Bundesministerium
Finanzen

Bundesministerium
Inneres

Digital Austria

#zukunftdigitalgestalten

DIGITALER AKTIONSPLAN

Digitale Souveränität für Österreich

Inhalt

Einleitung

Einleitung

Österreich ist mit anderen Staaten auf vielfältige Weise ökonomisch, technologisch und politisch vernetzt. Diese Vernetzung ist Treiber von Innovation und Austausch. Sie sichert Wirtschaftskraft und Wohlstand. Mit der zunehmenden Vernetzung gehen aber auch sicherheitspolitische Risiken einher. Staatliche wie nicht-staatliche Akteure verfolgen eigene Interessen, die nicht zwangsläufig mit den Wertvorstellungen, Zielen und Prinzipien Österreichs und Europas übereinstimmen. Gerade die letzten Jahre haben gezeigt, dass sich bisher kooperative Beziehungen schnell zu Konflikten umwandeln können. Damit werden Abhängigkeiten von einzelnen Staaten, Regionen oder Unternehmen zu einem strategischen Risiko.

Diese Gefahren sind im Bereich der digitalen Technologien – aufgrund der hohen Vernetzung und der starken Stellung einzelner Akteure – besonders relevant. Mit der zunehmenden Digitalisierung des Staats- und Verwaltungshandelns nehmen auch die digitale Abhängigkeit und Angreifbarkeit der staatlichen Einrichtungen zu. Das Bedrohungspotenzial reicht von einzelnen Störungen, etwa durch punktuelle Hackerangriffe, bis hin zu großflächigen Cyberattacken, die Ausmaße eines „digitalen Staatsnotstandes“ annehmen können.

→ Die Digitalisierung verstärkt generell klassische Sicherheitsrisiken (z. B. Cyberkriminalität), sie bewirkt aber neue, globale Bedrohungslagen in einer bisher unbekannten Intensität (z. B. Radikalisierung von Online-Nutzern, gezielte Verbreitung von Fake-News, Nutzung von Deep-Fakes, Gefährdung demokratiepolitisch relevanter Infrastruktur). Gleichzeitig eröffnet die digitale Transformation auch neue Möglichkeiten für sicherheitsrelevante Akteure zum Schutz freier Gesellschaften (z. B. Einsatz neuer Kommunikationsmöglichkeiten, effizientere Methoden der Informationsgewinnung für Einsatzorganisationen und Verwaltung).

→ Gerade angesichts der sich weiter verändernden „Weltordnung" sind die Europäische Union und Österreich doppelt gefordert: So muss sich die EU als eigenständiger, sicherheitspolitisch handlungsfähiger Akteur etablieren, um ihre Werte und Interessen fördern zu können. Zudem gilt es, den inneren Zusammenhalt der EU-Mitgliedsstaaten zu gewährleisten. Beides fordert die EU und Österreich auch im digitalen Bereich.

