

Technologieradar 2024

IT-Perspektiven
für den Public Sector

Technologieradar 2024

IT-Perspektiven
für den Public Sector

Vorwort der BRZ-Geschäftsführung

In dieser Publikation, die das aktuelle Technologieradar sowie ausgewählte aktuelle Schwerpunktthemen enthält, werfen unsere Expertinnen und Experten des BRZ einen Blick auf die Technologien 2024 und liefern gleichzeitig eine fundierte Bewertung, inwieweit sich diese für eine Verwendung in der Zukunft der digitalen Verwaltung eignen. Der Blick in die Zukunft ist für uns als IT-Unternehmen besonders wichtig: Das BRZ ist das Kompetenzzentrum für die Digitalisierung in der österreichischen Bundesverwaltung. Als IT-Marktführer im Public Sector setzen wir moderne Technologien ein, um die Anforderungen von Kunden sowie der Bürgerinnen und Bürger an digitale Services und Anwendungen zu erfüllen.

Gamechanger künstliche Intelligenz

Eine dieser modernen Technologien ist die Anwendung von künstlicher Intelligenz (KI). Die Diskussion um KI-Anwendungen hat im Jahr 2023 einen enormen Aufschwung erlebt. Das BRZ nutzt KI bereits seit mehreren Jahren in einigen Anwendungen, etwa im Bereich der Betrugsbekämpfung, bei der Verarbeitung großer Datenmengen oder bei der Anonymisierung von personenbezogenen Daten. Generative KI hat großes Potenzial, auch für die Anwendung im öffentlichen Sektor. Mit dem AI-Act gibt es nun auch einen europäischen Regulierungsansatz, der den Schutz der Persönlichkeitsrechte, Grundrechte, Vertrauen und Sicherheit in den Vordergrund stellt.

Auch andere Technologien, etwa zur Erhöhung der Sicherheit von Computersystemen, sowie das Thema

Daten rücken 2024 in den Fokus und werden in den Schwerpunktkapiteln detailliert erörtert.

Digitale Transformation mitgestalten

Es ist unser Anspruch, die digitale Verwaltung der Zukunft mitzugestalten und Wege aufzuzeigen, wie die digitale Transformation mit entsprechender Technologie sinnvoll umgesetzt werden kann. Dafür entwickeln und betreiben unsere Mitarbeiterinnen und Mitarbeiter moderne IT-Lösungen, begleiten kreative Prozesse und arbeiten so erfolgreich an der IT-Zukunft Österreichs.

Roland Ledinger
Geschäftsführer BRZ

Christine Sumper-Billinger
Geschäftsführerin BRZ



Vorwort Florian Tursky

Das Technologieradar des BRZ zeigt auf, welche Technologien heute schon nutzbar sind und wo Potenziale für die Zukunft der digitalen Verwaltung liegen. Als Staatssekretär für Digitalisierung ist es mir ein Anliegen, Bürgerinnen und Bürgern sowie Unternehmen durch digitale Angebote das Leben zu erleichtern und Österreich als Wirtschaftsstandort zu stärken, denn die Digitalisierung bietet unglaubliche Chancen und erfasst alle gesellschaftlichen und wirtschaftlichen Bereiche. Im internationalen Vergleich kann sich Österreich regelmäßig an die Spitze von Rankings einreihen und wird für seine Projekte, etwa im Bereich der Nutzung von KI für die Verwaltung, mit Preisen ausgezeichnet.

Österreich ist Vorreiter

2023 wurde mit dem Start des Regelbetriebs der ID Austria ein Meilenstein in der Digitalisierung der österreichischen Verwaltung gesetzt und die Grundlage für die Umsetzung weiterer digitaler Ausweise gelegt. Rund 2,5 Millionen Bürgerinnen und Bürger nutzen bereits die ID Austria, Service Provider registrieren rund 300.000 Anmeldungen pro Tag. Österreich ist hier Vorreiter und gilt als Vorzeigemodell für die Umsetzung der europaweiten digitalen Identität.

Digitale Souveränität stärken

Die zunehmende Digitalisierung erfordert auch Anstrengungen, die digitale Souveränität Österreichs zu stärken. Diese ist von entscheidender Bedeutung, um nicht nur unsere nationale



Florian Tursky
Staatssekretär für
Digitalisierung (BMF)

Sicherheit zu gewährleisten, sondern auch unsere Gesellschaft vor potenziellen Risiken zu schützen, indem beispielsweise Abhängigkeiten von großen Softwarekonzernen verringert werden. Ein Schlüsselement des Digitalen Aktionsplans, der die strategische Transformation Österreichs steuert, ist der Digitale Souveränitätskompass, der als Orientierungsinstrument für die österreichische Verwaltung und kritische Infrastruktur dient. Dieser ermöglicht die Bewertung und Ableitung von kurz-, mittel- und langfristigen Maßnahmen zur Stärkung der Widerstandsfähigkeit.

Künstliche Intelligenz sicher nutzen

Künstliche Intelligenz ist ein Thema, das auch in der Verwaltung immer mehr an Bedeutung gewinnt. Unser Ziel ist es, KI-Lösungen im Sinn einer digitalen Verantwortungsgesellschaft und europäischer Werte einzusetzen. Die rasanten technologischen Entwicklungen und weitreichenden Auswirkungen auf die Gesellschaft zeigen den politischen Handlungsbedarf für eine klare gesetzliche Regulierung deutlich. Mit einem KI-Maßnahmenpaket und der neu eingerichteten KI-Servicestelle gewährleisten wir Transparenz, Rechtssicherheit und Kompetenzaufbau in der Bevölkerung und für Unternehmen.

Inhalt

- 4 **Vorwort der
BRZ-Geschäftsführung**
- 5 **Vorwort
Staatssekretär Florian Tursky**
- 8 **Technologieradar 2024**
- 24 **BRZ-Schwerpunktthemen**
- 26 Data Governance
- 39 Generative künstliche
Intelligenz (Generative AI)
- 50 Zero Trust

*Sie wollen noch
mehr über das BRZ
und seine Produkte wissen?*
**Bestellen Sie den
BRZ-Newsletter auf brz.gv.at**



Technologieradar 2024

Als Teil der BRZ-Strategie bildet das Technologiemanagement, angesiedelt im Bereich des Enterprise Architekturmanagements, die Basis für innovative Lösungen (Solutions) für unsere Kunden und den technologischen Fortschritt des Unternehmens insgesamt. Das BRZ prüft Trends vor allem in Richtung ihrer Anwendbarkeit für den öffentlichen Sektor. Auch für das Technologieradar 2024 wurden wieder neue Technologien untersucht. Technologien, die bereits in bestellbaren Produkten zum Einsatz kommen, werden sukzessive aus dem Radar entfernt - denn der Blick liegt in Richtung Zukunft.

Das Technologieradar 2024 unterstützt bei der Identifikation, Auswahl und Bewertung von Technologien sowie anderen organisationsrelevanten Schwerpunkten und bringt diese in einer Grafik („Radar“) übersichtlich auf den Punkt. Im Radar 2024 wird erneut zwischen vier Kernbereichen, die für die zeitgemäße Unternehmensführung und Service-Entwicklung essenziell sind, unterschieden: Im Bereich „Geschäftstrends“ werden Themen mit Fokus auf den Bereich Digital Government identifiziert. Der zweite Quadrant beleuchtet das Thema „Technologien“, der dritte Quadrant das Themenfeld „Methoden & Arbeitsweisen“ der Zukunft. Der Quadrant zum Thema „Touchpoint“ zeigt Technologien auf, die sich mit Anforderungen von Nutzerinnen und Nutzern und mit Fragen rund um deren Interaktion mit digitalen Anwendungen und Technologien beschäftigen.

Neuerungen im Technologieradar 2024

- Zwölf Technologien wurden neu hinzugefügt, einige überarbeitet.
- Bring Your Own Environment (BYOE) wurde zum Bereich „Touchpoint“ verschoben.
- Data Driven Decision Support ersetzt Decision Intelligence und befindet sich nun im Bereich „Geschäftstrends“.
- Digitale Souveränität der Person wurde mit Self Sovereign Identity zusammengeführt.

Neu hinzugekommen:

Bereich Technologie

- Kognitive Services
- AI Copilot
- Retrieval Augmented Generation
- Cybersecurity Mesh
- LLM (Large Language Model)
- Generative KI

Bereich Touchpoint

- Demokratisierung der Technologie
- Integrierte One Stop Shops

Bereich Methoden & Arbeitsweisen

- Prompt Engineering
- Data Governance

Bereich Geschäftstrends

- Diversity, Equity and Inclusion in IT
- Data Driven Decision Support

Nicht mehr im Technologieradar enthalten:

- Small Data
- Blockchain
- SAFE®

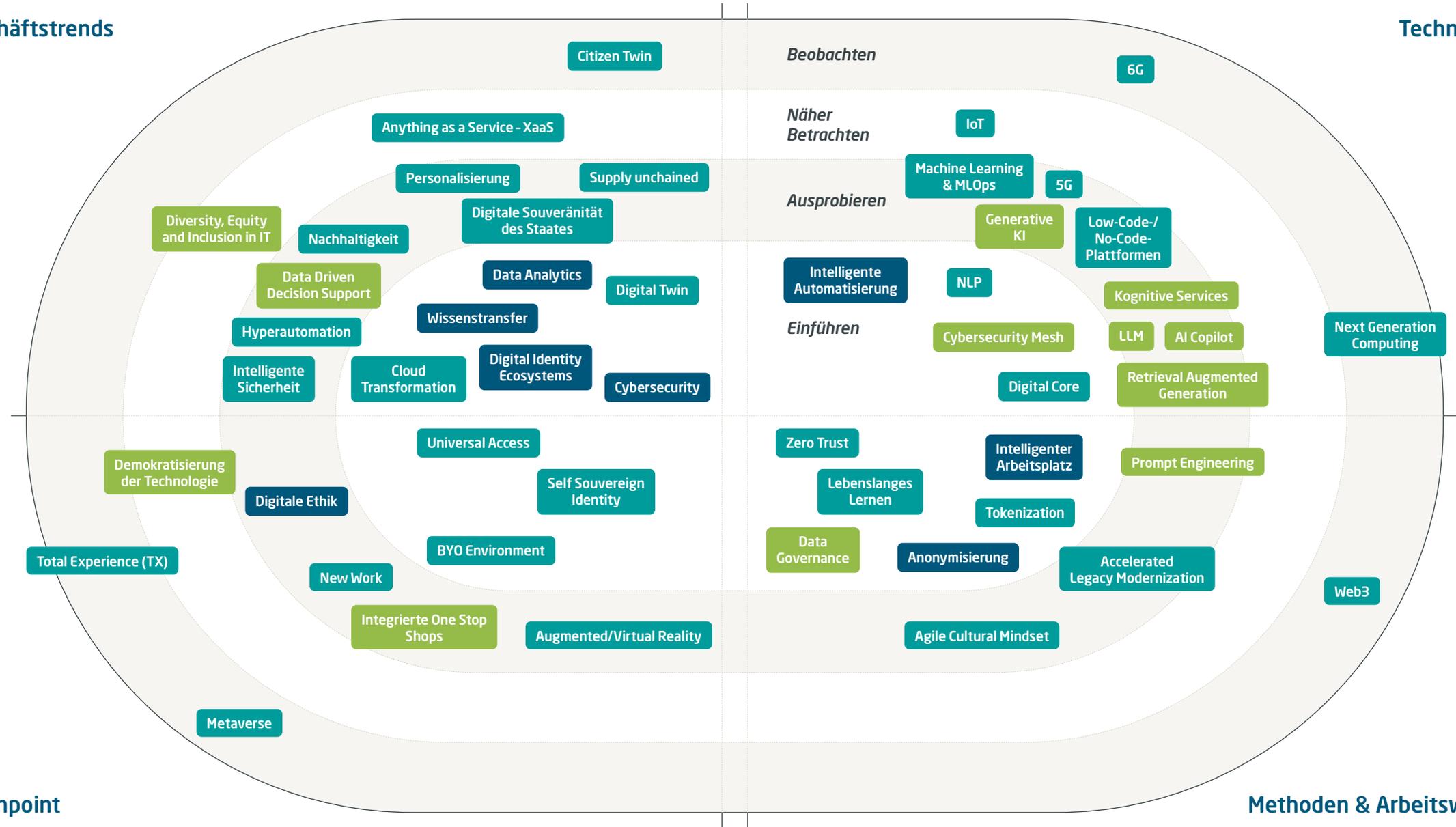
Abbildung 1:

