plan EU



WHITEPAPER · OKTOBER 2026

Digitale Abhängigkeit ist ein Geschäftsrisiko

Warum jede europäische Organisation wissen muss, wo ihre Software, Daten und Zahlungen liegen, und einen Exit-Plan für die Dienste braucht, auf die sie nicht verzichten kann.

ZUSAMMENFASSUNG

Kurz gesagt

Für E-Mail, Dokumente, Buchhaltung, Zahlungen und Hosting stützen sich europäische Organisationen in hohem Maß auf Dienste nichteuropäischer Anbieter. Das funktioniert meist hervorragend, bis eine Entscheidung außerhalb Europas dazu führt, dass ein Dienst eingeschränkt, abgeschaltet oder rechtlich unhaltbar wird.

DIE WICHTIGSTEN PUNKTE

- **Das Risiko ist nicht technisch, sondern rechtlich und politisch.** Gesetze, Sanktionen und Exportregeln im Herkunftsland des Anbieters können bestimmen, ob Ihr Dienst weiter funktioniert.
- **Die meisten Abhängigkeiten sind unsichtbar.** Sie liegen bei Ihren Dienstleistern und deren Unterauftragnehmern, nicht nur in Ihrer eigenen IT.
- **Die Regulierung verlangt es bereits.** DORA verpflichtet Finanzinstitute zu Exit-Strategien; NIS2 und die DSGVO verlangen Einblick in die Lieferkette; der Data Act erleichtert den Wechsel zwischen Cloud-Diensten.
- **Ein Wechsel ist nicht immer nötig, Vorbereitung schon.** Ein Exit-Plan je kritischem Dienst macht den Unterschied zwischen einer schwierigen Woche und wochenlangem Stillstand.

Dieses Whitepaper beschreibt, wo diese Abhängigkeiten liegen, welche Mechanismen sie zum Risiko machen, was die Regulierung verlangt und wie Sie in fünf Schritten von der Erkenntnis zu einem umsetzbaren Exit-Plan kommen.

Für wen? Vorstände, Geschäftsführer sowie Compliance- und IT-Verantwortliche europäischer Organisationen aller Branchen, mit besonderem Augenmerk auf Finanzinstitute, die unter DORA fallen.

1 Die stille Abhängigkeit

Fragen Sie eine beliebige Organisation, welche Software sie nutzt, und die Antwort kommt schnell: ein Office-Paket, eine Buchhaltungssoftware, ein CRM-System, ein Zahlungsdienstleister. Fragen Sie dann, wo diese Dienste laufen, welchem Recht der Anbieter unterliegt und was passiert, wenn der Dienst morgen nicht mehr verfügbar ist, und es wird still.

Das ist verständlich. Cloud-Dienste sind gerade deshalb beliebt, weil man nicht über sie nachdenken muss. Dadurch ist jedoch in kurzer Zeit eine Lage entstanden, in der der Geschäftsbetrieb vieler europäischer Organisationen von einer kleinen Zahl von Anbietern außerhalb Europas abhängt, ohne dass sich jemand bewusst dafür entschieden hätte.

Das Problem ist nicht, dass Sie nichteuropäische Dienste nutzen. Das Problem ist, dass Sie nicht wissen, was zu tun ist, wenn sie wegfallen.

Ein Beispiel, das hängen blieb

2025 wurde vielfach berichtet, dass der Chefankläger des Internationalen Strafgerichtshofs in Den Haag nach US-Sanktionen gegen den Gerichtshof keinen Zugang mehr zu seinem E-Mail-Konto bei einem US-Anbieter hatte. Über den genauen Hergang gibt es unterschiedliche Darstellungen. Für viele Organisationen wurde das Prinzip aber plötzlich greifbar: Die Entscheidung einer ausländischen Regierung kann über einen Anbieter unmittelbar auf eine europäische Organisation durchschlagen, auch wenn diese selbst nichts falsch gemacht hat.

Dasselbe kann aus weniger dramatischen Gründen geschehen: eine Preiserhöhung, die einen Dienst unbezahlbar macht, ein eingestelltes Produkt, ein durch eine automatische Prüfung gesperrtes Konto oder ein Anbieter, der übernommen wird.