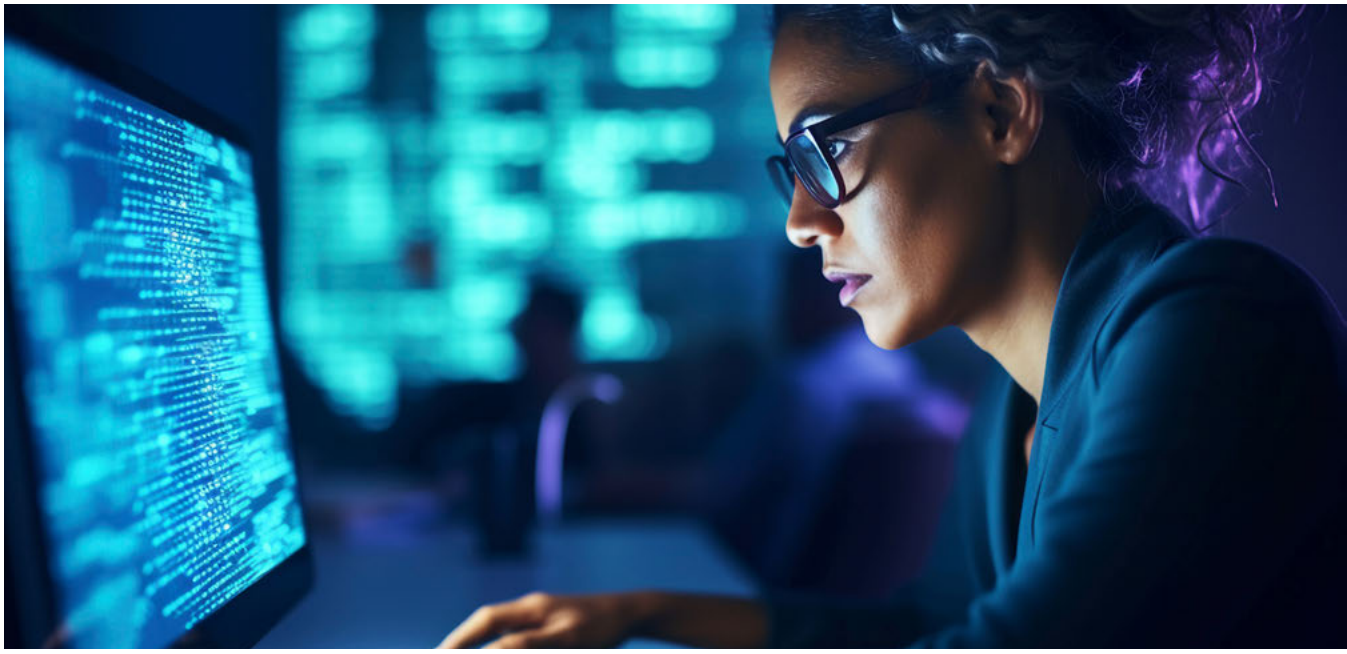
→ Vor diesem Hintergrund gewinnt in Wirtschaft, Wissenschaft und Verwaltung das Konzept der „Digitalen Souveränität" immer mehr an Bedeutung. Es zielt darauf ab, selbstbestimmtes digitales Handeln auch in einer vernetzten und von Abhängigkeiten geprägten Umgebung zu gewährleisten. Für den Digitalen Aktionsplan „Digitale Souveränität in einer vernetzten Welt" wurden daher auf Grundlage wissenschaftlicher Befunde und von Expert:innengesprächen ein Bewertungsmodell sowie Empfehlungen für „Digitale Souveränität" entwickelt.

„Digitale Souveränität“ als staatliche Aufgabe

„Digitale Souveränität“ als staatliche Aufgabe

→ „Digitale Souveränität“ zu wahren, ist Ausfluss verschiedener Rechtspflichten des Staates, die sich aus dem Verfassungs- und dem durch das EU-Recht beeinflussten Gesetzesrecht ergeben. Eine für den vorliegenden Digitalen Aktionsplan „Digitale Souveränität“ durchgeführte Analyse des LIT Law Lab zeigt: Für Digitalisierungsmaßnahmen gelten prinzipiell dieselben verfassungsrechtlichen Grundsätze und Anforderungen wie sonst für die staatliche Souveränität. Grundlegend ist die Ausübung der Staatsgewalt als Prozess der Erzeugung und Vollziehung von Rechtsnormen zu gewährleisten. Einem „digitalen Staatsnotstand“ ist dabei ebenso vorzubeugen wie herkömmlichen Formen des Staatsnotstands. Außerdem sind die Grundrechte und die ihnen inhärenten Schutzpflichten auch dann zu wahren, wenn das Staats- und Verwaltungshandeln zunehmend in den digitalen Raum verlagert wird.

→ Auch das einfache Gesetzesrecht setzt laut juristischer Analyse in vielfältiger Weise das Funktionieren der staatlichen Organe und ihrer Infrastruktur voraus – und zwar unabhängig davon, ob das Staats- und Verwaltungshandeln in analoger oder digitaler Form erfolgt. Im einfachen Gesetzesrecht finden sich mitunter sehr spezifische Anforderungen für die digitale Sicherheit (z. B. NISG, Entwurf zu einem B-KSG). Dazu gehören auch die vergaberechtlichen Vorgaben für die Beschaffung resilienter Technologie. Eine Weiterentwicklung des Gesetzesrechts im Sinne der Stärkung und Absicherung der digitalen Sicherheit und Resilienz war und ist vor allem aufgrund zahlreicher unionsrechtlicher Rechtssetzungsinitiativen geboten.



