



# Digitale Souveränität der Bundesverwaltung, W012 Version 1.0

Mantelweisung des Bereichs Digitale Transformation und IKT-Lenkung DTI

gestützt auf Artikel 40 der Verordnung vom 1. Mai 2025 über die digitalen Dienste und die digitale Transformation in der Bundesverwaltung (Digitalisierungsverordnung, DigiV),  
SR 172.019.1

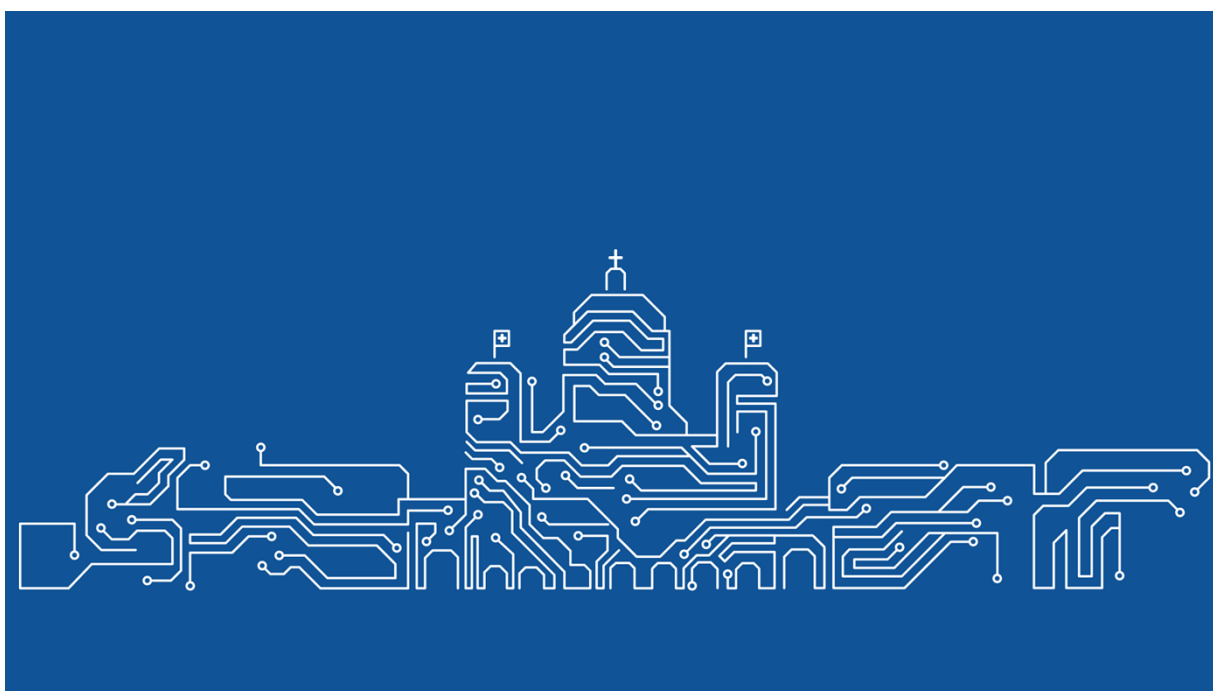


Abbildung 1 Erkennungsmotiv der Weisungen DTI

## **1 Kurzfassung**

### **1.1 Wen betrifft diese Weisung?**

Diese Mantelweisung gilt für die zentrale Bundesverwaltung.

### **1.2 Warum ist diese Weisung notwendig?**

Die Weisung soll sicherstellen, dass digitale Souveränität systematisch in allen relevanten Projekten geprüft und gestärkt wird. Ziel ist es, Handlungs- und Kontrollfähigkeit der Bundesverwaltung im digitalen Raum zu erhalten, Risiken frühzeitig zu erkennen und Spannungsfelder zwischen Zielsetzungen wie Kontrolle, Datenschutz oder Kosten effizient abzuwägen.

