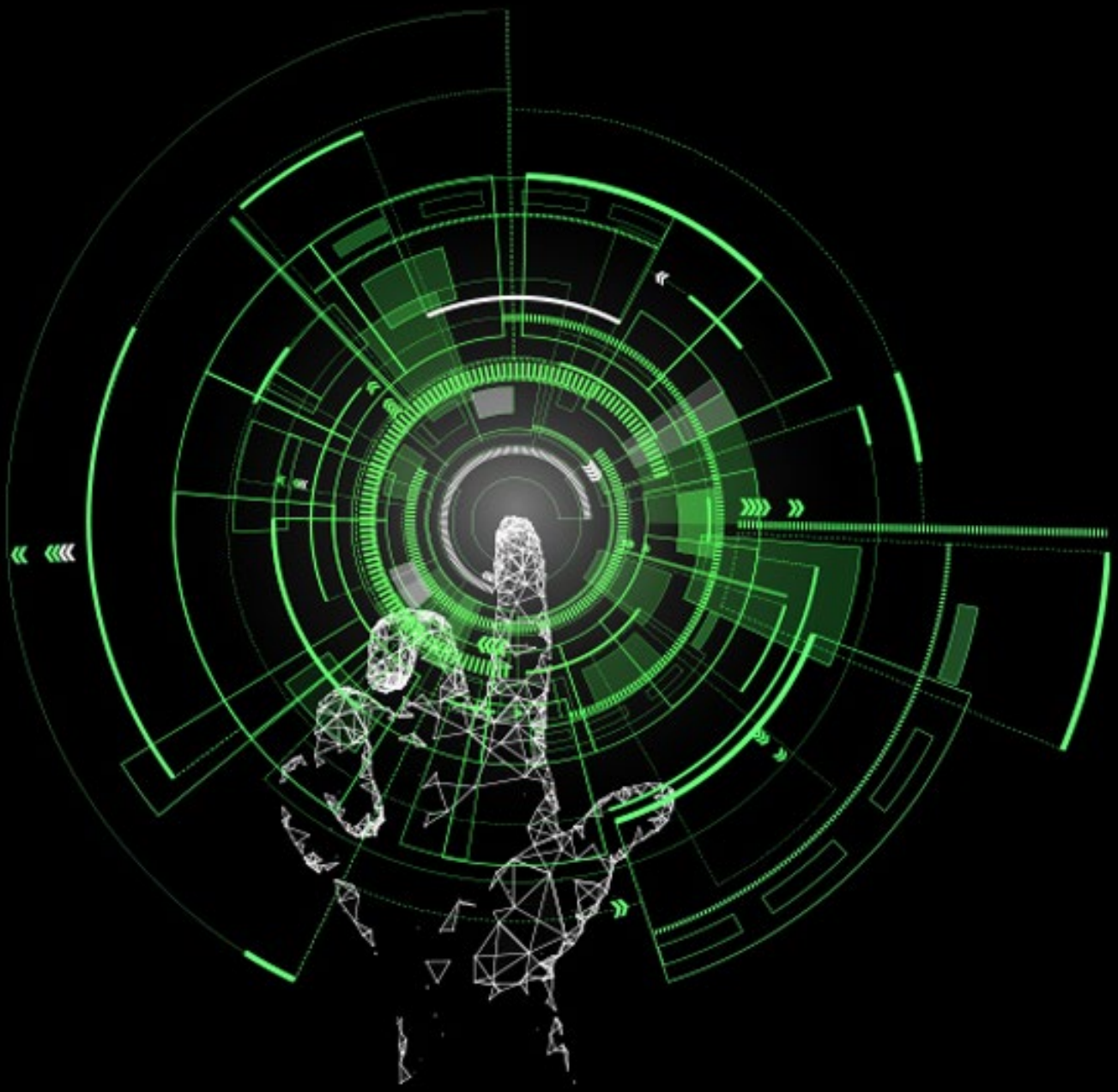
Deloitte.



