KÜNSTLICH
MENSCHLICH
INTELLIGENT
KOMPETENZZENTRUM

WHITEPAPER

Datensouveränität im Unternehmen

Ergebnisse der Online-Veranstaltung:
„Datensouveränität und Datensicherheit –
Was müssen KMUs wissen?“ vom 06.05.2025

Das Forschungs- und Entwicklungsprojekt KMI wird im Rahmen der Fördermaßnahme „Zukunft der Arbeit: Regionale Kompetenzzentren der Arbeitsforschung – Künstliche Intelligenz" im Programm „Innovationen für die Produktion, Dienstleistung und Arbeit von morgen" des Bundesministeriums für Forschung, Technologie und Raumfahrt (BMFTR) für die Laufzeit vom 01.12.2021 – 30.11.2026 gefördert und vom Projektträger Karlsruhe (PTKA) betreut.

Gefördert durch:

Bundesministerium
für Forschung, Technologie
und Raumfahrt

Kompetenzzentren
Arbeitsforschung

Autorinnen und Autoren:
Christian Walter[1]
Maria Heider[2]
Christina Mamtoumidou[2]
Sabine Hartig[2]

[1] Westsächsische Hochschule Zwickau
[2] Kompetenzzentrum Künstlich Menschlich Intelligent (KMI) am Institut für Angewandte Informatik e.V.

Oktober 2025

WHZ Westsächsische Hochschule Zwickau
Hochschule für Mobilität

Inhaltsverzeichnis

1 Einleitung

Ziel dieses Papers ist es, die Ergebnisse des Webinars “Datensouveränität und Datensicherheit – Was müssen KMUs wissen?” vom 06.05.2025 zusammenzufassen sowie einen Überblick über die wichtigsten Aspekte dieser Themen und deren Bedeutung für Unternehmen zu geben.

Beim Umgang mit Daten in Unternehmen sind drei Bereiche besonders wichtig: Datensouveränität, Datensicherheit und Datenschutz. Datensouveränität bedeutet, die Kontrolle über die eigenen Daten zu haben, was deren Erhebung, Speicherung und Verarbeitung einschließt. Sie ist ein zentraler Bestandteil der Digitalen Souveränität, die darauf abzielt, digitale Technologien insgesamt selbstbestimmt und unabhängig zu nutzen und zu gestalten. Für die Datensicherheit sind Maßnahmen zum Schutz der Daten vor unbefugtem Zugriff, Manipulation oder Datenverlust wichtig. Von großer Bedeutung ist schließlich auch der Datenschutz, der sicherstellt, dass persönliche Daten geschützt und vertraulich behandelt werden.

Betroffen sind Daten jeglicher Art, wie bspw. Prozess- oder Produktdaten, Sensordaten, Daten von Mitarbeiter:innen und Kund:innen aber auch Energiedaten. Unternehmen stehen hierbei vor der Herausforderung, für einen sicheren Datenaustausch zu sorgen, indem sie die Balance zwischen dem sicheren Halten der Daten im Unternehmen einerseits und dem Weitergeben der Daten andererseits wahren.

2 Rechtliche Rahmenbedingungen

Die rechtlichen Rahmenbedingungen für die Datensouveränität stützen sich auf drei wesentliche Rahmenwerke, welche sich abstufend ergänzen:

- Das erste Rahmenwerk für die Datenverwaltung in der EU ist der **Data Governance Act (DGA)**. Ziel ist das Schaffen eines vertrauenswürdigen Rahmenwerkes für die Datenverwaltung in der EU. Dadurch sollen die gemeinsame Nutzung, Zugang zu Daten und die freiwillige Datenweitergabe gefördert sowie parallel dazu der Datenschutz gewährleistet werden.
- Der zweite Rahmen ist die **Datenschutz-Grundverordnung** (DSGVO), welche den Umgang mit personenbezogenen Daten in der EU regelt.
- Das **Bundesdatenschutzgesetz (BDSG)** ergänzt die DSGVO mit speziellen Regelungen, die für den Datenschutz in Deutschland gelten.

Darüber hinaus wurde mit dem **Data Act** (Verordnung über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung) ein neues Gesetz geschaffen, welches ab dem 12. September 2025 EU-weit ein direkt anwendbares Recht wird.

