Compliance-Übersicht

CLOUD Act · Schrems II · DSGVO-Cloud · Gaia-X
Was europäische Organisationen wissen müssen

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

Über diese Übersicht

Vier Rechts- und Rahmenwerke bestimmen, wie europäische Unternehmen und Behörden Cloud-Dienste auswählen dürfen. Diese Übersicht fasst die Kernaussagen der vier Themenseiten von xworks.365 zusammen: Definition, Fakten, Auswirkungen, Handlungsempfehlungen und häufige Fragen – jeweils auf einen Blick.

01	**US CLOUD Act: Was er für europäische Unternehmen bedeutet**	xworks.net/sicherheit/cloud-act
02	**Schrems II: Datentransfers in die USA rechtssicher bewerten**	xworks.net/sicherheit/schrems-ii
03	**DSGVO-konforme Cloud: Anforderungen, Nachweise, Auswahl**	xworks.net/sicherheit/dsgvo-cloud
04	**Gaia-X: europäisches Rahmenwerk für souveräne Cloud-Dienste**	xworks.net/sicherheit/gaia-x

US CLOUD Act

US CLOUD Act: Was er für europäische Unternehmen bedeutet

Der Clarifying Lawful Overseas Use of Data Act verpflichtet US-Anbieter zur Datenherausgabe – unabhängig davon, wo die Daten liegen. Was daraus für Ihre Cloud-Auswahl folgt.

Was ist der US CLOUD Act?

Der US CLOUD Act ist ein 2018 in Kraft getretenes US-Bundesgesetz. Es verpflichtet Unternehmen, die der US-Jurisdiktion unterliegen, gespeicherte Kommunikations- und Nutzungsdaten auf behördliche Anordnung herauszugeben – auch dann, wenn diese Daten außerhalb der USA verarbeitet werden.

Maßgeblich ist damit nicht der Speicherort, sondern der Rechtsträger. Ein Rechenzentrum in Frankfurt oder Amsterdam schützt nicht vor einer Anordnung, wenn der Betreiber ein US-Konzern oder dessen Tochtergesellschaft ist.

Für europäische Verantwortliche entsteht dadurch ein Spannungsfeld: Die DSGVO verlangt eine Rechtsgrundlage für jede Offenlegung personenbezogener Daten, während der CLOUD Act eine Herausgabe verlangen kann, die den Betroffenen nicht mitgeteilt wird.

Die wichtigsten Fakten

IN KRAFT SEIT März 2018 (H.R. 4943)	**BETROFFENE** US-Unternehmen und deren Tochtergesellschaften weltweit
REICHWEITE Unabhängig vom physischen Speicherort der Daten	**DATENARTEN** Inhalts-, Verkehrs- und Bestandsdaten
TRANSPARENZ Anordnungen können mit Schweigepflicht verbunden sein	**NICHT BETROFFEN** Anbieter ohne US-Rechtsträger und ohne US-Mutter

Was das für Unternehmen und Behörden bedeutet

Der CLOUD Act ist kein theoretisches Risiko, sondern ein konkretes Kriterium in Datenschutz-Folgenabschätzung und Beschaffung.

■ Rechenzentrumsstandort reicht nicht

Die Zusage „Daten bleiben in Deutschland“ beantwortet die entscheidende Frage nicht. Prüfen Sie, welche juristische Person Vertragspartner ist und welche Konzernmutter dahintersteht.

■ Konflikt mit der DSGVO

Eine Herausgabe an US-Behörden ohne Rechtshilfeabkommen kann eine unzulässige Übermittlung nach Art. 48 DSGVO darstellen – das Risiko trägt der Verantwortliche, nicht der Anbieter.

■ Dokumentationsaufwand

Beim Einsatz US-naher Dienste sind zusätzliche Schutzmaßnahmen, Transfer Impact Assessments und regelmäßige Überprüfungen zu dokumentieren.

■ Support- und Betriebskette

Auch Fernwartung, Second-Level-Support oder Monitoring aus den USA können Zugriff auf personenbezogene Daten eröffnen.