Technologieradar 2024

Geschäftstrends



Technologie



 **Technologie**

Begriff	Anwendung im Public Sector	Status
5G/6G	Aktuell sind laut der International Telecommunication Union (ITU) 5,3 Milliarden Menschen online. Das Netzwerk ist die Basis aller Kommunikation. 5G macht hier keine Ausnahme. Und doch ist 5G nur eine Neuerung, die eine Geschwindigkeitserhöhung im Fokus hat und sonst wenig Innovation bietet. Der Netzausbau ist in den österreichischen Ballungsräumen mittlerweile auf hohem Niveau, andererseits sind die Endgeräte der Nutzer:innen noch nicht im großen Umfang 5G-tauglich. Auch werden bei Weitem nicht alle mit 5G möglichen Use Cases in Österreich umgesetzt. 6G ist der generische Name für den Mobilfunk der nächsten Generation. Die 6. Generation des Mobilfunks wird die aktuellen 5G-Fähigkeiten verbessern und diese hinsichtlich Spitzendatenrate (z. B. 100 Gbps bis 1 Tbps), Verbindungsdichte und Energieeffizienz deutlich übertreffen. Funktionen und der Zeitplan für 6G sind noch nicht final definiert, der kommerzielle Start ist um 2030 zu erwarten. Wichtig erscheint seit 5G auch die Verkürzung der Latenzzeit, damit Ortung und Lokalisierung wirklich im Sub-Meterbereich möglich wird. Das ist eine Voraussetzung für selbstfahrenden Verkehr und ähnliche Anwendungen.	Beobachten/ Ausprobieren
Next Generation Computing	<p>Computertechnologien, die neue Algorithmen und bisher nicht erreichbare Geschwindigkeiten und Speicherkapazitäten ermöglichen:</p> <p>Quantum Computing</p> <p>Die Forschung für Quantum Computing ist intensiv, die Erwartungen sind hochgesteckt. Dass daraus ein Computer entstehen kann, der Bürgerinnen und Bürgern als Endgerät für die tägliche Arbeit zur Verfügung steht, ist aus heutiger Sicht keine realistische Erwartungshaltung. Services, die auf Quantum Computing basieren, werden eher als Cloud-Service konsumierbar sein.</p> <p>Anwendungsgebiete, die das Potenzial für Realisierung haben:</p> <ul style="list-style-type: none"> > Optimierungsaufgaben, etwa in den Bereichen Finanzwirtschaft und Logistik sowie Optimierungen von Forschungsmodellen > Simulationen, beispielsweise um neue chemische Stoffe für Biotechnologie oder Medikamente zu finden > maschinelle Lernverfahren, etwa als quantenmaschinelles Lernen für verschiedenste Aufgabengebiete wie Mustererkennung > Generierung von echten Zufallszahlen <p>DNA-Computing</p> <p>Kann man das gesamte Internet, wie wir es heute kennen, auf einem Speicher in der Größe eines Schuhkartons sichern? DNA-Computing will dies möglich machen. Im Unterschied zu Quantum Computing verspricht DNA-Computing eine sehr hohe Speicherdichte und einen niedrigen Energieverbrauch. Die praktische Anwendung liegt derzeit noch in der Zukunft, allerdings lassen erste Berechnungen eine Speicherkapazität von 215 Petabyte Daten auf einem Gramm DNA-Erbinformation erwarten. Wegen der langsamen Reaktionszeiten von biomolekularen Einheiten wird auch an einer Kombination von elektrischen und biomolekularen Strukturen geforscht.</p>	Beobachten

Begriff	Anwendung im Public Sector	Status
NEU SCHWERPUNKTTHEMA Generative KI (Generative AI)	Obwohl künstliche Intelligenz (KI) schon seit Jahrzehnten existiert, hat die Einführung von ChatGPT im November 2022 das Potenzial dieser Technologie offengelegt. Diese Technologien werden unseren Zugang zur digitalen Welt verändern. Unter generativer KI versteht man die Fähigkeit von KI-Modellen, neue Variationen von Inhalten zu erstellen, darunter Bilder, Videos, Audio und Text. Generative KI-Anwendungen haben das Potenzial, ein breites Spektrum an Aufgaben zu automatisieren, wodurch die Produktivität gesteigert, Kosten gesenkt und neue Wachstumschancen eröffnet werden. Generative KI-Plattformen sind weltweit verfügbar und bieten allen Benutzerinnen und Benutzern generative Fähigkeiten. Die Demokratisierung von Informationen und Fähigkeiten wird sich auf ein breites Spektrum der Gesellschaft auswirken. Damit ist generative KI einer der disruptivsten Trends der 2020er-Jahre.	Ausprobieren
NEU Large Language Model (LLM)	Ein Large Language Model (LLM) ist die technologische Weiterentwicklung des Sprachmodellkonzepts in der künstlichen Intelligenz, die durch Anlernen von riesigen Datenmengen die Fähigkeiten dieser KI dramatisch erweitert. Mit sogenannten Deep-Learning-Techniken lassen sich diese Datensätze verwenden, um neue Inhalte zu verstehen, zusammenzufassen und zu generieren. Das LLM ist auch stark mit dem Trend „generative KI“ verbunden, bei der es sich tatsächlich um eine Art der künstlichen Intelligenz handelt, die speziell für die Generierung von für Menschen verständliche und natürliche Kommunikation entwickelt wurde. Die Modalität ist dabei nicht auf Text bzw. Sprache beschränkt, andere Modalitäten sind etwa Bilder, Videos und Audio. Sprachmodelle werden häufig in NLP-Anwendungen (Natural Language Processing) verwendet, bei denen eine Benutzer:in eine Abfrage in natürlicher Sprache eingibt, um ein Ergebnis zu generieren.	Ausprobieren
NEU AI Copilot	Mit dem Durchbruch der generativen KI (Generative AI) kommen Tools auf den Markt, die die Effizienz von bestehenden Tools deutlich verändern. Die Softwareentwicklung ist eine der ersten Branchen, die diese Fähigkeiten in ihre Entwicklungsumgebungen integrieren wird oder bereits integriert hat. Wenn auch nicht der Code selbst verbessert wird, weil der Code aus dem Internet auch nur durchschnittliche Qualität hat, so wird jedenfalls die Geschwindigkeit deutlich gesteigert, mit der geprüfter Code ausgeliefert werden kann. Das Angebot an Copiloten wächst exponentiell.	Ausprobieren
NEU Retrieval Augmented Generation (RAG)	Retrieval Augmented Generation (RAG) ist eine Technik zur Verarbeitung natürlicher Sprache (NLP), die die Stärken von abfragebasierten und generativen Modellen der künstlichen Intelligenz (KI) kombiniert. RAG-KI kann genaue Ergebnisse liefern, die bereits vorhandenes Wissen optimal nutzen. Sie kann dieses Wissen aber auch verarbeiten und konsolidieren, um einzigartige, kontextbezogene Antworten, Anweisungen oder Erklärungen in menschenähnlicher Sprache zu erstellen, anstatt nur die abgefragten Daten zusammenzufassen. RAG-KI erweitert das Potenzial von generativer KI. Die Technik vereint die Stärken von generativer KI und abfragebasierter KI. Sie unterscheidet sich von kognitiver KI, die zum Erzielen ihrer Ergebnisse die Arbeitsweise des menschlichen Gehirns nachahmt.	Ausprobieren
NEU Kognitive Services	Kognitive Services sind KI-Lösungen, die basierend auf menschlichem Verhalten entwickelt wurden. Dabei werden Bereiche wie Sprache, Seh- und Lernvermögen imitiert. Text-to-Speech wandelt Texteingaben in Sprachausgabe um. Maschinelles Sehen (computer vision) bietet eine automatische Erkennung von Objekten auf Bildern und Videos. Dabei werden Technologien aus dem Bereich der künstlichen Intelligenz verwendet.	Ausprobieren

Begriff	Anwendung im Public Sector	Status
Low-Code-/No-Code-Plattformen	Entwickler:innen und Engineers sind begehrte Mitarbeiter:innen und die digitale Transformation erzeugt eine steigende Nachfrage am Arbeitsmarkt. Neue Plattformen versprechen, aus jeder Mitarbeiterin und jedem Mitarbeiter eine Technologin bzw. einen Technologen zu machen und so zu einer Demokratisierung der Technologie beizutragen. Auch Low-Code-/No-Code-Plattformen können mit KI-Technologien angereichert werden. Starke Konkurrenz zu diesem Ansatz wird von den diversen AI Copiloten erwartet.	Ausprobieren
Internet of Things (IoT)	IoT (Internet of Things) ist ein Sammelbegriff für Technologien, die es ermöglichen, physische und virtuelle Objekte, Sensoren etc. miteinander zu vernetzen. Im Government-Umfeld können z. B. Mautsysteme oder Verkehrsleitsysteme mit IoT unterstützt werden.	Näher Betrachten
NEU Cybersecurity Mesh Architecture (CSMA)	Cybersecurity Mesh ist ein Begriff, der sich auf ein Netzwerk von Sicherheitsmaßnahmen und -technologien bezieht, die miteinander verbunden sind, um so eine umfassende und effektive Abwehr gegen Cyberbedrohungen zu gewährleisten. Es ermöglicht eine nahtlose Integration von Sicherheitslösungen und verbessert die Reaktionsfähigkeit auf Angriffe. Das Zero-Trust-Konzept ist die methodische Grundlage dieses Trends, der von Gartner geprägt worden ist. Viele Hersteller entwickeln ihre Security-Technologien in diese Richtung weiter. Kritisch gesehen wird, dass die gesamte Security dadurch oft von einem Hersteller bereitgestellt wird. Die Technologien oder Technologiekombinationen sind die Antwort auf die exponentiell gestiegenen Sicherheitsanforderungen im modernen Cloud Computing und Mobile Working.	Einführen
Machine Learning und MLOps	Machine Learning zählt zu den wichtigsten Teilgebieten aus dem Bereich der künstlichen Intelligenz und ist derzeit auch am weitesten fortgeschritten. Hier zeichnet sich ein Trend hin zu standardisierter Entwicklung und Bereitstellung für die spätere Wiederverwendung von Modellen ab. Dazu werden DevOps-Ansätze weiterentwickelt und zunehmend automatisiert. Das Spannungsfeld von Datenschutz und Privacy ist vor allem in der digitalen Verwaltung zu beachten. Auch hier bestehen bereits Lösungen zur gezielten Anonymisierung von Daten, um Anforderungen des Datenschutzes gerecht werden zu können.	Ausprobieren
Digital Core	Der Begriff „Digital Core“ bezieht sich auf das zentrale digitale Fundament eines Unternehmens oder einer Organisation. Es umfasst die technologischen und organisatorischen Elemente, die für die digitale Transformation und den Betrieb des Unternehmens in der digitalen Welt erforderlich sind. Der digitale Kern besteht aus verschiedenen Komponenten, wie z. B. einer integrierten Unternehmenssoftware (ERP-System), Datenbanken, Cloud-Infrastruktur, Analyse-Tools und digitalen Prozessen. Der digitale Kern ermöglicht es Unternehmen, ihre Geschäftsprozesse zu automatisieren, Daten effizient zu verwalten, Echtzeitinformationen zu nutzen und digitale Innovationen voranzutreiben. Ein starker digitaler Kern ist entscheidend, um wettbewerbsfähig zu bleiben und den Anforderungen einer zunehmend digitalisierten Welt gerecht zu werden. Digital-Core-Initiativen sind oft verbunden mit der Transformation in die Cloud.	Einführen
Natural Language Processing (NLP)	Es handelt sich um einen Bereich der KI, der sich mit der Interaktion zwischen menschlicher Sprache und Computern befasst. NLP ermöglicht es Computern, menschliche Sprache zu verstehen, zu analysieren und darauf zu reagieren. Es umfasst Techniken wie Texterkennung, Spracherkennung, Textklassifizierung, Sentimentanalyse, maschinelles Übersetzen und Frage-Antwort-Systeme. NLP wird in verschiedenen Anwendungen eingesetzt, wie z. B. bei Chatbots, Sprachassistenten, automatisierten Übersetzungen, Textanalysen und bei der Informationsextraktion. Infolgedessen ermöglicht NLP eine Vielzahl von Anwendungen und Automatisierungen, die zuvor maschinell nicht möglich waren, und bietet Unternehmen ein erhebliches Maß an Prozessverbesserung.	Einführen

Begriff	Anwendung im Public Sector	Status
Intelligente Automatisierung/ Intelligent Process Automation (IPA)	IPA (Intelligent Process Automation) definiert sich als eine Vielzahl von Technologien und Methoden, mit denen Abläufe effizienter gestaltet werden können. Das umfasst die Automatisierung von regelbasierten Abläufen mittels Robotic Process Automation (RPA) sowie die Einbindung von intelligenten digitalen Assistenten für die Kommunikation mit Nutzer:innen und Nutzern. Weiterer Bestandteil ist künstliche Intelligenz, die bei der Analyse großer Datenmengen und der Unterstützung bei der Entscheidungsfindung in komplexen Situationen eingesetzt wird.	Einführen

 **Geschäftstrends**

Begriff	Anwendung im Public Sector	Status
Supply unchained	Schon vor der Pandemie haben Unternehmen begonnen, Vertriebskanäle und Supply Chains zu modernisieren. Die teilweise Unterbrechung globaler Lieferketten in der COVID-19-Pandemie hat die Entwicklung der erforderlichen Technologien beschleunigt. Diese Technologien werden auch über die Krise hinaus eingesetzt. Unified Commerce oder Supply Unchained verknüpfen Informationstechnologie (IT) und operative Technologie (OT) auf ganzem Wege. Über die gesamte Lieferkette hinweg werden umfassend Daten gesammelt, verarbeitet und geteilt. Engpässe und Logistikprobleme können so bereits vorab erkannt werden. Die User Experience steigt durch diese detaillierte Information deutlich. Technologische Treiber sind Internet of Things (IoT), Edge Computing und Robotic Process Automation.	Ausprobieren
Personalisierung	Personalisierung soll eine maßgeschneiderte direkte Ansprache ermöglichen, die auf individuelle Bedürfnisse und Anforderungen von Kundinnen und Kunden eingeht. Es handelt sich um die Anpassung einer Dienstleistung oder eines Produktes auf Basis von verfügbaren Informationen und Daten. In Zeiten von „New Work“ kann damit auch die soziale Kommunikation und Zusammenarbeit gefördert und so positiv auf die Produktivität gewirkt werden.	Ausprobieren
NEU Data Driven Decision Support	Entscheidungsintelligenz in der Verwaltung ist eine angewandte Disziplin, die die Entscheidungsfindung verbessert, indem sie explizit versteht, wie Entscheidungen getroffen werden und wie ihre Ergebnisse durch Rückmeldung bewertet und verbessert werden. Um dies zu unterstützen, setzt sie systematisch datengesteuerte Technologien wie künstliche Intelligenz (KI) und fortschrittliche Analytik in jeder Phase der Tätigkeit ein. Entscheidungsintelligenz gilt für alle wichtigen Ebenen von Entscheidungstypen: einmalige strategische Entscheidungen, Managemententscheidungen und umfangreiche operative Entscheidungen.	Ausprobieren
Digitale Souveränität des Staates	Ein Staat oder Staatenbund ist im Idealfall dann digital souverän, wenn er in seinem Zuständigkeitsbereich selbstbestimmt handeln und das Monopol der Staatsgewalt auch ausschließlich ausüben kann, d. h. auch gegen den Widerstand anderer Staaten und insbesondere nichtstaatlicher Akteure. Durch die zunehmende Digitalisierung der Verwaltung und deren Services ist besonderes Augenmerk darauf zu legen, dass die dabei eingesetzten Produkte und Dienstleister die digitale Souveränität (u. a. durch Herstellerabhängigkeit, rechtliche Bedingungen je Anbieter-/Datenstandort, Informationssicherheit) nicht schwächen oder gar sukzessive abbauen. Digitale Souveränität ist auch ein wesentlicher Aspekt bei der Betrachtung von Cloud-Services für die öffentliche Verwaltung.	Ausprobieren

