Lehrstuhl für Recht und Sicherheit der Digitalisierung
TUM Center for Digital Public Services
Technische Universität München

Open Source – Open Government

Offenheit als Grundlage eines souveränen Rechtsstaats

Nürnberg Digital Festival | Ein Tag zur digitalen Souveränität | 2. Juli 2025

Univ.-Prof. Dr. Dirk Heckmann
Mitglied des Bayerischen Verfassungsgerichtshofs

Digitale Souveränität: Ein Weckruf!

WirtschaftsWoche

Nach Sanktionen durch US-Präsident Trump verlor der Chefankläger des Internationalen Strafgerichtshofs den Zugriff auf sein Microsoft-Nutzerkonto. Foto: Peter Dejong/AP/dpa

wiwo.de v. 25.05.2025 - Foto: Peter Dejong/AP/dpa

„Weckruf“ für mehr digitale Souveränität

Strafgerichtshof: Microsofts E-Mail-Sperre als Weckruf für digitale Souveränität

Microsoft hat nach Trump-Sanktionen das Mail-Konto des Chefanklägers des Internationalen Gerichtshofs blockiert. Kritiker: "Wir brauchen dringend Alternativen."

https://www.heise.de/news/Strafgerichtshof-Microsofts-E-Mail-Sperre-als-Weckruf-fuer-digitale-Souveraenitaet-10387368.html

POLITICO

Trump can pull the plug on the internet, and Europe can't do anything about it

Trump is back — and with him, the risk that the U.S. could unplug Europe from the digital world.

By **MATHIEU POLLET**
in Brussels

https://www.politico.eu/article/donald-trump-eu-internet-europe-us-trade-war-data-cyber/

Unsere digitale Schwachstelle: **Abhängigkeiten**

- **72 % der Anteile** im europäischen Cloud-Markt halten Amazon, Microsoft, Google
- **96 % der Beschäftigten** in deutschen Behörden arbeiten mit Microsoft Software
- **80 % der deutschen Verwaltungsdaten** in Datenbanken US-amerikanischer Anbieter
- **Reale Gefahren**:
  - Anordnung eines „Kill-Switch“ möglich
  - Abfluss oder Nutzung von Daten
  - Abschalten von Cloud-Services

Digitale Souveränität und kritische Abhängigkeiten

10 Digitale Souveränität

Digitale Souveränität als Staatsaufgabe

Wie Abhängigkeiten unsere Demokratie gefährden

Technologische Abhängigkeiten als offene Flanke

Handelsblatt Journal Eine Sonderveröffentlichung von Euroforum Deutschland | FEBRUAR 2025
https://veranstaltungen.handelsblatt.com/journal/

Gefährdung des Rechtsstaates

Eingeschränkte Gewährleistung von

- IT-Sicherheit
- Datenschutz und Datensicherheit
- Funktionsfähigkeit der digitalen Infrastruktur

→ souveräne Handlungsfähigkeit fraglich, demokratische Grundwerte bedroht

bidt

IHK Industrie- und Handelskammer Nürnberg für Mittelfranken

CDPS
TUM CENTER FOR DIGITAL PUBLIC SERVICES

Offenheit als Grundlage eines souveränen Rechtsstaats

Open Source als Schlüssel zu digitaler Souveränität?

Digitale Souveränität zwischen Freiheit und Kontrolle

Digitale Gewaltenteilung als Marktverantwortung

Kriterien zur rechtlichen Abgrenzung staatlicher und privatwirtschaftlicher Entfaltungsmöglichkeiten auf dem Markt der IT-Herstellung und IT-Services