### **1.3 Was regelt diese Weisung auf welche Weise?**

Die Weisung legt Vorgaben zur digitalen Souveränität fest. Mit digitaler Souveränität ist die für die Erfüllung staatlicher Aufgaben im digitalen Raum erforderliche Kontroll- und Handlungsfähigkeit gemeint.

Zur Beurteilung und Wahrung der digitalen Souveränität nutzt die Weisung ein zweidimensionales Modell:

- Ebenenmodell: Identifiziert die technologischen Schichten, auf denen Massnahmen ansetzen (z. B. Software, Plattformdienste, IT-Infrastruktur, Kommunikationsinfrastruktur).
- Eckwerte: Formulieren Zielrichtungen und Leitgedanken, die bei der Umsetzung als inhaltliche Leitlinien dienen, wie Unabhängigkeit & Kontrolle, Kosten & Wirtschaftlichkeit, Datenschutz & Informationssicherheit, Resilienz, Kooperation & Standardisierung sowie Innovation & Zweckmässigkeit.

### **1.4 Was wird von den Betroffenen dieser Weisung erwartet?**

Die Thematik der digitalen Souveränität soll in Projekten und Vorhaben bereits von Beginn weg geprüft und nachvollziehbar dokumentiert werden.

Bei Vorhaben mit digitalen Souveränitätsrisiken oder strategisch bedeutenden Abhängigkeiten wird der Digitalisierungsrat Bund (DRB) informiert und kann das Thema im Rahmen einer Aussprache behandeln.

## **1.5 Inhaltsverzeichnis**

<b>1</b>	<b>Kurzfassung.....</b>	<b>2</b>
<b>1.1</b>	<b>Wen betrifft diese Weisung? .....</b>	<b>2</b>
<b>1.2</b>	<b>Warum ist diese Weisung notwendig?.....</b>	<b>2</b>
<b>1.3</b>	<b>Was regelt diese Weisung auf welche Weise? .....</b>	<b>2</b>
<b>1.4</b>	<b>Was wird von den Betroffenen dieser Weisung erwartet? .....</b>	<b>2</b>
<b>1.5</b>	<b>Inhaltsverzeichnis .....</b>	<b>3</b>
<b>2</b>	<b>Ausgangslage.....</b>	<b>4</b>
<b>2.1</b>	<b>Ebenenmodell.....</b>	<b>4</b>
<b>2.2</b>	<b>Eckwerte.....</b>	<b>6</b>
<b>2.3</b>	<b>Zusammenspiel der Dimensionen .....</b>	<b>7</b>
<b>2.4</b>	<b>Anwendungsbeispiel .....</b>	<b>8</b>
<b>3</b>	<b>Vorgaben.....</b>	<b>10</b>
<b>3.1</b>	<b>Integration in HERMES Projektmanagement.....</b>	<b>10</b>
<b>3.2</b>	<b>Verantwortung .....</b>	<b>10</b>
<b>3.3</b>	<b>Berichterstattung und Nachvollziehbarkeit .....</b>	<b>10</b>

## **Anhänge**

<b>A.</b>	<b>Allgemeine Informationen zum Dokument .....</b>	<b>11</b>
<b>B.</b>	<b>Aufhebung bisheriger Vorgaben .....</b>	<b>11</b>
<b>C.</b>	<b>Übergangs- und Schlussbestimmungen .....</b>	<b>11</b>
<b>D.</b>	<b>Änderungen gegenüber Vorversion / Angaben zur Erstausgabe.....</b>	<b>11</b>
<b>E.</b>	<b>Bedeutung der Schlüsselwörter zur Bestimmung des Verbindlichkeitsgrades ....</b>	<b>11</b>
<b>F.</b>	<b>Beilagen, Referenzen und weiterführende Informationen.....</b>	<b>12</b>
<b>G.</b>	<b>Glossar .....</b>	<b>12</b>
<b>H.</b>	<b>Metadaten für die Suchoptimierung im Web .....</b>	<b>12</b>

## 2 Ausgangslage

Diese Mantelweisung enthält Vorgaben zur digitalen Souveränität der Bundesverwaltung. Mit digitaler Souveränität ist die für die Erfüllung staatlicher Aufgaben im digitalen Raum erforderliche Kontroll- und Handlungsfähigkeit gemeint.