Begriff	Anwendung im Public Sector	Status
Digital Twin (Digitaler Zwilling)	Die virtuelle Repräsentation eines physischen Objekts wird als digitaler Doppelgänger, digitaler Zwilling oder „Digital Twin“ bezeichnet. Im öffentlichen Bereich können digitale Zwillinge vor allem zur Simulation der Auswirkungen von Regulierung und Gesetzgebung auf die Gesellschaft eingesetzt werden. Es gibt bereits zahlreiche Studien in verschiedenen Staaten, das Digital-Twin-Konzept auf weitere Anwendungsgebiete in der Verwaltung auszudehnen (USA, Kanada, EU).	Einführen
Nachhaltigkeit	Die Herausforderung der Erhaltung unseres Planeten als lebensfreundliche Umgebung kann nur mit nachhaltigen Änderungen in Ressourcenverbrauch und Lebensweise gelingen. Diese Veränderungen hin zur Nachhaltigkeit werden von Bürgerinnen und Bürgern genauso wie von Organisationen und Unternehmen getragen werden müssen, der Gesetzgeber muss dafür den erforderlichen Rahmen schaffen. Informationstechnologie ist hier ein zentraler Baustein, denn sie ermöglicht die Messung und Prognose der aktuellen und künftigen Wirkung der Maßnahmen. Überdies schafft sie Transparenz und zeigt Potenziale zur Effizienzsteigerung (z. B. Abfallreduktion, Energiereduktion) auf und kann diese automatisiert zur Verfügung stellen. Auch die IT selbst ist nachhaltig zu gestalten. Zurzeit haben Technologien, die das größte Potenzial zur Verbesserung der Nachhaltigkeit haben, auch den größten ökologischen Fußabdruck. Technologien wie Blockchain und KI können nachhaltige Lösungen ermöglichen, aber auch erheblich zum Ausstoß von Treibhausgasen beitragen.	Ausprobieren
Data Analytics	Ziel ist es, nützliche Informationen, Muster und Korrelationen aus Datenmengen erkennen zu können und damit Optimierungspotenziale für Unternehmensprozesse zu identifizieren. Hier können neue Use Cases für die Verwaltung, auch gemeinsam mit Partnerkörperschaften entstehen. Mithilfe von Echtzeitanalysen können bestehende Anwendungen verbessert werden, indem der Status eines Bearbeitungsprozesses (z. B. die Anfrage eines behördlichen Dokuments) abgefragt wird. Mittels Einbindung von Schnittstellen in (vorhandene) Anwendungen kann in Echtzeit der Fall nachvollzogen und analysiert werden. Diese Entwicklung schafft einerseits mehr Transparenz und Effizienz, andererseits eine höhere Kundenzufriedenheit.	Einführen
Pensionierungsmanagement (Wissenstransfer)	Die bevorstehende Pensionierungswelle im öffentlichen Dienst erfordert von Organisationen ein verstärktes Augenmerk auf den effizienten Wissenstransfer. Mit dem Ausscheiden erfahrener Mitarbeiter:innen gehen wertvolle Kenntnisse und Erfahrungen verloren. In dieser Hinsicht ist es unabdingbar, dass Organisationen auf technologische Lösungen setzen, um dieses Wissen zu dokumentieren, zu speichern und nahtlos zu übertragen. Ein niederschwelliger Zugang zum Wissenstransfer spielt dabei eine entscheidende Rolle. Digitale intelligente Lösungen, vernetzte Wissensdatenbanken und Kollaborations-Tools erleichtern die Erfassung und Weitergabe des Know-hows der ausscheidenden Mitarbeitenden. Der gezielte Einsatz von Wissensmanagementtechnologie gewährleistet, dass Organisationen in Zeiten des demografischen Wandels effektiv und effizient in der Verwaltung und Erfüllung ihrer Aufgaben bleiben und ihr technologisches Potenzial vollständig ausschöpfen können.	Einführen

Begriff	Anwendung im Public Sector	Status
Digital Identity Ecosystems	Der Nachweis der Identität muss für Menschen auch in der digitalen Welt so einfach wie möglich erfolgen können. Zu einer digitalen Identität gehören daher spezifische elektronische Daten (u. a. Vorname, Nachname, Geburtsdatum), die eine physische Person eindeutig identifizieren. Durch die digitale Identität kann eine höhere Transparenz und somit auch Akzeptanz bei Interaktionen zwischen Behörden und Bürgern bzw. Bürgerinnen sichergestellt werden. Staaten haben ihre Aktivitäten hier deutlich intensiviert (eID und digitaler Führerschein in Österreich). Die digitale Identität von Bürgerinnen und Bürgern wird verwendet, um hauptsächlich die Online-Authentifizierung (eID) und elektronische Signaturen bei Interaktionen mit der Verwaltung abzudecken. Aber der Bedarf an digitaler Identität geht schnell über diese Grenzen hinaus: Mittelfristig gibt es eine Vielzahl von digitalen Identitäten, aber nur ein kleiner Anteil davon ist interoperabel über Sektoren und Ländergrenzen hinaus.	Einführen
NEU DEI: Diversity, Equity and Inclusion in IT	Diese Begriffe umfassen eine Reihe von Prinzipien und Praktiken, die darauf abzielen, eine diverse und inklusive Arbeitsumgebung zu schaffen, in der alle Mitarbeiter:innen, unabhängig von ihrer ethnischen Zugehörigkeit, ihrem Geschlecht, ihrer sexuellen Orientierung, ihrer Religionszugehörigkeit oder anderen Merkmalen fair behandelt werden. DEI fördert die Chancengleichheit, den Respekt und die Wertschätzung aller Mitarbeiter:innen und ermöglicht die Schaffung einer positiven Unternehmenskultur. Weiters kann DEI dazu beitragen, bessere Softwarelösungen zu entwickeln, die den Ansprüchen unterschiedlicher Benutzer:innen-Gruppen genügen, beispielsweise was User Experience, Bias-Mitigation und Barrierefreiheit betrifft.	Näher Betrachten
Hyperautomation	Hyperautomatisierung in der Verwaltung ist ein systematischer Ansatz von Verwaltungseinheiten und Regierung, so viele Geschäfts- und IT-Prozesse wie möglich schnell zu identifizieren, zu überprüfen und in IT-Systemen zu automatisieren. Es beinhaltet die orchestrierte Nutzung mehrerer Technologien, Tools oder Plattformen wie KI, robotergesteuerte Prozessautomatisierung, XaaS (Anything as a Service), Low-Code/No-Code und Softwarepakete.	Ausprobieren
Cloud Transformation	Der pandemiebedingte Boost bei Remote-Arbeit, welche die praktisch grenzenlose Kollaboration in der neuen Arbeitswelt eindrucksvoll als hochproduktives Arbeitsumfeld bestätigt hat, hat die Akzeptanz und den Einsatz von Cloud-Technologien vorangetrieben und zu starkem Wachstum in diesem Sektor geführt. Ein wesentlicher Teil unseres Lebens hat sich ins Internet verlagert, sei es in der Arbeitswelt oder im Privaten. Die verschiedenen Initiativen in der EU, dem Gewicht der US-Hyperscaler etwas entgegenzusetzen, das mit Datenschutz und Souveränität im Einklang steht, haben noch nicht zu einem konkurrenzfähigen Angebot geführt. Auf europäischer Ebene hat die EURITAS (Allianz der europäischen Verwaltungs-IT-Dienstleister) ein Framework zur Vernetzung von Private Clouds im Public Sector entwickelt (siehe auch BRZ-Perspektiven 2023).	Einführen
Citizen Twin/ Invisible Citizens	Digitale Modelle von Bürgerinnen und Bürgern werden entwickelt, um Statistiken zu erstellen, die den Stakeholdern helfen, Entscheidungen zu treffen, z. B. bei der Ausrichtung der medizinischen Behandlung oder auch, um sicherheitsrelevante Entwicklungen in sozialen Medien zu identifizieren. Aggregierte Versionen werden verwendet, um breitere Muster, Ressourcennutzung und gesellschaftliches Verhalten zu überwachen. Dabei sind stets robuste Privacy- und Digitale-Ethik-Regeln anzuwenden.	Beobachten

Begriff	Anwendung im Public Sector	Status
Intelligente Sicherheit	Moderne Technologien bieten neue Angriffsflächen für Cyberattacken. Durch die Verknüpfung von immer mehr Sensoren (siehe IoT) werden die möglichen Angriffspunkte potenziert. KI-gestützter Sicherheit wird daher in den nächsten Jahren zunehmende Wichtigkeit attestiert. Lesen Sie mehr zu diesem Thema in den BRZ-Perspektiven 2023.	Ausprobieren
Cybersecurity	Cybersecurity beschreibt den aktiven Schutz von Computersystemen, Netzwerken und Programmen vor digitalen Angriffen. Mit sogenannten Sicherheitsattacken wird versucht sensible Informationen zu erlangen, zu verändern oder zu zerstören. Ein umfassender Schutz reicht von der Aufklärung der Mitarbeiter:innen über Prozesse im Arbeitsumfeld bis hin zu eingesetzten Technologien und Softwareprodukten. Das Vertrauen der Nutzer:innen ist hier zu stärken, diese müssen sich auf die Datensicherheit verlassen können. Eine der Maßnahmen dafür ist ein Identitätsmanagement der nächsten Generation zur Erhöhung des Schutzes und des Vertrauens.	Einführen
Anything as a Service (XaaS)	XaaS umfasst mehrere Kategorien von IT-Infrastruktur- und Softwarediensten, einschließlich derjenigen, die in der Cloud als abonnementbasierter Dienst bereitgestellt werden. Beispiele für XaaS-Anwendungen sind: SaaS (Software als Dienstleistung), PaaS (Platform as a Service), IaaS (Infrastruktur als Service), BPaaS (Business Process as a Service), UCaaS (Unified Communications as a Service).	Näher Betrachten

 **Touchpoint**

Begriff	Anwendung im Public Sector	Status
Self Sovereign Identity (SSI)	Self Sovereign Identity ist ein Trend der digitalen Identität, der Einzelpersonen die Kontrolle über ihre digitalen Identitäten (Digitale Avatare) gibt. Ziel ist, das Vertrauen bei Transaktionen mit Stakeholdern zu erhöhen. Die EU hat mit eIDAS ein kompatibles System für die SSI entwickelt. Mit dem Trend zu dezentraler Identität und Bring Your Own Identity (BYOI) werden traditionelle Konzepte der Identitätsverwaltung herausgefordert bzw. werden Funktionen hinzugefügt, um solche Szenarien zu ermöglichen, etwa der digitale Altersnachweis in der App „eAusweise“. Die Erhöhung der digitalen Kompetenz in der Gesellschaft ist ein Schlüsselfaktor, ebenso wie das Zurückdrängen des „Digital Divide“, also des Zurücklassens von Teilen der Gesellschaft, die nicht aktiv am digitalen Leben teilnehmen können oder wollen.	Einführen
Universal Access/ Digitale Barrierefreiheit	Universal Access konzentriert sich auf theoretische, methodische und empirische Maßnahmen, die potenziell allen Bürgerinnen und Bürgern die Teilnahme an der Informationsgesellschaft ermöglichen sollen. Es handelt sich um den technologischen und nicht technologischen Zugang zur Informationsgesellschaft, in der sich alle Bürger:innen gleichberechtigt und aktiv beteiligen können. Digitale Barrierefreiheit ermöglicht die Kommunikation mit Systemen der Informationsverarbeitung auch für Menschen mit Beeinträchtigungen oder Behinderung. Neue Technologien wie z. B. Sprachassistenten oder die Verbindung von Screen-Readern und Text-to-Speech am Desktop und Smartphone ermöglichen neue Entwicklungspotenziale und fördern die Inklusion. Viele Staaten – wie auch Österreich – haben gesetzliche Grundlagen für digitale Barrierefreiheit geschaffen.	Einführen