Mit digitaler Souveränität ins europäische digitale Jahrzehnt

MAKING AN IMPACT THAT MATTERS since 1845

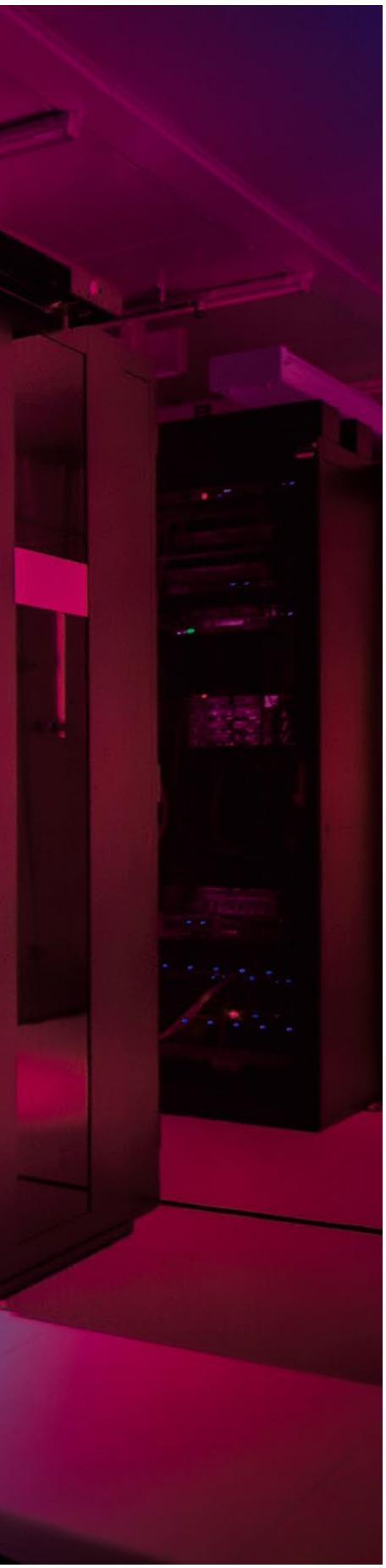
Was bedeutet digitale Souveränität für Europa?

In ihrer ersten „State of the Union Speech“ hat Ursula von der Leyen, Präsidentin der Europäischen Kommission, den Start in das europäische digitale Jahrzehnt ausgerufen.[1] Damit möchte die Europäische Union (EU) nichts anderes erreichen, als die digitale Souveränität der Union sowie die ihrer Mitgliedsstaaten in den Fokus zu rücken. Die EU hat die Dynamik von disruptiven Technologien, die die wirtschaftliche und soziale Entwicklung vorangetrieben haben und die eine ständig steigende Nachfrage nach digitalen Angeboten und Dienstleistungen nach sich ziehen, erkannt.

Auch im politischen Berlin ist das Schlagwort digitale Souveränität in aller Munde. Doch was ist das genau? Möchte sich die EU vor internationalen Digitalunternehmen abschotten und einen „Digitalen Eisernen Vorhang“ errichten? Keineswegs. Folgt man der Interpretation des Kommissars für den Binnenmarkt der EU Thierry Breton, so bedeutet digitale Souveränität nicht, sich technologisch abzuschotten, sondern vielmehr, europäische digitale Lösungen und technologische Kapazitäten weiterzuentwickeln, Fachkräfte auszubilden und in digitale Infrastruktur zu investieren. „Es geht nicht darum, der Versuchung der Isolation oder des Rückzugs in sich selbst nachzugeben, was unseren Interessen, unseren Werten und unserer Kultur zuwiderläuft. Es geht darum, Entscheidungen zu treffen, die für die Zukunft unserer Mitbürger entscheidend sein werden, indem wir europäische Technologien und Alternativen entwickeln, ohne die es weder Autonomie noch Souveränität geben kann.“[2] In die gleiche Kerbe schlugen Angela Merkel und die Regierungschefinnen von Dänemark, Estland und Finnland in ihrem offenen Brief an die Europäische Kommission: „Digitale Souveränität heißt für uns, auf unseren Stärken aufzubauen und unsere strategischen Schwächen zu reduzieren, nicht andere auszugrenzen oder protektionistisch zu handeln.“[3]

„Digitale Souveränität heißt für uns, auf unseren Stärken aufzubauen und unsere strategischen Schwächen zu reduzieren, nicht andere auszugrenzen oder protektionistisch zu handeln.“

Offener Brief von Angela Merkel, Kaja Kallas, Mette Frederiksen und Sanna Marin an die Europäische Kommission



Finanzielle Förderung

Um für das hehre Ziel der digitalen Souveränität aufzukommen, muss die EU die finanziellen Mittel für technologische Innovation in Europa erheblich anheben.

