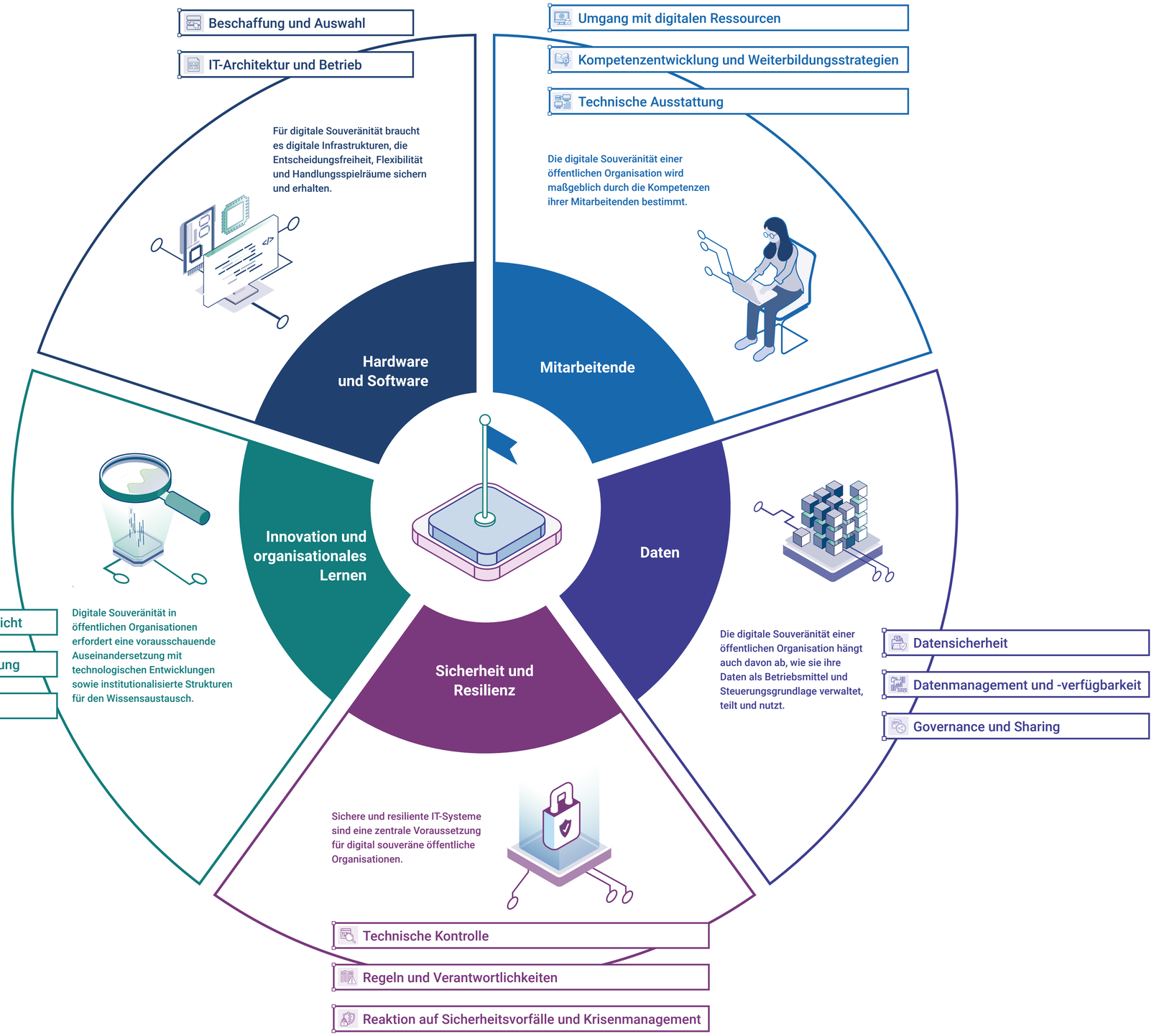
Kompetenzzentrum Öffentliche IT

ÖFIT-Wegbereiter

Digitale Souveränität

Gestaltungsfelder digitaler Souveränität



Datum, Projekt, Personen

Gefördert durch:
Bundesministerium des Innern
aufgrund eines Beschlusses des Deutschen Bundestages
Fraunhofer FOKUS

