By PwC Deutschland | 02.10.2025

EU Data Act: Neue Spielregeln für Datenzugang, Vertragsfairness und Cloud-Portabilität im Finanzsektor

RegCORE Client Alert | Digitaler Binnenmarkt der EU

Content

Verfasst vonJulia Siebrecht undDr. Michael Huertas

Kurzüberblick

DerEU Data Act (Verordnung (EU) 2023/2854) ist am 11. Januar 2024 in Kraft getreten und ist seit dem 12. September 2025 vollumfänglich anwendbar.**Show Footnote**Er ergänzt den bestehenden EU Data Governance Act (DGA, Verordnung (EU) 2022/868) und bildet neben der Datenschutzgrundverordnung (DSGVO), dem Digital Markets Act (DMA) und den Digital Services Act (DAS), einen zentralen Baustein der europäischen Datenstrategie.

Der EU Data Act regelt den Zugang zu und die Nutzung von Daten umfassend und setzt einen horizontalen, unionsweit einheitlichen Rechtsrahmen für den fairen Zugang zu und die Nutzung von Daten über Sektoren hinweg, um so fairen Wettbewerb zwischen den Akteuren zu fördern. Kernpunkte des EU Data Act sind die Stärkung der Datenportabilität, insbesondere durch einen leichteren Wechsel zwischen Cloud- und Edge-Diensten, die Verbesserung des Datenzugangs für Unternehmen sowie die Förderung offener und fairer Datenökosysteme, von denen Unternehmen, öffentliche Stellen und Verbraucher gleichermaßen profitieren.

Nutzer:innen erhalten Ansprüche auf Zugang zu, Nutzung und Weitergabe der durch vernetzte Produkte oder verbundene Dienste generierten Rohdaten. Dateninhaber müssen diese Daten zeitnah, in gängigen und maschinenlesbaren Formaten sowie zu fairen, angemessenen und nicht-diskriminierenden (FRAND) Bedingungen bereitstellen. Begünstigungen für Gatekeeper im Sinne des Digital Markets Act sind dabei ausgeschlossen.

Für die Anpassung von Altverträgen (unbefristet oder Laufzeit mehr als zehn Jahre ab dem 11. Januar 2024) ist eine Umsetzungsfrist bis zum 12. September 2027 vorgesehen.

Zentrale Erkenntnisse zum EU Data Act für den Finanzmarkt

Adressatenkreis

Unter den Anwendungsbereich des EU Data Act fallen unter anderem Hersteller vernetzter Produkte, Anbieter verbundener Dienste, Nutzer:innen und Datenempfänger:innen (sowohl im B2C- als auch im B2B-Bereich), Cloud- und Edge-Dienstleister sowie öffentliche Stellen, denen unter engen Voraussetzungen bei außergewöhnlichem Bedarf ein Datenzugriff eröffnet wird.

Zentrale Regelungsinhalte

Zugangsrechte zu Daten: Nutzer:innen von vernetzten Geräten oder Diensten erhalten ein Recht auf Zugriff auf die von ihnen erzeugten Daten inklusive der Möglichkeit, diese Daten an Dritte weitergeben zu lassen (Datenportabilität).

Vertragsfairness (B2B): Unternehmen müssen in bestimmten Konstellationen anderen Unternehmen Zugang zu Daten gewähren - und zwar zu fairen, angemessenen und nichtdiskriminierenden (FRAND)

Bedingungen. Der Schutz kleiner und mittlerer Unternehmen (KMU) vor Machtungleichgewichten wird ausdrücklich betont.**Show Footnote**

Pflichten für Cloud- und Edge-Dienste: Anbieter müssen Wechselhindernisse abbauen, die Portabilität und Interoperabilität von Daten sicherstellen und Migrations- sowie Exit-Prozesse vertraglich und technisch ermöglichen. Switching-Entgelte sind schrittweise zurückzuführen, sie sind ab dem 12. Januar 2027 nicht mehr zulässig. Wo Standards fehlen, ist ein Fallback-Export in strukturiertem, gängigem und maschinenlesbarem Format vorzuhalten.