2 Drei Mechanismen hinter dem Risiko

Die Abhängigkeit von einem nichteuropäischen Anbieter wird auf drei Wegen zum Risiko. Sie haben nichts mit der Qualität oder den guten Absichten des Anbieters zu tun.

01

Rechtshoheit

Ein Anbieter unterliegt dem Recht des Landes, in dem er niedergelassen ist. Der US CLOUD Act (2018) ermöglicht es zum Beispiel US-Behörden, Daten bei US-Anbietern anzufordern, auch wenn diese Daten in Europa gespeichert sind. Das kann mit der DSGVO kollidieren.

02

Sanktionen und Exportregeln

Regierungen können Unternehmen verpflichten, Dienste für bestimmte Personen, Organisationen oder Länder einzustellen. Der Anbieter hat dann keine Wahl. Für Sie kann das bedeuten, dass ein Dienst wegfällt oder ein Kunde oder Geschäftspartner nicht mehr erreichbar ist.

03

Technische Kontrolle

Bei Cloud-Diensten und vernetzten Geräten hält der Anbieter die technischen Schlüssel. Updates, Lizenzprüfungen oder das Abschalten von Funktionen können aus der Ferne erfolgen, mit oder ohne böse Absicht.

Nicht nur die Vereinigten Staaten

Die Debatte dreht sich oft um US-Technologiekonzerne, weil sie den größten Teil des Marktes bedienen. Dasselbe gilt aber für Anbieter aus anderen Ländern. Ein deutliches Beispiel sind vernetzte Fahrzeuge, Ladesäulen, Wechselrichter und andere Geräte mit Software, die aus der Ferne aktualisiert oder abgeschaltet werden kann. In den Vereinigten Staaten wurden im Januar 2025 Regeln erlassen, die Software aus China und Russland ab dem Modelljahr 2027 aus vernetzten Fahrzeugen fernhalten, genau aus diesem Grund. Für europäische Unternehmen mit Fuhrparks, Logistik oder Energieanlagen ist das eine direkte Frage: Wer kann Ihre Geräte aus der Ferne steuern?

Warum jetzt?

Diese Risiken gab es schon immer, aber drei Entwicklungen machen sie dringlicher: Die geopolitischen Verhältnisse sind weniger berechenbar geworden, immer mehr Geschäftsprozesse laufen ausschließlich in der Cloud, und die europäische Regulierung erwartet inzwischen, dass Organisationen diese Risiken nachweislich beherrschen.

3 Die verborgene Kette

Die größten Abhängigkeiten liegen oft nicht in Ihrer eigenen IT, sondern bei Ihren Dienstleistern. Ihr Buchhaltungsbüro, Ihr Lohnabrechner, Ihr IT-Dienstleister oder Ihr Wirtschaftsprüfer nutzt selbst Software und Hosting, und diese Entscheidungen sehen Sie nicht.

Beispiel: die Finanzkette

Ein Fondsverwalter lagert die Fondsadministration häufig an einen spezialisierten Administrator aus, arbeitet mit einer Verwahrstelle oder einem Treuhänder und einem externen Compliance-Dienstleister. Jede dieser Parteien arbeitet mit eigenen Systemen: einer Verwaltungssoftware, einer Dokumentenplattform, einer E-Mail-Umgebung, einem Hosting-Anbieter. Der Verwalter bleibt letztverantwortlich, hat aber oft keinen Einblick, welche Teile außerhalb Europas liegen.

GLIED	TYPISCHE FRAGE, DIE OFFEN BLEIBT
Eigene Organisation	Welche Dienste nutzen wir, und welche sind geschäftskritisch?
Direkter Dienstleister	Auf welcher Software und welchem Hosting läuft sein Dienst für uns?
Unterauftragnehmer (Unterauftragsverarbeiter)	Wo liegen die Daten und welchem Recht unterliegen diese Parteien?
Vertrag	Was ist zu Kündigung, Datenübergabe und Exit vereinbart?