Begriff	Anwendung im Public Sector	Status
BYOE (Bring Your Own Environment)	Die Arbeitswelt nach der Pandemie hat sich bereits verändert und wird sich auch weiter stark verändern. Der Trend BYOE kann aber nicht nur als Evolution von BYOD (Bring Your Own Device) gesehen werden. Der Arbeitsplatz kann nun neben dem Homeoffice überall sein, die verwendeten Technologien (PC, Tablet, Heimnetzwerk, Mobilfunkanbindung usw.) bringen Arbeitnehmer:innen selbst mit. Dies erfordert eine Sicherheit auf anderer Ebene, wenn sich Geräte nicht mehr in der unmittelbaren Arbeitsumgebung des Arbeitgebers befinden (siehe auch beim Kapitel zum Thema Zero Trust).	Einführen
NEU Integrierte One Stop Shops	Nutzerfreundliche digitale Services sind in den Alltag vieler Menschen eingekehrt. Bürger:innen sind zunehmend nutzerzentrierte und allumfassend integrierte digitale Services für spezifische Lebenssituationen gewohnt. Integrierte One Stop Shops stellen daher die jeweilige Lebenssituation statt eines einzelnen Behördenwegs in den Mittelpunkt und integrieren sich dort wo möglich auch mit privaten Services, etwa bei einem Umzug oder hinsichtlich Familienangelegenheiten.	Ausprobieren
NEU Demokratisierung der Technologie	Technologie den Nutzerinnen und Nutzern weltweit und breit zugänglich zu machen, ist durch moderne Ansätze machbar geworden. Durch den Zusammenfluss von Cloud Computing und Open Source sind neue Möglichkeiten entstanden, Technologien zu demokratisieren. Generative KI erleichtert Millionen von Benutzerinnen und Benutzern, die über keine Programmierkenntnisse verfügen, die Nutzung traditioneller KI-Technologien und Low-Code-/No-Code-Plattformen. LLM-Plattformen ermöglichen das Wissen in Unternehmen für Menschen in leicht verständlicher Weise zu übermitteln.	Näher Betrachten
Digitale Ethik	Digitale Ethik beschäftigt sich mit den Auswirkungen der Digitalisierung auf den Menschen als Individuum und auf die Gesellschaft. Die wesentlichen Aufgaben der digitalen Ethik sind, konsistente Begründungen für moralisches Handeln und normative Standards zu erarbeiten sowie deren soziale Auswirkungen zu untersuchen. Ein weiterer Aspekt ist die digitale Gleichberechtigung. Dabei wird in Zukunft die Effektivität von Maßnahmen mittels DEI (Diversity, Equity, Inclusion)-Tech-Tools gemessen bzw. verbessert und damit ein Beitrag zur Beseitigung von Benachteiligungen geleistet.	Ausprobieren
Augmented Reality/ Virtual Reality	Die virtuelle Realität (VR), auch Augmented Reality (AR), ist eine computergestützte Erweiterung der Realitätswahrnehmung, die alle menschlichen Sinnesmodalitäten ansprechen kann. Mittels gestützter Devices (wie z. B. einer größeren AR- oder VR-Brille) kann diese Darstellung und gleichzeitige Wahrnehmung der Wirklichkeit samt ihrer physikalischen Eigenschaften in einer virtuellen Umgebung in Echtzeit erfolgen. In der sogenannten „gemischten Realität“ wird die Realität mit der virtuellen Realität verschränkt. So können etwa virtuelle Objekte in Aufnahmen einer Handkamera projiziert werden. Mixed Reality kann vor allem Tests für Prototypen in der realen Welt erleichtern.	Ausprobieren
New Work	Die Lockdowns in der Pandemie waren der Auslöser für den tiefgreifenden kulturellen und wirtschaftlichen Wandel in der Arbeitswelt, aber nicht die einzige Ursache. Die Grundlage dafür war schon da: die digitale Transformation. Die Grenzen zwischen Arbeit und Freizeit verwischen, es geht nicht mehr um die Work-Life-Balance, sondern um Work-Life-Blending. Wenn immer mehr Arbeit automatisiert von Maschinen gemacht wird, was macht dann der Mensch? HR-Abteilungen spüren die veränderten Bedingungen und Unternehmen stellen sich darauf ein.	Ausprobieren

Begriff	Anwendung im Public Sector	Status
Total Experience	Total Experience (Gesamterlebnis) ist ein Ansatz, der die Disziplinen User Experience (UX), Citizen/Constituent Experience (CX), Employee Experience (EX) und Multi-Experience (MX) für eine ganzheitlichere Servicegestaltung und -bereitstellung kombiniert. Eine TX-Strategie verknüpft digitale und nicht digitale Techniken aus den Disziplinen CX, EX, UX und MX, um das Vertrauen von Bürgerinnen und Bürgern sowie Mitarbeitenden in und die Zufriedenheit mit staatlichen Dienstleistungen zu steigern.	Beobachten
Metaverse	Wird es ein anhaltender Erfolg oder ist der Hype schon wieder vorbei? Ziel des Metaverse ist das Verbinden von physischen und virtuellen Räumen, um die Multipräsenz einer Person (Digital Twin) zu ermöglichen. Anwendungsfälle sind etwa Meetings und Shared Experiences, Vorlesungen an Universitäten, Gaming, Handel mit digitalen Assets (Tokenization). Derzeit ist vieles im Experimentalstadium, es gibt viele Player. Gartner erwartet eine Entwicklung hin zu einem einzigen Metaverse, das nicht von einem einzelnen Unternehmen geführt wird. Der Technologie-Stack für das Metaverse ist Spatial Computing.	Beobachten

 **Methoden & Arbeitsweisen**

Begriff	Anwendung im Public Sector	Status
Intelligenter Arbeitsplatz	Ein intelligenter Arbeitsbereich (auch Smart Workspace genannt) setzt sich aus folgenden drei Faktoren zusammen: Raum, Technologie und Mensch. Beim Faktor Raum geht es darum, die Räumlichkeiten den unterschiedlichen Bedürfnissen und Arbeitssituationen (Call, Denkarbeit, Meeting) der Mitarbeiter:innen entsprechend anzupassen. Tätigkeiten und Räume werden bewusster auf Kollaboration (und deren Tools) ausgelegt. Meetings können dezentral abgehalten werden und Mitarbeiter:innen können verstärkt zeit- und ortsunabhängig arbeiten. COVID-19 hat die Dynamik dieses Trends stark beschleunigt und auch nach der Pandemie bleibt die Dynamik hoch.	Einführen
Tokenization	Das Ersetzen sensitiver und sensibler Daten durch Tokens ermöglicht eine Vielzahl neuer, sicherer Kommunikationswege. Das Teilen von Informationen zwischen Bürgern bzw. Bürgerinnen und administrativen Stellen kann so wesentlich einfacher und effizienter, bei gleichzeitig weit erhöhtem Schutz, geschehen. Tokenization und Blockchain sind beide wichtige Technologiebausteine im Web3.	Einführen
NEU Prompt Engineering	Vor der Eingabeaufforderung eines Large Language Models (z. B. ChatGPT) sitzt ein Prompt Engineer. Die Aufgabe des Prompt Engineers ist Abfrage und Tuning des LLM-Systems. Prompt Engineering ist eine Arbeitsweise innerhalb der KI, um die Aufgabe, die von der KI erledigt werden soll, optimal zu formulieren. Prompt Engineering hat die Aufgabe, das LLM mit promptbasierten Aufgaben zu trainieren. Im Anschluss kann das LLM als Service zur Verfügung gestellt werden. Das kommandobasierte Eingabeparadigma ändert sich mit der KI auf das neue Paradigma zur absichtsbasierten Interaktion, bei der Benutzer:innen dem Computer sagen, was sie wollen, und nicht, wie er es tun soll.	Ausprobieren

Begriff	Anwendung im Public Sector	Status
NEU SCHWERPUNKTTHEMA Data Governance	Data Governance bezieht sich auf die Verwaltung und Kontrolle beim Sammeln, Verwalten, Sichern und Speichern von Daten in einem Unternehmen oder einer Organisation. Es umfasst die Festlegung von Richtlinien, Verfahren und Prozessen, um sicherzustellen, dass Daten korrekt, konsistent, verfügbar, sicher und geschützt sind. Data Governance legt die Verantwortlichkeiten und Zuständigkeiten für die Datenverwaltung fest und sorgt dafür, dass Datenqualität, Datenschutz und Compliance-Standards eingehalten werden. Es beinhaltet auch die Definition von Datenstandards, Metadatenmanagement, Datenklassifizierung, Zugriffskontrolle und Datenlebenszyklusmanagement. Data Governance ist entscheidend, um das Vertrauen in Daten zu gewährleisten und eine solide Grundlage für datenbasierte Entscheidungen und Analysen zu schaffen. Data Governance wird auch verwendet, um eine geeignete Datenqualität sicherzustellen: Darunter fallen alle Maßnahmen oder Methoden, die dafür sorgen, dass die Daten genutzt werden können. Datenqualität wird im Allgemeinen anhand von sechs Größen gemessen: Korrektheit, Vollständigkeit, Konsistenz, Rechtzeitigkeit, Gültigkeit und Eindeutigkeit.	Einführen
Web3	Das Web3 basiert auf der Vision der Dezentralisierung, die durch Tokenization aller Objekte im Web erreicht werden soll. Web3 ist ein Stack von Technologien, Geschäfts- und Governance-Konstrukten, der es Benutzerinnen und Benutzern ermöglicht, ihre eigene Identität und Daten zu kontrollieren. Zu den Technologien gehören Blockchain als Mechanismus zur Vertrauensüberprüfung, Datenschutz- und Interoperabilitätsprotokolle, dezentrale Infrastruktur- und Anwendungsplattformen, dezentrale Identität und Unterstützung für Anwendungen wie dezentrale Finanzen. Ob und wie das Web3 unsere User Experience beeinflusst oder verbessert, ist noch nicht klar. Kritiker:innen sprechen davon, dass damit statt der Vision der Dezentralisierung die Grundlage für die weitgehende Monetarisierung aller realen und virtuellen Objekte geschaffen werden soll.	Beobachten
Anonymisierung	Basierend auf rechtlichen Grundlagen der DSGVO sind Anonymisierung und Pseudonymisierung nicht nur ein wichtiges Erfordernis für die Weitergabe und Verarbeitung von personenbezogenen Daten, sondern auch Voraussetzung für das Training von künstlicher Intelligenz. Um personenbezogene Daten für die Entwicklung von neuen Geschäftsmodellen zu nutzen, sind Anonymisierungstools einzusetzen.	Einführen
Accelerated Legacy Modernization	Eine Legacy-Anwendung ist eine Anwendung, die auf veralteten Technologien basiert, aber dennoch von entscheidender Bedeutung ist. Legacy-Modernisierung bedeutet veraltete Architekturen, Hardware- und Softwareanwendungen durch moderne Äquivalente zu ersetzen. Es gibt dabei verschiedene Modernisierungsansätze, meist werden Anwendungen in Modernisierungsprogrammen auf ein Cloud-Bereitstellungsmodell umgestellt. Im BRZ steht mit der Containerplattform PaaS eine geeignete Plattform für Legacy-Modernisierung bereit.	Ausprobieren
Lebenslanges Lernen	Die Art und Weise, wie Unternehmen ihre Mitarbeiter:innen weiterbilden, ändert sich rasant. Die Anforderungen an die Fähigkeiten der Mitarbeiter:innen hat eine Änderungsrate von 10 Prozent pro Jahr. Digitale Trends kommen mit hohem Tempo und fordern Anpassung an den Puls der digitalen Transformation. Um dem zu begegnen, werden in komprimierter Weise kontinuierlich individualisierte Lerninhalte im jeweiligen Kontext angeboten. Lerninhalte werden in kleinteiligen Einheiten in digitaler Form zur Verfügung gestellt. Diese Form des digitalen Wissenstransfers kann sowohl zum Inhouse-Wissenstransfer verwendet werden als auch zur Informationsübermittlung zu Kundinnen und Kunden.	Einführen

Begriff	Anwendung im Public Sector	Status
SCHWERPUNKTTHEMA Zero Trust	Wie kann bei exponentiell wachsenden Kommunikationswegen, Kommunikationsgeräten und Daten die Sicherheit auf einem akzeptablen Niveau gehalten werden? Zero Trust ist das neue Paradigma in der Cybersecurity. Da in diesen Szenarien der Perimeterschutz (z. B. die einmalige Anmeldung an einem System) nicht mehr ausreicht, ist eine neue Architektur gefordert. In einer Zero-Trust-Architektur wird bei jedem Datenzugriff eine Autorisierung und Validierung verlangt. Voraussetzung für die erfolgreiche Umsetzung sind hoch skalierende Systeme und Datenpfade sowie ein hoher Automatisierungsgrad. Zero Trust ist keine Technologie. Zero-Trust-Sicherheitsarchitekturen ersetzen die impliziten und statischen Konzepte älterer Sicherheitsarchitekturen durch dynamische und explizite Konzepte. Die Zero-Trust-Sicherheitsarchitektur beruht auf dem Prinzip, keinem Gerät, User oder Dienst innerhalb oder außerhalb des eigenen Unternehmensnetzwerks zu vertrauen. Das bereits seit 1990 bestehende Paradigma gewinnt in der sich rapide vernetzenden Welt stark an Bedeutung.	Einführen
Agile Cultural Mindset	Ein Agile Cultural Mindset ist eine Haltung eines Unternehmens, das in einem agilen Umfeld arbeitet. Dazu gehören Respekt, Zusammenarbeit, Verbesserungs- und Lernzyklen, Stolz auf Eigenverantwortung, Fokus auf die Wertschöpfung und die Fähigkeit, sich an Veränderungen anzupassen. Diese Haltung ist ein wichtiger Faktor, um leistungsstarke, agile Teams aufzubauen. Der Mehrwert für die Kundin und den Kunden ist schnell sichtbar.	Ausprobieren

Etablierte BRZ-Produkte, -Solutions und -Services

Im Technologieradar 2024 sind folgende Technologien nicht mehr aufgeführt, da sie bereits stark im BRZ verankert sind – etwa als Solution, Produkt oder Service:

Design Thinking

Als Design Thinking wird eine kreative Methode bezeichnet, die zur Lösung von Problemen oder Herausforderungen sowie zur Entwicklung neuer Ideen führen soll. Design-Thinking-Prozesse werden im BRZ laufend für die Entwicklung neuer Anwendungen oder Services bzw. für die Weiterentwicklung bestehender Anwendungen genutzt.

Elektronische Partizipation (E-Partizipation)

Mittels E-Partizipation können sich natürliche, aber auch juristische Personen an Entscheidungsfindungen sowie an politisch-administrativen Prozessen beteiligen. Mit BRZ eDem steht BRZ-Kunden ein leistungsstarkes Tool für E-Partizipationsprozesse zur Verfügung.

Open Data

Der Begriff Open Data beschreibt offene Daten, die von allen frei genutzt, weiterverwendet und auch geteilt werden können. Das BRZ betreibt den zentralen österreichischen Datenkatalog data.gv.at für den

österreichischen Bund sowie die nationalen und internationalen Schnittstellen.

Microservices

Microservices werden als Architekturmuster und organisatorischer Ansatz bezeichnet, die einzelne Prozesse und Funktionen entkoppeln. Dies geschieht durch die Bereitstellung kleinteiliger, eigenständiger, entkoppelter Services, die in der Regel ihre eigene Datenbank verwalten. Microservices sind Teil der BRZ-PaaS, die bereits die Grundlage für zahlreiche Anwendungen ist.