Kompetenzzentrum Öffentliche IT

ÖFIT-Wegbereiter

Digitale Souveränität

Hardware und Software

Für digitale Souveränität braucht es digitale Infrastrukturen, die die Entscheidungsfreiheit, Flexibilität und Handlungsspielräume sichern und erhalten.

Mitarbeitende +

Daten +

Sicherheit und Resilienz +

Innovation und organisationales Lernen +

Beschaffung und Auswahl

Wie können wir durch unsere Auswahl und Beschaffung von IT und IT-Dienstleistungen unsere künftige Entscheidungsfreiheit sicherstellen?

- Führen wir vor der Beschaffung von Software und Hardware Markterkundungen durch?
- Prüfen wir bei unseren Softwarebeschaffungen systematisch geeignete Open-Source-Alternativen?
- Kennen und berücksichtigen wir Angebote für die rechtssichere Nutzung von Open-Source-Software (OSS) für die öffentliche Verwaltung (z. B. Plattformen wie openCode.de)?
- Kooperieren wir wo möglich mit anderen Verwaltungen, um gemeinsam Anforderungen an IT-Anbieter zu definieren (z. B. in Arbeitskreisen, im Rahmen von Open-Source-Projekten oder Bietergemeinschaften)?
- Prüfen wir bei IT-Beschaffungen, in welchem Umfang IT-Produkte und -Dienstleistungen technische Offenheit bieten (z. B. offene, standardisierte Schnittstellen und Datenformate, Modularität)?
- Bewerten und dokumentieren wir vor Beschaffungen systematisch mögliche Abhängigkeiten und potenzielle Lock-in-Risiken (z. B. proprietäre Schnittstellen, fehlende Austauschbarkeit von Komponenten oder hohe Wechselkosten)?
- Stellen wir vor einer Beauftragung sicher, dass uns alle erforderlichen Informationen vorliegen, damit wir die Angebote fachlich, technisch, sicherheitsbezogen und datenschutzrechtlich bewerten können?
- Stellen wir bei der Auswahl von Hard- und Softwarekomponenten sicher, dass Anpassungen und Erweiterungen künftig mit angemessenen Kosten umsetzbar sind?
- Verzichten wir auf Online-Dienstleistungen, bei denen sich Anbieter vorbehalten, die Geschäftsbedingungen einseitig zu ändern? Falls nicht möglich: Achten wir besonders auf Risikomanagement-Maßnahmen (z. B. regelmäßige Datensicherung)?
- Verankern wir in unseren Ausschreibungen und Verträgen Anforderungen, die uns Einfluss auf die Produktgestaltung der Anbieter bieten oder vereinbaren wir alternative Sicherheitsmechanismen (z.B. verbindliche Portierungszusagen)?

IT-Architektur und Betrieb

Wie gestalten und betreiben wir unsere IT-Systeme so, dass sie flexibel und interoperabel sind – und mögliche Abhängigkeiten beherrschbar bleiben?

- Haben wir für unsere wichtigsten IT-Lösungen festgelegt, wie sie im Bedarfsfall kurzfristig durch Alternativen ersetzt werden können (z. B. verfügbare Ersatzlösungen, unkomplizierte Datenmigration durch standardisierte Formate, vertragliche Ausstiegsklauseln)?
- Betreiben wir kritische Anwendungen und Komponenten auf der Infrastruktur öffentlicher IT-Dienstleister oder vertrauenswürdiger europäischer Cloud-Anbieter?
- Unterziehen wir neue Softwareversionen und -updates zunächst einer internen Funktions- und Interoperabilitätsprüfung, bevor sie verteilt und in Betrieb genommen werden (z. B. hinsichtlich der Synchronisation von Server- und Klientensoftware bei Updates)?
- Befassen wir uns mit Möglichkeiten zum Ausstieg aus proprietären Lösungen (Exit) und sind uns Unterstützungsangebote bekannt (z. B. seitens des Zentrums für Digitale Souveränität ZenDis)?
- Falls wir Software(-komponenten) selbst entwickeln: Prüfen wir, ob durch uns entwickelte Lösungen durch andere nachgenutzt werden können und unterstützen dies?