Die Finanzierung kommt zum einen aus dem Recovery Fund der EU – so soll ein Fünftel des 750 Milliarden Euro großen Corona-Wiederaufbaufonds – „Next Generation EU" genannt – in die digitale Transformation der EU fließen.[4] Zum anderen kommen weitere Mittel aus dem regulären EU-Haushalt, den Haushalten der Mitgliedsstaaten sowie von erhofften Investitionen der europäischen Unternehmen. Das Digital Europe Program[5] steuert so in den kommenden Jahren bis zu 20 Milliarden Euro für Digitalisierungsprojekte bei. Geld im Haushalt einzuplanen, wird allerdings nicht ausreichen – die finanziellen Mittel müssen in konkreten Initiativen zielgerichtet investiert werden.

Die finanziellen Mittel von EU, Mitgliedsstaaten und europäischen Unternehmen müssen in konkreten Initiativen zielgerichtet investiert werden.

Digitale Initiativen auf Europaebene

Im Jahr 2020 hat die Europäische Kommission ihre Bemühungen trotz und auch aufgrund der Corona-Pandemie noch einmal deutlich verstärkt, digitale Strategien veröffentlicht und sektorübergreifende Initiativen vorgeschlagen, um somit das Fundament für die europäische digitale Souveränität zu legen.

Künstliche Intelligenz

Den Auftakt hat das Weißbuch zur künstlichen Intelligenz gemacht, in dem die EU ihren Anspruch untermauert, führend in diesem wichtigen Feld zu werden. Dieses Ziel soll mit einem dualen Ökosystem der Exzellenz und des Vertrauens erreicht werden – „vertrauenswürdige KI" (trustworthy AI) made in Europe.[6] Deloitte hat an der öffentlichen Konsultation der Europäischen Kommission teilgenommen und einen Weg zur vertrauenswürdigen *KI in Europa* aufgezeigt.

Datenökonomie und Cloud-infrastruktur

Zudem hat die EU die neue Datenstrategie veröffentlicht. Neben zusätzlichen Investitionen in Höhe von 10 Milliarden Euro (EU-Haushalt, Mitgliedsstaaten, Unternehmen) in den kommenden Jahren plant die EU, sektorale Datenräume aufzubauen. Mit diesem neuen Datenökosystem, welches auf europäischen Gesetzen und Werten wie Transparenz, Offenheit und Schutz der Privatsphäre basiert, möchte die EU neue Geschäftsfelder und Möglichkeiten zur Entwicklung neuer Produkte für Unternehmen aller Größen in Europa schaffen. Die europäischen Datenräume werden für folgende Sektoren entwickelt: Gesundheit, Industrie, Green Deal, Mobilität, Finanzmarkt, Energie, Landwirtschaft, öffentlicher Sektor sowie digitale Fähigkeiten.[7] Ursula von der Leyen betonte in ihrer „State of the Union Speech", dass die Europäische Kommission das deutsch-französische Projekt GAIA-X für die Schaffung der europäischen Datenräume nutzen möchte.[8]

In der internationalen Non-Profit-Organisation GAIA-X mit Sitz in Brüssel engagieren sich Frankreich und Deutschland sowie in der ersten Phase 22 Unternehmen aus den beiden Ländern. Gemeinsam entwickeln sie technische Standards nach europäischem Recht und formulieren Policy Guidelines für das gemeinsame Nutzen und Teilen von Daten, um innovative Produkte und Dienstleistungen basierend auf einer europäischen Cloudlösung für den digitalen Binnenmarkt zu schaffen.[9]

Teilen, Verarbeiten und produktives Nutzen von Daten gehören heute schon zum Kerngeschäft vieler Unternehmen und werden in Zukunft noch an Wichtigkeit gewinnen. Die EU schlägt einen einheitlichen Data Governance Act für den digitalen europäischen Binnenmarkt vor. Der Gesetzesvorschlag bedeutet eine Vereinfachung für die öffentliche Hand, Daten mit Wissenschaft, Unternehmen oder Zivilgesellschaft zu teilen. Sogenannte „data intermediaries" übermitteln die Daten an die Empfänger weiter, ohne sie dabei für sich mithilfe von Datenanalysen zu monetarisieren. Dazu soll in den Mitgliedsstaaten der EU jeweils eine öffentliche Behörde geschaffen werden, die die vorhandenen Daten registriert und die Datenströme steuert – jede Datenanfrage an die öffentliche Hand wird über diesen neuen „single point of contact" koordiniert. Das Bundesministerium für Bildung und Forschung erprobt in diesem Zusammenhang ein Datentreuhandmodell für „einen sicheren und vertrauensvollen Datenaustausch in Forschung und Wirtschaft".[10] Ein solches Modell ist sicherlich ein wirksames Werkzeug für den Ausbau europäischer digitaler Souveränität, sofern die Datentreuhänder auf technologische Lösungen aus Europa zurückgreifen. Mit dem Data Governance Act möchte die EU den Datenverkehr nicht verringern, sondern diesen eher mit neuen Verkehrsschildern und Ampeln – also einheitlichen digitalen Straßenregeln – in Europa steuern. Vielmehr erhofft sich die EU sogar eine Produktivitätssteigerung von 1,3 Billionen Euro bis 2027 sowie Ersparnisse von 120 Milliarden Euro pro Jahr im Gesundheitssektor durch Harmonisierung und erhöhte Rechtssicherheit.[11]