B2G-Datenteilung: Behörden können unter bestimmten Bedingungen Zugriff auf Daten von Unternehmen verlangen. Dabei sind die Anforderungen an Behörden, die Zugriff nehmen möchten, jedoch streng. Behördliche Datenanforderungen müssen zweckgebunden, verhältnismäßig, zeitlich begrenzt und gut begründet sein. Außerhalb echter Notlagen ist der Zugriff regelmäßig auf nicht-personenbezogene Daten beschränkt. Der Data Act schafft keine eigene Rechtsgrundlage für die Verarbeitung personenbezogener Daten. Vorrang haben die DSGVO und die ePrivacy-Verordnung, zudem sollen Geschäftsgeheimnisse und Immaterialgüterrechte gewahrt bleiben.**Show Footnote**

Schnittstellen zu bestehender Finanzmarktregulierung

Der EU Data Act entfaltet seine Wirkung nicht isoliert, sondern im Zusammenspiel mit bestehender und künftiger Finanzmarktregulierung. Besonders relevant sind folgende Schnittstellen:

PSD2 (perspektivisch PSD3/PSR): Heute müssen Banken Drittanbietern (TPPs) Zugriff auf Zahlungsverkehrs- bzw. Kontodaten über standardisierte Schnittstellen (APIs) geben, wenn ihr Kunde dies autorisiert („Open Banking“). Der EU Data Act erweitert den Rahmen deutlich, da er jegliche durch den Nutzer erzeugte Daten umfasst, insbesondere IoT- und Maschinendaten.

DORA:Während der EU Data Act die Interoperabilität und Portabilität fordert, setzt DORA erhöhte Sicherheits- und Resilienz-Standards. Für Finanzdienstleister müssen diese Anforderungen künftig unter einen Hut bekommen und die regulatorisch geforderte Balance zwischen Offenheit (EU Data Act) und Schutz vor Cyberrisiken (DORA) schaffen.

FIDAR: Mit dem Vorschlag für eine Financial Data Access Regulation (FIDAR) schafft die EU einen spezifischen Rahmen für den Zugang zu Finanzdaten, der über PSD2 hinausgeht und ein Open-Finance-Ökosystem etablieren soll. FIDA verpflichtet Finanzinstitute, Finanzdaten über standardisierte Schnittstellen bereitzustellen, sofern der Kunde zustimmt, und ergänzt damit den sektorenübergreifenden Ansatz des Data Act um eine branchenspezifische Komponente.

Zentrale Überlegungen zum EU Data Act für den Finanzmarkt

Connected Products / IoT: Bei Produktentwicklung und Vertragsgestaltung sind die Prinzipien „Access by Design“ sowie „Security/Privacy by Design“ konsequent umzusetzen – der Zugang zu Daten und deren Schutz müssen von Anfang an technisch und organisatorisch eingeplant werden:

- **Technische Anforderungen:**Erforderlich sind vor allem belastbare Schnittstellen, konsistente Datenmodelle, definierte Exportformate und feste Exportfrequenzen.
- **Rollen- und Rechtekonzepte:**Verantwortlichkeiten und Zugriffsrechte sind unter Wahrung des Prinzips der minimalen Rechtevergabe („Least Privilege“) eindeutig zu definieren und regelmäßig zu überprüfen.
- **Nachvollziehbares Logging und sichere Datenpfade:**Zugriffe und Datenbewegungen müssen umfassend (und manipulationssicher) protokolliert werden; der Datenabruf und die Weitergabe von Daten dürfen nur über verschlüsselte und authentifizierte Kanäle erfolgen.
- **Geschäftsgeheimnisse und geistiges Eigentum:**Geschäftsgeheimnisse und IP sind ausreichend, insbesondere durch Pseudonymisierung, Verschlüsselung und strikte Zugriffsbeschränkungen, zu schützen.

Exit-Fähigkeit bei Cloud- und Edge-Lösungen: Verträge müssen die Portabilität und Interoperabilität der Daten gewährleisten. Dies umfasst die Verpflichtung zur Unterstützung offener, standardisierter Schnittstellen und Formate. Vertraglich sind insbesondere angemessene Fristen für Anbieterwechsel oder die Beendigung des Dienstes festzulegen, um eine geordnete Migration zu ermöglichen

Auf operativer Ebene sollten geeignete, praxiserprobte Tools und Verfahren für die Migration von Daten und Workloads bereitgestellt werden. Regelmäßige Test-Exporte und Migrationsproben sowie Rollback- und Notfallpläne sind notwendig, um Risiken bei der Migration zu minimieren und die Geschäftskontinuität zu sichern.

Vertragsgestaltung und Altverträge: Neuverträge ab dem 12.09.2025 sind Data-Act-konform aufzusetzen. Bis zum 12.09.2027 müssen bestehende Cloud- oder Datenverträge mit einer Restlaufzeit von mindestens zehn Jahren (Ausgangspunkt: 11. Januar 2024) überprüft und ggf. angepasst werden.

Switching-Entgelte: Entgelte für den Anbieterwechsel (Switching Fees) müssen überprüft, schrittweise reduziert und bis spätestens 10.09.2027 gestrichen werden.

Governance: Richtlinien für Datennutzung, Zugriffsrechte und interne Prozesse müssen angepasst werden. Zuständigkeiten, Genehmigungsläufe und Dokumentationspflichten sind verbindlich festzulegen.

