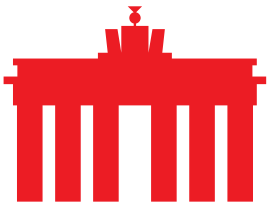

WE ARE SHAPING THE INTERNET.
YESTERDAY.TODAY.BEYOND TOMORROW.

eco

INFORMATION PAPER

Digital Sovereignty – Phenomenology and Operationalisation in the Internet Industry

Berlin, 15.11.2025

The term "digital sovereignty" has been present in political debate for quite some time and serves as a projection surface for numerous – and in some cases divergent – approaches and perspectives on the topic. Over the years, its meaning has repeatedly shifted. Initially, the term was primarily intended to reflect competence and capability in dealing with IT systems. The German study "Future Paths for Digital Germany 2020", commissioned by the IT Planning Council in 2013, still described digital sovereignty as the ability:

> *"to be able to meaningfully use ICT and digital media in searching for, evaluating and using data and information on the Internet, to be able to handle one's own data competently, to recognise and exploit the opportunities and advantages of digitalisation, but also to be aware of the potential dangers in using the Internet – both in terms of technical and organisational handling."*
>
> (IT Planning Council, 2013, 34)

Over time, this definition has been increasingly expanded. Already within the framework of the National IT Summit 2015, the term shifted in the German publication "Guidelines for Digital Sovereignty". Here, digital sovereignty is described as:

> *"the ability to act and make decisions independently in the digital space."*
>
> (German Federal Ministry for Economic Affairs and Energy (BMWi) – Focus Group 1, 2015, 1)

This description has gained increasing importance against the background of ever-deepening European regulation in the digital sector, both technically (NIS, NIS2), legally (GDPR) and, not least, competitively (DSA, DMA). At the same time, the complexity and scope of the topic of digital sovereignty have increased. A more detailed description by the German Academy of Science and Engineering – acatech – highlights this. Acatech defines it as follows:

> *"Digital sovereignty refers to the ability of individuals, companies and policymakers to freely decide how and according to which priorities the digital transformation should be shaped."*
>
> (acatech 2021, 8)

Behind this, acatech has developed a multi-layered model of fields of action and aspects that must be considered in this context, including the question of where the raw materials for components can be sourced. This model represents the depth and diversity of the subject matter in a contemporary and appropriate manner. At the same time, this model provides the Internet industry with key aspects that are necessary for the further operationalisation and application of this complex topic. This is also necessary to take into account the fact that sovereignty in individual fields of action can sometimes conflict with objectives in other fields of action – for example, in the case of data transfer to third countries.

eco identifies the following four dimensions of digital sovereignty, which were developed as particularly relevant within the framework of the Digital Workshop on 11 September 2025.

- Clarifying legal issues
- Clarifying handling of data
- Understanding technology design
- Tracking supply chains

These four dimensions are based on key questions that are relevant for determining digital sovereignty for the economy. Not all companies make the same decisions in all areas. This depends on priorities in a company's activities, the services and products offered, and strategic decisions at the company level.

Digital sovereignty means that companies can freely choose their respective providers and the underlying business model according to their needs and use cases. Open standards and interoperable solutions support this sovereignty, align with the dynamics of such business relationships, and can help reduce lock-in effects.

The following aspects arise for the four dimensions:

- **Clarifying legal issues**

The assessment of possible legal issues begins with the question of which legal system exists in which jurisdiction and how stable it is. The recent past in particular has shown that the rule of law is under pressure worldwide. And in authoritarian states, even established law is subject to reservations. When clarifying legal issues, companies should ensure that they are not substantially restricted in their business activities by written or practiced law and that they have the opportunity to enforce claims and fulfil contracts appropriately. This applies not only to the companies themselves, but also to the services and products offered.

In this context, it should also be discussed which actors (governments, public authorities, organisations) can intervene in services or products under which framework conditions – for example, through security laws, but also through consumer protection laws – and what effects this has. This should be done not only from the perspective of the technical implications of such interventions, but also with a view to the loss of trust among customers and clients.