→ Im Unionsrecht finden sich sektorspezifische Regelungen für bestimmte Bereiche und Aspekte der digitalen Sicherheit sowie – in Gestalt der DSGVO – generelle Regelungen über notwendige technische und organisatorische Maßnahmen wie für die digitale staatliche Kommunikation und den Datenexport. Die Anforderungen der DSGVO an ein Outsourcing von IT-Dienstleistungen und die staatliche Datenverwaltung und -sicherung sind mitunter sehr weitreichend. In sektorspezifischen Bereichen bestehen umfangreiche Regelungswerke vor allem für den Bereich der Cybersicherheit (NIS-RL, NIS-VO, NIS2-RL, Cyber Security Act, Cyber Resilience Act).

→ Eine staatliche Digitalisierungsstrategie muss laut Analyse auch die aus allen genannten Rechtsquellen resultierende „Vorsorgeverantwortung“ des Staates gegenüber Cyberbedrohungen einschließen. Staats- und Verwaltungshandeln muss unabhängig davon gewährleistet sein, ob es analog oder digital stattfindet. Wesentliche Bausteine dafür sind nicht nur eine Reduktion digitaler Abhängigkeiten („Insourcing“), eine Autarkie und Robustheit der IT-Systeme und eine bessere Vernetzung und Zusammenarbeit, sondern auch eine personelle Ausstattung der Verwaltung mit IT-Expert:innen, welche die Abhängigkeit von externen Dienstleister:innen erheblich reduzieren können, so die Analyse des LIT Law Lab.

Autonomes Handeln sichern

Autonomes Handeln sichern

In der Diskussion über „Digitale Souveränität“ geht es nicht um technologische Autarkie, sondern um autonomes Handeln. Nach der Definition des Kompetenzzentrums Öffentliche IT von 2017, der auch der Digitale Aktionsplan folgt, ist „Digitale Souveränität“ die „Summe aller Fähigkeiten und Möglichkeiten von Individuen und Institutionen, ihre Rolle(n) in der digitalen Welt selbstständig, selbstbestimmt und sicher ausüben zu können.“

Der Anspruch „Digitaler Souveränität“ ist es, die Fähigkeit für autonomes Handeln zu erhalten, zwischen eigenen Lösungen und Optionen vertrauenswürdiger globaler Partner frei und verantwortungsbewusst wählen zu können, und EU-rechtliche und nationale gesetzliche Bestimmungen (z. B. GPDR, AI-Legal Act, Chip-Act) innerhalb der eigenen Territorialgrenzen durchsetzen zu können. Wichtige Dimensionen der „Digitalen Souveränität“ sind in diesem Sinn nationale Sicherheit, vertrauenswürdige Infrastruktur und handlungsfähige Wirtschaft.

Bewertungs-modell

Bewertungsmodell für „Digitale Souveränität“ – der digitale Souveränitäts-kompass

→ Im Rahmen des Digitalen Aktionsplans wurde ein Bewertungsmodell für „Digitale Souveränität“ erstellt, dessen Ergebnisse sich in einem „digitalen Souveränitätskompass“ visualisieren lassen. Das Modell soll als Orientierungsinstrument für die österreichische Verwaltung und (kritische) Infrastruktur dienen und die Ableitung von kurz-, mittel- und langfristigen Maßnahmen für mehr „Digitale Souveränität“ ermöglichen.

→ Zur Umsetzung des Modells ist es zunächst erforderlich, bestehende (digitale) Abhängigkeiten insbesondere in den Bereichen Herstellung, Beschaffung und Anwendung systematisch zu identifizieren. Bei der Analyse ist zwischen den „technologischen Schichten“ Mikrochips, Netze und Kommunikationsinfrastruktur, Betriebssysteme und Software-Technologien, Cloud Computing und Daten zu differenzieren.

Technologische Schichten

Diese Schichten werden in vier digitalen Souveränitätsdimensionen bewertet.

1. NUTZUNGSSOUVERÄNITÄT

Sie umfasst Kompetenzen und Ressourcen für die Nutzung aller aktuell vorhandenen digitalen Technologien für die Umsetzung von institutionellen Anforderungen.

2. BETRIEBSSOUVERÄNITÄT

Sie umfasst Kompetenzen und Ressourcen für die Gestaltung und den Betrieb von technischen Infrastrukturen. Davon im Besonderen erfasst sind die Bewertung von Sicherheit, Resilienz, Wirtschaftlichkeit oder Skalierbarkeit.

3. PRODUKTIONSSOUVERÄNITÄT

Diese Dimension umfasst Kompetenzen und Ressourcen zur Fertigung von Hardware oder Software.