Predictive Analytics

Predictive Analytics ist der wichtigste Realisierungstrend aus dem ehemaligen Megatrend Big Data und ist ein Spezialbereich im Business Intelligence (BI)-Umfeld. Ziel von Predictive Analytics ist, herauszufinden, was passieren kann und warum es passiert. Das BRZ setzt Predictive Analytics bereits erfolgreich für seine Kunden ein, etwa im Bereich Betrugsbekämpfung.

SAFe®

Das „Scaled Agile Framework“ (SAFe®) ist ein weitverbreitetes Framework für agiles Arbeiten und ein Element von Lean Management, das im BRZ bereits seit mehreren Jahren umgesetzt wird.

Blockchain

Blockchain ist eine verteilte, dezentrale Datenbank, in der neue Datensätze – in Form von Blöcken – ergänzt, aber keine bestehenden Blöcke geändert werden können. Die

Weiterentwicklung der Blockchain ist eine Voraussetzung, um diese Technologie im Web3 erfolgreich einsetzen zu können. Das BRZ nutzt die Blockchain-Technologie etwa für das Tool „BRZ eDem“.

Small Data

Bei Small Data stehen Privacy- und Security-Aspekte im Vordergrund. Als Konzept findet sich der Ansatz in anderen Bereichen, etwa der intelligenten Sicherheit wieder.

Referenzen

- > Gartner Top Technology Trends in Government for 2022, Published 18 January 2022
- > Gartner Top Business Trends in Government for 2022, Published 18 January 2022
- > Gartner Government Digital Transformation and Innovation Primer for 2022, Published 4 February 2022
- > Gartner Top Strategic Technology Trends for 2022, Published 17 October 2022
- > Gartner Hype Cycle for Blockchain and Web3, 2022, Published 12 July 2022
- > Gartner Hype Cycle for Artificial Intelligence, 2022, Published 8 July 2022
- > Gartner Top Strategic Technology Trends for 2023: Metaverse, Published 17 October 2022
- > Gartner TechWatch October 2022: Innovations in Wi-Fi Sensing, Robotics, Massive IoT and Edge AI, Published 27 October 2022

Schwerpunktthemen 2024

In den drei folgenden Kapiteln widmen wir uns Themen, die für den technischen Fortschritt insbesondere im Bereich E-Government auf österreichischer, aber auch europäischer Ebene von Bedeutung sind:

- **Data Governance**, als Grundlage für den „Rohstoff“ Daten, der Grundlage für moderne KI-Anwendungen und andere Digitalisierungsvorhaben ist
- **Generative KI**, ein Megatrend, der das Thema künstliche Intelligenz für eine breite Masse an Benutzerinnen und Benutzern zugänglich und verständlicher gemacht hat und Chancen wie Risiken mit sich bringt
- **Zero Trust** als umfassender Ansatz für mehr Sicherheit beim Umgang mit IT-Systemen

Data Governance

„Daten sind das neue Gold“ und damit eine der wichtigsten Ressourcen für die fortschreitende Digitalisierung, für aufkommende KI-Lösungen sowie eine Grundlage für Innovation und Entscheidungsfindung in Unternehmen und Organisationen. Im Gegensatz zu Gold entsteht der Wert von Daten jedoch vor allem dann, wenn sie geteilt werden. Damit dies sicher gelingt, wird Data Governance für IT und Fachbereiche immer wichtiger. Auch in der öffentlichen Verwaltung ist es möglich, durch Data Governance einen verantwortungsvollen und effektiven Umgang mit Daten zu fördern und gleichzeitig rechtliche Vorgaben wie den Data Governance Act der Europäischen Kommission zu erfüllen.

Data Governance ist ein grundsätzlicher Ansatz zur Verwaltung von Daten während ihres Lebenszyklus, von der Erfassung über die Verwendung bis zur Vernichtung.

Status quo

Data Governance hat sich im Laufe der Zeit weiterentwickelt. Während man sich früher vor allem mit Zugangskontrollen und möglichen Datenqualitätsproblemen beschäftigt hat, geht es heute vor allem um die Wiederverwendung von Daten für datengetriebene Analysen oder die Entwicklung von Innovationen und künstlicher Intelligenz.

Abbildung 2: Data-Governance-Ansätze

Traditioneller Ansatz



Moderner Ansatz



Quelle: Gartner: Data and Analytics (Information) Governance, Präsentation, 2023.

Daten und E-Government

Data-Governance-Maßnahmen dienen auch dazu, das Vertrauen in Datennutzung zu erhalten.

Im Bereich E-Government konzentrierten sich früher Initiativen auf die Automatisierung von Verwaltungsprozessen. Heute geht man einen Schritt weiter und zielt auf die Optimierung und Neugestaltung von Prozessen mithilfe von Daten ab. Durch die Digitalisierung entstehen große Datenmengen, deren effiziente Nutzung aufgrund des technologischen Fortschritts neue Herausforderungen mit sich bringt. Sogenannte „Datensümpfe“, Schattendatenbestände oder proprietäre Datenformate verhindern eine Weiterverwendung von Daten. Ungenutzte Datenpotenziale bedeuten einen Verlust an Möglichkeiten für eine optimierte Verwaltung. Um dies zu vermeiden, bedarf es jedoch mehr als nur verfügbarer Datenmengen – intelligentes Datenmanagement und ein umfassendes Data Governance Framework sind entscheidend, um Vertrauen in die Datennutzung zu erhalten und die richtigen Entscheidungen zu treffen.

Der Data Governance Act ist eine Verordnung der EU, die einen Rahmen schafft, der die gemeinsame Nutzung von Daten erleichtert. Mit dem Data Governance Act hat die Europäische Kommission die Grundlagen für die Schaffung eines europäischen Datenaustauschmodells festgelegt.

Neben Effizienz- und Innovationsmotiven können auch bestimmte gesetzliche Anforderungen an die Weiterverwendung bestimmter Daten Treiber sein (z. B. EU-Richtlinie über offene Daten und die Weiterverwendung von Informationen des öffentlichen Sektors, Informationsweiterverwendungsgesetz, Data Governance Act EU-Verordnung). Auch hier kann eine bereits bestehende Data Governance die Mechanismen der Datenanfrage und -bereitstellung effizienter gestalten.

Begriffsdefinition: Data Governance

Data Governance geht über die Dimension eines einfachen technischen Instruments hinaus. Mit klaren Richtlinien, Prozessen und definierten Rollen bietet sie die Möglichkeit, Daten als strategisches Asset zu behandeln. Eine effektive Umsetzung von Data Governance verbessert nicht nur die Nutzung und Qualität von Daten, sondern gewährleistet auch deren Zugänglichkeit, Sicherheit und Compliance. Insbesondere im öffentlichen Sektor ist es von entscheidender Bedeutung, das Vertrauen der Öffentlichkeit zu erhalten und eine

effiziente Entscheidungsfindung zu fördern. Es muss betont werden, dass Data Governance kein reines IT-Thema ist, sondern nur im Zusammenspiel mit den Geschäftsbereichen erfolgreich sein kann. Data Governance ist ein fortlaufendes Programm, das darauf abzielt, den Wert von Daten zu maximieren und Risiken zu minimieren.

Der Wert von Daten

Der Wert von Daten liegt in den Informationen, die sie enthalten. Die primitivste Form der Data Governance ist ein restriktiver Zugang, der jedoch die Nutzung und Wiederverwendung von Daten erheblich einschränkt und sie nicht für Innovationen nutzbar macht. Data Governance zielt daher darauf ab, die Wertschöpfung von Daten durch eine gemeinsame Nutzung zu fördern.

Qualitativ hochwertige Daten sind wesentlich, um KI-Systeme erfolgreich zu trainieren.

Abbildung 3: Datenwertschöpfungskette



Quelle: OECD Digital Government Studies: The Path to Becoming a Data-Driven Public Sector, 2019.

Um dies zu erreichen, muss die gesamte Datenwertschöpfungskette von Data-Governance-Maßnahmen begleitet werden.

- > Für die Datenerzeugung bedeutet dies beispielsweise die Verwendung interoperabler Formate, datenzentrischer Architekturen und geeigneter fachlicher Beschreibungen.
- > Bei der Qualitätssicherung werden Personen, die mit Daten arbeiten, maschinell unterstützt.
- > Die Speicherung der Daten muss in einer geschützten Umgebung erfolgen.
- > Die Datensätze werden in Datenkatalogen erfasst, sodass sie von potenziellen Nachnutzern leicht gefunden und abgefragt werden können.

Ziel ist die sichere und einfache Weiterverwendung des entstehenden Datenprodukts für Analysen, KI-Entwicklung oder als Entscheidungshilfe. Ein wiederverwendetes Datenprodukt kann mit neuen Daten angereichert werden und in der Erstellung eines neuen Datenprodukts resultieren.

Vorteile, die durch Data Governance entstehen

Alle Daten im Überblick

- > schneller Überblick über die vorhandenen Daten
- > einfache Durchsuchbarkeit der Datensammlungen
- > Klarheit über Verantwortlichkeiten für Datenbestände
- > klare Regeln im Umgang mit Daten
- > Extrem große Datenmengen stellen keine Herausforderung mehr dar.

Verbesserung der Datenqualität

- > qualitätsgesicherte Daten
- > rechtssichere Aufbewahrung von Daten durch automatisierte Erinnerungen und Löschrregeln
- > gesteigertes öffentliches Vertrauen durch datengetriebene Entscheidungen und transparentere Verwaltungsvorgänge

- > kompetenter und bewusster Umgang mit Daten
- > Nachvollziehbarkeit der Datenherkunft

Wiederverwendbarkeit und Effizienz

- > Datensparsamkeit durch Vermeidung von Redundanzen, gezielte Archivierung operativer Daten, Löschung nicht mehr benötigter Daten
- > Minimierung der Aufwände für Datenaufbereitung und -bereitstellung durch Automatisierung
- > Trustworthy Data ermöglicht Trustworthy AI.
- > Reduktion des Risikos von Datenschutzverletzungen und Cyberbedrohungen
- > optimierte Verwaltungsprozesse

Elemente einer effizienten Data Governance

Die Einführung eines effektiven Data Governance Frameworks ist entscheidend, um die wachsende Bedeutung von Daten als strategisches Asset optimal zu nutzen. Das Framework muss eng mit den definierten Data-Governance-Zielen und der Gesamtstrategie der Organisation verknüpft werden, um einen umfassenden und zielgerichteten Ansatz sicherzustellen. Die Elemente des Frameworks lassen sich in strategische, organisatorische und operative Elemente unterteilen.

Ein Data Governance Framework enthält strategische, organisatorische und operative Elemente.

Strategische Elemente

Datenstrategie

Gute Data Governance erfordert eine klare Datenstrategie. Da Data Governance kein rein technisches Thema ist, ist eine strategische Priorisierung der gemeinsamen Nutzung und Wiederverwendung von Daten erforderlich. Eine nationale Datenstrategie legt klare Ziele und Leitlinien für die Datenverwaltung fest, um den Wert der Daten im Einklang mit der Gesamtstrategie zu maximieren.

Leadership

Ein weiteres zentrales Element ist die klare Definition von Verantwortlichkeiten und Zuständigkeiten bei der Festlegung und Umsetzung von Data-Governance-Praktiken. Je nach kulturellen und sozialen Gegebenheiten gibt es in den öffentlichen Verwaltungen unterschiedliche Modelle. In einigen Ländern wie Frankreich, aber auch in Teilen der österreichischen Verwaltung wird die Position eines „Chief Data Officer“ geschaffen, während in Schweden diese Rolle auf einen Lenkungsausschuss verteilt wird. Wichtig ist, dass es klar definierte, kompetente Stellen für die Gestaltung der fachlichen Regeln gibt.

Organisatorische Elemente

Data Governance Boards

Eine erfolgreiche Umsetzung erfordert ein kooperatives, institutionenübergreifendes Zusammenspiel in Form eines zentralen Data Governance Boards, das die Einhaltung der Standards, Richtlinien und Praktiken überwacht. Das Vorhandensein eines solch heterogen besetzten Gremiums stellt sicher, dass unterschiedliche Sichtweisen bei der Umsetzung berücksichtigt werden, um Maßnahmen zielgerichtet setzen zu können, und die Koordination zwischen den Institutionen reibungslos funktioniert.

Data Stewardship

Datenmanagement wird zunehmend von einer reinen IT-Angelegenheit zu einem strategischen Ziel, bei dem die Fachbereiche eine zentrale Rolle spielen. Data Stewards sind in diesem Zusammenhang eine bewährte Praxis. Dabei handelt es sich um fachliche Datenbeauftragte mit Datenkompetenz, die auf operativer Ebene bei der Überwachung von Datenstandards und Datenqualität unterstützen. Data Stewards arbeiten dabei in enger Zusammenarbeit mit den technischen Umsetzerinnen und Umsetzern. Bereits etablierte Datenbeauftragte – wie Datenschutzbeauftragte oder Open-Data-Beauftragte – können dabei als Anknüpfungspunkte dienen.

Für eine erfolgreiche Umsetzung einer Data Governance ist die Zusammenarbeit unterschiedlicher Expertinnen und Experten notwendig.

Rechtsrahmen, Standards und Leitlinien

Ein sicherer Rechtsrahmen und definierte Standards sind entscheidend für den Erfolg von Data Governance. Technische Standards, seien es gesetzliche Vorgaben, Industriestandards oder etablierte Normen, gewährleisten den Datenaustausch durch ein hohes Maß an Interoperabilität, wie es beispielsweise die INSPIRE-Richtlinie und der DCAT-Anwendungsprofilstandard in Europa ermöglichen.

Semantische Standards und Ontologien tragen zu einem einheitlichen Verständnis bei. Fachliche Regeln definieren bestimmte organisatorische Abläufe und Zuständigkeiten bei Datenentscheidungen. Auf Unionsebene wird zukünftig der Europäische Dateninnovationsrat eine wichtige Rolle bei der Definition von Datenstandards und Normen spielen.

