

Workshop: Bequem oder Souverän?

Der Cloud-basierte Arbeitsplatz der Zukunft.

Ein Workshop mit

Andreas Gabriel, Leitung Hochschulrechenzentrum

Thorsten Arendt, Stabsstelle Digitalisierung

Tobias Weiß, Abteilung Zentrale Systeme



CoCreate:
Wissen gemeinsam organisieren – Open Science

Bequem oder Souverän?



Motivation



Aktuelles zum Datenschutz



Vorstellung von openDesk




Brainstorming und Diskussion



Warum „Cloud Arbeitsplatz der Zukunft“?

 Offene Wissenschaft braucht digitale Arbeitsräume, die erklären, teilen, verbinden einfach machen

 Der digitale Arbeitsplatz prägt wie wir forschen, lehren und verwalten

Wissen gemeinsam organisieren heißt auch:
gemeinsam verstehen und gestalten! → CoCreate



Unser Maßstab – Unsere Leitbilder



Nachhaltig gestalten

zukunftsicher, offen und ressourcenschonend



Wissenschaftliche Freiheit sichern

unabhängig bleiben, selbst bestimmen



Offenheit und Teilhabe fördern

Zugang schaffen, Vielfalt unterstützen

Wenn diese Werte unser Handeln prägen, dann muss unsere digitale Infrastruktur diese auch tragen können.



Open Science beginnt beim Arbeitsplatz



Offene & übertragbare Datenformate

verhindern Lock-in und sichern Wiederverwendbarkeit & Weitergabe



Nachvollziehbare digitale Prozesse

Klarheit über Datenwege, Speicherung, Berechtigungen



Fähigkeit zur Kollaboration über Organisationsgrenzen

Gemeinsames Arbeiten mit internen & externen Partnern



Datenhoheit & Portabilität

Ermöglicht Kontrolle & reibungslose Exportszenarien





Open Science stärkt Digitale Souveränität



Weil Offenheit, Transparenz, Anschlussfähigkeit und Kontrolle genau die Fähigkeiten sind, die Souveränität ausmachen



Vom Anspruch zur Umsetzung



Aktueller Rahmen: Datenschutz und Digitalpakt



openDesk – Eine souveräne Alternative zu MS365



Austausch & Feedback – gemeinsam weiter denken



Aktuelles: Datenschutz



Bericht des Hessischen Beauftragten für Datenschutz und Informationsfreiheit zum Einsatz von Microsoft 365

Es wird daher empfohlen, für die zum Einsatz kommenden IT-Produkte immer auch alternative Produkte zu evaluieren, zu dokumentieren und zu verproben.¹⁵⁰ Dies soll die digitale Handlungsfähigkeit des Verantwortlichen für den Fall sicherstellen, dass ein im Einsatz befindliches IT-Produkt aus rechtlichen oder tatsächlichen Gründen nicht genutzt werden kann.

Quelle: https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/2025-11/hbdi_bericht_m365_2025_11_15.pdf



Aktuelles: Digitalpakt 2.0

Ein Kernthema: 🛡️ 🔒 👁️

Digitale Souveränität (Seite 4, 9)

- Stärkung der digitalen Souveränität als zentrales Ziel
- Vermeidung von „Vendor-Lock-Ins“
- Verpflichtet uns nicht direkt zu einem Tool
- Schafft Rahmen, in dem eine Erprobung einer **souveränen Alternative** als **strategisch sinnvoll, compliance-konform** und **finanziell attraktiv** erscheint



HESSISCHER DIGITALPAKT HOCHSCHULEN
(DIGITALPAKT 2.0)

2026-2031



Quelle: https://wissenschaft.hessen.de/sites/wissenschaft.hessen.de/files/2025-12/hessischer_digitalpakt_hochschulen_2026-2031.pdf

Digitale Souveränität: Ein Spektrum



Eine ausgewogene Strategie könnte einen Kompromiss zwischen Fremdbestimmung und Autarkie anstreben.