Datum, Projekt, Personen

Gefördert durch:
Bundesministerium des Innern
aufgrund eines Beschlusses des Deutschen Bundestages
Fraunhofer FOKUS

Kompetenzzentrum Öffentliche IT

ÖFIT-Wegbereiter

Digitale Souveränität

Hardware und Software +

Daten +

Sicherheit und Resilienz +

Innovation und organisationales Lernen +

Mitarbeitende

Die digitale Souveränität einer öffentlichen Organisation wird maßgeblich durch die Kompetenzen ihrer Mitarbeitenden bestimmt.

Umgang mit digitalen Ressourcen

Wie stellen wir sicher, dass der Umgang mit unseren IT-Systemen und Daten selbstbestimmt und sicher erfolgt und keine Sicherheitsrisiken für unsere Organisation entstehen?

Haben alle Mitarbeitenden in unserer Organisation die erforderlichen Kenntnisse …

- … zur sicheren Nutzung unserer IT-Systeme (z. B. Schutz vor Malware)?
- … zum sicheren Umgang mit Daten, darunter auch sensible und personenbezogene Daten (z. B. Datensicherung und -ablage)?
- … zur sicheren elektronischen Kommunikation (z. B. Verschlüsseln von E-Mails, Erkennen von Phishing-Mails)?
- … für sicherheitsbewusstes Verhalten im Arbeitsalltag (z. B. umsichtiges Teilen von Informationen nach dem Need-to-Know-Prinzip, klare Kommunikationsregeln, Umgang mit externen Anfragen)?
- … für die digitale Arbeitsorganisation (z. B. zeit- und ortsunabhängiges Arbeiten, digitale Kommunikation)?

Verfügen spezialisierte Mitarbeitende in unserer Organisation über die erforderlichen IT-Fachkenntnisse …

- … zur selbstständigen Bewertung und bei Bedarf (Weiter-)Entwicklung bzw. Betrieb von bei uns eingesetzten IT-Lösungen?
- … zur IT-Sicherheit (z. B. Netzwerksicherheit, Sicherheitsarchitekturen)?

Kompetenzentwicklung und Weiterbildungsstrategien

Wie unterstützen wir die kontinuierliche Weiterentwicklung unserer Mitarbeitenden und stärken ihre Autonomie im Umgang mit digitalen Technologien?

- Identifizieren wir den Kompetenz- und Fortbildungsbedarf unserer Belegschaft laufend?
- Bieten wir allen Mitarbeitenden regelmäßig interne Weiterbildungen zu digitalen Grundkompetenzen an (z. B. Informationssicherheit, Datenschutz, grundlegende Datenkompetenz)? Fördern wir alternativ externe Weiterbildungsmaßnahmen finanziell oder bieten andere Incentives?
- Vermitteln wir unseren Mitarbeitenden im Rahmen interner Bildungsmaßnahmen gezielt Strategien, Richtlinien und Konzepte zur digitalen Governance?
- Bauen wir Kompetenzen für den Umgang mit Open-Source-Lösungen gezielt auf – sowohl für Anwender:innen als auch für technische Rollen?
- Fördern wir den Aufbau praxisorientierter Kompetenzen für neue Technologien (z. B. KI-Tools, Assistenzsysteme), einschließlich sicherer und verantwortungsvoller Anwendung?

Technische Ausstattung

Wie gewährleisten wir ein sicheres Arbeitsumfeld durch passende technische Ausstattung?