4. FORSCHUNGS- UND ENTWICKLUNGSSOUVERÄNITÄT

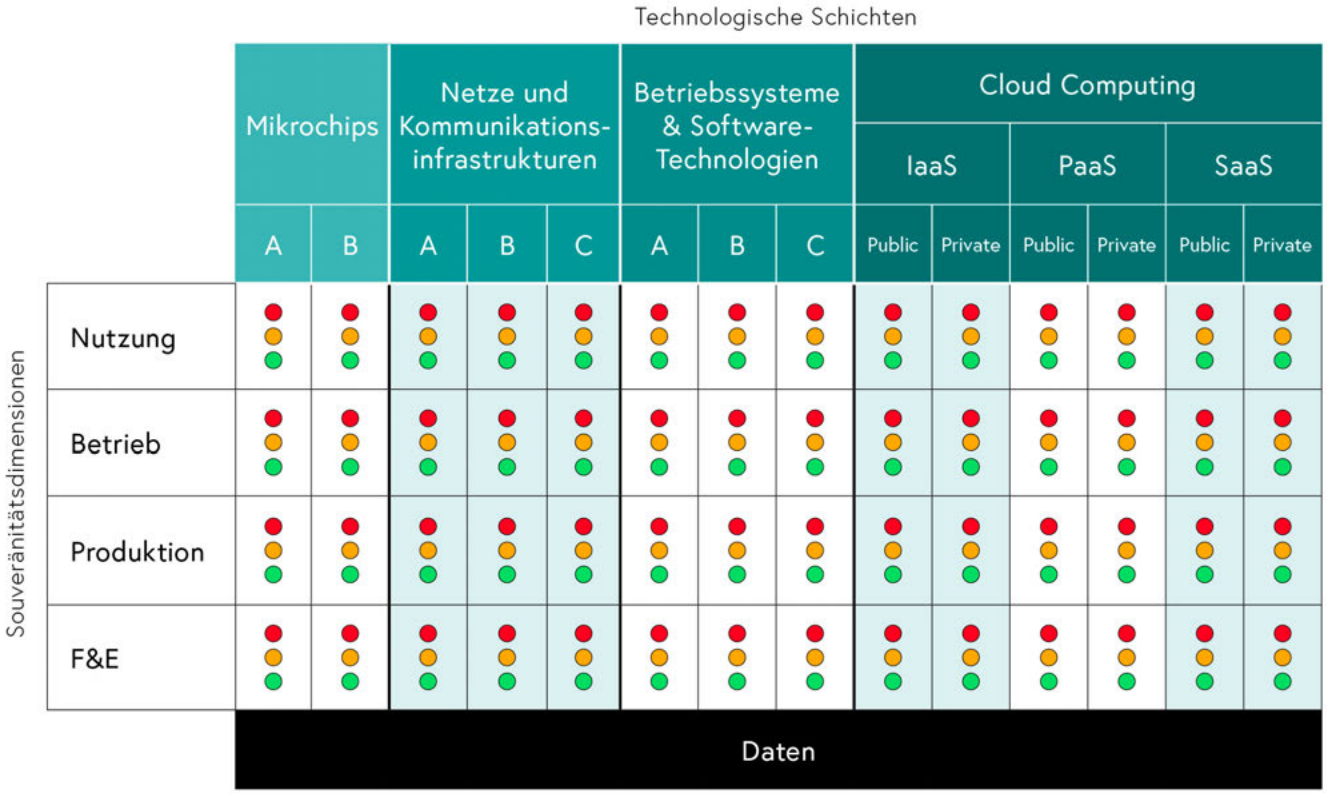
Sie umfasst Kompetenzen und Ressourcen zur Forschung in Industrie und Wissenschaft zur Informationstechnologie – von Mikrochips über Software bis hin zu Daten.

Souveränitätsdimensionen

Nutzung	Betrieb	Produktion	F&E

→ Behörden, einzelne Branchen oder Unternehmen kritischer Infrastruktur, die für sich selbst bestimmte Ambitionsniveaus („zu erreichender Status") für alle technologischen Schichten anhand der vier Souveränitätsdimensionen festgelegt haben, können auf dieser Basis in den einzelnen Technologieschichten eine Risiko-Nutzen-Bewertung für ihre Abhängigkeiten durchführen und daraus Maßnahmen für sich selbst ableiten.