Will die Bundesverwaltung digitale Mittel für die Erfüllung staatlicher Aufgaben nutzen, muss sie prüfen, welchen Grad an Kontroll- und Handlungsfähigkeit sie bezüglich dieser Mittel haben soll. Dabei gilt, je unmittelbarer die Erfüllung einer staatlichen Aufgabe von einer digitalen Ressource abhängt, desto höher sind die Anforderung an die digitale Souveränität.

In der Folge muss geklärt werden, in welchen Bereichen und auf welche Weise die Bundesverwaltung ihre digitale Souveränität wahren oder stärken kann. Hierzu orientiert sich die Bundesverwaltung an einem zweidimensionalen Ansatz:

- Ein **Ebenenmodell** zeigt auf, wo Massnahmen zur Stärkung der digitalen Souveränität ansetzen.
- Strategische **Eckwerte** formulieren Zielrichtungen und Leitgedanken.

Die beiden Dimensionen bilden ein Analyse- und Steuerungsmodell, mit dem die digitale Souveränität systematisch beurteilt und gewahrt werden kann.

### 2.1 Ebenenmodell

Die technologischen Schichtenstruktur bildet eine Dimension der digitalen Souveränität. Sie beschreibt, auf welchen technologischen Ebenen Souveränitätsaspekte zu betrachten sind. Die Ebenen basieren auf einer Studie der deutschen Akademie der Technikwissenschaften (acatech) «Digitale Souveränität – Status quo und Handlungsfelder».

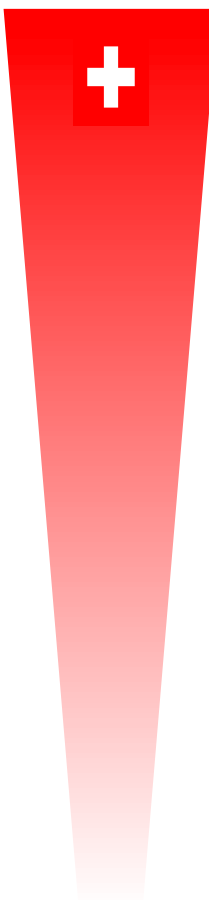
Ebene	Beschreibung	Handlungsspielraum
8. Rechts- und Wertesystem	<i>Rechtliche, ethische und sicherheitsbezogene Rahmenbedingungen (Beispiele: Handelsabkommen, E-Identity, Standards).</i>	
7. Softwaretechnologien und Softwaredienste (SaaS)	<i>Anwendungen, Betriebssysteme, Middleware und Open-Source-Software, die die Funktionslogik digitaler Systeme bestimmen (Beispiele: Büroautomation, Fachapplikationen, Office-Software, KI-Frameworks).</i>	
6. Datenräume	<i>Technische und organisatorische Strukturen, welche die sichere und vertrauenswürdige Bereitstellung, den Austausch und den Bezug von Daten aus verschiedenen Quellen und von verschiedenen Akteuren ermöglicht und regelt (Beispiele: Register, Mobilität, Gesundheit, Finanzen).</i>	
5. Plattformen und Plattformdienste (PaaS)	<i>Entwicklungs- und Anwendungsplattformen, Angebote, die Software-Ökosysteme für Unternehmen und Verbraucher bereitstellen. (Beispiele: Kubernetes, Docker, Datenwissenschaftsplattform).</i>	
4. IT-Infrastruktur und Infrastrukturdienste (IaaS)	<i>Virtuelle und physische Infrastrukturen, die Rechen-, Speicher- und Netzwerkressourcen über verteilte Systeme ermöglichen (Beispiele: Virtuelle Infrastruktur (Cloud), Storage, VMs, DBs, Rechenzentren, Digitale Arbeitsgeräte).</i>	
3. Kommunikationsinfrastruktur	<i>Breitband-, Mobilfunk- und Satellitennetzwerke, die als Rückgrat der digitalen Kommunikation dienen und hohe sicherheitsrelevante Bedeutung haben (Beispiel: Breitbandnetze, Glasfaserinfrastruktur, Mobilfunknetze, Satellitennavigation).</i>	
2. Grundversorgung, Ressourcen	<i>Bereitstellung und Sicherung der grundlegenden Versorgungsinfrastrukturen wie Strom-, Wärme- und Wasserversorgung, die als physische Voraussetzung für den Betrieb digitaler Systeme und der gesellschaftlichen Stabilität dienen.</i>	
1. Komponenten	<i>Mikrochips, Sensoren, Aktuatoren und Fertigungstechnologien, die die Basis aller digitalen Systeme bilden und zentrale technologische Abhängigkeiten schaffen (Beispiele: Mikrochips, Mikrocontroller, 3D-Druck).</i>	
0. Rohmaterialien, Vorprodukte	<i>Grundlegende Rohstoffe wie seltene Erden und Prozesschemikalien, die für die Herstellung elektronischer Komponenten unerlässlich sind (Beispiele: Seltene Erden, Silizium Wafer).</i>	

