



Schutz von Gesundheitsdaten entscheidend

12.12.2025, Unternehmens-Blog



Europa treibt die Unabhängigkeit und den Schutz sensibler Daten mit Nachdruck voran – und setzt dabei zunehmend auf eigene technologische Standards, sichere Infrastrukturen und klare gesetzliche Rahmenbedingungen. Besonders im Gesundheitswesen, wo Daten als hochsensibel gelten, gewinnt dieses Engagement an Bedeutung. Vom Digitalgipfel in Berlin gingen dazu deutliche Signale aus.

Europa steht an einem digitalen Wendepunkt. Während internationale Tech-Giganten wie Google, Amazon, Microsoft oder chinesische Cloudanbieter weltweit dominieren, wächst in der Europäischen Union der politische und wirtschaftliche Druck, digitale Schlüsseltechnologien nicht vollständig von außereuropäischen Playern abhängig zu machen. Beim Digitalgipfel in Berlin Ende November haben Deutschland und Frankreich daher ein deutliches Signal gesendet: Europa muss seine digitale Souveränität stärken – insbesondere beim Umgang mit sensiblen Daten. Für kein anderes Feld ist das so entscheidend wie für das Gesundheitswesen.

Der Wettstreit um Datenhoheit



Digitale Infrastruktur ist heute ein strategischer Faktor. Wer Rechenzentren, Cloud-Plattformen und KI-Modelle kontrolliert, kontrolliert auch Datenströme und Wertschöpfungsketten. Das gilt für Wirtschaftsunternehmen genauso wie für staatliche Institutionen. Europa besitzt in vielen Bereichen exzellente Forschung und starke Industrie, aber bei zentralen digitalen Basisdiensten ist der Kontinent bislang abhängig von außereuropäischen Anbietern. Diese Dominanz birgt Risiken – von der Datenweitergabe nach ausländischem Recht bis zu Unsicherheiten bei der langfristigen Verfügbarkeit und Kontrolle kritischer Dienste.

Investitionen stärken digitale Infrastruktur

Ein Beispiel dafür ist die Ankündigung der Schwarz-Gruppe, zu der Lidl und Kaufland gehören, elf Milliarden Euro in ein neues, hochmodernes Rechenzentrum im Spreewald zu investieren. Das ist einer der stärksten industriepolitischen Akzente der vergangenen Jahre. Das geplante Rechenzentrum soll nicht nur die digitale Infrastruktur der Unternehmensgruppe stärken, sondern auch ein Baustein europäischer Unabhängigkeit sein, der auch externen Kunden KI- und Cloud-Dienste „Made in Europe“ anbieten will. Damit wird erstmals in größerem Maßstab europäische Rechenkapazität aufgebaut, die technologisch mit außereuropäischen Anbietern mithalten kann.

Besondere Anforderungen für das Gesundheitswesen

Für das Gesundheitswesen ist die Frage der Datensouveränität existenziell, da die Gefahr besteht, dass Daten zu einem globalen Handelsgut werden. Kaum ein Lebensbereich enthält sensiblere, schützenswertere Informationen als Krankenakten, Diagnosen oder Medikationsdaten. Gleichzeitig wächst der Bedarf an innovativen digitalen Lösungen: elektronische Patientenakte, Telemedizin, Versorgungsplattformen, eRezept oder KI-gestützte Frühdiagnostik. Gerade deshalb braucht Europa eigene, datenschutzkonforme und rechtssichere digitale Infrastrukturen. Nur so lässt sich sicherstellen, dass Gesundheitsdaten nicht unter ausländisches Recht fallen und so für kommerzielle Zwecke ohne Zustimmung ausgewertet werden. Es muss verhindert werden, dass Gesundheitsdaten intransparent oder unkontrolliert verarbeitet werden, sondern jederzeit der Kontrolle der europäischen Institutionen und Gesundheitssysteme unterliegen.

Europäischer Gesundheitsdatenraum (EHDS) entsteht

Datenschutz ist dabei nicht nur ein rechtliches Gebot der europäischen Datenschutz-Grundverordnung (DSGVO), sondern zunehmend ein Wettbewerbsvorteil: Vertrauen ist die Grundlage dafür, dass Patientinnen und Patienten digitale Angebote akzeptieren. Einen entscheidenden Schritt stellt der entstehende Europäische Gesundheitsdatenraum (EHDS) dar. Er soll Behandlungsdaten, elektronische Patientenakten und Forschungsinformationen EU-weit sicher verfügbar machen – unter strengen Zugangskontrollen und klar geregelten Nutzungsrechten. Damit werden Daten-Silos reduziert und gleichzeitig Forschung, Prävention und Versorgung gestärkt.

Michael Baumgärtner, Abteilungsleiter Strategie/Produkte bei der AOK Systems, sieht einen weiteren Vorteil: „Dies kann unserem Unternehmen die Chance eröffnen, auf Daten zuzugreifen, die bisher aufgrund fehlender Anonymisierung nicht verfügbar waren.“



Cybersicherheit wird verstärkt

Auf dem Weg zur digitalen Souveränität arbeitet Europa deshalb an mehreren strategischen Säulen. So sollen eigene Cloud-Infrastrukturen, wie GAIA-X, und europäische Cloud-Standards die Datenhaltung in konformen, transparenten und souveränen Umgebungen ermöglichen. Große Investitionen – wie das neue Schwarz-Rechenzentrum – sollen Rechenleistung in Europa halten und Innovationen ermöglichen. Gleichzeitig wird die Cybersicherheit europaweit verschärft. Die neue NIS2-Richtlinie verpflichtet Betreiber kritischer Infrastrukturen, darunter Krankenkassen und medizinische Einrichtungen, zu höheren Sicherheitsstandards, moderner Angriffserkennung und strengem Risikomanagement. Ergänzend dazu sorgt der EU AI Act für klare Regeln beim Einsatz von Künstlicher Intelligenz: Gesundheits-KI gilt als Hochrisikosystem und muss besonders transparent, sicher und überprüfbar sein. Europa baut damit Schritt für Schritt ein Schutzsystem auf, das Datenschutz, digitale Unabhängigkeit und technologische Innovation verbindet. Gerade für das Gesundheitswesen schafft diese Entwicklung eine stabile Basis, um moderne digitale Anwendungen sicher und vertrauenswürdig einsetzen zu können.

Autorin: Eva Franz, Marketing Managerin, AOK Systems GmbH