- Sind unsere Mitarbeitenden mit den notwendigen dienstlichen Geräten ausgestattet, einschließlich mobiler Geräte für das mobile Arbeiten? Planen und organisieren wir diese Ausstattung kontinuierlich?
- Sind unsere Beschaffungsprozesse so gestaltet, dass die notwendige IT-Ausstattung für unsere Mitarbeitenden schnell und bedarfsgerecht bereitgestellt wird?
- Haben wir klare, verbindliche Regeln zum Einsatz privater Geräte für organisationsinterne Zwecke (bring-your-own-device) und setzen sie durch?

Datum, Projekt, Personen

Gefördert durch:
Bundesministerium des Innern
aufgrund eines Beschlusses des Deutschen Bundestages
Fraunhofer FOKUS

Kompetenzzentrum Öffentliche IT

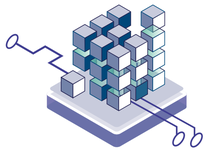
ÖFIT-Wegbereiter

Digitale Souveränität

Hardware und Software +

Mitarbeitende +

Daten −



Daten

Die digitale Souveränität einer öffentlichen Organisation hängt auch davon ab, wie sie ihre Daten als Betriebsmittel und Steuerungsgrundlage verwaltet, teilt und nutzt.

Sicherheit und Resilienz +

Innovation und organisationales Lernen +

Datensicherheit

Wie schützen wir unsere Daten vor unbefugtem Zugriff und sichern ihre Integrität?

- Haben wir ein aktuelles Informationssicherheits-Managementsystem?
- Verhindern technische und organisatorische Maßnahmen, dass unbefugte Dritte – externe wie interne – Zugriff auf unsere Daten haben?
- Übertragen wir schutzbedürftige Daten nur verschlüsselt?
- Sind entsprechend schutzbedürftige Daten mittels eines Datensicherheitskonzepts verschlüsselt geschützt und abgelegt? Erfolgt bei einer Ablage auf externen Servern die Verschlüsselung ausschließlich über die eigene Organisation?
- Sind mit sämtlichen externen Dienstleistern, die in unserem Auftrag Daten verarbeiten, rechtskonforme Auftragsverarbeitungsverträge (AVVs) abgeschlossen, die regelmäßig auf ihre fortbestehende Angemessenheit geprüft werden?
- Existieren Prozesse und Verantwortlichkeiten, um Datenleaks festzustellen, zu beheben und zu melden?

Datenmanagement und -verfügbarkeit

Wie gewährleisten wir die ordnungsgemäße Verwaltung unserer Daten und ihre Verfügbarkeit?

- Erstellen wir von relevanten Daten regelmäßig Backups?
- Halten wir unsere Daten ausschließlich auf internen Servern? Falls fremdadministrierte Cloudlösungen genutzt werden: Existiert ein Herausgabe- und Löschanspruch für die aufbewahrten Daten sowie eine Zustimmungspflicht bei der Übergabe gespeicherter Daten an einen neuen Betreiber?
- Überprüfen wir unsere Regeln und technischen Maßnahmen zum Umgang mit (insbesondere schutzbedürftigen) Daten regelmäßig und aktualisieren sie bei Bedarf?
- Gewährleisten technische und organisatorische Maßnahmen, dass die für einen geordneten Geschäftsbetrieb notwendigen Daten für die Mitarbeitenden angemessen verfügbar sind (z. B. redundante Datenhaltung, Edge Server, Load Balancing)?

Governance und Sharing

Wie nutzen und teilen wir Daten so, dass wir unsere Gestaltungsfähigkeit ausbauen und Zusammenarbeit ermöglichen?

