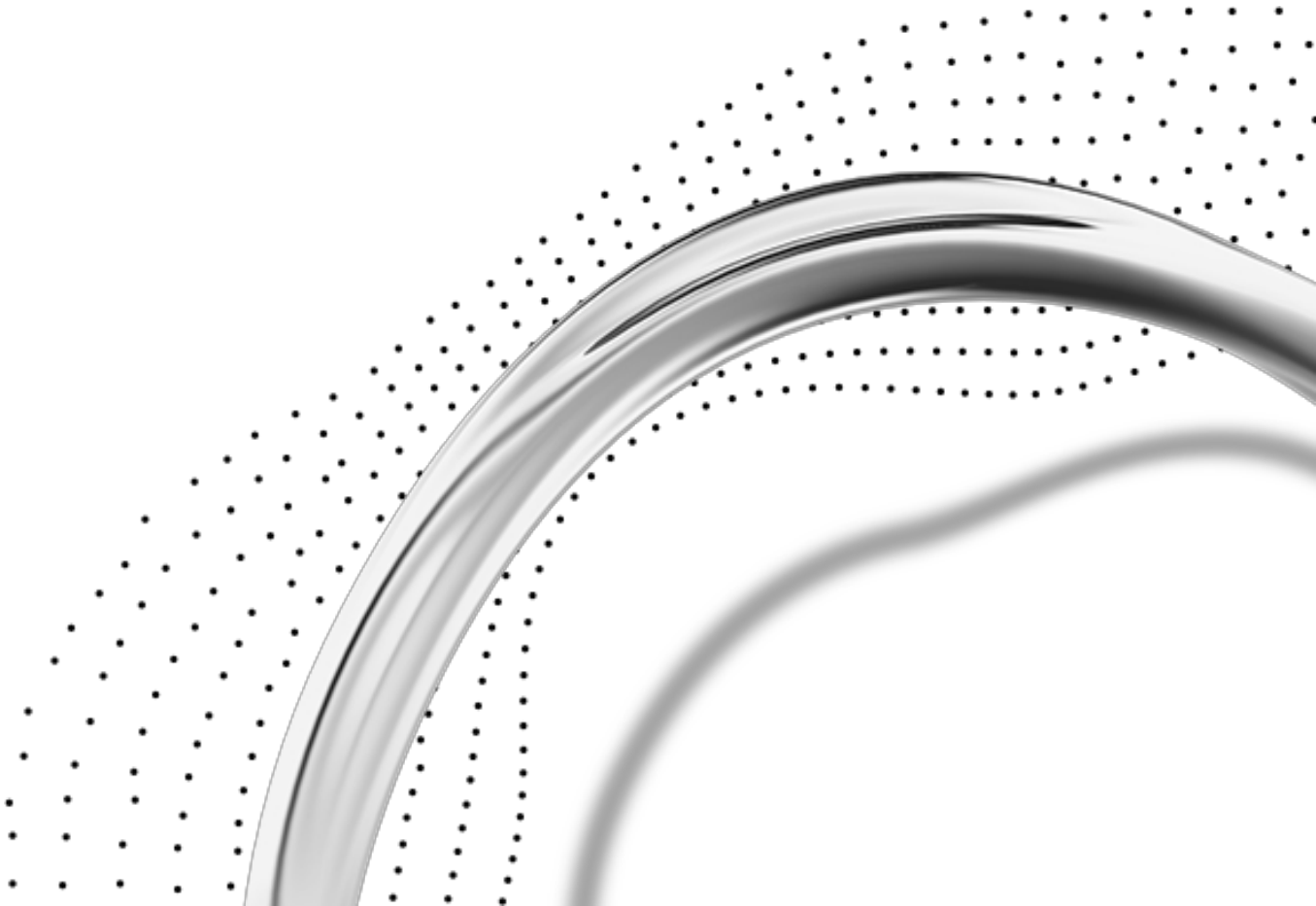
Discussion paper

Criteria for assessing digital sovereignty

— What can be measured can be achieved



Contents

	Executive Summary	3
1.	**Digital sovereignty is crucial**	4
2.	**Making digital sovereignty measurable – what is measurable becomes achievable**	6
3.	**From principles to parameters: Catalogue of criteria**	9
4.	**A risk-based application of the criteria**	14
5.	**Sovereignty check**	15
	Appendix: Criteria for measuring digital sovereignty	17

Executive Summary

The availability of digital services and technologies is vital for public administration. This availability can be restricted by external factors, such as political influence or technological dependencies. It is the responsibility of public administration to ensure the stable and secure operation of its information technology (IT).