Darüber hinaus schafft die EU für Organisationen Anreize, sich als „data altruism organisations" zu registrieren – so sollen Individuen und Unternehmen angereizt werden, ihre Daten der Öffentlichkeit zu Forschungszwecken zur Verfügung zu stellen. Das Spenden von Daten soll der Wissenschaft dabei helfen, Lösungen für komplexe Probleme wie Klimawandel oder Heilung von Krankheiten zu entwickeln.[12]

Cybersicherheit

Ohne Sicherheit keine Souveränität. Die genannten digitalen Initiativen sind ohne eine robuste Cybersicherheit der Systeme, Infrastruktur und Daten nicht viel wert. Daher hat auch hier die EU Vorschläge für zwei Richtlinien veröffentlicht, die eine Vertiefung und Erweiterung der europäischen Cybersicherheit vorsehen: die Network Information Security Directive (NIS Directive 2[13]) und die Critical Entities Resilience (CER) Directive[14]. In unserem Beitrag zur öffentlichen Konsultation zur NIS-Richtlinie haben wir elf Empfehlungen für eine höhere *Cyberresilienz* formuliert. Beide Richtlinien erkennen neue Cyberrisiken – auch im Zusammenhang mit der COVID-19-Pandemie – an und erweitern den Rahmen der kritischen Sektoren. So rücken zum Beispiel die Hersteller von Medikamenten, Trinkwasserproduzenten,

Fazit

Anbieter von Videokonferenzen, aber auch bestimmte Bereiche der öffentlichen Verwaltung[15] mehr in den Fokus. Eine stärkere Harmonisierung der Anforderungen an Cybersicherheit in der EU sowie eine stringentere Zusammenarbeit den nationalen Cyberaufsichten sollen ebenso mit dem Update der Richtlinien erreicht werden. Die CER Directive (CERD) ruft die Mitgliedsstaaten außerdem dazu auf, ihre nationalen Cybersicherheitsstrategien zu aktualisieren und regelmäßige Risikobewertungen durchzuführen.

Weiterhin veröffentlichte die Europäische Kommission im Dezember 2020 eine neue „Cybersicherheitsstrategie für die digitale Dekade". Technologische Souveränität und Resilienz sind dabei Schwerpunkte. Diese sollen durch eine paneuropäische „Joint Cyber Unit", die die europäischen operativen Kapazitäten besser koordinieren und zusammenführen kann, gestärkt werden.[16]

Als Gesellschaft müssen wir uns stets mit der Frage auseinandersetzen, wie wir technologische Innovationen gemeinsam mit *Corporate Digital Responsibility* im Einklang mit unseren Ansprüchen im digitalen Zeitalter voranbringen können. Um globale Standards für Technologien vorzugeben, muss die EU zunächst das entsprechende Marktgewicht in den genannten Bereichen erlangen oder auf Augenhöhe mit den USA und China kommen. Hier gilt es, die von Angela Merkel genannten Stärken und strategischen Schwächen zu adressieren und anzupacken. Dafür bedarf es konstanter, gezielter Investitionen in den Ausbau der digitalen Infrastruktur, in Kerntechnologien und in die Vertiefung digitaler Kompetenzen der europäischen Bürgerinnen und Bürger. Staatliche Alleingänge sind zum Scheitern verurteilt – eine stringentere Harmonisierung der Aktivitäten der Mitgliedsstaaten ist damit unerlässlich und oberstes Gebot. Europa kann seine digitale Souveränität stärken, indem es die genannten Initiativen pragmatisch und technologieoffen in enger Zusammenarbeit und im Austausch mit Wirtschaft, Forschung und Zivilgesellschaft umsetzt – basierend auf europäischen Werten wie Sicherheit, Transparenz und Nachhaltigkeit. Es ist eine ständige Aufgabe der Politik, den Mehrwert von Innovation und neuen Technologien zu erkennen, zu kommunizieren und klare Spielregeln zu schaffen, damit Bürgerinnen und Bürger sowie Unternehmen Technologie mit Begeisterung nutzen und mit der gebotenen Offenheit neue Produkte oder Dienstleistungen erschaffen. Mit der Umsetzung in konkrete Ergebnisse werden Unternehmen und Forschung einen messbaren Mehrwert für Gesellschaft und Wirtschaft generieren. Digitale Souveränität ist für Europa längst nicht mehr „nice to have" – sie hat sich zu einem „must have" und „must do" entwickelt. Das größte Risiko für die EU ist es, untätig zu bleiben.