- Haben wir definierte Rollen oder Zuständigkeiten für den Umgang mit Daten – etwa hinsichtlich Datenqualität, Datenzugang oder für die Koordination einer Datenstrategie (z. B. Chief Data Officer, Datenbeauftragte)?
- Setzen wir Datenqualitätsstandards ein und definieren Kriterien wie Konsistenz, Vollständigkeit oder Aktualität der Daten?
- Sind unsere Daten anhand anerkannter Metadatenstandards beschrieben, um diese gezielt auffindbar und nachnutzbar zu machen, auch, damit wir sie nach Möglichkeit leicht teilen können (z. B. Verwendung von DCAT-AP zur standardisierten Beschreibung)?

Datum, Projekt, Personen

Gefördert durch: Bundesministerium des Innern aufgrund eines Beschlusses des Deutschen Bundestages

Fraunhofer FOKUS

Kompetenzzentrum Öffentliche IT

ÖFIT-Wegbereiter

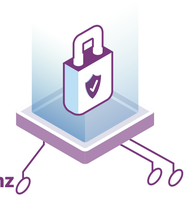
Digitale Souveränität

Hardware und Software +

Mitarbeitende +

Daten +

Sicherheit und Resilienz −



Sichere und resiliente IT-Systeme sind eine zentrale Voraussetzung für digital souveräne öffentliche Organisationen.

Innovation und organisationales Lernen +

Datum, Projekt, Personen

Technische Kontrolle

Wie gewährleisten wir die technische Sicherheit unserer IT-Komponenten und -systeme und wie schützen wir unsere Infrastruktur?

- Ist die Sicherheitszertifizierung der IT-Komponenten, wie z. B. CC-Zertifizierung, ein wesentliches Beschaffungskriterium?
- Binden wir nur Komponenten in unser Netzwerk ein, die zuvor einer Sicherheitsprüfung unterzogen wurden, z. B. gemäß BSI-Grundschutz?
- Existieren getrennte IT-Infrastrukturen oder Netze sowie spezifische Geräte für unterschiedliche Zwecke und Sicherheitsanforderungen (z. B. Gästenetz/ Gäste-WLAN)?
- Stellen wir die Einhaltung bestimmter Nutzungsregeln durch zentrale Konfiguration sicher (z. B. zur Wahrung eines erforderlichen Sicherheitsniveaus)?
- Verfügen wir über etablierte Standards sowie technische Maßnahmen zur Erkennung und koordinierten Abwehr von IT-Angriffen – und werden diese Schutzmechanismen regelmäßig aktualisiert (z. B. Firewalls, Virenscanner, IDS/IPS)?
- Werden Softwareupdates und notwendige Konfigurationsdaten zeitnah nach ihrer Veröffentlichung zentral koordiniert an alle relevanten Geräte verteilt und dort in Betrieb genommen?
- Schalten wir Softwarekomponenten, für die keine Sicherheits-Updates mehr bereitgestellt werden, mit dem Supportende ab und ersetzen sie?
- Verfolgen wir laufend IT-Sicherheitsmitteilungen, z. B. des BSI oder von CERTs, und leiten geeignete Reaktionen ein, wenn von uns eingesetzte Komponenten oder Dienste betroffen sein könnten?

Regeln und Verantwortlichkeiten

Wie fördern wir eine Sicherheitskultur und klare Verantwortlichkeiten?

- Verfügen wir über verbindliche und praxistaugliche Regeln für das Verhalten der Mitarbeitenden im Hinblick auf IT-Sicherheit (z. B. Regeln zum Angriffsschutz, Verhalten bei der Internetkommunikation)?
- Sind die organisationsinternen Verantwortlichkeiten und Rollen im Kontext IT-Sicherheit eindeutig festgelegt (z. B. IT-Sicherheitsbeauftragte, CDOs, Resilienzmanager) und verfügen die Verantwortlichen über die Befugnis, diese innerhalb der Organisation durchzusetzen?
- Üben wir das Zusammenspiel aller Beteiligten im Krisenfall regelmäßig und bewerten wir die Ergebnisse?

Reaktion auf Sicherheitsvorfälle und Krisenmanagement

Wie reagieren wir auf Sicherheitsvorfälle, damit Schäden möglichst gering bleiben?

