Industrie 4.0* and *Article 35c*.[3] The project should focus on two main use cases: **smart product services**, i.e. the sale of machinery as a service, and **smart factories**, i.e. factories in which all the machines are connected to each other, regardless of their manufacturer, in line with the Industrie 4.0 model. It is important to emphasise the following points:

- In order to **guarantee connectivity**, the platform should support standards relevant to Industrie 4.0 (OPC/UA, LWM2M, MQTT ...) and use 5G technology.
- Real-time data processing and visualisation should be enabled in the **edge layer** via AI/machine learning/data analytics.
- The control and management of the smart factory should be implemented via the **control layer**.

A **platform based on these principles** should be planned and piloted by a **consortium** of relevant actors. **Existing European software solutions** (e.g. Siemens MindSphere, SAP Digital Manufacturing Cloud, ADAMOS/Software AG and Bosch IoT Suite) would each provide an independent marketing basis, while the

3 | See Federal Ministry for Economic Affairs and Energy 2020.

interfaces would be developed and integrated in open source to provide **shared connectivity**.

A jointly developed platform would help to **defragment** the European platform landscape, generating **significant economies of scale** and **substantially reducing time-to-market** for the **digitalisation of European industry**. This would **significantly accelerate** the national and European **digitalisation strategies for industry and SMEs**. In this context, it is important to **promote** an **innovation and start-up culture** (including access to capital) that encourages the agile, state-of-the art development of user-centred, European solutions.

At the same time, the establishment of a **Europe-based IIoT architecture standard** can help to **secure the Digital Sovereignty** of European industry. **Europe's expertise in the field of telecommunications** (Deutsche Telekom, Ericsson, Nokia) can be harnessed to this end and **combined with the industrial know-how** of Europe's leading technology companies.

Summary

This level is key to the innovations developed in Levels 5 and 6, since the **availability of the relevant services is vital for scaling up new business models**. **Strong US platforms** have already become established in the **B2C sector**, where policy and regulatory measures are needed in order to address the existing dependencies.

The **B2B sector** is **not yet dominated by any particular platforms**, and many industries are only just beginning the process of digitalisation. In order to ensure the future success, Industrie 4.0 leadership and thus sovereignty of Germany and Europe in this sector, innovative, domain-specific platforms and business models **must be established here and now**. The current European offer is too fragmented. Consequently, the **establishment of a collaborative IIoT platform** is key to ensuring the sovereignty of European industry. It can thus be assumed that a **collaborative regulatory sandbox** to support the implementation of such a platform would be widely welcomed by government, industry and business.

5 European data spaces

E.g. for **mobility**, health, public sector, digital public space

Regulatory sandbox: Data Space Mobility
Institution: GAIA-X, German and European strategy for data

What is included in this level?

In the digital age, **the role of data as a key resource for science, industry and society is more important than ever**. The ability to use, combine and analyse data underpins innovation and economic prosperity, knowledge generation and social cohesion.

Despite the immense opportunities and the ongoing progress with digitalisation, **Germany has by no means fully leveraged the huge potential of the available data** for science, industry and society, or indeed for Digital Sovereignty. There are many reasons for this, including insufficient standards, uncertainty about the legal framework and unwillingness to share data.

The digital economy is **data-driven**. Particularly those applications that use **artificial intelligence** (AI) **rely** entirely on large **datasets** to develop algorithms based on patterns detected in the data. The goal should therefore be to establish large, connected, open and secure data spaces in Europe.

In the **B2C sector**, these data spaces have now been established in the US and China, and German and European companies in this sector are already struggling to obtain the data that they need to innovate. Sovereignty questions are also arising in connection with the **control of data spaces** with European data by non-European actors. In order to address these issues, it is vital to maintain Europe's **regulatory sovereignty** (key issues: the **lack of a European response** to the US **CLOUD Act** in terms of **access to data**, and the **Digital Services Act with regard to content regulation**) and **governance sovereignty** (key issue: provider compliance with European (GDPR) standards).

Similar **data spaces have for the most part yet to be established in the B2B sector**. If the US and Chinese hyperscalers manage to establish or control the major data spaces in this sector too, there will be serious economic consequences for Germany and Europe, and serious constraints on their freedom of choice and sovereignty.