Based on this necessity, the 'Digital Sovereignty of Public Administration' was defined as a guiding principle by the IT Planning Council (IT-PLR) and fleshed out through strategic objectives[1].

These objectives can be translated into a catalogue of specific assessment criteria that enable a systematic sovereignty check of IT solutions and infrastructures, extending to entire public authorities (processes, structures, etc.).

The catalogue of criteria proposed here is based on the strategic objectives of the IT-PLR and will be further developed in collaboration with openCode as part of an open consultation process until mid-May 2026.

Take partin the consultation process with openCodedirectly:

www.souveränitätscheck.de

1. Federal Ministry of the Interior, Building and Community (BMI). (January 2021). Resolution 2021/09: Strategy for Strengthening Digital Sovereignty in Public Administration IT. Berlin. IT Planning Council. https://www.it-planungsrat.de/fileadmin/beschluesse/2021/Beschluss2021-09_Strategie_zur_Staerkung_der_digitalen_Souveraenitaet.pdf , last accessed on 19 March 2026.

1. Digital sovereignty is crucial

"Digital sovereignty" refers to the ability of organisations – as well as individuals and states – to exercise their roles in the digital world independently, autonomously and securely.[2] Decisions and actions should always be designed and implemented in a manner that is legally compliant, secure, sustainable and economically viable.

This includes the conscious management of dependencies and ensuring the reversibility (ability to exit) of essential digital components.[3] The digital sovereignty of public administration is therefore not a technical niche issue, but a prerequisite for the rule of law, public services and democratic resilience in the 21st century.

However, control over the public digital infrastructure does not currently lie with the public sector. This jeopardises its ability to act in the long term and is already restricting it: a 2020 survey by the Municipal Joint Office for Administrative Management (KGSt) revealed that 87 per cent of the municipalities surveyed consider themselves to be wholly or partly dependent on individual software and cloud providers.[4]

In the 'tech stack'[5] of German federal authorities and public sector IT service providers, one finds almost everywhere the same applications from a handful of – mostly US – providers. This applies to all layers of the stack, but particularly to office software, workstation and server operating systems. According to a 2019 market analysis, 96 per cent of all direct federal authorities in these areas use software from just one provider.[6]

2. "Strengthening the Digital Sovereignty of Public Administration; Key Points – Objectives and Areas of Action" (Resolution at the 31st meeting of the IT-PLR, Decision 2020/07, and Resolution of the IT Council No. 2020/01).
3. Goldacker, G. (2017). Digital Sovereignty – What exactly is digital sovereignty? Fraunhofer Institute FOKUS, Competence Centre for Public IT (ÖFIT). https://publica.fraunhofer.de/entities/publication/8a0846aa-ec67-4788-8f0b-4bb540d97162, last accessed on 19 March 2026; Mohabbat Kar, R., and Thapa, B. E. P. (2020). Digital Sovereignty as Strategic Autonomy – Managing Dependencies in the Digital State (White Paper); Fraunhofer Institute FOKUS, Competence Centre for Public IT (ÖFIT). https://publica.fraunhofer.de/entities/publication/67656462-b94f-499b-ad44-b2cc1834dec3, last accessed on 19 March 2026.
4. Municipal Joint Office for Administrative Management (KGSt). (May 2020). Open Source in Local Authorities: Results of a Survey (KGSt Food for Thought). Cologne. https://www.kgst.de/documents/20181/34177/2020_Denkanstoss_Open+Source+in+Kommunen_Umfrage.pdf/22fd4755-0418-9f98-b69d-5cd3b845a477, last accessed on 19 March 2026.
5. A combination of technological components used to create IT applications and infrastructures.
6. PwC Strategy& (Germany) GmbH. (2019). Strategic market analysis on reducing dependencies on individual software providers: A study commissioned by the Federal Ministry of the Interior, Building and Community. Berlin. https://wibe.de/wp-content/uploads/20190919_strategische_marktanalyse-compressed.pdf, last accessed on 19 March 2026.