BEWERTUNGSMODELL
DIGITALER SOUVERÄNITÄTSKOMPASS



Exemplarische Darstellung der Bewertung

Die Bewertung „Digitaler Souveränität" wird im „Souveränitätskompass" in Form eines Ampelsystems veranschaulicht. Damit kann vereinfacht aufgezeigt werden, ob die jeweilige Souveränitätsdimension für eine bestimmte Komponente einer technologischen Schicht sicherheitspolitisch relevant (rot), relevant (gelb) oder unbedenklich (grün) ist.

Beispiele für Souveränitätsdimensionen

Der nachfolgende Überblick zeigt mögliche Ausprägungen der Souveränitäts-dimensionen in den einzelnen technologischen Schichten.

MIKROCHIPS

Im Österreichischen Forschungs- und Technologiebericht 2022 wird das Ziel definiert, Forschung und Entwicklung im Halbleiterbereich bis 2030 voranzu-treiben. Österreich zählt bei der Mikroelektronik mit innovativen Unternehmen bereits zu einem bedeutenden Standort in Europa und kann von öffentlichen Förderungen und privaten Investitionen profitieren.

NETZE UND KOMMUNIKATIONSINFRASTRUKTUREN

Im Bereich der 5G-Technologie setzen zukünftige 5G-Leitmärkte auf innovative Netzwerktechnik aus Europa. Die Etablierung einer 5G-Plattform mit interessier-ten österreichischen Stakeholdern, wie etwa Netzbetreibern, Diensteanbietern, Behörden, Herstellern, Leitbetrieben und Interessenvertretungen, kann zu einer Bündelung der Aktivitäten beitragen und Synergieeffekte bewirken.

BETRIEBSSYSTEME UND SOFTWARE-TECHNOLOGIEN

Die Bedeutung von Open-Source-Software nimmt aus staatlicher Perspektive zu. Der Diskurs zur Abhängigkeit von Betriebssystemen und Software-Technologien hat sich verschoben: Der Fokus liegt zunehmend auf Cloud Computing.

CLOUD COMPUTING

Die Qualität der Cloud-Umgebungen von Hyperscalern zu erreichen, ist aufgrund des Entwicklungsvorsprungs und der hohen Investitionssummen in Österreich nur schwer bzw. nicht erreichbar. Aus Perspektive des öffentlichen Sektors emp-fiehlt sich eine breite Nutzung des vorhandenen Angebots von Public Clouds.

DATEN

Wichtige Möglichkeiten und Kompetenz zur Nutzung. Für staatliche Register ist notwendig, dass die Daten auf einer behördeneigenen oder von staatlicher Seite wirtschaftlich beherrschten Infrastruktur verarbeitet werden, wie sie in Österreich beispielsweise durch die BRZ GmbH betrieben wird.