Die Antworten auf diese Fragen gibt es meistens, in Auftragsverarbeitungsverträgen, Listen von Unterauftragsverarbeitern und Vertragsklauseln, aber sie sind verstreut und es kostet viel Zeit, sie zusammenzutragen. Genau daran scheitert es in der Praxis.

Tipp. Bitten Sie Ihre wichtigsten Dienstleister um ihre aktuelle Liste der Unterauftragsverarbeiter, einschließlich Sitzland und Speicherort der Daten. Nach der DSGVO darf ein Auftragsverarbeiter keinen Unterauftragsverarbeiter ohne Ihre Genehmigung einsetzen und muss Sie vorab über Änderungen informieren.

4 Was die Regulierung verlangt

Europäische Regeln verpflichten niemanden, ausschließlich europäische Anbieter zu nutzen. Sie verlangen aber, dass Organisationen ihre Abhängigkeiten kennen, Risiken beherrschen und bei Bedarf wechseln können.

REGELUNG	FÜR WEN	WAS RELEVANT IST
DORA Verordnung (EU) 2022/2554, anwendbar seit 17. Januar 2025	Banken, Versicherer, Wertpapierfirmen, zugelassene Fondsverwalter und andere Finanzunternehmen (nur registrierte „kleine" AIFM sind ausgenommen)	Informationsregister aller IKT-Dienstleistungsverträge; Risikobewertung vor Vertragsschluss; verpflichtende Exit-Strategien für IKT-Dienste, die kritische oder wichtige Funktionen unterstützen; Beachtung des Konzentrationsrisikos.
NIS2 Richtlinie (EU) 2022/2555	Wesentliche und wichtige Einrichtungen unter anderem in Energie, Verkehr, Gesundheit, digitaler Infrastruktur und öffentlicher Verwaltung	Sorgfaltspflicht für die Sicherheit der Lieferkette, einschließlich der Bewertung von Anbietern und Dienstleistern.
DSGVO Verordnung (EU) 2016/679	Jede Organisation, die personenbezogene Daten verarbeitet	Übermittlung in Länder außerhalb des EWR nur mit geeigneten Garantien; seit dem Schrems-II-Urteil (2020) ist im Einzelfall zu prüfen, ob das Recht des Empfängerlandes diese Garantien untergräbt.
Data Act Verordnung (EU) 2023/2854, anwendbar seit 12. September 2025	Kunden und Anbieter von Cloud-Diensten	Recht auf Wechsel zu einem anderen Anbieter; Wechselentgelte werden abgebaut und entfallen ab Januar 2027. Das macht einen Exit-Plan praktisch besser umsetzbar.

Hinweis. Diese Tabelle ist eine vereinfachte Übersicht und keine Rechtsberatung. Welche Pflichten genau für Ihre Organisation gelten, hängt von Branche, Größe und Zulassungen ab. Für jede Regelung können Sie auf den Gesetzesseiten prüfen, ob sie für Sie gilt.

5 Von der Erkenntnis zum Exit-Plan

Plan EU arbeitet mit einem festen Vorgehen in fünf Schritten. Die ersten Schritte können Sie selbst mit dem Scan durchlaufen; bei der Vertiefung und dem Exit-Plan begleiten wir Sie.

1

Domain

Anhand Ihres Domainnamens erfassen wir öffentlich sichtbare Dienste, etwa E-Mail- und Hosting-Anbieter.

2

Branche

Ihre Branche bestimmt, welche Regulierung und welche typischen Abhängigkeiten relevant sind.

3

Fragen je Bereich

Kurze Multiple-Choice-Fragen je Bereich: Bürosoftware, Buchhaltung, Zahlungen, Hosting, Kommunikation, Dienstleister.

4

Bericht

Für jede Antwort eine Einstufung auf der Risikoskala von Plan EU, mit Erläuterung und europäischen Alternativen.

5

Exit-Plan und Beratung

Für jeden nichteuropäischen Dienst ein Stufenplan. Auf Wunsch prüfen wir Verträge, sammeln die Antworten der Anbieter und begleiten den Wechsel.