The IT landscape of public administration is a monoculture – and that harbours risks: [7]

+ Uncertainties regarding data protection
due to extraterritorial legal access to data

+ Limited information security
due to a lack of control over code and data

+ Inflexibility
due to a lack of switching options and technological lock-in

+ Uncontrollable costs
due to rising licence fees for cloud-based SaaS models

+ Externally driven innovation
due to dependence on proprietary development cycles[8] of global providers

These risks are exacerbated by current technical and geopolitical developments: the trend towards subscription-based, cloud-based Software-as-a-Service solutions offers less control over code and data and is accompanied by rising licence costs.[9] Added to this is a new element of unpredictability in transatlantic relations: the possibility of the US government deliberately influencing European public IT infrastructure can no longer be ruled out. The debate surrounding the blocked email account of Karim Khan, Chief Prosecutor of the International Criminal Court, highlighted this risk in May 2025.[10]

7. Ibid.
8. Proprietary development cycles here refer to development cycles controlled by a technology provider without any influence from users or customers.
9. Kirlidokme, B. (2025, 21 February). German government spends over a billion on software – US tech giants benefit. Frankfurter Rundschau. https://www.fr.de/wirtschaft/bundesregierung-gibt-mehr-als-eine-milliarde-fuer-software-aus-93586564.html, last accessed on 19 March 2026.
10. Laaff, M. (2025, 23 July). This email cannot be delivered: What if Donald Trump forces Big Tech to shut down its services in Europe? For a long time, this was just a theory. Then an important email address at the Criminal Court stopped working. Die Zeit. https://www.zeit.de/digital/internet/2025-07/microsoft-email-sperre-karim-khan-donald-trump-istgh , last accessed on 19 March 2026.

2. Making digital sovereignty measurable - from measurable to ly feasible

The political and public discourse on digital sovereignty is intensifying. International hyperscalers are also using the term to reassure their customers that there are no concerns regarding their sovereignty – such as IT security and data protection – in the public cloud. Server locations in the EU, air-gapped or confidential clouds are said to guarantee digital sovereignty. However, it is often overlooked that the jurisdiction of foreign companies in principle allows access to IT infrastructure even within the EU. Digital sovereignty risks becoming a mere marketing term.

At the same time, there is no robust basis for assessing how digitally sovereign public administration is today. The European Union's (EU) Cloud Sovereignty Framework provides the first criteria for evaluating cloud offerings. On this basis, the Federal Office for Information Security (BSI) is now developing general sovereignty criteria for cloud solutions. However, there are no reliable criteria for the digital sovereignty of public transport as a whole.[11] The digital sovereignty of public transport cannot currently be validly assessed, compared or managed.

Therefore, clearly defined criteria are needed against which digital sovereignty can be measured. This is not just a matter of the (in)dependence of individual software solutions, but of the capacity of public institutions to act as a whole – including their entire IT infrastructure and the digital services built upon it. Only in this way can sovereignty be made measurable and achievable for the administration, because: "You can't manage what you can't measure."

enables measurability:

- Identification of critical dependencies
- Strategic investment management
- Demonstration of robust IT in terms of compliance, security and resilience
- Comparability between public authorities
- In the long term, a presentation of the development of digital sovereignty in public transport

11. European Commission. (October 2025). Cloud Sovereignty Framework (Version 1.2.1). Luxembourg: European Commission. https://commission.europa.eu/document/download/09579818-64a6-4dd5-9577-446ab6219113_en?filename=Cloud-Sovereignty-Framework.pdf, last accessed on 19 March 2026.