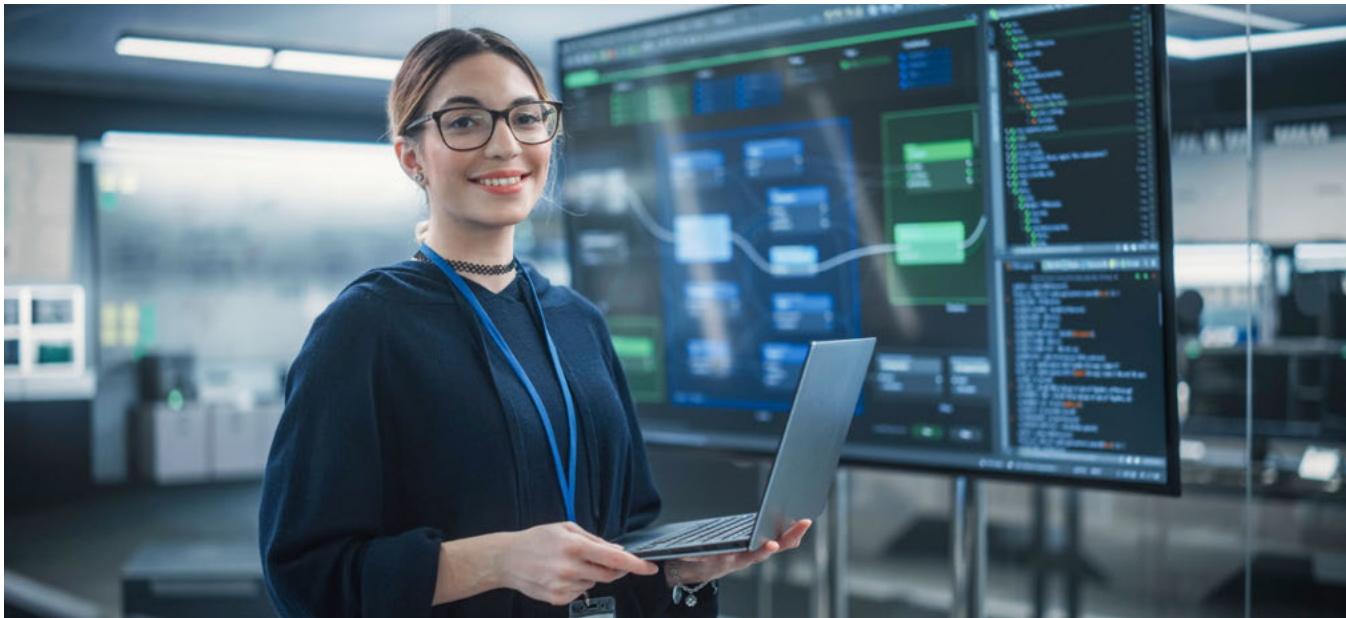
Empfehlungen

Empfehlungen für „Digitale Souveränität“

Zur Entwicklung und Stärkung „Digitaler Souveränität“ empfehlen die Expert:innen des Digitalen Aktionsplans auf Basis des vorgelegten Bewertungsmodells vier zentrale Maßnahmenansätze.

1. ENTWICKLUNG „DIGITALER THEMENKOMPASS FREIHEIT UND SICHERHEIT“

Um vorausschauend einschätzen zu können, welche digitalen Entwicklungen besonders relevant für die Gewährleistung digitaler Souveränität sind, ist eine fortlaufende Identifikation, Bewertung und Priorisierung sicherheitspolitisch relevanter digitaler Themen mittels Szenariotechnik empfehlenswert. Durch eine permanente Umfeldbetrachtung können Ambitionsniveaus der „Digitalen Souveränität“ definiert sowie frühzeitig Handlungsoptionen und Gegenmaßnahmen für unerwünschte Entwicklungen abgeleitet werden.



2. STRATEGISCHE DISKUSSION DER TECHNOLOGISCHEN SCHICHTEN UND FESTLEGUNG DES (NATIONALEN) AMBITIONSNIVEAUS

Bei der Bewertung der „Digitalen Souveränität" bzw. beim Umgang mit Abhängigkeiten auf Basis der Ergebnisse des „Souveränitätskompasses" handelt es sich in erster Linie um strategische Entscheidungen. Sie erfordern stets eine differenzierte und individuelle Betrachtung von spezifischen Technologiebereichen.

3. ANWENDUNG DES BEWERTUNGSMODELLS DURCH EINZELNE ORGANISATIONEN UND KRITISCHE INFRASTRUKTUREN

Für die Festsetzung von konkreten Ambitionsniveaus „Digitaler Souveränität" ist es notwendig, dass Behörden und kritische Infrastruktur für sich selbst herausarbeiten, welche Abhängigkeiten bestehen und wie sie diese managen. Angesichts kritischer Abhängigkeiten oder Defiziten in der Nutzung von Technologien sind Risikoanalysen zweckmäßig.

4. ANWENDUNG DES BEWERTUNGSMODELLS AUF DIE BESCHAFFUNG

Die Nutzung des Bewertungsmodells und die Prüfung der Souveränitätsdimensionen der zu beschaffenden Komponenten ermöglicht es, Beschaffungsentscheidungen vorausschauend zu treffen.

Flankierende standortpolitische Maßnahmen und Rahmenbedingungen für mehr „Digitale Souveränität" sind u. a. gezielte Innovationsförderung, digitaler Kompetenzaufbau, die Stärkung des digitalen Grundverständnisses der Verwaltung, die Ausweitung der Förderprogramme KIRAS und FORTE, die Weiterentwicklung der Beschaffung mit Blick auf Sicherheitsfragen und der Ausbau europäischer Kooperationen.

IMPRESSUM

Herausgeber und inhaltliche Verantwortlichkeit: Bundesministerium für Finanzen, Johannesgasse 5, 1010 Wien, Austria, www.digitalaustria.gv.at • Fotografie: Adobe Stock, S. 08 KI-generiert • Änderungen und Druckfehler vorbehalten • Wien, November 2023