Wie Sie CLOUD-Act-Risiken vermeiden

Diese Kriterien gehören in jede Ausschreibung und jeden Anbietervergleich:

- ✓ Vertragspartner ist eine europäische juristische Person ohne US-Mutterkonzern.
- ✓ Alle Primär-, Backup- und Protokolldaten werden ausschließlich in der EU gespeichert.
- ✓ Betrieb, Administration und Support erfolgen ausschließlich aus der EU.
- ✓ Verschlüsselung ist dokumentiert, die Schlüsselverantwortung ist eindeutig geregelt.
- ✓ Unterauftragsverarbeiter sind vollständig gelistet und ebenfalls EU-ansässig.
- ✓ Ein vollständiger Datenexport in offenen Formaten ist jederzeit ohne Zusatzkosten möglich.

Häufige Fragen zum CLOUD Act

Gilt der CLOUD Act auch für Daten in deutschen Rechenzentren?

Ja. Entscheidend ist die US-Jurisdiktion des Anbieters, nicht der Standort der Server. Auch Daten in einem deutschen Rechenzentrum können betroffen sein, wenn der Betreiber zu einem US-Konzern gehört.

Schützt Verschlüsselung vor dem CLOUD Act?

Nur dann zuverlässig, wenn der Anbieter die Schlüssel nicht besitzt und nicht erzeugen kann. Sobald Schlüssel im Zugriff des Anbieters liegen, kann eine Herausgabeanordnung auch die Entschlüsselung umfassen.

Ist xworks.365 vom CLOUD Act betroffen?

Nein. xworks.365 wird von der mediaBEAM GmbH, einer deutschen Gesellschaft ohne US-Muttergesellschaft, in einem eigenen ISO/IEC 27001-zertifizierten Rechenzentrum in Deutschland betrieben. Es besteht keine US-Jurisdiktion.

Ausführlich online: xworks.net/sicherheit/cloud-act

Schrems II

Schrems II: Datentransfers in die USA rechtssicher bewerten

Mit dem Urteil C-311/18 hat der EuGH das Privacy Shield gekippt und Standardvertragsklauseln an eine Einzelfallprüfung geknüpft. Was das für Cloud-Dienste heute bedeutet.

Was besagt das Schrems-II-Urteil?

Am 16. Juli 2020 erklärte der Europäische Gerichtshof das EU-US Privacy Shield für ungültig. Begründung: Die Zugriffsmöglichkeiten US-amerikanischer Nachrichtendienste und der fehlende gerichtliche Rechtsschutz für EU-Bürgerinnen und -Bürger gewährleisten kein der DSGVO gleichwertiges Schutzniveau.

Standardvertragsklauseln bleiben grundsätzlich zulässig, reichen aber allein nicht aus. Verantwortliche müssen im Einzelfall prüfen, ob im Empfängerland ein gleichwertiges Schutzniveau besteht, und gegebenenfalls zusätzliche technische und organisatorische Maßnahmen ergreifen.

Das 2023 beschlossene EU-US Data Privacy Framework hat die Lage entschärft, aber nicht abschließend geklärt: Es ist bereits Gegenstand juristischer Auseinandersetzungen. Wer Datenverarbeitung vollständig in der EU hält, umgeht diese Unsicherheit strukturell.

Die wichtigsten Fakten

URTEIL EuGH, 16.07.2020, Rechtssache C-311/18	**FOLGE** Privacy Shield ungültig
SCC Weiterhin gültig, aber prüfpflichtig	**PFLICHT** Transfer Impact Assessment je Drittlandtransfer
NACHFOLGER EU-US Data Privacy Framework (2023), rechtlich umstritten	**SICHERSTE OPTION** Keine Drittlandübermittlung

Konsequenzen für die Cloud-Nutzung

Schrems II verlagert die Beweislast auf den Verantwortlichen – also auf Ihr Unternehmen oder Ihre Behörde.

■ Transfer Impact Assessment

Für jeden Drittlandtransfer ist zu dokumentieren, welche Zugriffsrechte im Empfängerland bestehen und welche zusätzlichen Maßnahmen dagegen wirken.