Examples of existing dependencies

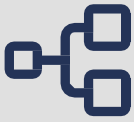
Example: Cloud

The issue of digital sovereignty in cloud services has been politically relevant for years. In 2019, the Sovereign Cloud Stack (SCS)[12]project was launched as part of Gaia-X, initially funded by the Federal Agency for Leapfrog Innovations (SPRIND) and, until the end of 2024, by the Federal Ministry for Economic Affairs and Energy (BMWE). The aim was to use open standards and interfaces to achieve the greatest possible independence from proprietary technologies and products in cloud operations.

In 2020, the Federal IT Commission (FITKO) and the Federal Ministry of the Interior (BMI) established the ability to switch between providers as a key criterion in the strategy for the German Administrative Cloud. In 2023, the Data Protection Conference (DSK) published a position paper[13]setting out requirements for sovereign cloud usage: full control over data, transparent technical processes, and the option to switch providers or operate the system in-house. Without these conditions, the DSK does not consider cloud solutions to be legally compliant.

12. See also: https://gaia-x.eu/ and https://scs.community/de/
13. See https://www.datenschutzkonferenz-online.de/media/weitere_dokumente/2023-05-11_DSK-Positionspapier_Kritierien-Souv-Clouds.pdf , last accessed on 19 March 2026.

Examples of existing dependencies



Example: AI

With services based on artificial intelligence (AI), it is difficult to understand how the models used were trained and how their results are produced. Whilst Open Weight Models (OWM) disclose the model parameters, they rarely reveal the training data used. The widely used Closed Source Models (CSM), on the other hand, operate as a complete 'black box'.

Furthermore, providers of CSM often use user queries (prompts, uploaded files, user feedback and interactions) to retrain their models and further develop their services
– to this end, these queries are often stored by the providers and used for subsequent queries. This can result in the content of these previous queries being made accessible to other users, thereby failing to ensure adequate data security.

The strengthening of sovereign AI technologies in Germany and Europe was identified as a core strategic objective at the German Conference of Minister Presidents (MPK).[14] The development of sovereign AI applications requires modular software architectures with standardised interfaces, an operating infrastructure that is as independent as possible, and the responsible handling of user data.

Open-source AI, in particular OWM, offers the opportunity here to reduce dependencies and ensure complete control over data and applications. However, it requires an active community, professional governance and appropriate operational expertise to ensure the long-term maintainability and further development of applications.

14. Conference of Heads of Government of the German Federal States. (March 2025). Resolution Item 2: Securing technological sovereignty – strengthening AI hubs in Europe and Germany. Berlin. https://www.ministerpraesident.sachsen.de/ministerpraesident/07_TOP2_Beschluss_MPK_RS.pdf, last accessed on 19 March 2026.

3. From principles to parameters: Criteria catalogue

Following the analysis of the public sector's 'tech stack' in 2019, the IT-PLR developed a strategy to sustainably safeguard the administration's capacity to act. The core of the strategy is the strengthening of digital sovereignty in three dimensions: freedom of choice, design capability and influence.[15]

The public administration should be able to select IT solutions, components and providers flexibly and switch between them as required at a reasonable cost. It should also be able to help shape its IT, which requires both the relevant specialist expertise and suitable cooperation structures on the one hand, and adaptable, open technologies on the other. Furthermore, public administration must be able to effectively represent its requirements to technology providers, for example when it comes to contractual terms, security standards or operation within its own data centre.

Based on these strategic objectives for digital sovereignty, specific criteria can be derived to systematically assess the digital sovereignty of public authorities and organisations.

15. Federal Ministry of the Interior, Building and Community (BMI). (January 2021). Resolution 2021/09: Strategy to strengthen digital sovereignty for public administration IT. Berlin. IT Planning Council. https://www.it-planungsrat.de/fileadmin/beschluesse/2021/Beschluss2021-09_Strategie_zur_Staerkung_der_digitalen_Souveraenitaet.pdf , last accessed on 19 March 2026.