Tabelle 1: Technologisches Schichtenmodell in Bezug auf digitale Souveränität

Die Ebenen 3 bis 8 bilden jene technologischen Schichten ab, in denen die Bundesverwaltung eigene Gestaltungsmöglichkeiten besitzt und ihre digitale Souveränität direkt beeinflussen kann. Der Gestaltungsspielraum der Bundesverwaltung nimmt von den oberen zu den unteren Ebenen in der Tendenz ab. Grund sind die mit den jeweiligen Ebenen verbundenen Sachzwänge sowie die Handlungskompetenzen der Bundesverwaltung im Bereich der Digitalisierung. Bereiche ausserhalb dieses unmittelbaren Handlungsspielraums in den Ebenen 0

bis 2 – etwa vorgelagerte Produktions- oder Rohstoffketten – werden in dieser Weisung nicht behandelt.

## 2.2 Eckwerte

Die Eckwerte der digitalen Souveränität bilden eine weitere Dimension der Betrachtung. Sie legen den normativen Handlungsrahmen für die Beurteilung und Stärkung der digitalen Souveränität fest. Eckwerte sind generelle Zielrichtungen und Leitgedanken, die bei der Umsetzung von Digitalvorhaben berücksichtigt werden müssen. Sie haben je nach Vorhaben unterschiedliche Priorität und können in der praktischen Umsetzung Spannungsfelder erzeugen, die im Einzelfall abzuwägen sind.

**Übergeordnete Eckwerte:** Die beiden übergeordneten Eckwerte bilden den grundsätzlichen Orientierungsrahmen für alle weiteren Beurteilungen der digitalen Souveränität.

- **Unabhängigkeit und Kontrolle:** Die Bundesverwaltung soll in der Lage sein, die Erfüllung ihrer Aufgaben unter Rückgriff auf digitale Ressourcen möglichst eigenständig zu gestalten und eine angemessene Kontrolle über die Ressourcen und Daten ausüben zu können. Ziel ist, Abhängigkeiten von einzelnen Anbietern, Technologien oder proprietären Lösungen zu vermeiden oder gezielt zu reduzieren. Da eine vollständige Unabhängigkeit in den meisten Fällen nicht realistisch ist, soll zumindest die Kontrollfähigkeit erhalten bleiben – also die Möglichkeit, die Funktionsweise von digitalen Ressourcen zu überprüfen.
- **Kosten und Wirtschaftlichkeit:** Digitale Souveränität soll effizient und ressourcenschonend erreicht werden. Der Einsatz finanzieller, technischer und personeller Mittel muss im Verhältnis zum erzielten Nutzen stehen. Dabei sind sowohl kurzfristige Wirtschaftlichkeitsaspekte (z. B. Betriebskosten, verfügbare Ressourcen) als auch langfristige Effekte (z. B. nachhaltige Finanzierungsmöglichkeiten) zu berücksichtigen. Wirtschaftlichkeit wird somit nicht allein als Kostenreduktion verstanden, sondern auch durch nachhaltige Investitionen.