Consequently, the **development** and rapid **implementation** of attractive solutions for industrial **data ecosystems** and measures to strengthen sovereignty must be **supported** and promoted by **policymakers**. Initiatives such as **GAIA-X** and **International Data Spaces** (IDS) constitute important **starting points for policy measures** and **conceptual blueprints**. Several European and German government papers have already recognised the importance of **trusted data spaces** that enable secure domain-specific and cross-domain data access and exchange. Published on 27.01.2021, the Data Strategy of the German Federal government[4] is an important instrument and should be systematically implemented.

The example Data Space Mobility – the problem and the status quo

In order to accomplish data sovereignty in the mobility sector in Germany and Europe, it is **vital** to be able to **connect heterogeneous data** and **services** so as to enable user-friendly and sustainable modern mobility. An example is the connection of different modes of transport to create an intermodal transport chain.

The big advantage of connecting data in a data space is that it facilitates the realisation of new mobility services and **complementary** (B2B and B2C) **business models**.

Two basic requirements must be met in this context:

1. Successful implementation of the data space will require a **commitment from all the relevant stakeholders** to contribute their data. Efforts to obtain this commitment have been ongoing for some years, but have yet to produce the desired results.

2. A **regulatory** and **industrial policy framework** must be developed to ensure that the establishment of the data space gives a chance to new – often start-up driven – initiatives in Europe, rather than simply allowing the hyperscalers to increase their dominance even faster.

Proposals and objectives

An initiative has been launched to establish a **trusted, secure, decentralised Data Space Mobility (German: Datenraum Mobilität – DRM)** based on European values, in order to create market conditions that stimulate competition and ensure a **common level playing field** (see Figure 5).

The aim of the DRM is to help its users to accelerate the **implementation** of innovative **data- and AI-based mobility solutions**

4 | See Federal Chancellery 2021.

and give them a chance of succeeding without having to contend with dominant non-European hyperscalers right from the outset.

It is essential to ensure common usage rules and trusted data standards, access rights and responsibilities based on **European values**. **Data is shared voluntarily**. SMEs, start-ups and R&D projects can also make use of the DRM.

The project is currently focusing on **three key points**:

1. The concrete details of the **business model's governance and design**, which are based on **European values**

2. Defining the DRM's specific **technology requirements**

3. How to go about the market rollout, Europeanisation and scaling of the data space

The DRM acts as a **data hub** that facilitates the exchange of data. Different sub-data spaces are connected to each other via connectors, in a decentralised model. The connectors guarantee secure data interaction.

The **Mobility Data Marketplace (MDM)** or National Point of Access for Mobility Data is one of the DRM's key sub-data spaces. It contains data such as static and dynamic travel and traffic data, public transport company data and route plans. The DRM connects the stakeholders' voluntarily provided data and services, e.g. vehicle, infrastructure and weather data and information about roadworks and major disruption events.

The data infrastructure and system architecture are based on the **IDS reference architecture**. This also ensures the ability to **connect** with **GAIA-X**. The IDS model guarantees the data sovereignty of the individual data providers, since conditions of use can be attached to the data they provide. Identification, authentication and data protection are guaranteed.

The **commitment** of the **data providers** and **users** is critical to the project's success. Discussions are currently underway with a representative group of actors (private and public mobility service providers, OEMs, platform companies and digital businesses). The aim is to establish the basic principles for cooperation by clarifying the policy and legal framework and drafting an overall DRM strategy. This will then encourage other actors relevant to the mobility sector to get involved.