3. From Principles to Parameters: Criteria Catalogue

A. Organisation and Capabilities

This category focuses on an organisation's management and control capabilities with regard to risks and the fulfilment of requirements for digitally sovereign services. The assessment examines whether digital sovereignty is established as a strategic objective and whether the organisation possesses the necessary capabilities to influence technology providers and make sovereign decisions.

- Strategy (existence and effectiveness of a sovereignty-oriented digital strategy)
- IT Governance & Management
- Risk Management
- Procurement and contracting
- Client Capability
- Competencies as a prerequisite for influencing suppliers

This dimension addresses the key question:
Is the organisation even capable of actively managing digital sovereignty?

3. From principles to parameters: Criteria catalogue

B. Digital applications and services

This category assesses the design and interchangeability of the applications used, as well as Control over these applications. The key question is to what extent digital services are designed to be modular, transparent and interoperable, and whether their use ensures the ability to switch providers (exit capability). The following areas are examined:

- Transparency and documentation
- Traceability and security of the supply chain
- Application architecture and modularity
- Standards and interfaces
- Dependencies at the software level

The question here is:
Do the applications used enable technological self-determination – or do they lead to dependencies that restrict the ability to act?

3. From principles to parameters: Criteria catalogue

C. Information and data

This category examines the extent to which data sovereignty is guaranteed. The focus is on regulatory, technical and operational conditions that enable the sovereign handling of data. Areas considered are:

- Data location
- Data security
- Data protection
- Data structures

The assessment examines whether
public authorities can exercise full control over their data at all times – including access, storage, processing, deletion and migration.

3. From principles to parameters: Criteria catalogue

D. Operations and Infrastructure

This category assesses technical and organisational operational sovereignty. The focus
These include operational independence, resilience to external influences, and the ability to switch providers. The following are considered:

- Dependency at the operational or provider level
- Customer relationship
- Ability to exit
- Resilience and business continuity
- Security and compliance in operations

This dimension answers the question:
Can the administration operate its systems continuously, securely and independently, even in the event of external disruptions or geopolitical tensions?

4. A risk-based application of the criteria

Not every IT component entails the same risks. A risk-based assessment is therefore necessary to ensure digital sovereignty, cost-effectiveness and practical feasibility. The depth and priority of the assessment depend in particular on:[16]

Data criticality:
Requirements regarding the confidentiality, integrity and availability of the data processed by the IT infrastructure.

Security posture:
Technical and organisational protective measures, vulnerability exposure and the maturity level of security controls.

Legal risk:
Regulatory requirements that must be met, for example data protection, data transfers, sector-specific legislation or standards such as NIS2, CRA and the AI Act.

Administrative processes:
The nature, scope and criticality of the management processes that rely on the organisation's IT infrastructure.

Degree of dependency:
Dependence on individual suppliers and proprietary solutions, as well as the feasibility of data migration to avoid lock-in effects.

Supply chain reliability:
Stability and integrity of the supply chain, including compliance with legal requirements such as the Public Procurement Regulation or the Supply Chain Due Diligence Act.

16. Federal Ministry of the Interior and Homeland Affairs. (2024). Requirements for technology providers and solutions (Decision No. 2024/01).

5. Sovereignty check

The defined categories, criteria and risk aspects form the basis for a practical sovereignty check at the level of individual authorities with their respective IT infrastructure: Each criterion can be operationalised through assessment questions that enable digital sovereignty to be systematically evaluated. In addition, evidence and audit methods can be defined – such as documentation, guidelines, technical test reports or certifications. This enables authorities to identify which requirements are met and where action is needed to strengthen their digital sovereignty.

The sovereignty check is being developed – based on the proposed categories and criteria – in an open consultation process using the openCode platform of the Centre for Digital Sovereignty in Public Administration. The catalogue of criteria will be jointly discussed, reviewed and further developed until mid-May 2026. This will result in a practical, flexible tool for assessing digital sovereignty, which, thanks to the consultation, will also have broad support and create a sense of commitment.