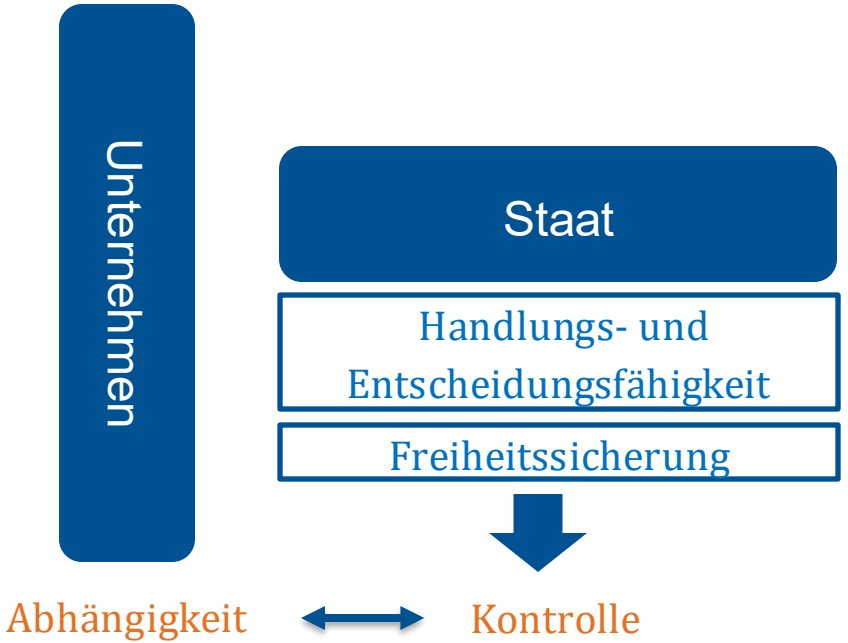
Eine Studie im Auftrag des Verbandes der mittelständischen IT-Dienstleister und Softwarehersteller für den öffentlichen Sektor, DATABUND e.V.

Passau und Berlin, im März 2016

Autoren

Univ.-Prof. Dr. Dirk Heckmann, MdBayVerfGH
Lehrstuhl für Öffentliches Recht, Sicherheitsrecht und Internetrecht
Forschungsstelle für IT-Recht und Netzpolitik
Universität Passau

Dr. Wilfried Bernhardt, Staatssekretär a.D.
Stv. Vorsitzender des Nationalen E-Government-Kompetenzzentrums



https://www.tum-cdps.de/wp-content/uploads/2020/06/13-Heckmann-Digitale-Gewaltenteilung-2016.pdf

Open Source: als Vision …

Vorteile früh erkannt (Anfang 2000er Jahre):

- Open Source: als „Chance zur europäischen digitalen Unabhängigkeit“
- Erste Open-Source-Projekte:
  Desktop-Projekt LiMux München (2003-2017)

Logo des Limux-Projektes (Bild: Stadt München)

https://www.golem.de/specials/limux-projekt/

… oder Illusion?

Auf der Kehrseite:

- langwieriger, kostenintensiver Umstieg
- Fehlende Interoperabilität
- Eingeschränkte Funktionalitäten

→ doch zurück zu proprietärer Software

LIMUX-ENDE

Münchner Stadtrat stimmt für Windows-Migration

Der zuständige Verwaltungsausschuss des Münchner Stadtrats hat das Ende des Limux-Projektes besiegelt und für eine Migration zu Windows gestimmt. Die soll 2022 abgeschlossen sein, die Kosten dafür bleiben geheim.

https://www.golem.de/news/limux-ende-muenchner-stadtrat-stimmt-fuer-windows-migration-1711-131041.html

… aber Open Source ist doch viel sicherer (?)

Sicherheitskonzept oder Risikofaktor – Kehrseite der Offenheit

Transparenz als Sicherheitskonzept:

- ermöglicht Aufdecken
- und Schließen von Sicherheitslücken

Aber: Zugriff potenzieller Störer

- Sicherheitslücke in Log4j-Java-Bibliothek
- Potentielle Ausweitung des Crowdstrike-Vorfalls

Bundesamt für Sicherheit in der Informationstechnik

Nationales IT-Lagezentrum BSI

SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

Kritische Schwachstelle in log4j veröffentlicht (CVE-2021-44228)