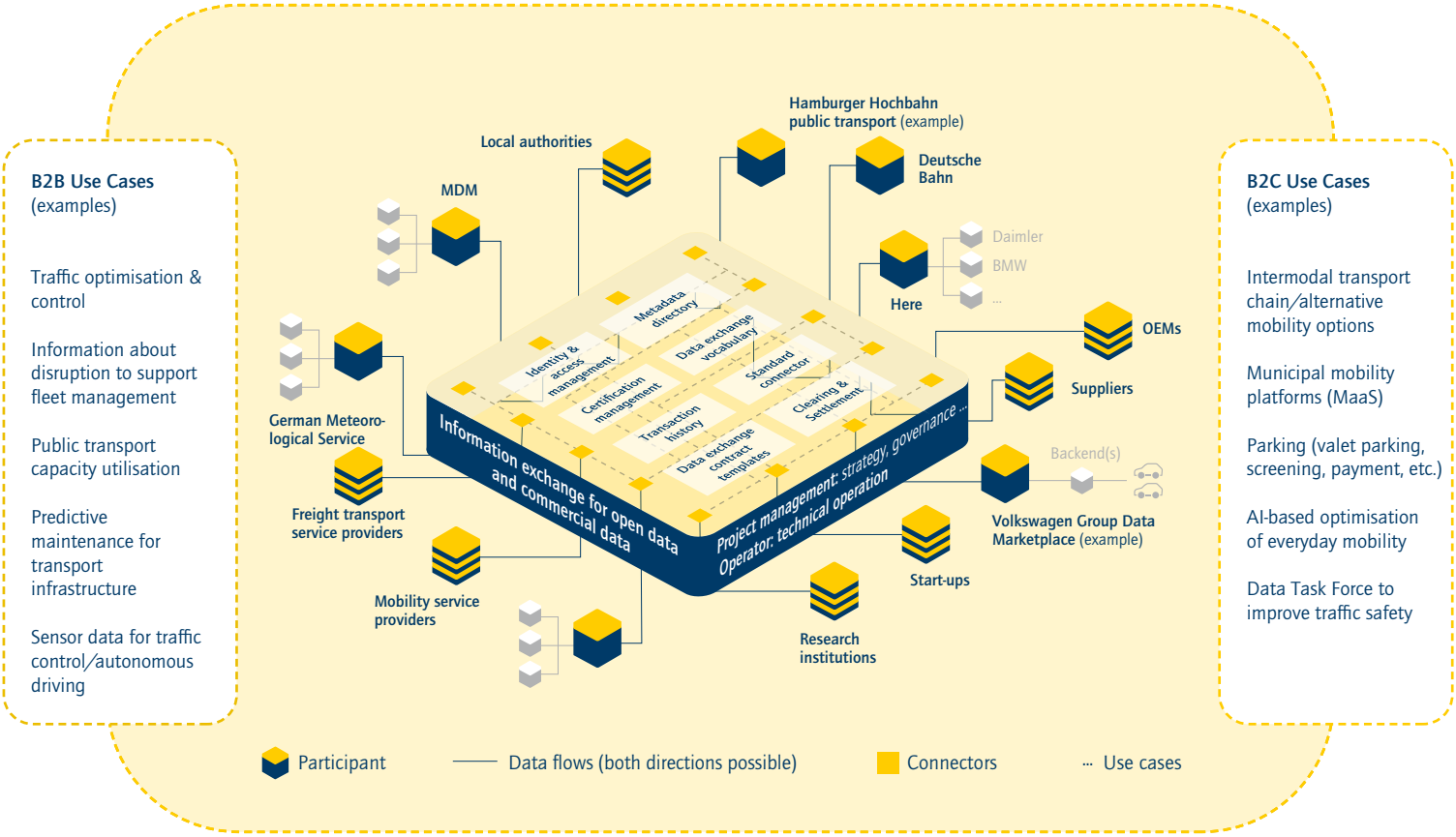


Figure 5: Illustration of the decentralised Data Space Mobility (source: DRM 2021)

Summary

Trusted **data spaces** that enable **secure domain-specific** and **cross-domain data interaction** are indispensable for the implementation of tomorrow's data-driven, platform-based business models. The **DRM** is an initiative of the German government and various private and public mobility providers that aims to establish a comprehensive data network for mobility by the end of 2021. The data space connects different sub-data spaces and ensures the data sovereignty of the participants. Policy support for and promotion of **responsible data use** is vital to success in the digital economy. With its focus on innovation, the German government's recently adopted data strategy provides an important framework in this context..