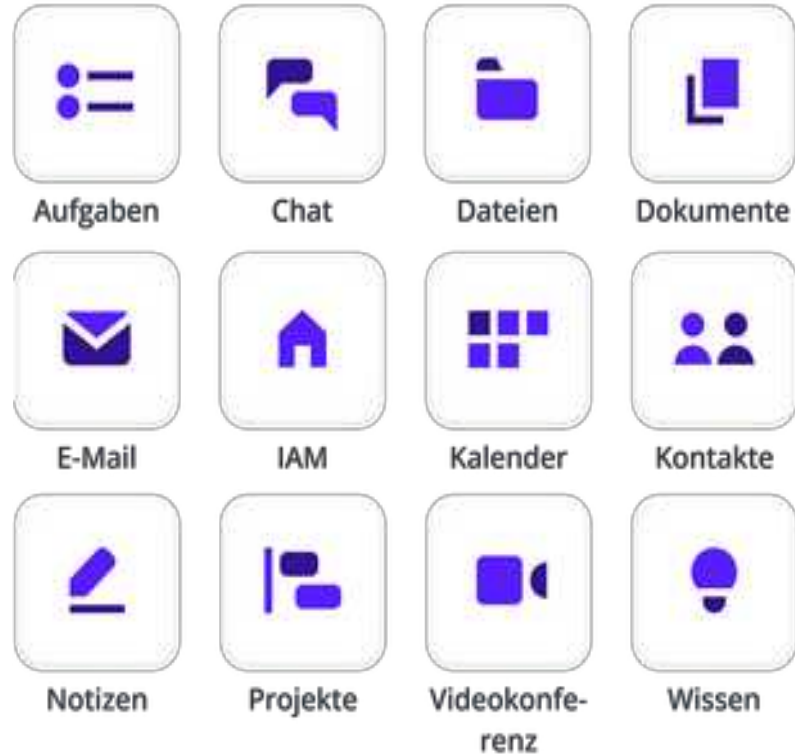
Quelle: <https://www.bitkom.org/sites/main/files/file/import/BITKOM-Position-Digitale-Souveraenitaet.pdf>



Vorstellung: openDesk



Quelle: <https://opendesk.eu/>



Diskussion / Feedback

OpenDesk Demo:

<https://portal.demo.opendesk.eu>

Alternativ:

<https://shorturl.at/9jZHj>

jana.mueller / 0p3nD35k

thomas.schulz / 0p3nD35k



BACKUP SLIDES







Digitale Souveränität: Eine Definition

~ beschreibt „die Fähigkeiten und Möglichkeiten von Individuen und Institutionen, ihre Rolle(n) in der digitalen Welt **selbstständig, selbstbestimmt** und **sicher** ausüben zu können“.

Quelle: https://www.it-planungsrat.de/fileadmin/beschluesse/2021/Beschluss2021-47_ZenDis_AL1.pdf



Unsere Perspektive: Gelebte Digitale Souveränität bedeutet

-  **Offene Formate**
Unabhängigkeit von einzelnen Anbietern
-  **Transparente Prozesse**
Kontrolle & Entscheidungsfreiheit
-  **Fähigkeit zur Kollaboration**
Handlungsfähigkeit über Systemgrenzen
-  **Datenhoheit & Portabilität**
Exit-Optionen & langfristige Verfügbarkeit



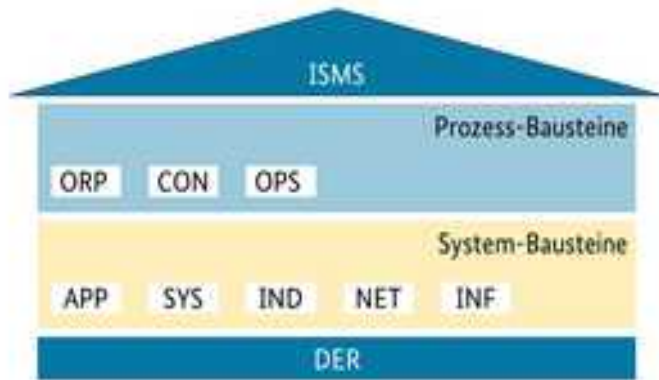
Diskussion: Souverän mit MS365?