Erhöhung der Warnstufe auf Rot

CSW-Nr. 2021-549032-15M0, Version 1.5, 17.12.2021

IT-Bedrohungslage*: 4 / Rot

Open Source: neue alte Strategie

- Koalitionsvereinbarung für die Stadtratsperiode 2020-2026 (München): OS-Prinzip

> Wo immer technisch und finanziell möglich setzt die Stadt auf offene Standards und freie **Open Source**-lizenzierte Software und vermeidet damit absehbare Herstellerabhängigkeiten. Diese Abwägung nehmen wir als Kriterium für Ausschreibungen mit auf, eine Abweichung von diesem Grundsatz muss begründet werden. Die Stadt unterhält ein öffentlich zugängliches Open Source

- „KoaV 2025“ zwischen CDU, CSU und SPD: „Verantwortung für Deutschland“

> **Wir sorgen für unsere digitale Souveränität**
>
> Wir definieren Ebenen übergreifend offene Schnittstellen, offene Standards und treiben Open Source mit den privaten und öffentlichen Akteuren im europäischen Ökosystem gezielt voran, unter anderem

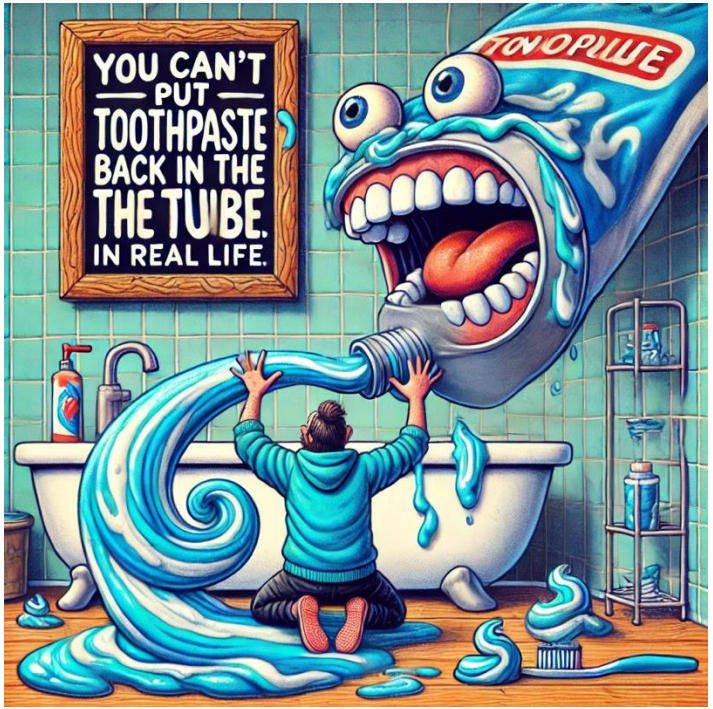
https://www.koalitionsvertrag2025.de/sites/www.koalitionsvertrag2025.de/files/koav_2025.pdf

Wege zur Herstellung digitaler Souveränität

Eine Mission Impossible?

Zur Erinnerung:

- **72 % der Anteile** im europäischen Cloud-Markt halten Amazon, Microsoft, Google
- **96 % der Beschäftigten** in deutschen Behörden arbeiten mit Microsoft Software
- **80 % der deutschen Verwaltungsdaten** in Datenbanken US-amerikanischer Anbieter



„Lösungen“ auf einen Blick

- US-amerikanische Software in europäischen „**Mantel-Unternehmen**“
- „bindende“ „**Digital Resilience Commitment**“-Klauseln in Lizenzverträgen mit Microsoft
- **Notfallpläne**, Bewertungssystem für Souveränität, risikoorientierte Szenarien-Planung, Schwachstellenanalyse
- **Sukzessive Reduzierung der Abhängigkeiten (De-Risking)**
- **Wettbewerb** auf bestehendem Markt fördern, echte Wahlfreiheit schaffen
- **Multi-Cloud-Strategie**
- **Konsequenter Umstieg auf Open-Source und offene Standards beim Aufbau eigener, souveräner IT-Infrastruktur**
- OS-Mindestanteil bei öffentlicher Beschaffung (**OS-Grundsatz**)
- Europaweite Kooperation und Zusammenarbeit bei dem Aufbau einer gemeinsamen **europäischen Souveränitätsinfrastruktur**
- OS-Grundsatz normativ verankern (**Public Money, Public Code**).
- **Mut und starker politischer Wille:** „Digitalpolitik ist Machtpolitik“

Herstellung digitaler Souveränität

- Wir haben den Weckruf gehört.
- Aber wann stehen wir auf?