3 Sichere Nutzung von datenbasierten Assistenzsystemen

3.1 Sicherheitsrisiken

Trotz rechtlicher Vorgaben sind kontinuierlich zahlreiche Versuche zu beobachten, diverse Sicherheitsmaßnahmen in Unternehmen zu durchbrechen. Aus diesem Grund ist es entscheidend, die wichtigsten Sicherheitsrisiken zu kennen, um potenzielle Angriffe bestenfalls frühzeitig zu erkennen und zu verhindern oder effektiv abwehren zu können:

- Ein großes Risiko besteht in **Phishing-Angriffen**, die ein häufiges Einfallstor darstellen, um beispielsweise wichtige Zugangsdaten zu erlangen.
- **Ransomware** stellt ein weiteres erhebliches Risiko dar, da sie kritische Daten verschlüsselt oder sperrt und Unternehmen dadurch erpressbar macht.
- Auch **KI-Systeme** bilden eine **Plattform für Angriffe**, da externe Akteur:innen

durch gezielte Mechanismen auf sensible Daten zugreifen können. Ein Beispiel hierfür ist Prompt Injection bei großen Sprachmodellen, bei der durch manipulative Eingaben vertrauliche Informationen ausgegeben werden.

Um einen möglichen Datenklau oder -verlust infolge solcher Angriffe zu vermeiden oder zu minimieren, ist es wichtig, präventive Maßnahmen und Methoden zur Sicherung der Datensouveränität umzusetzen.

3.2 “Pfeiler der Datensicherheit”

Im Anschluss lassen sich die zentralen Pfeiler der Datensicherheit näher betrachten, die Unternehmen als Grundlage für einen umfassenden Schutz ihrer Daten dienen:

Vertraulichkeit

- Grundsätzlich sollten Daten in allen Stadien - während der Speicherung sowie einer möglichen Übertragung - vertraulich behandelt werden. Einsicht sollten nur autorisierte Nutzer:innen haben.

Verfügbarkeit

- Es sollte jederzeit gewährleistet sein, auf die informationstechnischen Systeme und auf die darin hinterlegten Daten zugreifen zu können.

Integrität

- Daten- und Systemintegrität geben vor, dass die Daten sowie die Funktionsweise des verarbeitenden Systems korrekt sind. Notwendige Änderungen müssen stets nachvollziehbar sein, wofür eine Versionsverwaltung verwendet werden kann.

3.3 Methoden zur Sicherung der Datensouveränität

Daraus ergeben sich erforderliche technische und organisatorische Maßnahmen, um die IT-Schutzziele zu gewährleisten:

Verschlüsselung von Daten

- Um die Vertraulichkeit und Integrität zu gewährleisten, sollten Daten sowohl bei der Übertragung als auch bei der Speicherung verschlüsselt werden.

Zugriffskontrolle und Authentifizierungsprotokolle

- Ein weiterer zentraler Baustein zur Sicherung der Datensouveränität ist die Zugriffskontrolle, also die gezielte Steuerung, wer auf welche Daten zugreifen darf. Dies umfasst rollenbasierte Zugriffsrechte, bei denen Nutzer:innen nur auf die Daten und Systeme zugreifen können, die für ihre jeweilige Aufgabe notwendig sind.
- Ergänzt wird dies durch Authentifizierungsprotokolle, wie Zwei-Faktor-Authentifizierung (2FA) oder Single Sign-On (SSO), die den Zugang zusätzlich absichern und unautorisierte Zugriffe verhindern.

Regelmäßige Sicherheitsüberprüfungen

- Zur Erhöhung der Sicherheit sollten regelmäßige Software-Updates und Datensicherungen durchgeführt werden. Hilfreich ist es außerdem, die Bedeutung der Daten festzulegen und einen Überblick über den Zugriff und die Weitergabe der Daten zu behalten.

3.4 Technische Umsetzung

Die praktische Umsetzung der Methoden erfolgt einerseits durch das Halten der Daten in der Firma und andererseits mithilfe verschiedener technischer Ansätze, die sich hinsichtlich Sicherheit und Nutzungsbedingungen voneinander unterscheiden:

- **Trusted Execution Environment (TEE)**, z.B. über Intel SGX, SCONE oder Fortanix, ermöglicht die Verarbeitung von Daten direkt auf dem Prozessor in einem stark abgeschirmten Bereich. Dies bietet sehr hohe Sicherheit, ist jedoch technisch anspruchsvoll.
- **Remote Data Sandbox**, z.B. JupyterHub oder Apache Zeppelin, stellt eine einge-

schränkte Umgebung zur Verfügung, in der Daten bearbeitet werden können, ohne dass Unbefugte Zugriff haben. Sie ist einfach zu nutzen und eignet sich vor allem für Datenanalysten oder KI-Entwickler:innen.