Monitoring: Die Kontinuierliche Beobachtung regulatorischer Entwicklungen und technischer Standards ist unerlässlich.

Ausblick

Seit 12. September 2025 gelten die Kernvorgaben des Data Act. Vertragsmuster, Exit-Playbooks und technische Schnittstellen sollten – soweit nicht bereits erfolgt – an die neuen Anforderungen angepasst werden. Ohne saubere Datenarchitektur und FRAND-fähige Konditionen drohen Verzögerungen, Compliance-Lücken und Vertrauensverluste.

Für die Anpassung von Altverträgen (unbefristet oder Laufzeit mehr als zehn Jahre ab dem 11. Januar 2024) bleibt noch Zeit bis zum 12. September 2027.

Die Änderungen eröffnen einerseits erhebliche Chancen, da mit Zustimmung der Kunden externe Datenquellen wie Smart-Car- oder Smart-Home-Daten in Produkt- und Konditionengestaltung einfließen können. Andererseits müssen eigene Datenmodelle, API-Architekturen und Vertragswerke so ausgestaltet werden, dass Anforderungen an Datenzugang, Interoperabilität und Portabilität erfüllt sind. Das erfordert technische Standardisierung, belastbare Exportpfade und FRAND-fähige Konditionen in der Vertragspraxis.

Über uns

PwC Legal unterstützt eine Reihe von Finanzdienstleistungsunternehmen und Marktteilnehmern bei der vorausschauenden Planung von Veränderungen, die sich aus einschlägigen Entwicklungen ergeben. Zu diesem Zweck haben wir ein multidisziplinäres und multijurisdiktionales Team von Branchenexperten zusammengestellt, das unsere Mandanten dabei unterstützt, Herausforderungen zu bewältigen und Chancen zu nutzen sowie proaktiv mit ihren Marktteilnehmern und Aufsichtsbehörden in den Dialog zu treten.

Darüber hinaus haben wir eine Reihe von RegTech- und SupTech-Tools für beaufsichtigte Institute entwickelt, darunter das**Rule Scanner**Tool von PwC Legal, das durch ein zuverlässiges Set an Managed Solutions von PwC Legal Business Solutions unterstützt wird. Dieses ermöglicht ein Horizon Scanning und eine Risikokartierung sämtlicher gesetzlicher und regulatorischer Entwicklungen sowie von Sanktionen und Bußgeldern – erfasst von mehr als 2.500 gesetzgeberischen und aufsichtsrechtlichen Entscheidungsträgern sowie weiteren Branchenstimmen in über 170 Jurisdiktionen mit Relevanz für Finanzdienstleistungsunternehmen und deren Geschäftstätigkeit.

Ebenso bieten wir unter Nutzung unserer Rule Scanner-Technologie eine weitere Lösung an, mit der Finanzdienstleistungsunternehmen ihre internen Richtlinien und Verfahren digitalisieren können. Dadurch lässt sich ein umfassendes Dokumentationsinventar mit einer etablierten Dokumentationshierarchie und einem eingebetteten Glossar erstellen, das über eine Versionskontrolle entlang eines definierten zeitlichen Rahmens (rückblickend wie vorausschauend) verfügt. So wird sichergestellt, dass Änderungen in einer Richtlinie konsequent auch in andere Richtlinien- und Verfahrensdokumente übernommen werden, kritische Abhängigkeiten im Ablauf abgebildet sind und gesetzgeberische sowie aufsichtsrechtliche Entwicklungen gekennzeichnet werden, sofern sie Handlungsbedarf in den betreffenden Richtlinien und Verfahren erfordern.

Das PwC Legal-Team hinter dem Rule Scanner ist stolzer Preisträger des renommierten**„2024 Disruptive Technology of the Year Award“**von ALM Law.com sowie des**„2025 Regulatory, Governance and Compliance Technology Award“**im Jahr 2025.

Wenn Sie die oben genannten Entwicklungen oder deren mögliche Auswirkungen auf Ihr Unternehmen im Allgemeinen näher besprechen möchten, wenden Sie sich bitte an einen unserer Ansprechpartner oder an

das RegCORE-Team von PwC Legal über**de_regcore@pwc.com**oder unserer**Website**.

Kontaktieren Sie uns

Julia Siebrecht

Manager Frankfurt am Main
Tel.: +49 160 8482630
E-Mail:**julia.siebrecht@pwc.com**

Dr. Michael Huertas

Partner Frankfurt am Main
Tel.: +49 160 97375760
E-Mail:**michael.huertas@pwc.com**

Keywords

EU-Recht, Gesetzgebung