Technologien

Politik

Recht

Alternativen entwickeln bzw. nutzen!

Technologien

Entwicklung europäischer Alternativen zu den US-Anbietern

enisa | EUROPEAN UNION VULNERABILITY DATABASE

DERSTANDARD

CVE: Aus für Sicherheitslücken-Datenbank in letzter Minute abgewendet, EU arbeitet an Alternative

Die US-Cybersicherheitsbehörde Cisa finanziert den Betrieb für elf Monate weiter, die European Vulnerability Database gibt es in einer ersten Testversion

Alternativen entwickeln bzw. nutzen!

Technologien

Entwicklung europäischer Alternativen zu den US-Anbietern

Nextcloud

Proton Mail

Linux™

gaia-x

gescheitert?!

Rahmenbedingungen verbessern!

Politik

Klarheit schaffen bei den Bedürfnissen: Strategieentwicklung

Bundesministerium
für Digitales und
Staatsmodernisierung

Digitale Souveränität sichern

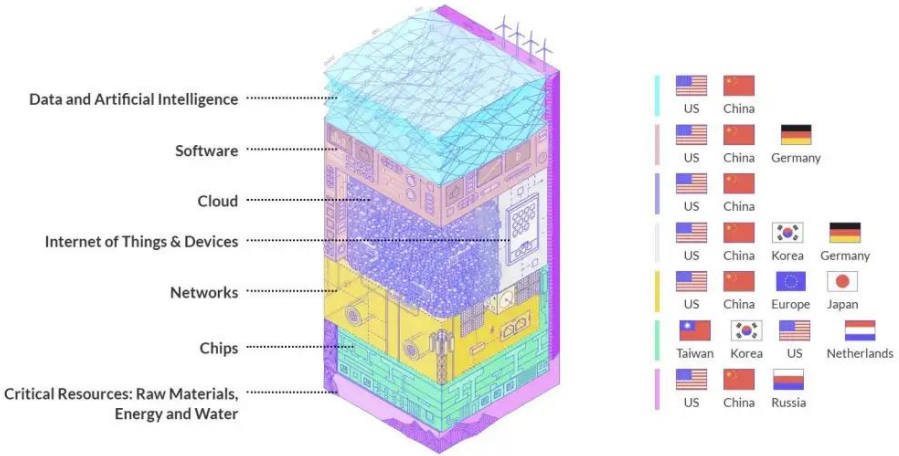
Die jüngsten geopolitischen Krisen zeigen: Technologische Abhängigkeiten sind ein strategisches Risiko. Deutschland richtet seine Digitalpolitik neu aus – mit einem klaren Ziel: mehr Eigenständigkeit und Sicherheit durch europäische Kooperation und Investitionen in Schlüsseltechnologien.

Digitalminister will offene Standards und Open Source zum Leitprinzip machen

Digitalminister Wildberger macht sich auf der re:publica für mehr Souveränität stark und fordert Alternativen auch beim digitalen Zahlen und Social Media.

https://www.heise.de/news/Digitalminister-will-offene-Standards-und-Open-Source-zum-Leitprinzip-machen-10412300.html

Rahmenbedingungen verbessern!



EuroStack – A European Alternative for Digital Sovereignty

© EuroStack

In Europa und in den Mitgliedstaaten

Recht versus Unrecht: Kann man (digitale) Souveränität erzwingen?