- **Data Clean Room**, z.B. über Plattformen wie Snowflake, Google, Amazon Web Services, erlaubt mehreren Parteien die gemeinsame Nutzung von Daten, ohne dass Rohdaten direkt eingesehen werden können. Die Sicherheit wird über strenge Regeln gewährleistet, die Nutzung erfordert jedoch meist Plattformkenntnisse.
- **Self-Sovereign Identity (SSI)/ Secure Data Sharing** ermöglicht es, Daten gezielt und kontrolliert mit berechtigten Personen zu teilen. Die Sicherheit hängt von der eingesetzten Technik ab, der Zugriff ist flexibel, und die Nutzung ist in der Regel einfach, z.B. über APIs.

3.5 Rollen im Umgang mit Datensouveränität und Datensicherheit

Um die Methoden zur Sicherung umsetzen zu können, ist es empfehlenswert, innerhalb des Unternehmens den Mitarbeitenden bestimmte Rollen in Bezug zur Datensouveränität zuzuordnen. Grundsätzlich ist die Unternehmensleitung die zuständige Instanz für die Datensouveränität.

Im Folgenden werden die Rollen im Detail aufgeführt, die für eine Umsetzung von Datensouveränität relevant bzw. hilfreich sein können:

- **IT-Sicherheitsbeauftragte** sind für die Implementierung und Überwachung von technischen und organisatorischen Sicherheitsmaßnahmen zuständig. Ihre Aufgabe ist es, die Unternehmensdaten vor Cyberangriffen und anderen Sicherheitsrisiken zu schützen.
- **IT-Administrator:innen und Netzwerktechniker:innen** sorgen bei der Einrichtung und Nutzung der Systeme für Sicherheit, was die Verwaltung von Benutzer:innenkonten, Zugriffsrechten und die Aufrechterhaltung der Netzwerksicherheit beinhaltet.
- **Softwareentwickler:innen und -architekt:innen** integrieren Datenschutz und -

sicherheit in den Lebenszyklus der Softwareentwicklung, um sicherzustellen, dass Applikationen und Systeme von Grund auf sicher sind.

- **Data Scientists** spielen eine zentrale Rolle bei der Wahrung der Datensouveränität, da sie mit der Erhebung, Aufbereitung und Analyse sensibler Daten betraut sind. Sie achten darauf, dass Daten verantwortungsvoll genutzt, korrekt anonymisiert und ausschließlich im vorgesehenen Rahmen verarbeitet werden.
- **Datenschutzbeauftragte** sind in Deutschland gemäß DSGVO vorgeschrieben und tragen die Verantwortung für die Einhaltung der Datenschutzvorschriften innerhalb des Unternehmens. Sie beraten und schulen Mitarbeiter:innen und sind Ansprechpartner:innen für Datenschutzfragen.
- **Rechtsberater:in mit Spezialisierung auf IT-Recht** sind innerhalb des Unternehmens für rechtliche Fragen rund um Datensouveränität und Datenschutz zuständig. Sie sorgen dafür, dass gesetzliche Vorgaben eingehalten und rechtssichere Prozesse im Umgang mit Daten etabliert werden.
- **Cybersecurity-Expert:innen** haben sich auf die Abwehr von Angriffen spezialisiert und die Absicherung digitaler Systeme verantwortlich. Sie entwickeln Schutzstrategien, führen Risikoanalysen durch und stellen sicher, dass Datensicherheit dauerhaft gewährleistet ist.
- **Compliance Manager:innen** stellen sicher, dass ein Unternehmen in allen Bereichen, einschließlich Datensicherheit und -souveränität, gesetzeskonform handelt. Sie entwickeln Richtlinien und überwachen deren Einhaltung.

4 Hinweise und Empfehlungen zur Umsetzung in der unternehmerischen Praxis

Im ersten Schritt sollte in Unternehmen ein Bewusstsein für Datensouveränität geschaffen werden und diese als festen Bestandteil der Unternehmenskultur zu verankern. Die Sensibilisierung und Schulung der Mitarbeitenden für einen verantwortungsvollen Umgang mit Daten ist ein zentraler Faktor.

Darauf aufbauend empfiehlt sich eine kritische Beurteilung der bestehenden Anwendungen und der Datenlage. Welche Daten liegen im Unternehmen vor, wo werden sie gespeichert (Server, Cloud, lokal), und wer hat Zugriff darauf? (z.B. nur Teamleitung hat Einsicht in personenbezogene Daten). Anschließend sollten klare Zuständigkeiten definiert und grundlegende Sicherheitsmaßnahmen umgesetzt werden. Dazu zählen beispielsweise die Zwei-Faktor Authentifizierung (2FA), regelmäßige Backups oder rollenbasierte Zugriffskontrollen.