- Haben wir klare technische und organisatorische Abläufe für Sicherheitsvorfälle festgelegt (z. B. Abschaltung infizierter Systeme?
- Sind für meldepflichtige Informationssicherheitsvorfälle Meldestellen, Meldewege und detaillierte Abläufe festgelegt und dokumentiert?
- Umfasst unsere Reaktion auf IT-Sicherheitsvorfälle neben Dokumentation, Schadensbehebung und Ursachenanalyse auch die Identifikation und proaktive Behebung ähnlicher Schwachstellen?

Gefördert durch:
Bundesministerium des Innern
aufgrund eines Beschlusses des Deutschen Bundestages
Fraunhofer FOKUS

Kompetenzzentrum Öffentliche IT

ÖFIT-Wegbereiter

Digitale Souveränität

Hardware und Software +

Mitarbeitende +

Daten +

Sicherheit und Resilienz +

−

Innovation und organisationales Lernen

Digitale Souveränität in öffentlichen Organisationen erfordert eine vorausschauende Auseinandersetzung mit technologischen Entwicklungen sowie institutionalisierte Strukturen für den Wissensaustausch.

Technologische Voraussicht

Wie stellen wir sicher, dass neue Technologien identifiziert und bewertet werden?

- Gibt es eine systematische Herangehensweise, um innovative digitale Werkzeuge zu identifizieren und ihre Eignung für unsere Aufgaben zu bewerten?
- Sind Zuständigkeiten und Verantwortlichkeiten für die strategische Identifizierung von Digitalisierungs- und Innovationsthemen festgelegt?
- Ist digitale Innovation integraler Bestandteil der Entwicklung der Organisation?
- Fördern wir interne Austauschformate, in denen Mitarbeitende innovative Ideen teilen können – und haben wir Strukturen, um diese systematisch zu erfassen, zu bewerten und weiterzuentwickeln?

Erprobung und Verankerung

Wie schaffen wir gute Bedingungen, um digitale Lösungen erproben zu können – und schlussendlich dauerhaft zu verankern?

- Führen wir Pilotprojekte durch, um digitale Lösungen in unserem Umfeld zu testen, bevor diese in den Regelbetrieb aufgenommen werden?
- Haben Mitarbeitende die Möglichkeit, neue digitale Ansätze in einem geschützten Rahmen auszuprobieren (z. B. geschützte Testplattform, Lern- oder Experimentierraum, Hackathons)?
- Gibt es in unserer Organisation Mechanismen zur systematischen Evaluation und Skalierung erfolgreicher Pilotprojekte?
- Existieren Prozesse, um erfolgreich erprobte Lösungen in der gesamten Organisation zu verankern?
- Wenden wir gezielte Methoden und Maßnahmen an, um Mitarbeitende bei der Einführung neuer Technologien aktiv einzubeziehen (z.B. Co-Creation-Formate, Feedback-Tools, Workshops)?
- Evaluieren wir regelmäßig die Effektivität und Effizienz neuer digitaler Werkzeuge und passen unsere Abläufe gegebenenfalls an?

Wissenstransfer

Wie schaffen wir hilfreiche Strukturen für den Wissens- und Erfahrungsaustausch?

- Verfügen wir über etablierte Strukturen, um systematisch Wissen und Erfahrungen aus anderen Organisationen (Verwaltung, ggf. auch Wirtschaft und Wissenschaft) zu erschließen und für unsere Organisation nutzbar zu machen?
- Ermöglichen wir unseren Mitarbeitenden, sich aktiv an externen Netzwerkformaten und Kooperationsprojekten zu beteiligen (z. B. Communities of Practice, Fach-/Anwendertreffen, gemeinsame Pilotprojekte) und stellen dafür organisatorische Unterstützung bereit (z. B. Zeit, Freistellung, Ressourcen)?

Datum, Projekt, Personen

Gefördert durch:
Bundesministerium des Innern
aufgrund eines Beschlusses des Deutschen Bundestages
Fraunhofer FOKUS