**Spezifische Eckwerte:** Im Spannungsfeld dieser beiden übergeordneten Eckwerte sind die folgenden spezifischen Eckwerte mit ihren eigenen Zielrichtungen und Wechselwirkungen von Bedeutung:

- **Resilienz**  
Anwendungen, Infrastrukturen und Prozesse müssen so gestaltet sein, dass sie auch bei Störungen, Angriffen oder Ausfällen funktionsfähig bleiben oder rasch wiederhergestellt werden können.
- **Datenschutz und Informationssicherheit**  
Personen- und Geschäftsdaten dürfen nur im Einklang mit rechtlichen Vorgaben bearbeitet und durch geeignete technische und organisatorische Massnahmen vor unbefugtem Zugriff, Verlust oder Manipulation geschützt werden.
- **Kooperation und Standardisierung**  
Daten, Wissen, Anwendungen und Infrastrukturen sollen gemeinsam mit vertrauenswürdigen Partnern (z.B. Kantone, Verwaltungen anderer Staaten, zivilgesellschaftliche Organisationen, Unternehmen), genutzt werden, idealerweise über standardisierte Schnittstellen und harmonisierte Daten, sowie klar definierte Verantwortungen und Abläufe.
- **Innovation und Zweckmässigkeit**  
Prozesse und Technologien sollen einfach angewendet werden können und vielfältige Anwendungs- und Skalierungsmöglichkeiten bieten.

## 2.3 Zusammenspiel der Dimensionen

In einem **ersten Schritt** ist festzustellen, ob die digitale Souveränität der Bundesverwaltung betroffen ist. Diese ist betroffen, wenn die Erfüllung einer staatlichen Aufgabe, welche die Bundesverwaltung zu erfüllen hat, massgeblich von einer digitalen Ressource abhängt.

Auf dieser Grundlage werden in einem **zweiten Schritt** gezielt Massnahmen zur Stärkung der Kontroll- und Handlungsfähigkeit ausgearbeitet. Diese Analyse und Ableitung erfolgen entlang zweier Dimensionen: die technologischen Ebenen (2.1) und die Eckwerte (2.2).

- Die Ebenen zeigen auf, wo Massnahmen zur Stärkung der digitalen Souveränität ansetzen müssen.
- Die Eckwerte geben an, was mit diesen Massnahmen erreicht werden soll – sie formulieren die Zielrichtungen und Leitgedanken.