6 Software technology

App development, Office, ERP, AI, middleware, robotics software, blockchain, algorithms, **EU open source**, VR/AR, QC

Regulatory sandbox: n/a
Institution: Federal Agency for Disruptive Innovation, AI network

What is included in this level?

The existence of **European developers and providers** and a wide **range of international products** means that there are very **few critical issues** in terms of access to app development tools, ERP systems, middleware, and software for robotics and blockchain/distributed ledger technologies. However, organisations do become dependent on certain products once they have implemented a particular system.

Significant dependencies exist with regard to **operating systems (Windows, iOS, Android)** and **Microsoft Office**, which are a de facto standard for many private individuals, companies and public authorities. Lock-in to the providers' ecosystems is reinforced by **growing reliance** on the functionality of their **online services**, as illustrated by the switch to the Microsoft 365 cloud service model.

As with European providers' ERP systems, switching to an alternative provider is far from straightforward. Access to European ERP systems could be used as a bargaining chip in an extreme scenario where there was a threat of restrictions being imposed on access to Windows and Office. In general, however, the aim should be to reduce dependencies.

The targeted use of open-source software in specific areas could help to reduce dependencies and strengthen Digital Sovereignty in the software sector. The public sector has an important role to play in strengthening both innovation in this field and the corresponding community. It is important to avoid repeating past errors – it will be crucial to ensure a strategic **focus on reducing dependencies** and **establishing open and federated platforms** that can provide a foundation for start-ups and for a fast-growing European digital industry that produces concrete applications which add value for customers. The following points could merit further investigation:

- Consideration of the targeted use of open-source software for the **digitalisation of government and public administration** based on the adoption of a strategic procurement policy and promotion of open-source solutions
- The use of **open-source hardware components** and open-source software for the **operation of highly sensitive areas**
- The **development** (via competitive tendering) and **promotion** (with very concrete targets) of **open-source software and platforms**
- The establishment of **standards** (for interfaces, security levels, libraries) to enable high reusability of components beyond the public administration context
- **Support for initiatives** such as the Open Source Business Alliance, the Gardener Cloud Foundation and the Eclipse Foundation at European level

The relevant initiatives should **learn from previous attempts to switch software systems**. In the past, several public authority projects have failed in their attempts to develop and run their own non-commercial software. On the other hand, commercially developed and often "invisible" open-source software is already being used very successfully in the server and application settings of municipal, regional and central government.

European software start-ups have an **opportunity to provide innovative products in this area**. To do so, however, they will need a **common level playing field** that obliges their global competitors to observe the European regulatory framework. It is vital to **step up** enforcement of governance sovereignty among suppliers who are not aligned with European regulations.

Digital Sovereignty issues can still arise with **open-source software** – some open-source software and communities are dependent on commercial providers, and not all open-source developments are always available as digital commons.

TensorFlow, for example, is a software library developed by **Google** that is very popular among **AI developers**. It provides a means of tying the developer community more closely to Google and its ecosystem and offers the company early insights into the latest trends and areas of application. Consequently, as well as the promotion of open-source software and platforms, building knowledge about open-source development and licensing models and about how open-source communities operate is also key to achieving Digital Sovereignty.

Other factors that play an important role in determining the degree of Digital Sovereignty and the range of strategic alternatives in the open-source sector include the **geographical distribution of developer communities**, **reliance on proprietary operating systems** (especially for smartphones, as well as the associated ecosystems and business models) and on software components, and norms and standards. Moreover, the use of open source soft-

ware is governed by various legal conditions for the protection of **intellectual property rights (IPR)**.

Summary

Fundamentally, the **need for action** at this level is connected to the existence of significant **dependencies** on US providers of **OS and Office products**, which can be leveraged in a targeted manner to create new dependencies on the cloud services of the providers in question. Government must play a central role in reducing these dependencies.

While **open-source software has the strategic potential to strengthen Digital Sovereignty** and foster innovation, it is **not** a panacea that **guarantees success**.

Targeted, strategic procurement policies can strengthen the existing open-source community and support the **development of usable digital commons**. The public sector and its service providers can promote strategic independence from individual companies by supporting the global open-source community through their community work. **A common** public sector **security framework** can encourage the use and reusability of open-source solutions and facilitate their sharing among public authorities. It is recommended that any initiatives and funding in this area should be based on a comprehensive **analysis of the formal and informal structures** of the relevant open-source ecosystems.