Zudem wird für den Umgang mit datenbasierten Anwendungen geraten, sich auf Anbieter:innen von Cloudsystemen zu fokussieren und nach Zertifikaten wie "Datenschutz IDW PH 9.860.1", "BSI C5 Cloud Security", "ISAE 3402" und "TÜV" zu suchen. Anbieter:innen im EU-Rechtsraum sollten hier bevorzugt werden. Bei KI-Diensten ist zusätzlich auf Serverzertifizierungen, sichere Softwareinfrastrukturen und Vertraulichkeitsvereinbarungen (NDA) zu achten (z.B. Wo stehen die Server der KI-Anwendung? Welche Daten werden gespeichert?).

5 Unterstützungsangebote für KMU

Unterstützung erhalten KMU in Branchenverbänden (z.B. Bitkom e. V., Silicon Saxony, Deutschland sicher im Netz e.V.), Bundesministerien, bei den Industrie- und Handelskammern (IHK), den Kompetenzzentren und den Mittelstand-Digital-Zentren. Vielfältige Angebote und Austauschformate wie Workshops und Infomaterialien ermöglichen einen niedrigschwelligen Einstieg in das Thema.

6 Schlusswort

Der souveräne Umgang mit Daten ist nicht nur eine technische, sondern auch ei-

ne strategische und kulturelle Herausforderung. Unternehmen, die frühzeitig Verantwortung übernehmen, schaffen Vertrauen bei ihren Kund:innen, verbessern die interne Zusammenarbeit und sichern ihre Innovationsfähigkeit. Dabei sollte die Umsetzung als kontinuierlicher Prozess verstanden werden, der regelmäßige Überprüfungen und Anpassungen umfasst, etwa durch interne Audits, Schulungen oder Software-Updates.

Entwicklungen wie die europäische Cloud-Initiative GAIA-X oder das „Dateninstitut für Deutschland“ zeigen, dass ein souveräner und sicherer Umgang mit Daten künftig ein zentraler Wettbewerbsfaktor sein wird. Ziel ist der Aufbau eines europäischen Daten-Ökosystems mit klaren Regeln, Standards und einer verlässlichen Infrastruktur für eine vertrauenswürdige und zukunftsfähige Datenwirtschaft.

7 Referenzen

Bundesamt für Sicherheit in der Informationstechnik. Cloud Computing Compliance Criteria Catalogue. (aufgerufen am 28.07.2025) https://www.bsi.bund.de/dok/13447-812

Bundesamt für Sicherheit in der Informationstechnik (2023). AI SECURITY CONCERNS IN A NUTSHELL. Bonn, Germany.

European Commission. (2025). A European strategy for data. https://digital-strategy.ec.europa.eu/en/policies/strategy-data

European Commission. (2024). European Data Governance Act. https://digital-strategy.ec.europa.eu/en/policies/data-governance-act

European Parliament and Council of the European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) https://eur-lex.europa.eu/eli/reg/2016/679/oj

Feth D. und Polst S. (2023). Benutzerfreundliche Umsetzung von Datensouveränität in Digitalen Ökosystemen. Fraunhofer IESE. https://www.iese.fraunhofer.de/content/dam/iese/publikation/digitale-oekosysteme-daten-souveraenitaet-fraunhofer-iese.pdf

Lohmöller, J. et al. (2024). The unresolved need for dependable guarantees on security, sovereignty, and trust in data ecosystems. Data and Knowledge Engineering, 151, 102301.

Niebel, C., Reiberg, A., und Kraemer, P. (2022). Gaia-X für KMU. Gaia-X Hub: München, Germany.

8 Impressum

Kompetenzzentrum KMI
Dr. Christian Zinke-Wehlmann (Leiter)

Institut für Angewandte Informatik (InfAI) e. V.
Goerdelerring 9
04109 Leipzig

Telefon: +49 341 229037 0
Telefax: +49 341 229037 99
E-Mail: info@infai.org

Vertretungsberechtigter Vorstand:
Prof. Dr. Bogdan Franczyk (1. Vorsitzender)
Prof. Dr. Erhard Rahm (2. Vorsitzender)
Prof. Dr. André Ludwig
Prof. Dr. Roland Fassauer

Vorstandsbeisitzer:
Prof. Dr. Sören Auer
Prof. Dr. Gerhard Heyer
Prof. Dr. Gerik Scheuermann

Geschäftsführung:
Ingolf Römer, Andreas Heinecke, Prof. Dr. Roland Fassauer

Registereintrag:
Registergericht: Amtsgericht Leipzig
Registernummer: VR 4342

Umsatzsteuer-ID:
Umsatzsteuer-Identifikationsnummer nach §27a
Umsatzsteuergesetz: DE274344504