### Digitale Souveränität der Bundesverwaltung

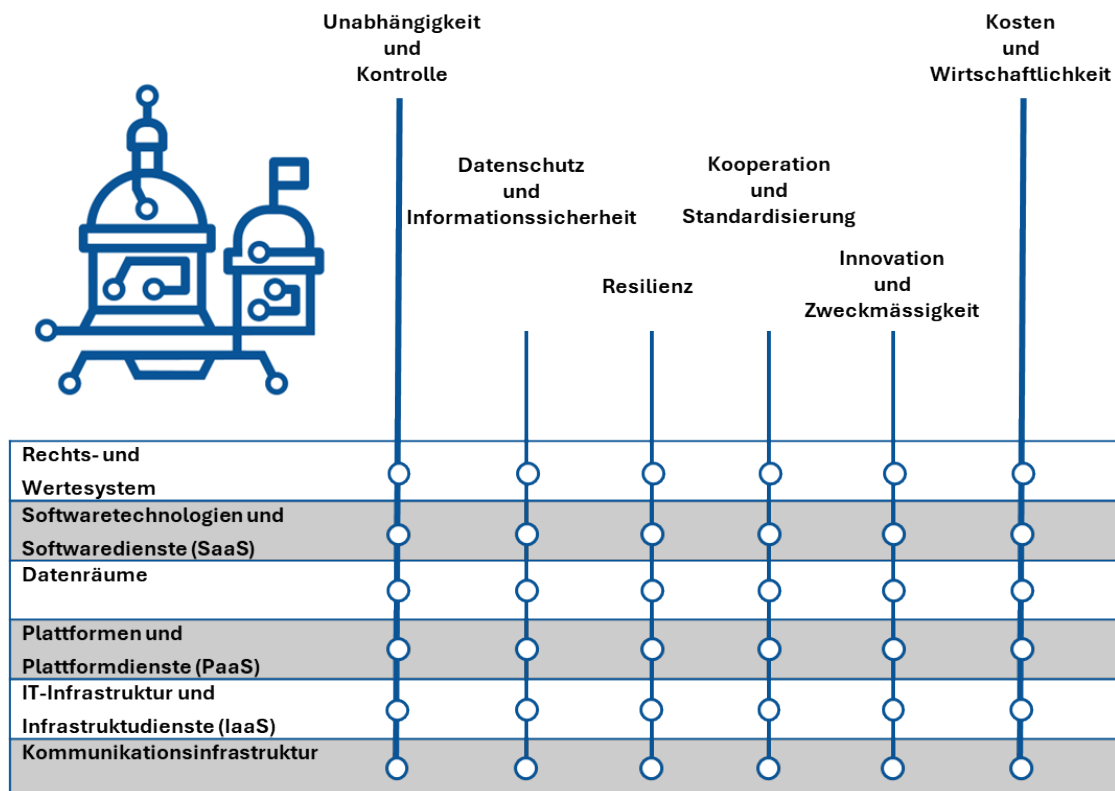


Abbildung 2: Visualisierung Analyseraster digitale Souveränität

Die Abbildung zeigt beispielhaft das Zusammenspiel zwischen Ebenen und Eckwerten auf. Diskussionen um Massnahmen zur Stärkung der digitalen Souveränität müssen einerseits auf die relevanten technologischen Ebenen eingegrenzt werden und andererseits die relevanten Eckwerte adressieren. So ist es möglich, im jeweiligen Projektkontext frühzeitig mögliche Spannungsfelder zwischen Eckwerten zu erkennen (z. B. zwischen Kosten und Unabhängigkeit oder zwischen Innovation und Datenschutz) und diese auf der richtigen technologischen Ebene zu verorten. Dieses Vorgehen ermöglicht, dass in der Bundesverwaltung Entscheide zur digitalen Souveränität systematisch und nachvollziehbar getroffen werden können.

## 2.4 Anwendungsbeispiel

Im folgenden Anwendungsbeispiel wird illustriert, wie die digitale Souveränität eines Vorhabens systematisch beurteilt werden kann. Es zeigt praxisnah, welche Schritte Projektverantwortliche durchlaufen, um sowohl den Handlungsbedarf als auch die relevanten technologischen Ebenen und Eckwerte zu identifizieren und daraus gezielte Fragestellungen abzuleiten.

**Beispiel:** Eine Verwaltungseinheit plant, eine neue KI-Anwendung zur automatisierten Informationsextraktion von und Informationsablage in Dossiers der elektronischen Geschäftsverwaltung (GEVER) einzuführen.

**1. Schritt:** Erstbeurteilung - Feststellen, ob und in welchem Ausmass digitale Souveränität betroffen ist

- Die Applikation unterstützt die Erfüllung staatlicher Aufgaben, die per Gesetz der Bundesverwaltung zugeordnet sind. Da staatliche Aufgaben von zum Teil hoher Bedeutung betroffen sind, besteht eine hohe Abhängigkeit von der Funktionsfähigkeit und Sicherheit des Systems und damit ein hoher Anspruch an die Kontroll- und Handlungsfähigkeit. Die digitale Souveränität ist somit in relevantem Ausmass betroffen.