■ Zusätzliche Schutzmaßnahmen

Wirksam sind vor allem Maßnahmen, die einen Klartextzugriff ausschließen – etwa Verschlüsselung mit ausschließlich europäischer Schlüsselhoheit.

■ Fortlaufende Überprüfung

Die Bewertung ist keine Einmalaufgabe: Ändert sich die Rechtslage oder die Anbieterstruktur, muss die Prüfung wiederholt werden.

■ Aufsichtsbehördliches Risiko

Fehlende oder unvollständige Prüfungen sind ein häufiger Prüfpunkt der Datenschutzaufsicht und können Anordnungen bis hin zum Verarbeitungsverbot nach sich ziehen.

So werden Sie Schrems-II-fest

Der pragmatische Weg führt über die Vermeidung des Transfers:

- ✓ Bestandsaufnahme: Welche Dienste übermitteln personenbezogene Daten in Drittländer?
- ✓ Bewertung: Welche Verarbeitungen sind besonders sensibel (Personal, Gesundheit, Bürgerdaten)?
- ✓ Ersetzen: Für sensible Verarbeitungen europäische Anbieter ohne Drittlandbezug wählen.
- ✓ Absichern: Für verbleibende Transfers SCC, TIA und zusätzliche Maßnahmen dokumentieren.
- ✓ Verankern: Souveränitätskriterien in Beschaffungsrichtlinien und Verträge übernehmen.
- ✓ Überprüfen: Jährliche Wiederholung der Bewertung, inklusive Unterauftragsverarbeiter.

Häufige Fragen zu Schrems II

Sind Standardvertragsklauseln nach Schrems II noch gültig?

Ja, sie bleiben ein zulässiges Transferinstrument. Der Verantwortliche muss aber zusätzlich prüfen und dokumentieren, ob im Empfängerland ein gleichwertiges Schutzniveau tatsächlich erreicht wird.

Löst das EU-US Data Privacy Framework das Problem?

Es erleichtert Transfers an zertifizierte US-Unternehmen, ist aber juristisch angegriffen. Wer langfristig planen muss, sollte sensible Verarbeitungen nicht von seinem Fortbestand abhängig machen.

Wie vermeide ich ein Transfer Impact Assessment vollständig?

Indem keine personenbezogenen Daten in Drittländer gelangen: europäischer Anbieter, europäische Rechenzentren, europäischer Support und europäische Unterauftragsverarbeiter.

Ausführlich online: xworks.net/sicherheit/schrems-ii

DSGVO

DSGVO-konforme Cloud: Anforderungen, Nachweise, Auswahl

Welche Pflichten die Datenschutz-Grundverordnung bei Cloud-Diensten auslöst – und woran Sie einen Anbieter erkennen, der sie tatsächlich erfüllt.

Was heißt „DSGVO-konforme Cloud“?

Cloud-Nutzung ist im Regelfall Auftragsverarbeitung nach Art. 28 DSGVO. Verantwortlich bleibt Ihre Organisation – der Anbieter verarbeitet Daten ausschließlich nach Ihrer Weisung und muss dies nachweisbar sicherstellen.

DSGVO-Konformität ist deshalb kein Siegel, sondern eine Kette überprüfbarer Zusagen: Auftragsverarbeitungsvertrag, technische und organisatorische Maßnahmen, Transparenz über Unterauftragsverarbeiter, Löschkonzept, Meldewege bei Datenschutzverletzungen und Unterstützung bei Betroffenenrechten.

Ein europäischer Anbieter ohne Drittlandbezug vereinfacht diese Kette erheblich, weil Transferprüfungen nach Kapitel V der DSGVO vollständig entfallen.

Die zentralen Pflichten im Überblick

ART. 28 Auftragsverarbeitungsvertrag mit allen Pflichtinhalten	**ART. 32** Angemessene technische und organisatorische Maßnahmen
ART. 30 Verzeichnis von Verarbeitungstätigkeiten	**ART. 33/34** Meldung von Datenschutzverletzungen binnen 72 Stunden
ART. 15–20 Auskunft, Löschung, Datenübertragbarkeit	**KAPITEL V** Prüfpflicht bei Drittlandübermittlungen

Worauf es in der Praxis ankommt

Die häufigsten Beanstandungen betreffen nicht die Technik, sondern fehlende Nachweise und unklare Verantwortlichkeiten.