Datenkompetenzen, Wissensaufbau, Data Literacy

Erfolgreiche Data Governance erfordert sowohl fachliche als auch technische Kompetenzen sowie anfängliche Unterstützung bei der Umsetzung von Praktiken. Der Aufbau von Datenkompetenz fördert ein gemeinsames Verständnis des Wertes von Daten, ermöglicht eine kritische Bewertung und effektive Nutzung von Daten und verbessert damit die Entscheidungsfindung. Data Governance legt den Rahmen fest, während Data Literacy sicherstellt, dass dieser aktiv genutzt wird, um den maximalen Nutzen aus den Daten zu ziehen.

Operative Elemente

Datenlebenszyklus

Im Rahmen der Umsetzung müssen alle Aspekte des Datenlebenszyklus technisch und organisatorisch von Data-Governance-Maßnahmen unterstützt und begleitet werden. Je nach Aktivität spielen dabei unterschiedliche Technologien und Kompetenzen eine Rolle.

DCAT: Data Catalog Vocabulary

Die INSPIRE-Richtlinie zielt darauf ab, eine Geodateninfrastruktur innerhalb der EU zu schaffen. Diese soll den Austausch raumrelevanter Informationen zwischen Organisationen des öffentlichen Sektors und den Zugang der Öffentlichkeit zu Geodaten in ganz Europa erleichtern.

Datenkompetenz fördert das Verständnis über den Wert von Daten.

Architektur und Dateninfrastruktur

Datenzentrische Architekturen und Infrastrukturen gewährleisten die Einhaltung der Data Governance, insbesondere bei der Speicherung oder Nutzung von Daten. Plattformen und Konnektoren ermöglichen es, Daten im Einklang mit bestimmten Richtlinien zu finden und zu teilen. Das Ziel ist, dass Datenaustauschplattformen verwaltungsintern und für den externen Datenaustausch genutzt werden können, unterstützt durch standardisierte Technologien, Werkzeuge und Prozesse. In Italien (www.interop.pagopa.it), Estland (www.x-tee.ee) oder Finnland (x-road.global) gibt es einige Beispiele, wie dies erfolgreich gelingen kann. Auf Unionsebene stellt data.europa.eu ein wichtiges Datenportal dar, wo Verwaltungsdaten aller Mitgliedstaaten auffindbar sind.

Technische Fähigkeiten der Data Governance

Im festgelegten Framework kann eine Data-Governance-Plattform zur Erreichung der definierten Ziele dienen. Diese Plattform kann gezielte Funktionalitäten bereitstellen, um effektive Unterstützung zu gewährleisten.

Aktive Metadaten und Analytik

Die Verwendung von aktiven Metadaten ermöglicht die praktische Nutzung von Analyseergebnissen durch operative Warnungen und Empfehlungen. Die Erkennung von Mustern in Datenoperationen erlaubt eine KI-gestützte Rekonfiguration von Daten und darauf basierenden Operationen, sodass Analysemodelle nicht nur die Datenaufbereitung, sondern auch die Versionierung von Modellen und Berichten unterstützen.

Fachdatenmodell und Glossar

Die Erstellung und Verwendung eines fachlichen Datenmodells einschließlich eines Glossars erleichtert die Analyse und die Erstellung von Richtlinien. So kann ein Überblick über alle fachlichen Geschäftsobjekte und deren Beziehungen zwischen den Datenelementen geschaffen werden, um semantische Unklarheiten zu

beseitigen. Darüber hinaus vereinfacht die Klassifikation das Auffinden und die Aufbewahrung von Daten. Diese Kategorisierung ist insbesondere im Zusammenhang mit Risikomanagement, Compliance und Datensicherheit von Bedeutung.

Datenherkunft und Datenfluss

Eine detaillierte Darstellung des Datenflusses, einschließlich aller Schritte und Transformationen, die ein Datenelement von der Quelle bis zum Endpunkt durchläuft, erlaubt eine umfassende Analyse der Auswirkungen. Dabei können Metadatenelemente bis auf Spalten- oder Transformationslogikebene untersucht werden, um die Folgen von Änderungen zu ermitteln.

Datenkatalog

Ein Datenkatalog, der auf technischen Metadaten basiert, ist eine Zusammenstellung von Namensdefinitionen und Attributen für Datenelemente, die in einer Datenbank genutzt oder aufgenommen werden. Er hat zum Ziel, die Bedeutung und Anwendung von Datenelementen zu beschreiben, und gibt Anweisungen zur Auslegung, akzeptierten Bedeutung und Darstellung.

Datenqualität

Durch automatisierte Prüfungen, Regelwerke und die Visualisierung von Datenqualitätsindikatoren können Korrekturmaßnahmen abgeleitet werden, um eine kontinuierliche Verbesserung der Datenqualität über den gesamten Datenlebenszyklus zu gewährleisten. Dadurch wird sichergestellt, dass die Daten den definierten Qualitätsstandards entsprechen.

Konnektivität und Integration

Die Bereitstellung von Möglichkeiten zum schnellen und effizienten Import und Export von Metadaten, einschließlich Rollen, zwischen dem zentralen Repository und Werkzeugen von Drittanbietern fördert die Interoperabilität und Harmonisierung von Metadaten. Dieses Konzept basiert auf der Idee der maschinellen Verarbeitbarkeit oder der Fähigkeit, verschiedene Aspekte der Metadatenspezifikationen automatisch zu verarbeiten.

Metadaten sind strukturierte Daten, die Informationen über Merkmale anderer Daten enthalten.

Referenzdatenmanagement

Referenzdatenmanagement ermöglicht die einheitliche Verwaltung und Aktualisierung von Schlüsselreferenzdaten. Dadurch sind alle Systeme in der Lage, konsistent auf dieselben aktuellen Referenzdaten zuzugreifen, was die Genauigkeit und Zuverlässigkeit von Entscheidungen verbessert.

Workflow und Zugriffsverwaltung

Die Unterstützung von Workflows ermöglicht eine reibungslose Steuerung und Automatisierung von Datenmanagementprozessen. Von der Erfassung der Daten bis zur Veröffentlichung erlaubt dies eine effiziente und transparente Abwicklung, die die Konsistenz und Integrität der Daten gewährleistet. In Kombination mit der Einrichtung und Zuteilung von Rollen und Organisationsbeziehungen für Funktionen gewährleistet dies eine effektive Zusammenarbeit im Rahmen der Datenverwaltung.

Europäische Datenstrategie

Im Jahr 2020 hat die Europäische Kommission die Europäische Datenstrategie veröffentlicht und sich zum Ziel gesetzt, den Anteil an der globalen Datenwirtschaft bis 2030 signifikant zu erhöhen. Als eine Maßnahme zur Umsetzung dieses Ziels gilt die Etablierung eines Data Governance Frameworks. Mit der EU-Verordnung zum Data Governance Act (2022 in Kraft getreten) wurde beschlossen einen organisationsübergreifenden und unionsweiten Data-Governance-Ansatz zu verfolgen. Durch die Schaffung von Anreizen zum Datenteilen soll ein europäischer Datenraum entstehen, der datengetriebene Innovationen fördert. Die Verwaltung soll durch zusätzliche Instrumente und Kompetenzen dazu motiviert werden, öffentlich generierte Daten zu teilen. Wenn dies nicht in Form offener Daten möglich ist, dann auch unter Einhaltung bestimmter Nutzungsbedingungen. Um die unionsweite Data Governance mit Leben zu füllen und insbesondere das Teilen von Daten im öffentlichen Besitz zu ermöglichen, wird das Vorhandensein einer bereits gelebten verwaltungsweiten Data Governance ein kritischer Erfolgsfaktor sein.

BRZ-Involvement

2023 einigte sich die österreichische Bundesregierung im Rahmen des Digital Austria Act darauf, eine österreichische Datenstrategie für die Verwaltung zu entwickeln. Das BRZ unterstützt als Kompetenzzentrum für Digitalisierung die Erstellung der Datenstrategie für Österreich. Neben der Expertise in der sicheren Speicherung und Verarbeitung von Daten spielt Data Governance im BRZ bereits in einigen Verfahren eine wichtige Rolle.

Das BRZ begleitet in seinem Format BRZ DigiConnect die Umsetzung des Data Governance Acts in Österreich.

Anwendungsbeispiel: Data Governance Austria-Plattform

Die Data Governance Austria-Plattform wurde im Auftrag des Bundesministeriums für Finanzen vom BRZ entwickelt und umgesetzt und dient als webbasierte, mandantenfähige und skalierbare Plattform zur Sammlung, Verwaltung und Bereitstellung von Wissen über Daten im Data-Warehouse-Umfeld des BMF. Durch die Beschreibung und Visualisierung der fachlichen und technischen Datenwelt sowie durch die Abbildung der Zusammenhänge wird die Datenkompetenz aller Beteiligten gestärkt und eine effiziente Zusammenarbeit gefördert. Die leistungsstarke Lösung für das Metadatenmanagement wird als zentrales Betriebssystem des BRZ angeboten und stellt ein praxisorientiertes und kundenfreundliches Rundumpaket bereit, das auf bewährten Methoden basiert und konzeptionell anderen Ressorts eine effiziente Teilnahme an der Plattform ermöglicht. Die Data Governance Austria-Plattform leistet damit einen wichtigen Beitrag zur Digitalisierungsstrategie des Bundes und wurde im Rahmen der ADV Data Excellence Konferenz im April 2023 mit dem Data Excellence Award ausgezeichnet.

Anwendungsbeispiel: Datenmanagementportal BKA

Das BRZ unterstützt das Bundeskanzleramt beim Aufbau und Betrieb des Datenmanagementportals. Dabei handelt es sich um einen Shared

Service, der einer Open-Source-Strategie folgt und den Fachbereichen Data Governance as a Service anbietet. Über den gesamten Datenlebenszyklus hinweg, von der Datenerzeugung über die Nutzung bis hin zur Archivierung, wird darauf geachtet, dass große, auch unstrukturierte, Datenmengen möglichst automatisiert in standardisierte und interoperable Formate gebracht werden und dabei eine hohe Qualität aufweisen – indem etwa KI-Anwendungen bei der Qualitätssicherung unterstützen. In einem verwaltungsinternen Datenkatalog werden Datenbestände erfasst, um ihre Auffindbarkeit für eine mögliche Wiederverwendung zu erhöhen. Im Sinne der Nachvollziehbarkeit können Entscheidungen über Daten revisionssicher im ELAK dokumentiert werden. Damit erhalten Fachbereiche die Möglichkeit, ihre Daten leichter für datengetriebene Innovationen und Optimierungen teilbar zu machen. Auf diese Weise konnten bereits Bilddaten aus der Denkmalforschung für die Entwicklung von KI-Modellen direkt auf dem BKA AI Hub (siehe BRZ-Perspektiven 2022) genutzt werden.

Conclusio

Zusammenfassend bietet eine effektive Umsetzung von Data Governance in der öffentlichen Verwaltung zahlreiche Vorteile. Durch die Einhaltung rechtlicher Vorgaben und die Gewährleistung von Datenqualität und Datensicherheit kann das Vertrauen der Öffentlichkeit gewonnen und bewahrt werden. Die Nutzung von Daten als strategisches Asset kann zu evidenzbasierten Entscheidungen, zur Optimierung von Verwaltungsprozessen und zur Entwicklung nützlicher Anwendungen führen. In Zukunft wird die Bedeutung von Data Governance weiter zunehmen, insbesondere durch die Einführung des Data Governance Acts der Europäischen Kommission. Es ist zu erwarten, dass die rechtlichen und technologischen Entwicklungen, insbesondere im Bereich der künstlichen Intelligenz, in diesem Zusammenhang voranschreiten und neue Möglichkeiten für die Verwaltung eröffnen werden.

WEBTIPP:
Das Portal data.gv.at
veröffentlicht Open
Data der Verwaltung.

Generative künstliche Intelligenz (Generative AI)

Generative KI ist ein Bereich des maschinellen Lernens, spezialisiert auf die Erstellung neuer, origineller Inhalte wie Texte, Bilder und Audiodateien. Diese Technologie umfasst verschiedene Methoden wie Variational Autoencoders (VAEs), Generative Adversarial Networks (GANs) und Large Language Models (LLMs). Aufgrund ihrer Fähigkeit, Beziehungen zwischen Wörtern in riesigen Textmengen zu erfassen, haben sich LLMs besonders zur Erstellung von Text hervorgetan und sind zu einem zentralen Bestandteil in diesem Feld geworden.

LLM ist die Abkürzung für „Large Language Model“, der Technologie hinter Systemen wie ChatGPT der Firma OpenAI.

Generative KI-Modelle, einschließlich LLMs, werden auf Billionen von Wörtern und Milliarden von Parametern trainiert, indem sie aus riesigen Quellen von Originalinhalten lernen, Information zu komprimieren, und diese neu zusammenführen.

Die Technologie verfügt über ein hohes Potenzial, die Produktivität von Fachkräften zu erhöhen und Fachwissen breiter zugänglich zu machen. Generative KI findet Anwendung in einer Vielzahl von Bereichen, von der Erstellung von Text und Bildern bis hin zur Audioproduktion, und hat auch Einsatzmöglichkeiten im öffentlichen Sektor. Für ihre effektive Nutzung sind spezialisiertes Wissen und eine sorgfältige Handhabung erforderlich, insbesondere um Herausforderungen wie unvorhergesehene Modellreaktionen und Verhaltensänderungen nach Updates erfolgreich zu meistern.

Status quo

Mit der Veröffentlichung von ChatGPT wurde generative KI erstmals für eine breite Masse an Benutzerinnen und Benutzern – auch ohne Vorkenntnisse im Bereich künstlicher Intelligenz – erlebbar. Aber nicht nur die Generierung von Texten hat in den letzten Monaten einen Boom erlebt und wurde „massentauglich“, auch Bilder und sogar einfache Videosequenzen können von

unkompliziert zugänglichen KI-Systemen erstellt werden. Große Softwarehersteller sind auf den Zug aufgesprungen und implementieren generative KI zunehmend in ihrer Standardsoftware bzw. im Betriebssystem.