7 European system of laws and values

Cybersecurity, cryptography, **e-identity**, EU certification (consumer protection) and standards

Regulatory sandbox: cybersecurity centre
Institution: BSI + network of cyberregions in Germany

What is included in this level?

At this level, the key question as far as Digital Sovereignty is concerned is whether **fundamental European convictions** and values can be translated into **concrete standards for the European Single Market** that must be observed by all **companies, services and products** (value by design), regardless of whether they are European, American or Asian.

The successful **implementation of value by design** can generate innovative products and services that provide a **competitive advantage** and thus drive economic growth. A flourishing digital economy promotes both stability and sovereignty.

In an increasingly digitalised world ("everything is connected"), cyberattacks will also become more common ("everything is hacked"). The importance of **being able to defend against cyberattacks** cannot be overstated – ultimately, such attacks can affect every level of the layer model. Moreover, autocratic regimes are increasingly launching **attacks** specifically **targeted at European values** and the upholding of the **economic and legal order** that they underpin.

As far as the technology dimension that provides the focus of this paper is concerned, it is essential to ensure **sovereign control** over the **key cybersecurity technologies** and the **technological and organisational infrastructure for their deployment**.

Focus on cybersecurity – the status quo

While **Germany and Europe** have no shortage of the relevant cybersecurity technologies or actors with the necessary expertise, what is **missing** is **effective European coordination of the existing resources**.

Europe, and in particular **Germany**, are **strongly** positioned in the field of **cybersecurity technology R&D**. This includes everything from **cryptography research** to **FinTech start-ups** such as Fraugster and Risk.Ident, who develop AI-based, scalable software solutions that protect individuals and organisations against identity theft and account takeover and forgery.

A number of organisations with responsibility for this area already exist. Germany has established and expanded the **Federal Office for Information Security (BSI)**, a government agency responsible for preventing, detecting and **responding to** cyberattacks. The Allianz für Cyber-Sicherheit (Alliance for Cybersecurity) is working to strengthen Germany's overall resilience to cyberattacks. Meanwhile, the **Bundesdruckerei (BDr)** Group is a leading and highly innovative state-owned actor engaged in the technical development of **security solutions** and the associated infrastructure.

Industry is also mindful of the importance of cybersecurity. Bodies such as the Plattform Industrie 4.0 working groups on the "Security of Networked Systems" and the "Legal Framework" are working on ways of **preventing a rise in digital vulnerabilities** due to greater connectivity in **industrial production**. There are **now various trusted initiatives** such as the DCSO (Deutsche Cyber-Sicherheitsorganisation) that rapidly disseminate information about attack vectors.

In principle, Europe already **possesses the technical expertise** required for the **security assessment** and certification of complex systems, especially those made by **foreign companies**. However, attempts to do so **often fail** because the necessary documents are not disclosed or because full access to the relevant systems is withheld. It is up to **policymakers** to address this **challenge**.

Proposals

Harmonisation of the heterogeneous cybersecurity landscape in Germany and Europe must be driven by policymakers. Important steps in this direction have already been taken in the shape of the EU **Cybersecurity Act** (which, among other things, introduces new guidelines and a harmonised cybersecurity certification framework for information and communication technology), the Directive on security of network and information systems (**NIS Directive**) and the **European strategy for data**.

Closer cooperation between EU member state government agencies and the **European Union Agency for Cybersecurity (ENISA)** should also be institutionalised.

Joint initiatives should be undertaken to **continue the development of cybersecurity solutions and ensure their widespread implementation**, especially in the three following areas:

- **Encryption technologies**: The number one priority is ongoing research – through and within the EU –into **cryptographic principles**, the development of **strong encryption techniques**

including post-quantum cryptography, and the promotion of their widespread **deployment**, e. g. through certification and through mandatory minimum standards in critical areas. In addition, the remaining gaps in certification (especially for components) should be closed.