■ Auftragsverarbeitungsvertrag

Muss Gegenstand, Dauer, Art und Zweck der Verarbeitung, Datenkategorien, Weisungsrechte, Löschung und Kontrollrechte konkret regeln – nicht nur den Gesetzestext wiederholen.

■ Unterauftragsverarbeiter

Eine vollständige, aktuelle Liste mit Sitz und Aufgabe ist Pflicht. Änderungen müssen vorab mitgeteilt werden, mit Widerspruchsmöglichkeit.

■ Löschung und Aufbewahrung

Löschfristen müssen technisch umsetzbar sein – inklusive Backups, Protokolldaten und Archiven.

■ Betroffenenrechte

Auskunfts- und Exportanfragen müssen fristgerecht bedienbar sein. Ein Selbstbedienungsexport in offenen Formaten reduziert den Aufwand deutlich.

Prüfliste für die Anbieterauswahl

Diese Punkte sollten Sie schriftlich bestätigt bekommen:

- ✓ Auftragsverarbeitungsvertrag nach Art. 28 DSGVO liegt vor und ist prüfbar.
- ✓ Verarbeitung, Backup und Protokollierung finden ausschließlich in der EU statt.
- ✓ Vollständige Liste der Unterauftragsverarbeiter inklusive Sitzland.
- ✓ Dokumentierte TOMs: Verschlüsselung, Zugriffskontrolle, Protokollierung, Notfallkonzept.
- ✓ Anerkannte Zertifizierungen wie ISO/IEC 27001 und BSI-orientierte Nachweise.
- ✓ Definierte Löschfristen und ein vollständiger Datenexport in offenen Formaten.

Häufige Fragen zur DSGVO in der Cloud

Reicht ein Rechenzentrum in der EU für DSGVO-Konformität?

Nein. Der Standort ist eine Voraussetzung, aber nicht ausreichend. Es kommt zusätzlich auf den Rechtsträger, den Auftragsverarbeitungsvertrag, die technischen Maßnahmen und die Unterauftragsverarbeiter an.

Wer haftet bei einem Datenschutzverstoß in der Cloud?

Primär die verantwortliche Stelle, also Ihre Organisation. Der Auftragsverarbeiter haftet für eigene Pflichtverletzungen. Deshalb sind Nachweise und Kontrollrechte im Vertrag so wichtig.

Ist xworks.365 DSGVO-konform?

Ja. xworks.365 wird von einem deutschen Unternehmen in einem eigenen ISO/IEC 27001-zertifizierten Rechenzentrum in Deutschland betrieben, mit Auftragsverarbeitungsvertrag, dokumentierten TOMs und ohne Datentransfer in Drittländer.

Ausführlich online: xworks.net/sicherheit/dsgvo-cloud

Standards · Gaia-X

Gaia-X: europäisches Rahmenwerk für souveräne Cloud-Dienste

Was Gaia-X ist, welche Prinzipien dahinterstehen und wie Sie die Ideen für Ihre Anbieterauswahl nutzen – auch unabhängig von einer formalen Teilnahme.

Was ist Gaia-X?

Gaia-X ist eine europäische Initiative für eine vernetzte, offene Dateninfrastruktur. Sie betreibt selbst keine Cloud, sondern definiert Regeln, Beschreibungsformate und Nachweise, mit denen Anbieter ihre Eigenschaften überprüfbar dokumentieren – vom Sitz der Gesellschaft über den Verarbeitungsort bis zu Interoperabilität und Ausstiegsoptionen.

Der Kern ist Transparenz: Statt Marketingaussagen sollen maschinenlesbare, prüfbare Selbstbeschreibungen den Vergleich von Diensten ermöglichen. Dadurch werden Souveränitätsmerkmale zu einem Auswahlkriterium wie Preis oder Verfügbarkeit.

Auch ohne formale Gaia-X-Teilnahme lassen sich die Prinzipien direkt anwenden: offene Standards, dokumentierte Datenflüsse, klare Rechtsträgerschaft und garantierte Portabilität.