Companies should also consider the strategic priorities that are directly relevant to them and their business model when evaluating existing or stipulating licensing arrangements. Only in this way can dependencies through imposed obligations – whether prescribed by law or agreed under private law – be avoided.

- **Clarifying handling of data**

The handling of data is often at the centre of many digital policy discussions, including digital sovereignty. Here, it is important to understand that the question of which data should be stored where and how is closely linked to the question of who can ultimately gain access to the relevant data. Not only should access to personal data be examined, but the handling of non-personal data should also be considered. The leakage of production data or specifications can lead to significant competitive disadvantages. Therefore, if necessary, questions regarding data localisation should be included in the considerations. Rules on the local storage of certain data must be taken into account when selecting a service, as must access to data by local public authorities or organisations.

This consideration goes beyond purely data protection issues. Laws regulating public safety and the work of security services and intelligence services must also be considered in this context – for example, for the purposes of law enforcement, as in the European e-Evidence Package or the US Cloud Act. In this context, it is also useful to examine exactly how data processing takes place: whether it is processed directly by a customer or whether the customer forwards it to other contractors within the framework of commissioned data processing or other business models. Access by external service providers to one's own data – whether personal or not – is also relevant in this context.

Finally, there is also the question of redundancy in maintaining data. Here, a conflict of objectives could arise between data minimisation principles on the one hand and redundancy aspects on the other, which must be carefully weighed up on a case-by-case basis.

- **Understanding technology design**

Technology is at the heart of the debate on digital sovereignty. While legal control focuses particularly on contractual or statutory aspects, technological control addresses pragmatic, application-oriented questions. Here, companies should examine more closely what possible alternatives they have for using a technology – and how exactly they want to use a technology (maintenance by their own staff or by the staff of a contractual partner).

Companies should also be able to answer the strategic question of whether they want the capability not only to use deployed technologies they employ, but also to (further) develop them if necessary. The possibility of switching to alternative technologies or using alternative products can only be managed with significantly higher transaction costs in the case of technical lock-ins. Here, too, companies must make sensible trade-off decisions.

Particularly in the area of disruptive cross-sectional technologies such as artificial intelligence, there are currently no European or national products on the market. This raises the question of how they can make sensible use of the technology in the market, or whether they want to impose restrictions on themselves in terms of use and accept the corresponding competitive disadvantage.

- **Tracking supply chains**

The availability of software and components is relevant in various respects. On the one hand, it is necessary to be able to continuously offer a service or product. On the other hand, a better understanding of the question of where components or software code come from is also relevant for identifying or closing vulnerabilities or security gaps.

In this context, aspects such as the origin of components, their availability – also in a temporal context – and their possible functionality become relevant. Finally, companies should also discuss how access to the corresponding components and software code is designed. Here, measures can be taken either through licences (open source) or through appropriate procedures (key escrow) that still allow access to the software even if it is otherwise no longer available.

- **Summary**

In the overall view, digital sovereignty does not present a monolithic picture. Rather, companies must decide on a case-by-case basis, which aspects they prioritise and what effects this will have. Not all providers and users in the market operate under the same assumptions. For example, a German local authority will prioritise data localisation more highly than an internationally active corporation that depends on cross-border data exchange.

It is therefore problematic to make concrete legal requirements for all possible application and usage scenarios. The currently discussed amendment to Section 128 of the German Act against Restraints of Competition (GWB) – which includes “considerations of digital sovereignty” in public tenders and would need to be further specified and explained on a case-by-case basis – is, in the view of the Internet industry, a sensible approach to addressing the question of how to deal pragmatically with digital sovereignty.

At the same time, it is important to take a closer look at the general factors in the market that are required for the selection of providers. A harmonised European digital single market offers better opportunities for scaling business models and is central to promoting European digital sovereignty. In this context, it is important to critically review existing regulation in terms of its necessity and to limit spillover effects as strictly as possible. General economic framework conditions should also be considered to support, for example, the development of an ecosystem of digital infrastructures with redundant data centre capacities.