WHITEPAPER

Digitale Souveränität in der Praxis

Wie Unternehmen und öffentliche Einrichtungen ihre IT-Unabhängigkeit sichern und DSGVO-konform zusammenarbeiten.

xworks.365
Eine Plattform der mediaBEAM GmbH · xworks.net

Über dieses Whitepaper

Digitale Souveränität ist von einem politischen Schlagwort zu einem konkreten Beschaffungs- und Architekturkriterium geworden. Dieses Whitepaper zeigt, was digitale Souveränität wirklich bedeutet, welche Dimensionen dahinterstehen, wie Organisationen sie Schritt für Schritt erreichen – und wie xworks.365 diese Anforderungen in der Praxis abbildet.

01	**Was ist digitale Souveränität?**	Definition und vier Dimensionen
02	**Begriffe kurz erklärt**	Datenhoheit, souveräne Cloud, Datenresidenz, Lock-in
03	**Wie gelingt digitale Souveränität?**	Sechs Schritte für Unternehmen und Behörden
04	**Recht und Compliance im Überblick**	DSGVO, CLOUD Act, Schrems II, BSI, ISO, Gaia-X
05	**Digitale Souveränität mit xworks.365**	Umsetzung in der Praxis
06	**Fazit und nächste Schritte**	Checkliste für die Anbieterauswahl

01 · Grundlagen

Was ist digitale Souveränität?

Digitale Souveränität ist die Fähigkeit einer Organisation, selbstbestimmt über ihre Daten, ihre eingesetzte Technologie und ihren IT-Betrieb zu entscheiden – ohne in rechtliche, technische oder wirtschaftliche Abhängigkeit von einzelnen Anbietern oder Drittstaaten zu geraten.

Der Begriff wird häufig mit „Datenhoheit“ oder „Datensouveränität“ gleichgesetzt. Tatsächlich ist digitale Souveränität weiter gefasst: Sie umfasst neben dem Speicherort auch den Rechtsträger des Anbieters, die Betriebs- und Supportkette, die Kontrolle über Verschlüsselungsschlüssel sowie die Möglichkeit, eine Lösung jederzeit wieder zu verlassen.

Für Unternehmen und öffentliche Auftraggeber ist digitale Souveränität deshalb kein reines Rechenzentrumsthema, sondern eine Beschaffungs- und Architekturentscheidung: Welche Abhängigkeiten entstehen, wie lassen sie sich begrenzen und welche Nachweise verlangt man vom Anbieter.

Die vier Dimensionen digitaler Souveränität

DATENSOUVERÄNITÄT
Alle Primär-, Backup- und Log-Daten liegen in der EU. Sie bestimmen, wer zugreift, wie lange gespeichert wird und wann gelöscht wird.

RECHTLICHE SOUVERÄNITÄT
Der Vertragspartner unterliegt ausschließlich EU-Recht. Keine extraterritoriale Zugriffsverpflichtung, etwa durch den US CLOUD Act.

TECHNOLOGISCHE SOUVERÄNITÄT
Offene Standards und dokumentierte Schnittstellen statt proprietärer Formate. Der Wechsel bleibt technisch jederzeit möglich.

OPERATIVE SOUVERÄNITÄT
Betrieb, Administration und Support erfolgen aus der EU – inklusive der Personen, die im Störungsfall Zugriff auf Systeme erhalten.

Begriffe rund um digitale Souveränität

Datenhoheit, souveräne Cloud, Datenresidenz – die wichtigsten Begriffe kurz erklärt.