- Verbindlichkeit von ausländischem **Recht**
 - CLOUD Act
 - „Compliance“-Risiken trotz DSGVO-konformer Angebote
- **Transparenzpflicht** bei „externen Lieferketten“ (APIs, KI)
- **Kosten** und strategische Abhängigkeit
 - Kontrolle über Innovationen (z.B. notwendige lokale Anpassungen)
 - Langfristige Kostenbetrachtung (Starke Preiserhöhungen vs. immense Wechselkosten)



Herleitung aus dem IT-Grundschutz ⁽¹⁾

- Herausgegeben vom Bundesamt für Informationssicherheit
- Unser IT-Sicherheitskonzept orientiert sich daran
- Modular aufgebaut



Modularer Aufbau des IT-Grundschutz

OPS.2.2 Bundesamt für Sicherheit in der Informationstechnik OPS.2: Betrieb von Dritten

OPS.2.2 Cloud-Nutzung

1. Beschreibung

1.1. Einleitung

Cloud Computing bezeichnet das dynamisch an den Bedarf angepasste Anbieten, Nutzen und Abrechnen von IT-Dienstleistungen über ein Netz. Angebot und Nutzung dieser Dienstleistungen erfolgen dabei ausschließlich über definierte technische Schnittstellen und Protokolle. Die Spannbreite der im Rahmen von Cloud Computing angebotenen Dienstleistungen umfasst das komplette Spektrum der Informationstechnik und beinhaltet unter anderem Infrastruktur (z. B. Rechenleistung, Speicherplatz), Plattformen und Software.

Empfehlungen zur Nutzung der Cloud

Quelle:

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2023/



Herleitung aus dem IT-Grundschutz ⁽²⁾

- Zentrale Operations-Leitlinie zur Cloud-Nutzung OPS 2.2
- Sie fordert
 - **Exit** Strategie (OPS.2.2.A14 und OPS.2.2.A15)
 - **Backup** Strategie (OPS.2.2.A16)
 - Weitere Basis-Anforderungen, wie die **Dokumentationspflichten** (OPS.2.2.A1 – A4)

Quelle:

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2023/04_OPS_Betrieb/OPS_2_2_Cloud-Nutzung_Edition_2023.pdf?__blob=publicationFile&v=3



Konzept des IT-Planungsbeirats

- Gemäß § 1 IT-Staatsvertrag übernimmt der IT-Planungsrat folgende Aufgaben: **Koordination** und **Normierung**
- Zur Stärkung der Digitalen Souveränität erging folgender **Beschluss**:

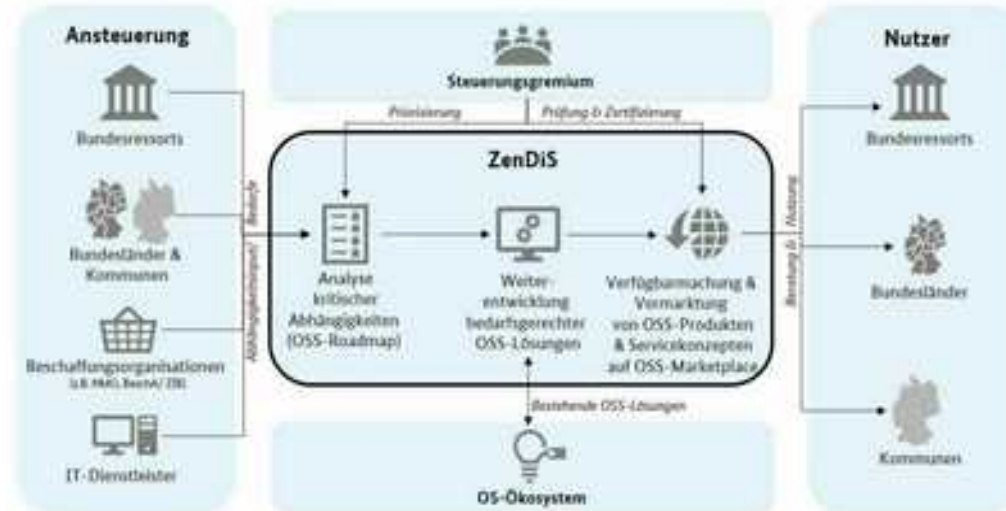


Ziele und Lösungsansätze zur Stärkung der Digitalen Souveränität

Quelle: https://www.it-planungsrat.de/fileadmin/beschluesse/2021/Beschluss2021-47_ZenDis_AL1.pdf



Das Zentrum für Digitale Souveränität



Gesamtübersicht des Zentrums für digitale Souveränität (ZenDiS)

Quelle: https://www.it-planungsrat.de/fileadmin/beschluesse/2021/Beschluss2021-47_ZenDis_AL1.pdf



Workshop: Bequem oder Souverän?

Der Cloud-basierte Arbeitsplatz der Zukunft.