**2. Schritt:** Beurteilung entlang der beiden Dimensionen

Anschliessend wird geprüft, auf welchen technologischen Ebenen die digitale Souveränität besonders relevant ist und welche Eckwerte im Vordergrund stehen:

Betroffene Ebenen:

- Ebene 7 – Softwaretechnologien und Softwaredienste (SaaS): Die Wahl der Fachanwendung, ihrer Architektur und ihrer Abhängigkeiten von proprietären Komponenten bestimmt die Kontrollfähigkeit der Verwaltung.
- Ebene 5 – Plattformdienste (PaaS): Läuft die Fachanwendung auf einer internen oder externen Entwicklungs- oder Betriebsplattform, ist auch diese Ebene betroffen. Es ist zu beurteilen, ob und in welchem Ausmass die Nutzung der Plattform Auswirkungen auf die digitale Souveränität hat – etwa im Hinblick auf Abhängigkeiten, Vertragsgestaltung, Verfügbarkeit oder Kontrollmöglichkeiten.

Relevante Eckwerte:

- Unabhängigkeit und Kontrolle: Kann die Verwaltung den Betrieb und die Weiterentwicklung der Anwendung eigenständig steuern oder besteht eine starke Abhängigkeit vom Anbieter? Kann das Produkt in nützlicher Frist substituiert werden?
- Datenschutz und Informationssicherheit: Wie werden Personendaten oder Geschäftsdaten bearbeitet und geschützt?
- Kosten und Wirtschaftlichkeit: Stehen Aufwand und Nutzen in einem angemessenen Verhältnis, auch langfristig?

**3. Schritt:** Ableitung von Spannungsfeldern und Fragestellungen

Auf Basis dieser Einordnung werden konkrete Fragestellungen für die Studien- und Konzeptphase abgeleitet, z. B.:



- Wie kann die Bundesverwaltung sicherstellen, dass sie die Anwendung bei Bedarf selbst betreiben oder den Anbieter wechseln kann?
- Welche Anforderungen sind an Datenschutz und Datenhaltung zu stellen?
- Welche Abwägungen ergeben sich zwischen höherer Unabhängigkeit (z. B. Eigenbetrieb) und Kosten (z. B. externer Cloud-Betrieb)?

Diese Fragen fließen in die Studienphase des Projekts ein und werden dort systematisch geprüft und dokumentiert. Damit wird gewährleistet, dass die digitale Souveränität bereits zu Beginn des Vorhabens berücksichtigt wird.

### **3 Vorgaben**

Die Weisung ist für alle unterstellten Verwaltungseinheiten verbindlich. Sie **MÜSSEN** die digitale Souveränität bei allen relevanten IKT-Vorhaben prüfen und berücksichtigen.

#### **3.1 Integration in HERMES Projektmanagement**

Die Beurteilung der digitalen Souveränität wird im HERMES-Projektvorgehen über organisationsspezifische Prüfpunkte sichergestellt.

Die Prüfpunkte **MÜSSEN** in den Checklisten aller Meilensteine erfasst und durch die Projektleitung bei jedem Meilenstein bearbeitet werden.

Die inhaltliche Beurteilung erfolgt mit Hilfe der von der Bundeskanzlei bereitgestellten Hilfsmittel, soweit diese zur Verfügung stehen. Diese Hilfsmittel enthalten unterstützende Instrumente für die Beurteilung.

#### **3.2 Verantwortung**

- Die Projektleitung ist verantwortlich für die Bearbeitung der Prüfpunkte und die Planung und Überwachung der erforderlichen Aktivitäten im Projekt.
- Die Auftraggeberin stellt sicher, dass die Resultate in die Entscheidungsprozesse einfließen.

#### **3.3 Berichterstattung und Nachvollziehbarkeit**

Die Ergebnisse der Beurteilung **MÜSSEN** dokumentiert werden.