Take partin the consultation process with openCodedirectly:

www.souveränitätscheck.de

Appendix

Criteria for measuring digital sovereignty

Strategic objectives

- **Design capability** = the ability to actively help shape IT infrastructure and digital services and adapt them as required
- **Freedom to switch** = the ability to select IT solutions, components and providers flexibly and to switch between them as required at a reasonable cost
- **Influence over IT providers** = the ability to effectively represent requirements to technology providers

Criteria for measuring digital sovereignty			
A	**Organisation and capabilities**		**Objective**
A1	**Strategy**	Is digital sovereignty embedded in the organisation's digital strategy and overarching guidelines?	● ◆
A2	**IT governance & Management**	Have responsibilities, processes and control structures been defined and implemented in IT operations?	● ◆
A3	**Risk Management**	Are technological, organisational and strategic risks identified and managed with regard to dependencies?	● ■ ◆
A4	**Procurement and Contract Award**	Are procurement processes designed in such a way that competition, transparency and alternatives are taken into account?	● ■ ◆
A5	**Contracting authority capability**	Is the organisation capable of managing IT projects independently and effectively monitoring suppliers?	● ◆
A6	**Competencies**	Does the organisation have the necessary (IT) expertise, specialist staff and knowledge base to act with confidence?	■ ◆ ●
B	**Digital applications and services**		**Objective**
B1	**Transparency/ Documentation**	Is there comprehensive documentation of applications in terms of functionality, interfaces and data structures, as well as the interaction of components within the system context with other applications or services, for the purposes of use, auditing, maintenance and commissioning?	● ■
B2	**Traceability and security of the supply chain**	Is the origin of hardware and software components of the Is the organisation – including production sites, countries involved, suppliers outside the EU and transparency across the entire supply chain – known and verifiable?	● ■
B3	**Application architecture /modularity**	Are applications portable, modular in design and decoupled?	● ■
B4	**Standards**	Do applications use open interfaces and established standards to ?	● ■
B5	**Dependency on software level**	To what extent do lock-in risks exist due to proprietary software or a lack of alternatives?	■ ◆

Criteria for measuring digital sovereignty			
C	**Data**		**Objective**
C1	**Data location**	Where is data stored and processed (locally, in the EU, in third countries) and how can this be monitored?	■ ◆
C2	**Data security**	Is data fully encrypted, and are there appropriate policies and technical and organisational measures in place to ensure end-to-end data security?	●
C3	**Data protection**	Are legal requirements (e.g. GDPR) complied with and secured through technical and organisational measures?	● ◆
C4	**Data structures**	Is data stored in open, interoperable formats, ensuring portability and reusability?	● ■
D	**Operation and infrastructure**		**Objective**
D1	**Dependency at the operator/provider level**	To what extent is there a dependency on individual operators, service providers or cloud providers, and can these be regulated under EU law?	■ ◆
D2	**Customer relationship**	Does the customer relationship allow for influence over software development and digital services, for example through transparent release planning and active requirements management?	● ◆
D3	**Exit capability**	Is it feasible to switch providers or return to in-house operation and proven?	■
D4	**Resilience & Business Continuity**	How robust are the systems against failures, crises or attacks, and how quickly can operations be resumed?	●
D5	**Security and compliance in operations**	Are regulatory and organisational (EU) requirements are consistently checked and complied with during ongoing operations?	● ◆

About ZenDiS

The Centre for Digital Sovereignty in Public Administration (ZenDiS) was established by the federal government in 2022. As a centre of expertise and services, ZenDiS supports public administration at federal, state and local levels in securing their long-term operational capacity in the digital sphere – primarily by eliminating critical dependencies on individual technology providers. To this end, ZenDiS is focusing in its initial phase on promoting the use of open-source software in public administration. ZenDiS is a limited liability company (GmbH) and is currently wholly owned by the federal government. The Federal Ministry for Digital Affairs and State Modernisation (BMDS) is responsible for managing the holding. ZenDiS is based in Bochum.

Publisher
Centre for Digital Sovereignty in Public Administration (ZenDiS) GmbH Suttner-Nobel-Allee 4 | 44803 Bochum

Contact
Lutz Niemeyer | Communications | lutz.niemeyer@zendis.de

Status
March 2026