Ein Workshop mit

Andreas Gabriel, Leitung Hochschulrechenzentrum

Thorsten Arendt, Stabsstelle Digitalisierung

Tobias Weiß, Abteilung Zentrale Systeme



CoCreate:
Wissen gemeinsam organisieren - Open Science



Marburg
University

Link zum Videoordner: <https://next.hessenbox.de/index.php/s/9Tc46fCSRBC64WP> (geht nicht aus Urheberrechtsgründen)

Bequem oder Souverän?



Motivation



Aktuelles zum Datenschutz




Vorstellung von openDesk




Brainstorming und Diskussion



Warum „Cloud Arbeitsplatz der Zukunft“?

 Offene Wissenschaft braucht digitale Arbeitsräume,
die erklären, teilen, verbinden einfach machen

 Der digitale Arbeitsplatz prägt wie wir forschen, lehren
und verwalten

Wissen gemeinsam organisieren heißt auch:
gemeinsam verstehen und gestalten! → CoCreate



Unser Maßstab – Unsere Leitbilder



Nachhaltig gestalten

zukunftsicher, offen und ressourcenschonend



Wissenschaftliche Freiheit sichern

unabhängig bleiben, selbst bestimmen



Offenheit und Teilhabe fördern

Zugang schaffen, Vielfalt unterstützen

Wenn diese Werte unser Handeln prägen, dann muss unsere digitale Infrastruktur diese auch tragen können.



F. 4 – Andreas Gabriel, Leitung HRZ

Infrastruktur ist nicht wertneutral. Sie entscheidet darüber, ob wir unabhängig forschen können oder von Lizenzmodellen diktiert werden.

Open Science beginnt beim Arbeitsplatz



Offene & übertragbare Datenformate

verhindern Lock-in und sichern Wiederverwendbarkeit & Weitergabe



Nachvollziehbare digitale Prozesse

Klarheit über Datenwege, Speicherung, Berechtigungen



Fähigkeit zur Kollaboration über Organisationsgrenzen

Gemeinsames Arbeiten mit internen & externen Partnern



Datenhoheit & Portabilität

Ermöglicht Kontrolle & reibungslose Exportszenarien



F. 5 – Andreas Gabriel, Leitung HRZ

Datensouveränität beginnt beim Dateiformat. Proprietäre Formate sind Sackgassen; offene Standards sind die Versicherung für die langfristige Nachnutzung von Forschung

Verdeutlichen Sie, dass "Lock-in-Effekte" nicht nur technischer Natur sind, sondern die Nachvollziehbarkeit wissenschaftlicher Prozesse gefährden. Ein starker Kommentar wäre: "Wer die Datenformate kontrolliert, kontrolliert langfristig die Archivierung unserer Forschungsergebnisse."



Open Science stärkt Digitale Souveränität




Weil Offenheit, Transparenz, Anschlussfähigkeit und Kontrolle genau die Fähigkeiten sind, die Souveränität ausmachen



Vom Anspruch zur Umsetzung

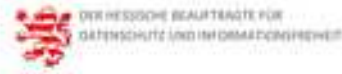
 Aktueller Rahmen: Datenschutz und Digitalpakt

 openDesk – Eine souveräne Alternative zu MS365

 Austausch & Feedback – gemeinsam weiter denken



Aktuelles: Datenschutz



Bericht des Hessischen Beauftragten für Datenschutz und Informationsfreiheit zum Einsatz von Microsoft 365

Es wird daher empfohlen, für die zum Einsatz kommenden IT-Produkte immer auch alternative Produkte zu evaluieren, zu dokumentieren und zu verproben.¹⁵⁰ Dies soll die digitale Handlungsfähigkeit des Verantwortlichen für den Fall sicherstellen, dass ein im Einsatz befindliches IT-Produkt aus rechtlichen oder tatsächlichen Gründen nicht genutzt werden kann.



Quelle: https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/2025-11/hbdi_bericht_m365_2025_11_15.pdf

F. 8 – Tobias Weiß, Abt. Zentrale Systeme

Die Empfehlung des Hessischen Beauftragten für Datenschutz (HBDI) ist eine Handlungsaufforderung. Die Evaluation von Alternativen wie openDesk ist eine notwendige Risikovorsorge für unsere digitale Handlungsfähigkeit.