In den nächsten Artikeln beleuchten wir verschiedene Felder mit ganzheitlichem Blick. Wir gehen genauer darauf ein, wie es gelingt, diese „must have" und „must do" mit einem digitalen Ökosystem „made in Europe" zu meistern. Mit einer umsetzungsorientierten Perspektive legen wir den Fokus auf die Entwicklung der europäischen Datenökonomie und Cloudinfrastruktur im öffentlichen Sektor, das Vorantreiben einer europäischen KI sowie die Robustheit der europäischen Cybersecurity.

Digitale Souveränität ist für Europa längst nicht mehr „nice to have" – sie hat sich zu einem „must have" und „must do" entwickelt. Das größte Risiko für die EU ist es, untätig zu bleiben.

Ihre Ansprechpartner

Peter J. Wirnsperger
Partner | Public Sector
Tel: +49 (0)40 32080 4675
pwirnsperger@deloitte.de

Felix Dinnessen
Partner | Public Sector
Tel: +49 (0)221 9732 4128
fdinnessen@deloitte.de

Dr. Soentje Julia Hilberg
Director | Deloitte Legal
Tel: +49 (0)30 2546 8225
shilberg@deloitte.de

Weiterer Ansprechpartner
Mosche Orth
Public Policy Manager | EU Policy Centre
Tel: +49 (0)151 58071859
moorth@deloitte.de

[1] Europäische Kommission, *Die Weichen für das kommende Jahr stellen*, September 2020, abgerufen am: 17.03.2021
[2] Europäische Kommission, *Europe: The Keys To Sovereignty*, September 2020, abgerufen am: 17.03.2021
[3] *Appell von vier Regierungschefinnen an die EU*, Handelsblatt, März 2021, abgerufen am: 17.03.2021
[4] Europäische Kommission, *Recovery and Resilience Facility,* abgerufen am: 17.03.2021
[5] Europäische Kommission, Europe: *The Keys To Sovereignty*, September 2020, abgerufen am: 17.03.2021
[6] Europäische Kommission, *Zur Künstlichen Intelligenz – ein europäisches Konzept für Exzellenz und Vertrauen*, Februar 2020, abgerufen am: 18.03.2021
[7] Europäische Kommission, *Eine europäische Datenstrategie*, Februar 2020, abgerufen am: 18.03.2021
[8] Europäische Kommission, *Die Weichen für das kommende Jahr stellen*, September 2020, abgerufen am: 17.03.2021
[9] *GAIA-X: A Federated Date Infrastructure for Europe*, abgerufen am: 18.03.2021
[10] *Förderung von Datentreuhandmodellen*, Januar 2021, abgerufen am: 18.03.2021
[11] Europäische Kommission, *Data Governance Act*, November 2020, abgerufen am: 18.03.2021
[12] Europäische Kommission, *Data Governance Act*, November 2020, abgerufen am: 18.03.2021
[13] Europäische Kommission, *Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau*, Dezember 2020, abgerufen am: 18.03.2021
[14] Europäische Kommission, *Richtlinie über Resilienz kritischer Einrichtungen*, Dezember 2020, abgerufen am: 18.03.2021
[15] Einrichtungen der öffentlichen Verwaltung (im Sinne des Artikels 4 Nummer X der *NIS-2-Richtlinie*) von Zentralregierungen
[16] Europäische Kommission, *Die Cybersicherheitsstrategie der EU für die digitale Dekade*, Dezember 2020, abgerufen am: 18.03.2021

Deloitte.

Stand 04/2021