Datenhoheit	Das Recht und die tatsächliche Fähigkeit, über die eigenen Daten zu verfügen: Zugriff, Weitergabe, Aufbewahrung und Löschung liegen in Ihrer Hand.
Datensouveränität	Die Durchsetzbarkeit der Datenhoheit im konkreten Betrieb – technisch über Verschlüsselung und Rechtekonzepte, rechtlich über Verträge und Jurisdiktion.
Souveräne Cloud	Eine Cloud-Umgebung, die vollständig unter EU-Recht betrieben wird: EU-Rechtsträger, EU-Rechenzentren, EU-Support, Schlüsselhoheit beim Kunden oder beim europäischen Betreiber.
Datenresidenz	Beschreibt ausschließlich den geografischen Speicherort der Daten. Datenresidenz in Deutschland allein macht eine Lösung noch nicht souverän.
US CLOUD Act	US-Gesetz, das US-Anbieter zur Herausgabe von Daten an US-Behörden verpflichtet – unabhängig vom Speicherort und auch für europäische Tochtergesellschaften.
Schrems II	EuGH-Urteil von 2020, das den Privacy Shield für ungültig erklärte und für Datentransfers in Drittstaaten zusätzliche Schutzmaßnahmen verlangt.
Gaia-X	Europäische Initiative für eine föderierte, interoperable Dateninfrastruktur mit gemeinsamen Regeln zu Transparenz, Portabilität und Selbstbestimmung.
Vendor Lock-in	Abhängigkeit von einem Anbieter, weil Daten, Formate oder Prozesse nicht ohne erheblichen Aufwand migriert werden können.

03 · Vorgehen

Wie gelingt digitale Souveränität?

Sechs Schritte, mit denen Unternehmen und Behörden ihre digitale Souveränität systematisch steigern.

01 **Bestandsaufnahme der Abhängigkeiten**

Erfassen Sie alle eingesetzten Cloud-Dienste, deren Rechtsträger, Speicherorte und Subunternehmer. Häufig zeigt sich hier bereits ungeplante Schatten-IT.

02 **Schutzbedarf der Daten festlegen**

Klassifizieren Sie Daten nach Vertraulichkeit und Kritikalität. Nicht jedes Dokument braucht dasselbe Schutzniveau – aber jede Klasse braucht eine Entscheidung.

03 **Rechtsrahmen prüfen**

Bewerten Sie DSGVO-Konformität, Schrems-II-Risiken und die Reichweite des US CLOUD Act für jeden Anbieter. Maßgeblich ist der Rechtsträger, nicht der Serverstandort.

04 **Souveräne Plattform auswählen**

Fordern Sie belegbare Nachweise: EU-Rechtsträger, EU-Rechenzentren, EU-Support, Zertifizierungen wie ISO/IEC 27001 und BSI-Grundschutz sowie offene Schnittstellen.

05 **Migration in Wellen planen**

Starten Sie mit einer Pilotgruppe, migrieren Sie anschließend fachbereichsweise. Parallelbetrieb über offene Standards wie IMAP und CalDAV reduziert das Risiko.

06 **Exit-Fähigkeit dauerhaft sichern**

Testen Sie den vollständigen Datenexport regelmäßig – nicht erst bei der Kündigung. Offene Formate und dokumentierte APIs halten den Wechsel jederzeit möglich.

Die Schritte lassen sich unabhängig vom Anbieter anwenden. Mit xworks.365 sind die Schritte 3 bis 6 bereits durch Rechtsträger, Zertifizierungen und offene Standards abgedeckt.

04 · Recht

Recht und Compliance im Überblick

Die Regelwerke, die über die Souveränität einer Cloud-Lösung entscheiden.

DSGVO-KONFORME CLOUD

Auftragsverarbeitung nach Art. 28 DSGVO, dokumentierte technische und organisatorische Maßnahmen, Löschkonzepte und Betroffenenrechte – vollständig innerhalb der EU umgesetzt.

US CLOUD ACT

xworks.365 wird von einem deutschen Unternehmen betrieben und unterliegt keiner extraterritorialen Herausgabepflicht gegenüber US-Behörden.

SCHREMS II

Kein Drittlandtransfer, keine Standardvertragsklauseln und keine zusätzlichen Schutzmaßnahmen nötig, weil die Verarbeitung die EU nicht verlässt.

BSI-GRUNDSCHUTZ

Sicherheitsarchitektur nach BSI-Vorgaben, ausgezeichnet mit dem BSI-IT-Sicherheitskennzeichen für vertrauenswürdige Kommunikationsdienste.