Digital Sovereignty can only be achieved in this area by building up **extensive expertise within Europe** rather than relying on an external provider. It is vital to ensure the availability of state-of-the-art techniques at all times, even if, for political reasons, certain strong encryption techniques are not ultimately used in commercial products.

- **An institutionalised cyber defence capability**: **SMEs** in particular often lack the means to implement state-of-the-art cybersecurity measures of their own, **relying** instead on **awareness-raising**, the **dissemination of information**, and **rapid external assistance** in the event of a crisis.
  It is thus necessary both to expand the relevant **government advisory services** and to recognise **private sector cyber defence centres** or partner organisations as important components of the **cybersecurity ecosystem** that can bring together the relevant experience and help to counter attacks cost-effectively by enabling cost synergies and pooling information. This will call for a **clear division of labour** between the **public and private sector actors**, to ensure that they do not end up competing with each other (which would pose a threat to the private actors' business models) and to prevent gaps in the monitoring and effective combating of threats.
- **E-Identity**: **Forgery-proof digital identities** are key to enabling trusted data exchange and secure activity in digital spaces.
  It is vital to ensure that personal IDs are developed in a user-centric manner and **are easy for members of the public to use**. As yet, no European solution has become established in the market. If existing European identity providers such as the Bundesdruckerei came together to develop a European e-ID solution, this could help to enable user-friendly digital services and, with the right design, even allow **full control over the data**.
  As well as people, **machines must also be clearly identifiable** if they are to fulfil their full potential in the context of Industrie 4.0 and the IoT. The relevant solutions must therefore be developed as a matter of urgency.
  All of this only makes sense as part of an **interoperable European ID ecosystem. Without this, it will be impossible to achieve the critical international mass** needed to establish globally relevant standards based on European values that manufacturers will be willing to follow. This approach could build on the existing European **eIDAS** (electronic IDentification, Authentication and Trust Services) **ecosystem** of sovereign digital identities.
  Consequently, the joint initiative of the German government and the private sector to establish a digital identities ecosystem is to be welcomed as an urgently necessary measure. However, the initiative will only succeed if it wins the backing of the **European Commission** and a **critical mass of member states**.

Summary

In order to achieve **Digital Sovereignty** in the field of **cybersecurity**, it is necessary to have control over the full spectrum of different elements, from basic research to implementation. Europe currently has this control, and must maintain it going forward. This technological basis is key to ensuring sovereign activity in the digital sphere – **based on European values** – for both the economy and European society as a whole. This issue must be addressed **through the European Single Market** in order to provide the critical international mass needed to successfully establish the relevant standards.

References

Buchenau et al. 2021
Buchenau, M./Koch, M./Tyborskim R.: *Wirtschaft und Wissenschaft fordern Quantencomputer binnen fünf Jahren*, 2021. URL: https://www.handelsblatt.com/technik/it-internet/druck-auf-bundesregierung-wirtschaft-und-wissenschaft-fordern-quantencomputer-binnen-fuenf-jahren/26796470.html [retrieved:19.02.2021].

DRM 2021
Datenraum Mobilität: *Dezentral vernetzter Datenraum Mobilität* [unpublished manuscript], 2021.

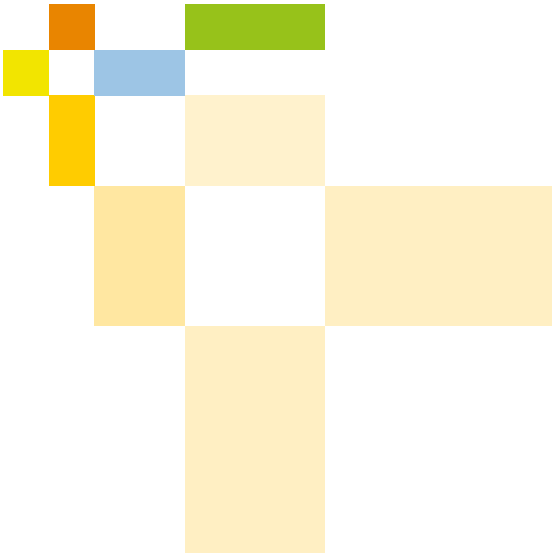
Federal Chancellery 2021
Federal Chancellery: *Datenstrategie der Bundesregierung. Eine Innovationsstrategie für gesellschaftlichen Fortschritt und nachhaltiges Wachstum*, Berlin 2021.