Die Risikoskala

● Souverän	◐ Beherrschbar	○ Verwundbar	■ Kritisch
Europäischer Anbieter, Daten und Verwaltung innerhalb der EU.	Nicht europäisch, aber nicht geschäftskritisch oder leicht zu ersetzen.	Nicht europäisch und wichtig für den Geschäftsbetrieb.	Nicht europäisch, geschäftskritisch und schwer zu ersetzen.

Der Scan speichert keine Daten, die für den Bericht nicht nötig sind. Wir bewerten Situationen, nicht Anbieter: Der Bericht beschreibt sachlich, wo ein Dienst angesiedelt ist und was das für Sie bedeutet. Mehr dazu in unserer Methodik.

6 Was ein guter Exit-Plan enthält

Ein Exit-Plan ist kein Umzugsplan. Er ist eine Vorbereitung, die dafür sorgt, dass Sie wechseln können, wenn es nötig ist, geplant oder unter Druck. Für jeden Dienst in der Kategorie verwundbar oder kritisch halten Sie mindestens Folgendes fest:

- **Funktion und Verantwortlicher.** Welcher Geschäftsprozess hängt von dem Dienst ab und wer ist verantwortlich?
- **Daten.** Welche Daten liegen dort, in welchem Format können Sie sie exportieren und wie oft tun Sie das?
- **Alternative.** Mindestens eine europäische Alternative, mit einer groben Schätzung von Kosten und Dauer.
- **Vertrag.** Kündigungsfrist, Vereinbarungen zur Datenübergabe, Unterstützung beim Exit und Ihre Rechte nach dem Data Act.
- **Notfallszenario.** Was tun Sie in den ersten 48 Stunden, wenn der Dienst unerwartet wegfällt?
- **Abhängigkeiten.** Welche anderen Systeme oder Schnittstellen fallen mit aus?
- **Prüftermin.** Wann wird der Plan überprüft und geübt?

Für Dutzende häufig genutzte Dienste liegt ein solcher Plan bereits in unseren Exit-Plänen bereit.

Fünf Dinge, die Sie diesen Monat tun können

1. Erstellen Sie eine Liste der zehn Dienste, ohne die Ihre Organisation innerhalb eines Tages stillsteht.
2. Notieren Sie für jeden Dienst das Sitzland des Anbieters und den Speicherort der Daten.
3. Fordern Sie bei Ihren wichtigsten Dienstleistern deren Liste der Unterauftragsverarbeiter an.
4. Testen Sie, ob Sie Ihre wichtigsten Daten tatsächlich in einem brauchbaren Format exportieren können.
5. Durchlaufen Sie den Scan auf plan-eu.eu für einen ersten Überblick.

Quellen

- Verordnung (EU) 2022/2554 über die digitale operationale Resilienz im Finanzsektor (DORA), insbesondere Artikel 28.
- Richtlinie (EU) 2022/2555 (NIS2), insbesondere Artikel 21 zur Sicherheit der Lieferkette.
- Verordnung (EU) 2016/679 (DSGVO), Kapitel V; EuGH, 16. Juli 2020, C-311/18 (Schrems II).
- Verordnung (EU) 2023/2854 (Data Act), Kapitel VI zum Wechsel zwischen Datenverarbeitungsdiensten.
- Clarifying Lawful Overseas Use of Data Act (CLOUD Act), Vereinigte Staaten, 2018.

plan EU

PLAN-EU.EU

Über Plan EU

Plan EU hilft europäischen Organisationen, ihre digitalen Abhängigkeiten zu erfassen und einen umsetzbaren Exit-Plan aufzustellen. Mit einem Online-Scan, einem klaren Bericht und maßgeschneiderter Beratung, von der DORA-Zweitmeinung bis zur Begleitung beim Wechsel zu einer europäischen Alternative.

plan-eu.eu

info@plan-eu.eu

Plan EU ist eine Initiative der Luce Holding B.V. Dieses Whitepaper wurde sorgfältig auf Grundlage öffentlicher Informationen mit Stand Oktober 2026 erstellt und dient der allgemeinen Information. Es begründet keine Rechte und stellt keine Rechts-, Steuer- oder Anlageberatung dar. Plan EU ist keine Einrichtung der Europäischen Union.