Aktuelles: Digitalpakt 2.0

Ein Kernthema:   

Digitale Souveränität (Seite 4, 9)



HESSISCHER DIGITALPAKT HOCHSCHULEN
(DIGITALPAKT 2.0)
2026-2031

- Stärkung der digitalen Souveränität als zentrales Ziel
- Vermeidung von „Vendor-Lock-Ins“
- Verpflichtet uns nicht direkt zu einem Tool
- Schafft Rahmen, in dem eine Erprobung einer **souveränen Alternative** als **strategisch sinnvoll, compliance-konform** und **finanziell attraktiv** erscheint



Quelle: https://wissenschaft.hessen.de/sites/wissenschaft.hessen.de/files/2025-12/hessischer_digitalpakt_hochschulen_2026-2031.pdf

F. 9 – Tobias Weiß, Abt. Zentrale Systeme

Strategischer Hebel: Der Pakt fordert das „Together first“-Prinzip. Marburg kann durch kooperative Projekte zur digitalen Souveränität zusätzliche Mittel aus dem Projektbudget erschließen.

Diese Projektbudgets für kooperative Projekte (wie openDesk-Pilotierungen) sind der Schlüssel für die Finanzierung der Transformation.

Digitale Souveränität: Ein Spektrum



Eine ausgewogene Strategie könnte einen Kompromiss zwischen Fremdbestimmung und Autarkie anstreben.

Quelle: <https://www.bitkom.org/sites/main/files/file/import/BITKOM-Position-Digitale-Souveraenitaet.pdf>



F. 10 – Tobias Weiß, Abt. Zentrale Systeme

Ziel ist nicht die Isolation (Autarkie), sondern die Wahlfreiheit. Souveränität heißt, zwischen vertrauenswürdigen Partnern entscheiden zu können, statt alternativlos gebunden zu sein.

Vorstellung: openDesk



Quelle: <https://opendesk.eu/>



F. 11 – Tobias Weiß, Abt. Zentrale Systeme

Zum Thema openDesk (Folie 12): "openDesk ist nicht nur eine Programmsammlung, sondern der Versuch, die Interoperabilität zwischen verschiedenen Open-Source-Tools auf Enterprise-Niveau zu heben."

Diskussion / Feedback

OpenDesk Demo:

<https://portal.demo.opendesk.eu>

Alternativ:

<https://shorturl.at/9jZHj>



jana.mueller / 0p3nD35k

thomas.schulz / 0p3nD35k



F. 12 – Thorsten Arendt, Stabsstelle Digitalisierung

Echte Kostenrechnung: Wir müssen Preiserhöhungen und strategischen Kontrollverlust gegen den Aufwand der Migration aufwiegen.

BACKUP SLIDES



F. 13 – Thorsten Arendt, Stabsstelle Digitalisierung

Echte Kostenrechnung: Wir müssen Preiserhöhungen und strategischen Kontrollverlust gegen den Aufwand der Migration aufwiegen.





Digitale Souveränität: Eine Definition

~ beschreibt „die Fähigkeiten und Möglichkeiten von Individuen und Institutionen, ihre Rolle(n) in der digitalen Welt **selbstständig, selbstbestimmt** und **sicher** ausüben zu können“.

Quelle: https://www.it-planungsrat.de/fileadmin/beschluesse/2021/Beschluss2021-47_ZenDis_AL1.pdf



Unsere Perspektive: Gelebte Digitale Souveränität bedeutet

-  **Offene Formate**
Unabhängigkeit von einzelnen Anbietern
-  **Transparente Prozesse**
Kontrolle & Entscheidungsfreiheit
-  **Fähigkeit zur Kollaboration**
Handlungsfähigkeit über Systemgrenzen
-  **Datenhoheit & Portabilität**
Exit-Optionen & langfristige Verfügbarkeit



Diskussion: Souverän mit MS365?

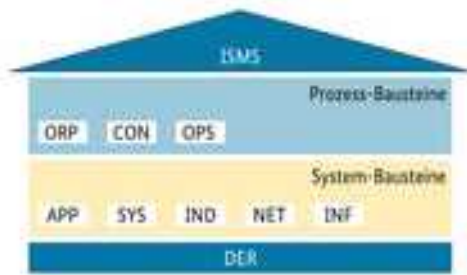
- Verbindlichkeit von ausländischem **Recht**
 - CLOUD Act
 - „Compliance“-Risiken trotz DSGVO-konformer Angebote
- **Transparenzpflicht** bei „externen Lieferketten“ (APIs, KI)
- **Kosten** und strategische Abhängigkeit
 - Kontrolle über Innovationen (z.B. notwendige lokale Anpassungen)
 - Langfristige Kostenbetrachtung (Starke Preiserhöhungen vs. immense Wechselkosten)