Ergibt die Beurteilung, dass ein Vorhaben Risiken oder Abhängigkeiten von grosser politischer oder strategischer Tragweite aufweist, **SOLL** die Auftraggeberin den Digitalisierungsrat Bund (DRB) darüber informieren.

In solchen Fällen **KANN** im DRB eine Aussprache oder Information zur digitalen Souveränität des betroffenen Vorhabens erfolgen.

## Anhänge

### A. Allgemeine Informationen zum Dokument

Version und Status	Version 1.0 In Kraft
Originalsprache	Deutsch
Beschluss vom	10. Dezember 2025
Inkraftsetzung am	1. Januar 2026

### B. Aufhebung bisheriger Vorgaben

keine

### C. Übergangs- und Schlussbestimmungen

Diese Weisung gilt für alle neuen IKT-Vorhaben, die ab dem in Abschnitt A festgelegten Inkrafttreten initiiert werden.

Bereits laufende Vorhaben unterliegen nicht rückwirkend dieser Weisung. Die Verwaltungseinheiten können die Leitlinien und Kriterien freiwillig anwenden, insbesondere wenn sich dies als zweckmässig für die Sicherstellung der digitalen Souveränität erweist.

### D. Änderungen gegenüber Vorversion / Angaben zur Erstausgabe

Dies ist die Erstausgabe.

### E. Bedeutung der Schlüsselwörter zur Bestimmung des Verbindlichkeitsgrades

Der Verbindlichkeitsgrad der einzelnen Bestimmungen dieser Weisung wird mittels folgender Schlüsselwörter in Grossbuchstaben gekennzeichnet. Die Verbindlichkeitsgrade basieren auf dem internationalen Standard IETF/RFC 2119 BCP14 und lehnen sich damit an eine verbreitete Praxis in der internationalen Standardisierung.

Schlüsselwort	Verbindlichkeitsgrad
MUSS	Anordnung, Anforderung, Bestimmung die einzuhalten ist. Für Ausnahmen und Abweichungen muss ein schriftliches Gesuch gestellt und vom Bereich DTI genehmigt werden. (MUST, REQUIRED, SHALL)
SOLL	Anordnung, Anforderung, Bestimmung, die einzuhalten ist. Ausnahmen und Abweichungen, z.B. aus wirtschaftlichen oder sicherheitstechnischen Aspekten, müssen schriftlich begründet werden. Eine explizite Ausnahmegewährung des Bereichs DTI ist nicht erforderlich. (SHOULD, RECOMMENDED)
DARF NICHT	Option, die nicht gewählt, bzw. Massnahme, die nicht umgesetzt werden darf. (MUST NOT, SHALL NOT)
DARF	Option, die explizit erlaubt ist. Die potenziell Nutzenden bzw. Anwendenden der Option entscheiden, ob sie diese nutzen wollen. Der Anbieter muss die Option unterstützen bzw. anbieten.

KANN                      Option, die akzeptiert ist.  
Der Anbieter der Option entscheidet darüber, ob er diese unterstützen  
bzw. anbieten will.

## **F.    Beilagen, Referenzen und weiterführende Informationen**

Die Mantelweisungen haben eine strategische Flughöhe und bilden die neue Hauptstufe der Weisungen. Darauf referenzierende und untergeordnete Weisungen vertiefen ein Thema inhaltlich selbstständig und berücksichtigen alle dazu notwendigen Regelungen.

### **ID                      Beilagen**

## **Links zu weiterführenden Informationen**

## **G.    Glossar**

<b>Abkürzung/ Begriff</b>	<b>Bedeutung</b>
-------------------------------	------------------

## **H.    Metadaten für die Suchoptimierung im Web**

Thema DigiV Art. 40 Abs 1	Teilstrategie
Strategiebezug	Sicherheit (auch Vertrauenswürdigkeit / Souveränität)
Fähigkeitsdomäne	Strategische Steuerung & Führung
Bezug zur Architekturvision 2050	Standardmässig digital