Federal Ministry for Economic Affairs and Energy 2020
Federal Ministry for Economic Affairs and Energy: *Eckpunkte zur Umsetzung des Konjunkturpakets Ziffer 35c. Zukunftsinvestitionen Fahrzeughersteller und Zulieferindustrie sowie Forschung und Entwicklung*, Berlin 2020.

Kagermann et al. 2020
Kagermann, H./Süssenguth, F./Körner, J./Liepold, A.: *The Innovation Potential of Second-generation Quantum Technologies* (acatech IMPULSE), München 2020.

SAP 2021
SAP: *Gardener – an Open, Coherent and Extensible Standard* [unpublished manuscript], 2021.

Telefonica 2020
Telefónica Deutschland: *Die Vorteile der Open-RAN-Architektur*, 2020. URL: https://www.basecamp.digital/mobilfunk-fuer-dummies-die-vorteile-der-open-ran-architektur/ [retrieved: 19.02.2021].



About acatech – National Academy of Science and Engineering

acatech advises policymakers and the general public, supports policy measures to drive innovation, and represents the interests of the technological sciences internationally. In accordance with its mandate from Germany's federal government and states, the Academy provides independent, science-based advice that is in the public interest. acatech explains the opportunities and risks of technological developments and helps to ensure that ideas become innovations – innovations that lead to greater prosperity, welfare, and quality of life. acatech brings science and industry together. The Academy's Members are prominent scientists from the fields of engineering, the natural sciences and medicine, as well as the humanities and social sciences. The Senate is made up of leading figures from major science organisations and from technology companies and associations. In addition to its headquarters at the acatech FORUM in Munich, the Academy also has offices in Berlin and Brussels.

Authors:

Prof. Dr. Henning Kagermann
acatech – National Academy of Science and Engineering
Karolinenplatz 4
80333 München

Karl-Heinz Streibich
acatech – National Academy of Science and Engineering
Pariser Platz 4a
10117 Berlin

Dr. Katrin Suder
TAE Advisory & Sparring GmbH
Eppendorfer Landstraße 46
20249 Hamburg

Series editor:

acatech – National Academy of Science and Engineering, 2021

Secretariat
Karolinenplatz 4
80333 München
T +49 (0)89/52 03 09-0
F +49 (0)89/52 03 09-900

Berlin Office
Pariser Platz 4a
10117 Berlin
T +49 (0)30/2 06 30 96-0
F +49 (0)30/2 06 30 96-11

Brussels Office
Rue d'Egmont/Egmontstraat 13
1000 Brüssel (Belgien)
T +32 (0)2/2 13 81-80
F +32 (0)2/2 13 81-89

info@acatech.de
www.acatech.de

Recommended citation:
Kagermann, H./ Streibich, K.-H./Suder, K.: *Digital Sovereignty Status Quo and Perspectives* (acatech IMPULSE), Munich 2021.

Bibliographical information published by the Deutsche Nationalbibliothek.
The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie;
detailed bibliographical data is available online at http://dnb.d-nb.de.

Coordinated and edited by: Florian Süssenguth, Dr. Johannes Winter
Translation: Joaquin Blasco
Layout concept, conversion and typesetting: GROOTHUIS. Gesellschaft der Ideen und Passionen mbH
für Kommunikation und Medien, Marketing und Gestaltung; groothuis.de
Cover photo: © shutterstock/Vladimir Vihrev

The original version of this publication is available at www.acatech.de

Digital Sovereignty is a key strategic policy issue. The importance of sovereignty in the use of digital platforms and applications grows with each new area of private, economic and public life that they are used in. Digital Sovereignty is not just a question of competitiveness, but also of the political autonomy of the European Union and its member states, the innovativeness of businesses, and the freedom of research institutions and all Europeans in the digital world.

This acatech IMPULSE publication presents a layer model that aims to contribute to the formulation of a concrete definition of Digital Sovereignty and above all to the development of concrete policy options for the different technology levels that build on each other to make up the model.