Aufgrund des Potenzials, Kosten zu sparen und Einnahmen zu generieren, werden neue Anwendungen und Entwicklungen im Bereich der generativen KI in atemberaubendem Tempo vorangetrieben.

Generative KI gewinnt auch an Bedeutung, da sie nachweislich die Produktivität von Fachkräften erheblich steigert. Eine Studie des Massachusetts Institute of Technology (MIT) aus dem Jahr 2023 zeigte, dass der Einsatz generativer KI die Produktivität hochqualifizierter Arbeitskräfte um bis zu 40 Prozent erhöhen kann. Diese Technologie ermöglicht es, komplexe Aufgaben effizienter zu bewältigen, insbesondere wenn sie innerhalb ihrer technologischen Möglichkeiten eingesetzt wird.

Generative KI kann die Produktivität von Arbeitskräften erhöhen und bei der Erledigung komplexer Aufgaben unterstützen.

Generative KI bei Standardsoftwareherstellern

Microsoft, Google, Oracle und OpenAI haben kürzlich bedeutende Fortschritte und neue Angebote im Bereich der künstlichen Intelligenz vorgestellt. Microsoft veröffentlichte 2023 den Microsoft Copiloten. Dieser KI-„Begleiter“ kann auf Anfragen antworten und Aktionen ausführen, basierend auf Web- und Unternehmensdaten. Oracle entwickelte den Oracle Cloud Infrastructure (OCI) Generative AI-Dienst. OpenAI lancierte ChatGPT Enterprise, eine Version seines Chatbot-Dienstes mit erweiterten Sicherheits- und Datenschutzfunktionen sowie unbegrenzter Nutzung und Leistungsverbesserungen. Meta veröffentlichte Code Llama, eine auf Codeerstellung fokussierte Version von Llama 2, die sowohl Code als auch natürliche Sprache generieren kann und in mehreren Größen und Varianten verfügbar ist.

Generative KI kann in vielen Branchen angewendet werden, beispielsweise im Bereich der Medizin, der Architektur sowie in vielen Kreativberufen.

Nutzen von generativer KI

Der Nutzen von generativer KI ist vielfältig und branchenübergreifend, z. B. im Gesundheitswesen, wo sie bei der Entwicklung neuer Medikamente hilft, oder in der Architektur, wo sie beim Entwurf innovativer Gebäudestrukturen unterstützt. Auch im Kreativbereich wie in der Werbung und im Marketing bietet sie Möglichkeiten zur Erstellung einzigartiger Inhalte. Durch generative KI werden komplexe Analysen und Datengenerierung zugänglicher, was die Einstiegsschwelle für viele Tätigkeiten senkt.

Die häufigsten Anwendungsfälle für generative KI lassen sich wie folgt kategorisieren:

- **Texterzeugung:**
Die Ausgabe des Modells ist textbasiert (aber nicht darauf beschränkt) auf natürlicher Sprache. Dies ist der Hauptanwendungsfall für LLMs, die auf Transformer-Modellen wie GPT basieren.
Anwendungsfälle umfassen:
 - Zusammenfassung von Text
 - Beantwortung von Fragen
 - Übersetzung zwischen Sprachen
 - Erstellen und Überarbeiten von Code und Konfiguration
 - Beschreibung des Inhalts eines Bildes
- **Bildgenerierung**
 - Die Ausgabe des Modells sind digitale Bilddaten oder 3D-Modellrepräsentationsdaten.
- **Audiogenerierung**
 - Umwandlung von Text in Sprache
 - Generieren von Musik
 - Imitieren von Sprachprofilen
- **Generieren strukturierter Daten**
 - synthetische Daten
 - Anonymisierung von Daten

Herausforderungen und Chancen generativer KI

Generative KI, wie jede disruptive Technologie, steht vor Herausforderungen, die jedoch gleichzeitig als Katalysator für Innovation und kontinuierliche Verbesserung dienen. Die Überwindung dieser Herausforderungen ist nicht nur notwendig, sondern bietet auch die Gelegenheit, zukunftsfähige Lösungen zu entwickeln und neue Fähigkeiten zu erlangen. Stillstand in der Technologieentwicklung kann Rückschritt bedeuten, und das Nichthandeln birgt ebenso Risiken wie die Einführung neuer Technologien. Generative KI bringt spezifische Herausforderungen mit sich, die im Kontext der Anwendungsarchitektur berücksichtigt werden müssen:

1. Halluzination

- > Phänomen, bei dem KI-Modelle fiktive oder irreführende Informationen in ihren Ausgaben erzeugen, die nicht in den Eingabedaten vorhanden sind

Chance:

Das Bewusstsein und die Bekämpfung von „Halluzinationen“ führt zu robusteren Modellen und einem tieferen Verständnis der Grenzen und Möglichkeiten von KI.

Bekannte Systeme wie ChatGPT „halluzinieren“ mitunter: Sie erfinden etwas, das nicht der Realität entspricht.

2. Urheberrecht und geistiges Eigentum

- > häufige Nutzung urheberrechtlich geschützten Materials in Trainingsdaten
- > fehlende Absicherung durch Machine-Learning-Diensteanbieter gegen Plagiat und Urheberrechtsverletzungen
- > Einsatz von Lizenzen, die den Gebrauch in kommerziellen Kontexten limitieren

- > Verantwortung der Nutzer:innen bei der Überprüfung von generierten Inhalten auf Plagiate oder Urheberrechtsverletzungen

Chance:

Die Auseinandersetzung mit Urheberrechtsfragen regt zur Entwicklung neuer rechtlicher Rahmenbedingungen an, die Innovation fördern und gleichzeitig geistiges Eigentum schützen.

3. Kosten für Training und Inferenz

- > hohe Rechenanforderungen beim Training von KI-Modellen
- > Notwendigkeit der Zusammenarbeit zwischen Anwendungsarchitekten, Data Scientists sowie Ingenieurinnen und Ingenieuren
- > Inferenz erfordert weniger Ressourcen als Training, aber der Einsatz von speziellen Prozessoren für optimale Leistung führt zu höheren Hardware- oder Cloud-Service-Kosten.
- > Betriebsausgaben für Modellinferenz sind oft proportional zur Nutzung.

Chance:

Die Investition in effiziente Trainings- und Inferenzmethoden kann langfristige Einsparungen und Wettbewerbsvorteile mit sich bringen.

4. Neue Testherausforderungen

- > Die nicht deterministische Natur der KI erschwert standardisierte Softwaretests und macht diese subjektiver.

Chance: Die Entwicklung neuer Testprotokolle verbessert nicht nur KI-Anwendungen, sondern trägt auch zur allgemeinen Sicherheit in der digitalen Welt bei.

5. Neue Sicherheitsherausforderungen

- > Mit der Popularität von Technologien steigt auch das Interesse von Angreifern, diese zu kompromittieren. Die unstrukturierte Natur von System- und Anwendungsprompts in generativer KI erhöht die Schwierigkeit, sich zu verteidigen.

Chance:

Die Entwicklung neuer Sicherheitsprotokolle verbessert nicht nur KI-Anwendungen, sondern trägt auch zur allgemeinen Sicherheit in der digitalen Welt bei.

6. Alignment

- > bezieht sich auf die Abstimmung der Ziele und Ergebnisse eines generativen KI-Modells mit den Absichten und Erwartungen der Benutzer:innen oder Stakeholder. Es ist wichtig, dass die Ausgaben des Modells nicht nur technisch korrekt, sondern auch kontextuell angemessen, ethisch vertretbar und im Einklang mit den spezifischen Anforderungen der Anwendung sind.

Chance:

Die Abstimmung der KI-Ziele mit den Bedürfnissen der Nutzer:innen fördert ethisch vertretbare und kundenorientierte Technologieentwicklung.

Generative KI in der Verwaltung

Bei der Einführung von KI-basierten Technologien ist im öffentlichen Sektor besondere Sorgfalt geboten, da er Dienstleistungen bereitstellt, die für das Funktionieren des Staates und die Rechte und Pflichten der

Generative KI kann auch in der Verwaltung eingesetzt werden, jedoch gelten besonders hohe Sorgfaltsmaßstäbe.

Bürger:innen wesentlich sind. Die öffentliche Verwaltung muss Schlüsselprinzipien wie Rechenschaftspflicht, Transparenz, Unparteilichkeit und Zuverlässigkeit im Integrationsprozess von KI-Lösungen sorgfältig berücksichtigen.

Anwendungsbeispiel: Large Language Models (Chatbots)

Eine mögliche Anwendung großer Sprachmodelle (LLMs) im öffentlichen Sektor liegt im Bereich von Chatbots und virtuellen Assistenten. Diese Modelle können rund um die Uhr eingesetzt werden, um einen schnellen und effizienten Kundendienst zu bieten, Fragen zu beantworten und grundlegende Probleme ohne menschliches Eingreifen zu lösen. Große Sprachmodelle könnten auch in Entscheidungsprozessen eingesetzt werden, beispielsweise bei der Bewertung von Förderanträgen oder bei der Feststellung der Berechtigung für soziale Dienste. Durch die schnelle und genaue Verarbeitung und Analyse großer Datenmengen haben LLMs das Potenzial, fairere und schnellere Entscheidungen zu unterstützen. Allerdings fehlt LLMs noch ein nuanciertes Verständnis für menschliche Emotionen, Absichten und Kontexte, weshalb ein gewisses Maß an menschlicher Aufsicht weiterhin notwendig sein wird. Ein weiteres Anwendungsgebiet von LLMs in der öffentlichen Verwaltung ist die Dokumenten- oder Textanalyse. Ein LLM könnte darauf trainiert werden, Schlüsselinformationen in komplexen Dokumenten, wie Rechtsverträgen, zu identifizieren, was die Überprüfungszeit durch Beamte reduziert.

Anwendungsbeispiel: Bürger:innen Copilot

Generative KI ermöglicht es, IT-Systeme mit natürlicher Sprache zu verwenden und zu steuern. Um das zu verwirklichen, wird es notwendig sein, die bestehenden Regeln aus dem User Experience Design neu zu denken. Gleichzeitig ist anzunehmen, dass generative KI mit hoher Geschwindigkeit in neue und bestehende Unternehmens-

und Kundenanwendungen hinzugefügt wird. So ist vorstellbar, dass in Zukunft die Benutzer:innen die Erwartung haben, dass sie mit IT-Anwendungen in natürlicher Sprache interagieren können. Diese Entwicklung würde voraussichtlich auch vor digitalen Government-Systemen nicht haltmachen.

Die wahrscheinlich anschaulichste Anwendung von generativer KI ist der Chatbot. Er könnte beispielsweise dazu verwendet werden, Informationen behördlicher Webseiten einfacher zugänglich zu machen. Basierend auf generativen LLMs kann durch das Einbinden von domänenspezifischen Daten und Informationen ein Chatbot für konkrete Anwendungen aufgebaut werden. Es ist absehbar, dass zukünftig Informationen zu Anfragen, wie beispielsweise dem Beantragen eines neuen Reisepasses, vermehrt über Chatbots abgefragt werden könnten. In diesen Systemen werden relevante Datenquellen in Vektordatenbanken gespeichert. Bei Anfragen werden die passenden Daten herausgesucht und dem Modell mitgeschickt. So wird sichergestellt, dass dem Modell die relevanten Datenquellen für die Antwort zur Verfügung stehen. Ebenfalls kann dadurch erreicht werden, dass in der Antwort die Quellen angegeben werden, um eine weitere Recherche zu ermöglichen.

Anwendungsbeispiel: AMS Berufsinformat

Der AMS Berufsinformat ist ein KI-unterstütztes Chattool und beantwortet seit Jänner 2024 Fragen rund um die Themen Berufe, Aus- und Weiterbildung. Es nutzt dafür fortschrittliche KI-Technologie, insbesondere ChatGPT, zur Formulierung dynamischer Antworten. Der AMS Berufsinformat wurde in Zusammenarbeit mit der AMS-IT und der Firma goodguys GmbH entwickelt und wird im BRZ betrieben.

> **AMS Berufsinformat**
www.ams.at/berufsinformat

Anwendungsbeispiel: Prozessoptimierung mit generativer KI

Viele Prozesse können mithilfe von generativer KI optimiert werden. Durch die Möglichkeit, neue Texte auf Basis bestehender Dokumente und Informationen zu generieren, kann das Erstellen von Entwürfen für Schriftstücke eine große Effizienzsteigerung darstellen. Dabei gibt es die Möglichkeit, den Inhalt der Texte zu personalisieren. Ebenfalls kann generative KI für die Extraktion von Wissen und die Erstellung von Zusammenfassungen eingesetzt werden, um die Recherchearbeit von Expertinnen und Experten zu unterstützen.

BRZ-Involvement

Generative KI bringt viele Möglichkeiten für effizientere Arbeitsweisen in IT-Unternehmen wie dem BRZ. Es ist vorstellbar, dass die Technologie bei der Umsetzung von Projekten in vielen Bereichen eine Rolle spielt. In der Entwurfsphase könnte generative KI für das Erstellen von Prototypen verwendet werden. In der Entwicklung könnte der Einsatz von KI-Codingtools für die Generierung von Code, Dokumentation, Tests und Testdaten zur Anwendung kommen, sofern die Nutzung in einem sicheren Rahmen gewährleistet ist.

In der vom BRZ betriebenen Such-Applikation Findok werden Transformermodelle benützt, um Empfehlungslisten für Dokumente zu berechnen, die dem aktuell angezeigten Dokument ähnlich sind. Transformerarchitekturen sind entscheidend für große Sprachmodelle (LLMs), da sie mittels „Attention“-Mechanismen ein tiefgreifendes Verständnis und die Generierung von Text ermöglichen. Um Datenschutz und Sicherheit zu gewährleisten, wird die Berechnung der Ähnlichkeit in der BRZ-Cloud durchgeführt.