Die Prinzipien im Überblick

TRANSPARENZ Prüfbare Angaben zu Betrieb, Standort und Rechtsträger	**INTEROPERABILITÄT** Offene Schnittstellen statt proprietärer Bindung
PORTABILITÄT Wechsel des Anbieters ohne Datenverlust	**SOUVERÄNITÄT** Kontrolle über Daten und Zugriffsregeln bleibt beim Nutzer
OFFENHEIT Offene Standards und offene Governance	**ERGÄNZEND** ISO/IEC 27001, BSI IT-Grundschutz, C5

Was Gaia-X für Ihre Beschaffung bedeutet

Die praktische Stärke von Gaia-X liegt in klaren, vergleichbaren Kriterien – unabhängig davon, ob ein Anbieter formal beteiligt ist.

■ Vergleichbarkeit

Strukturierte Selbstbeschreibungen machen Angebote vergleichbar und erschweren unbelegte Souveränitätsversprechen.

■ Ausstieg mitgedacht

Portabilität wird zum Bestandteil der Bewertung – nicht erst zum Thema bei der Kündigung.

■ Interoperable Architektur

Offene Protokolle wie IMAP, SMTP, CalDAV, CardDAV und WebDAV ermöglichen den Betrieb gemischter Landschaften ohne Insellösungen.

■ Anschluss an Standards

Gaia-X ersetzt keine Zertifizierung, sondern ergänzt ISO/IEC 27001 und BSI IT-Grundschutz um Transparenz- und Portabilitätsanforderungen.

Gaia-X-Prinzipien als Auswahlkriterien

Übernehmen Sie diese Anforderungen direkt in Ihre Ausschreibung:

- ✓ Rechtsträger, Verarbeitungsorte und Unterauftragsverarbeiter sind vollständig offengelegt.
- ✓ Alle Funktionen sind über offene, dokumentierte Standards nutzbar.
- ✓ Ein vollständiger Export aller Daten in offenen Formaten ist jederzeit möglich.
- ✓ Zugriffs- und Protokollierungsregeln sind transparent und überprüfbar.
- ✓ Anerkannte Zertifizierungen belegen die technische und organisatorische Sicherheit.
- ✓ Migrationspfade zu anderen Anbietern sind vertraglich beschrieben.

Häufige Fragen zu Gaia-X

Ist Gaia-X eine europäische Cloud?

Nein. Gaia-X betreibt keine eigene Infrastruktur, sondern definiert ein Rahmenwerk aus Regeln und Nachweisformaten, an dem sich Cloud- und Datendienste ausrichten können.

Brauche ich Gaia-X, um souverän zu arbeiten?

Nein, aber die Prinzipien helfen bei der Auswahl. Entscheidend bleiben europäischer Rechtsträger, EU-Verarbeitung, offene Standards und ein vollständiger Datenexport.

Wie verhält sich xworks.365 zu diesen Prinzipien?

xworks.365 setzt auf offene Standards (IMAP, SMTP, CalDAV, CardDAV, WebDAV), offene Dokumentformate, vollständigen Datenexport und Betrieb durch eine deutsche Gesellschaft in einem eigenen zertifizierten Rechenzentrum.

Ausführlich online: xworks.net/sicherheit/gaia-x

Fazit und nächste Schritte

Die vier Themen greifen ineinander: Der CLOUD Act beschreibt das Zugriffsrisiko, Schrems II die rechtliche Bewertung von Transfers, die DSGVO die Pflichten des Verantwortlichen und Gaia-X den Rahmen für interoperable, souveräne Dienste. Wer Anbieter ohne US-Rechtsträger wählt, Betrieb und Support in der EU hält und Datenexport in offenen Formaten sicherstellt, reduziert alle vier Risikodimensionen gleichzeitig.

xworks.365 wird von der mediaBEAM GmbH in einem eigenen, ISO/IEC 27001-zertifizierten Rechenzentrum in Deutschland betrieben – E-Mail, Kalender, Dateien, Dokumente und Videokonferenzen auf einer Plattform.

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