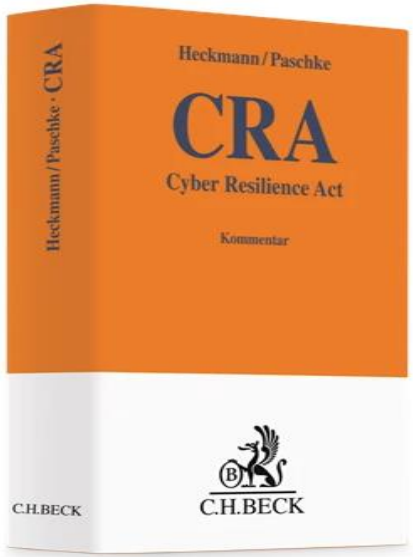
Recht

Rechtlicher Rahmen: europäische Ebene

Art. 24, 25 CRA

Pflichten der Verwalter quelloffener Software

Sicherheitsbescheinigungen für freie und quelloffene Software



https://www.beck-shop.de/heckmann-paschke-cyber-resilience-act-cra

Rechtlicher Rahmen: Bundesebene

§ 4 Abs. 3 OZG

Elektronische Abwicklung von Verwaltungsverfahren; (...)

(...) (3) Bei der Bereitstellung der IT-Komponenten im Sinne des Absatzes 1 **sollen** offene Standards und offene Schnittstellen verwendet werden und **soll** Open-Source-Software **vorrangig** vor solcher Software eingesetzt werden, deren Quellcode nicht öffentlich zugänglich ist oder deren Lizenz die Verwendung, Weitergabe und Veränderung einschränkt.

§ 16a EGovG

Open Source

Die Behörden des Bundes **sollen** offene Standards nutzen und bei neu anzuschaffender Software Open-Source-Software **vorrangig** vor solcher Software beschaffen, deren Quellcode nicht öffentlich zugänglich ist oder deren Lizenz die Verwendung, Weitergabe und Veränderung einschränkt.

Rechtlicher Rahmen: Landesebene (Bsp.: Bremen)

Gesetz zur Gewährleistung der digitalen Souveränität der Freien Hansestadt Bremen - Land und Stadtgemeinde -

DRUCKEN SENDEN

Veröffentlichungsdatum: 26.07.2022 **Inkrafttreten** 01.01.2023
Fundstelle Brem.GBl. 2022, S. 420
Zitiervorschlag: "Gesetz zur Gewährleistung der digitalen Souveränität der Freien Hansestadt Bremen - Land und Stadtgemeinde - vom 12. Juli 2022 (Brem.GBl. 2022, S. 420)"

§ 1

IT-Sicherheit und digitale Souveränität, Verlässlichkeit der Versorgung

(1) Zur Gewährleistung der öffentlichen digitalen Daseinsvorsorge und einer dafür erforderlichen weitreichenden digitalen Souveränität der öffentlichen Verwaltung darf die Freie Hansestadt Bremen (Land) Verträge über Leistungen zur Deckung ihres IT-Bedarfs ausschließlich mit einer anderen juristischen Person des öffentlichen Rechts, zu der das Verhältnis einer öffentlich-öffentlichen Zusammenarbeit im Sinne von § 108 des Gesetzes gegen Wettbewerbsbeschränkungen besteht, schließen. Die Stadtgemeinde Bremen darf Verträge im Sinne des Satzes 1 mit der Freien Hansestadt Bremen (Land) sowie den in Satz 1 benannten Auftragnehmern schließen.

(2) Die Einbeziehung von Unternehmen, welche den Voraussetzungen des Absatzes 1 nicht genügen (sonstige Unternehmen), zur Erfüllung eines Vertrages durch die juristische Person des öffentlichen Rechts als Auftragnehmerin soll nur erfolgen, wenn andernfalls unverhältnismäßige Nachteile zu befürchten sind. Unverhältnismäßige Nachteile liegen insbesondere vor, wenn Leistungen für die Deckung des IT-Bedarfs notwendig sind, die nur von sonstigen Unternehmen hergestellt oder angeboten werden oder wenn der Einsatz von Lösungen der juristischen Person des öffentlichen Rechts qualitativ oder quantitativ deutlich schlechtere Ergebnisse als eine Lösung eines privaten Anbieters begründet erwarten lässt. In Fällen, in denen Verträge über die in Absatz 1, Satz 1 genannten Beschaffungen vor Inkrafttreten dieses Gesetzes mit sonstigen Unternehmen geschlossen wurden, dürfen diese Verträge bis zum Ablauf der vertraglichen Bindung fortgeführt werden.