Die Entwicklung von Konzepten für den Einsatz von Large Language Models (LLMs) bzw. Sprachmodellen in IT-Verfahren zur Predictive Analytics ist im Gange. LLMs können in verschiedenen

Anwendungsfällen genutzt werden, wie beispielsweise für die Verarbeitung unstrukturierter Daten bei der Auswahl von Fällen, für die automatisierte Erstellung von Risikobeschreibungen und Leitfäden für Risikobewertungen sowie Betrugsbekämpfung. Durch den Einsatz generativer Modelle ist die Erstellung von authentisch wirkenden Bildern und Dokumenten erheblich vereinfacht worden. Um potenzielle Gefahren zu minimieren, ist es unerlässlich, bestehende Betrugsbekämpfungssysteme zu stärken und neue Maßnahmen zu implementieren.

Conclusio

Die Zukunft der generativen KI im öffentlichen Sektor ist nicht nur vielversprechend, sondern auch richtungsweisend für andere Sektoren. Wenn ethische Überlegungen und Datenschutz konsequent berücksichtigt und in die Strategie integriert werden, steht der Weg für transformative Veränderungen offen. Generative KI hat das Potenzial, die öffentliche Verwaltung grundlegend zu revolutionieren – durch Steigerung der Effizienz, Einsparung von Ressourcen und Verbesserung der Dienstleistungen für Bürger:innen.

Die aktive Einbindung aller Stakeholder ist der Schlüssel zur Realisierung dieses Potenzials. Durch eine offene und transparente Zusammenarbeit können Herausforderungen gemeistert und gleichzeitig ein Rahmen für verantwortungsvolle Nutzung und Innovation geschaffen werden. In diesem dynamischen Umfeld wird generative KI nicht nur als ein technologisches Werkzeug, sondern vielmehr als ein Katalysator für positive Veränderungen und verbesserten Bürgerservice dienen.

In den kommenden Jahren sollte die Chance ergriffen werden, die Nutzung der generativen KI im öffentlichen Sektor aktiv zu gestalten. Diese Phase ist entscheidend, um den Grundstein für eine effiziente, inklusive und bürgerfreundliche Verwaltung zu legen. Es liegt an den Beteiligten, nicht nur zu reagieren, sondern die Entwicklung dieser Technologie aktiv voranzutreiben und zu formen.

Zero Trust

Zero Trust (ZT) ist ein Sicherheitskonzept der IT, das darauf abzielt, die traditionelle Netzwerksicherheit zu überwinden und eine umfassende Absicherung von IT-Unternehmensressourcen zu gewährleisten. Das Konzept basiert auf der Annahme, dass ein:e Benutzer:in oder Gerät im Netzwerk nie automatisch vertrauenswürdig ist und daher ständig überprüft und authentifiziert werden muss. Zero Trust ist als Framework für den Schutz digitaler Unternehmensressourcen in der zunehmend cloud- und mobilorientierten Geschäftswelt konzipiert.

Status quo

Der Zero-Trust-Ansatz stellt die traditionelle Vorstellung von Vertrauen innerhalb einer Organisation bzw. innerhalb eines Unternehmens grundsätzlich infrage. Es wird davon ausgegangen, dass Vertrauen, und damit verbunden der Zugriff auf Anwendungen und Systeme, nicht automatisch basierend auf dem Standort, dem Netzwerkzugriff oder einer einmalig durchgeführten Anmeldung (Authentifizierung) einer Benutzerin bzw. eines Benutzers gewährt werden sollte. Stattdessen wird das Vertrauen durch kontinuierliche Überprüfung und Authentifizierung von Benutzerinnen und Benutzern, Geräten (Client und Server) und Anwendungen gewonnen.

Das Zero-Trust-Konzept wurde erstmals in den 1990er-Jahren beschrieben und hat sich weithin als neues Security-Paradigma etabliert.

Auf einen Blick: Grundprinzipien von Zero Trust

Zero Trust basiert auf vier grundlegenden Prinzipien:

1. Jeder Benutzerin und jedem Benutzer und jedem Gerät wird nur jener minimale Zugriff gewährt, der für die Erfüllung ihrer oder seiner Aufgaben erforderlich ist.

Zero Trust ist eine effektive Methode, um die Sicherheit von Unternehmensressourcen zu verbessern und das Risiko von Datenverlusten und Cyberangriffen zu verringern.

2. Die Identität jeder Benutzerin und jedes Benutzers und jedes Geräts wird ständig überprüft und authentifiziert.
3. Der Datenverkehr innerhalb des Netzwerks wird verschlüsselt und überwacht.
4. Der Datenverkehr zwischen Benutzerinnen sowie Benutzern und Ressourcen wird kontinuierlich überwacht und analysiert, um verdächtige Aktivitäten zu erkennen.

Zero Trust bietet eine Reihe von Vorteilen für Unternehmen. Durch die Implementierung dieses Konzepts können Unternehmen ihre Sicherheitsmaßnahmen verbessern und das Risiko von Datenverlusten und Cyberangriffen verringern. Zero Trust ermöglicht auch eine granulare Kontrolle über den Zugriff auf Unternehmensressourcen und erhöht die Transparenz und Sichtbarkeit des Netzwerkverkehrs. Insgesamt bietet Zero Trust eine effektive Methode, um die Sicherheit von Unternehmensressourcen zu verbessern und das Risiko von Datenverlusten und Cyberangriffen zu verringern. Es erfordert jedoch eine sorgfältige Planung und Implementierung, um die volle Wirkung zu erzielen.

Umsetzung des Zero-Trust-Ansatzes

Aus der Definition des „Nullvertrauens“ leiten sich folgende Erfordernisse an IT-Architekturen und Systeme ab:

1. Misstrauen gegenüber allen Verbindungen:

Der Zero-Trust-Ansatz geht davon aus, dass grundsätzlich keine Verbindung oder Kommunikation im Netzwerk vertrauenswürdig ist. Das gilt sowohl für interne als auch externe Verbindungen. Alle Kommunikationen und Transaktionen müssen daher gründlich überprüft werden.

2. Identity Management:

Identitäten sind ein zentraler Bestandteil in einem Zero-Trust-Modell. Alle Entitäten – sei es eine Person, eine Maschine oder eine Anwendung – müssen ihre Identität nachweisen, bevor auf Ressourcen zugegriffen wird. Dies erfordert eine robuste Authentifizierung und Autorisierung.

3. Kontinuierliche Überwachung und Analyse:

Zero Trust setzt auf kontinuierliche Überwachung und Analyse des Netzwerkverkehrs und der Systeme. Anomalien können auf Sicherheitsverletzungen hinweisen. Die Überwachung erstreckt sich auch auf die Lieferkette, um verdächtige Aktivitäten oder Angriffe frühzeitig zu erkennen.

4. Datenverschlüsselung:

Um sicherzustellen, dass selbst bei einem Sicherheitsvorfall Daten geschützt bleiben, ist die Verschlüsselung von entscheidender Bedeutung. Dies gilt sowohl für Daten im Ruhezustand als auch für Daten während der Übertragung.

5. Segmentierung des Netzwerks:

Die Segmentierung des Netzwerks ist ein weiterer zentraler Aspekt von Zero Trust. Indem das Netzwerk in verschiedene Segmente unterteilt wird, kann das Risiko einer Beeinträchtigung des gesamten Systems minimiert werden.

6. Lieferketten-Risikomanagement:

Um die Sicherheit über die gesamte Lieferkette hinweg sicherzustellen, ist es wichtig, dass Unternehmen nicht nur ihre eigenen Sicherheitspraktiken stärken, sondern auch gewährleisten, dass ihre Lieferanten und Partner strenge Sicherheitsstandards einhalten. Dies kann Audits, Vertragsbestandteile und regelmäßige Überprüfungen umfassen.

7. Asset Management:

Eine lückenlose Dokumentation der Unternehmens-Assets bildet die Basis für ein lückenloses Berechtigungssystem für Anwendungen, Nutzer:innen und Geräte.

8. Sicherheitsbewusstsein fördern:

Die Kultur des Unternehmens im Umgang mit dem Sicherheitsbewusstsein ist ein entscheidender Faktor für eine erfolgreiche Umsetzung des Zero-Trust-Ansatzes. Alle Beteiligten im Unternehmen, von Mitarbeiterinnen und Mitarbeitern bis hin zu Lieferanten (Unternehmen), müssen sich der Bedeutung von Sicherheit bewusst sein und entsprechende Schulungen erhalten.

Maßnahmen zur Umsetzung

Zur Umsetzung eines Zero-Trust-Konzepts bedarf es einer Reihe unterschiedlicher Maßnahmen:

1. **Awareness** schaffen
2. **Verwaltung und Inventarisierung von unternehmensweiten Assets**, wie etwa Geräte, Systeme und Anwendungen. Ebenso betroffen sind Personen (Mitarbeiter:innen), Verträge, Standards und Regulative.
3. **Asset-Klassifizierung**: Jedes erfasste Asset wird entsprechend seiner Bedeutung und Risikostufe klassifiziert. Die Klassifizierung geht einher mit einer Bewertung des Assets, in der die Bedeutung für den Unternehmenszweck beurteilt wird. Diese Klassifizierung ermöglicht es, den Schutzbedarf und das Risiko des Assets zu ermitteln und auf Basis dessen entsprechende Sicherheitsrichtlinien festzulegen und Risikominimierungsmaßnahmen abzuleiten.
4. **Kontinuierliche Überwachung von Assets** und Screening nach ungewöhnlichen Aktivitäten bzw. Sicherheitsverletzungen
5. **Identity Management**, etwa durch Multi-Faktor-Authentifizierung

6. **Schutz von IT-Assets** durch Festlegung von Sicherheitsrichtlinien, Verschlüsselung oder die Umsetzung des „Least-Privilege-Prinzips“

7. **Endpoint Protection**, d. h. Schutz der Endgeräte

Herausforderungen bei der Umsetzung von Zero Trust

Die Einführung einer Zero-Trust-Denkweise stellt Unternehmen und Organisationen vor die Herausforderung, einen kulturellen Wandel für Mitarbeitende anzustoßen. Dieser kulturelle Wandel kann Mitarbeiterinnen und Mitarbeitern durch Schulungen, Sensibilisierungsprogramme und eine kontinuierliche Kommunikation über die Vorteile und Ziele von Zero Trust nähergebracht werden.

Der Faktor Mensch

Menschen, das heißt in der Regel die Mitarbeiter:innen eines Unternehmens, haben das größte Potenzial, die Assets eines Unternehmens zu schützen, aber gleichzeitig auch das größte Potenzial, Schaden zu verursachen. Schulungen, spielerische Awareness-Programme und aktives Informationsmanagement zu unternehmensweiten Sicherheitsprogrammen sind die Grundlage für ein weitreichendes Sicherheitsbewusstsein und schaffen Verständnis für die Sicherheitsaktivitäten im Unternehmen. Das gilt nicht nur für interne Mitarbeiter:innen, sondern auch für Externe und Lieferanten.

Der Angst vor vollständiger Überwachung von Mitarbeiterinnen und Mitarbeitern bei der Umsetzung von Zero-Trust-Maßnahmen ist ein Hemmschuh für den Einsatz dieses Modells. Der Grat zwischen notwendigen Aufzeichnungen und vollständiger Überwachung ist schmal.

Zero Trust ist somit nicht nur ein technisches Konzept, sondern berührt auch soziale Aspekte.

Zero Trust bedeutet auch einen kulturellen Wandel im Unternehmen herbeizuführen.

Zero Trust ist nicht nur ein technischer Ansatz, sondern berührt auch soziale Aspekte, etwa die Frage nach dem Umfang von Überwachungsmaßnahmen von Mitarbeitenden eines Unternehmens.

Datenschutz

Bei Zero Trust geht es auch darum, Daten zu sammeln und zu analysieren, um das Nutzer:innen-Verhalten zu bewerten und Anomalien zu erkennen. Unternehmen und Organisationen müssen daher das Sicherheitsbedürfnis mit Datenschutzbedenken in Einklang bringen. Die Implementierung von Datenschutzmaßnahmen wie der Anonymisierung von Daten oder der Einführung strenger Zugriffskontrollen, um den Zugriff auf vertrauliche Informationen einzuschränken, ist von entscheidender Bedeutung, um das Vertrauen zu wahren und die Datenschutzbestimmungen einzuhalten. Die Einbeziehung der Betriebsratsorganisation oder ähnlichen Funktionen zur Kontrolle der sinnvollen, notwendigen Umsetzung von Zero-Trust-Maßnahmen sind Basis für ein Vertrauen der Mitarbeiter:innen in das Modell.

Conclusio

Das Zero-Trust-Modell erhöht die Sicherheit in einem Unternehmen bzw. einer Organisation signifikant, führt aber auch zu hohem Umsetzungsaufwand und zu kulturellen Veränderungen. Die Schritte zur Einführung sind so klein wie möglich zu halten, um die bestehenden Prozesse und Mitarbeiter:innen nicht zu überfordern. Generell sind insbesondere die Akzeptanz und erfolgreiche Schulung des Personals bei der Umsetzung der Grundstein für eine erfolgreiche Einführung eines Zero-Trust-Konzeptes.

Impressum

Medieninhaber, Herausgeber:
Bundesrechenzentrum GmbH
Hintere Zollamtsstraße 4, 1030 Wien
kommunikation@brz.gv.at

Verlagsort: Wien

Projektleitung: Julian Unger

Redaktion:
Aloisius Caraet, Johann Kalhs, Lisa Neuhofer,
Werner Neuwirth, Nikolaus Schrack,
Robert Seyfriedsberger, Hakim Tafer,
Alessandro Volcich

Grafik: trafikant – Handel mit Gestaltung, 1050 Wien

Lektorat: Mag. Michaela Kapusta

Bildnachweise:
BRZ/Klaus Vyhnaek (S. 4)
BMF (S. 5)

Druck/Herstellungsort:
Print Alliance HAV Produktions GmbH
Druckhausstraße 1, 2540 Bad Vöslau

Alle Angaben ohne Gewähr. Stand: 02/2024.