Folie 15 (Risiko-Kommunikation): Vertiefen Sie den Punkt zum CLOUD Act. Erklären Sie kurz, dass dieser US-Behörden Zugriff auf Daten ermöglichen kann, selbst wenn diese in der EU gespeichert sind, was im Widerspruch zur geforderten Datenhoheit steht

Herleitung aus dem IT-Grundschutz ⁽¹⁾

- Herausgegeben vom Bundesamt für Informationssicherheit
- Unser IT-Sicherheitskonzept orientiert sich daran
- Modular aufgebaut



Modularer Aufbau des IT-Grundschatz

OPS.2.2 OPS.2: Betrieb von Dritten

 Bundesamt für Sicherheit in der Informationstechnik

OPS.2.2 Cloud-Nutzung

1. Beschreibung

1.1. Einleitung

Cloud Computing bezeichnet das dynamisch an den Bedarf angepasste Anbieten, Nutzen und Abnehmen von IT-Dienstleistungen über ein Netz. Angebot und Nutzung dieser Dienstleistungen erfolgen dabei ausschließlich über definierte technische Schnittstellen und Protokolle. Die Spannbreite der im Rahmen von Cloud Computing angebotenen Dienstleistungen umfasst das komplette Spektrum der Informationstechnik und beinhaltet unter anderem Infrastruktur (z. B. Rechenleistung, Speicherplatz), Plattformen und Software.

Empfehlungen zur Nutzung der Cloud



Quelle:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompodium_Einzel_PDFs_2023/

Folie 10 (IT-Grundschatz konkretisieren): Ergänzen Sie einen Hinweis auf den Baustein OPS.2.2 Cloud-Nutzung. Betonen Sie hierbei, dass Souveränität eine Voraussetzung für die Erfüllung dieser Sicherheitsstandards ist.

Herleitung aus dem IT-Grundschutz ⁽²⁾

- Zentrale Operations-Leitlinie zur Cloud-Nutzung OPS 2.2
- Sie fordert
 - **Exit** Strategie (OPS.2.2.A14 und OPS.2.2.A15)
 - **Backup** Strategie (OPS.2.2.A16)
 - Weitere Basis-Anforderungen, wie die **Dokumentationspflichten** (OPS.2.2.A1 – A4)

Quelle:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2023/04_OPS_Betrieb/OPS_2_2_Cloud-Nutzung_Edition_2023.pdf?__blob=publicationFile&v=3



Konzept des IT-Planungsbeirats

- Gemäß § 1 IT-Staatsvertrag übernimmt der IT-Planungsrat folgende Aufgaben: **Koordination** und **Normierung**
- Zur Stärkung der Digitalen Souveränität erging folgender **Beschluss**:

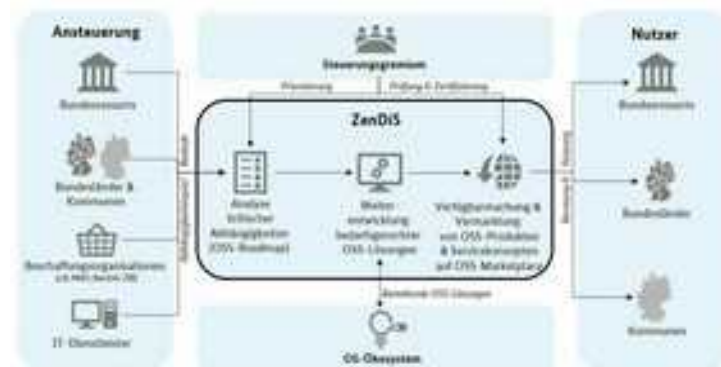


Ziele und Lösungsansätze zur Stärkung der Digitalen Souveränität

Quelle: https://www.it-planungsrat.de/fileadmin/beschluesse/2021/Beschluss2021-47_ZenDis_AL1.pdf



Das Zentrum für Digitale Souveränität



Gesamtübersicht des Zentrums für digitale Souveränität (ZenDiS)

Quelle: https://www.it-planungsrat.de/fileadmin/beschluesse/2021/Beschluss2021-47_ZenDiS_AL1.pdf