ISO/IEC 27001

Zertifiziertes Informationssicherheits-Managementsystem für Betrieb, Rechenzentrum und Entwicklungsprozesse.

GAIA-X UND EUROPÄISCHE CLOUD

Offene Standards, Datenportabilität und Transparenz über die Betriebskette – die Prinzipien, auf denen europäische Dateninfrastrukturen aufbauen.

Ausführliche Detailseiten online: xworks.net/sicherheit/cloud-act · /schrems-ii · /dsgvo-cloud · /gaia-x

05 · Praxis

Digitale Souveränität mit xworks.365

xworks.365 ist eine vollständig integrierte Collaboration-Plattform der mediaBEAM GmbH: E-Mail, Kalender und Aufgaben, Cloud-Speicher und Dokumentenmanagement, Office-Bearbeitung im Browser, Chat und Videokonferenzen – betrieben in einem eigenen, ISO/IEC 27001-zertifizierten Rechenzentrum in Deutschland.

EIN ANBIETER, EIN RECHTSRAHMEN

Vertragspartner ist ein deutsches Unternehmen. Es gibt keine US-Muttergesellschaft und damit keine extraterritoriale Herausgabepflicht.

BETRIEB UND SUPPORT IN DEUTSCHLAND

Rechenzentrum, Administration und Support liegen in einer Hand – inklusive der Personen, die im Störungsfall Zugriff erhalten.

OFFENE STANDARDS STATT LOCK-IN

IMAP, SMTP, CalDAV, CardDAV, WebDAV und dokumentierte APIs. Daten und Dokumente lassen sich jederzeit vollständig exportieren.

NACHWEISBARE SICHERHEIT

ISO/IEC 27001, Sicherheitsarchitektur nach BSI-Vorgaben und das BSI-IT-Sicherheitskennzeichen für vertrauenswürdige Kommunikationsdienste.

DSGVO OHNE ZUSATZKONSTRUKTE

Auftragsverarbeitung nach Art. 28 DSGVO, dokumentierte TOM, Löschkonzepte – ohne Standardvertragsklauseln oder Transfer-Impact-Assessment.

SKALIERBAR FÜR BEHÖRDEN UND UNTERNEHMEN

Mandantenfähig, White-Label-fähig und im Einsatz bei Kommunen, Schulträgern, Systemhäusern und Telkos mit Millionen Nutzerkonten.

06 · Fazit

Fazit und nächste Schritte

Digitale Souveränität entsteht nicht durch einen Serverstandort, sondern durch die Summe aus Rechtsträger, Betriebskette, offenen Schnittstellen und belegbaren Zertifizierungen. Organisationen, die diese vier Punkte bei der Anbieterauswahl konsequent prüfen, reduzieren rechtliche Risiken und wirtschaftliche Abhängigkeit gleichzeitig – ohne auf Funktionsumfang zu verzichten.

Checkliste für die Anbieterauswahl

- ✓ Wer ist Vertragspartner – und welchem Recht unterliegt dieser Rechtsträger?
- ✓ Wo liegen Primärdaten, Backups und Logs? Gibt es Subunternehmer außerhalb der EU?
- ✓ Wer betreibt und supportet die Plattform, und wer erhält im Störungsfall Zugriff?
- ✓ Welche Zertifizierungen liegen vor (ISO/IEC 27001, BSI-Grundschutz, IT-Sicherheitskennzeichen)?
- ✓ Lassen sich alle Daten in offenen Formaten exportieren – und wurde das getestet?
- ✓ Welche offenen Schnittstellen und Standards werden unterstützt (IMAP, CalDAV, WebDAV, API)?
- ✓ Wie sind Löschkonzepte, Aufbewahrungsfristen und Betroffenenrechte umgesetzt?

Mehr erfahren: xworks.net/digitale-souveraenitaet · Demo anfragen: xworks.net/kontakt/demo