Rechtlicher Rahmen: Landesebene (Bsp.: Bayern)

BayDiG Text gilt ab: 01.01.2025 Fassung: 22.07.2022 **Gesamtansicht**

Art. 3 Digitale Entscheidungsfähigkeit des Freistaates Bayern

(1) [1]Die eigenständige digitale Entscheidungs- und Handlungsfähigkeit des Freistaates Bayern ist durch geeignete Maßnahmen zu sichern. [2]Der Freistaat Bayern unterhält hierfür staatliche Rechenzentren und staatlich verfügbare Netze, geeignete Cloud-Dienste und weitere geeignete Technologien und Anwendungen. [3]Der Freistaat Bayern wirkt mit dem Bund und anderen Ländern im Bereich der Digitalisierung in geeigneter Weise zusammen.

(2) Der Freistaat Bayern schützt die Funktionsfähigkeit und den Zugang zu kritischen staatlichen Infrastrukturen und Netzen.

(3) Der Freistaat Bayern, die Gemeindeverbände und Gemeinden treffen nach Maßgabe dieses Gesetzes angemessene Maßnahmen zur Abwehr von Gefahren für die Sicherheit ihrer informationstechnischen Systeme.

(4) [1]Die Behörden des Freistaates Bayern sollen bei Neuanschaffungen offene Software verwenden und offene Austauschstandards nutzen, soweit dies wirtschaftlich und zweckmäßig ist. [2]Den Gemeindeverbänden und Gemeinden sowie den sonstigen Körperschaften des öffentlichen Rechts wird die Verwendung offener Software im Sinne des Satzes 1 empfohlen.

(5) Die Behörden des Freistaates Bayern sollen bei Neuanschaffungen von Software die Gebrauchstauglichkeit, das Benutzererlebnis und die Benutzerfreundlichkeit berücksichtigen sowie Nutzersicht und Wirtschaftlichkeit gleichrangig behandeln.

Umsetzen!

LibreOffice statt Word und Excel: Dänisches Ministerium sagt Tschüss zu Microsoft

Dänemark macht Ernst mit der Abkehr von marktbeherrschender US-Software. Das Ministerium für Digitalisierung will bis Herbst auf Open-Source-Programme umstellen.

12.06.2025, 09:22 ◇ 12.06.2025, 13:58

Thesen zur Offenheit als Grundlage eines souveränen Rechtsstaats

1. **Digitale Souveränität ist der Schlüssel für einen zukunftsfähigen, sicheren Rechtsstaat.**
   Geopolitische Krisen machen deutlich: Wir müssen unabhängig und resilient werden.
2. **Offene, vertrauenswürdige Technologien sind der Motor eines souveränen digitalen Ökosystems.**
   Was wir brauchen: ein klarer, gemeinsamer Fahrplan – technologisch, strategisch und rechtlich.

Thesen zur Offenheit als Grundlage eines souveränen Rechtsstaats

3. **Demokratie braucht digitale Unabhängigkeit.**
   Nur wer souverän handelt, kann unsere Grundwerte dauerhaft schützen.

4. **Souveränität gelingt nur gemeinsam.**
   Staat, Wirtschaft und Gesellschaft – Offenheit und Transparenz schaffen das nötige Vertrauen.

5. **Wir haben wenig Zeit.**
   Der beste Zeitpunkt zum Umdenken, entscheiden und handelt ist: jetzt!

Happy to discuss!

Dirk-Heckmann

dirk.heckmann@tum.de

www.TUM-CDPS.de