Einführung

Das Gesetz über digitale Märkte (DMA) führt umfangreiche Datenportabilitätspflichten für benannte Anbieter zentraler Plattformdienste ("designierte Unternehmen") ein und verpflichtet diese, Daten auf Anfrage mit Endnutzern und deren autorisierten Dritten zu teilen. Während Datenportabilität ein grundlegendes Recht nach EU-Recht darstellt, birgt die Umsetzung der DMA-Verpflichtungen bei gleichzeitigem Schutz individueller und unternehmerischer Rechte komplexe Herausforderungen. Besonders kritisch ist dabei das Zusammenspiel mit der Datenschutz-Grundverordnung (DSGVO) und deren Sicherheitsanforderungen, einschließlich der Notwendigkeit gültiger Rechtsgrundlagen für Datenübermittlungen. Der aktuelle Rahmen ermöglicht es Drittparteien, ob innerhalb oder außerhalb der EU tätig, erhebliche Mengen an Kundendaten ohne angemessene Sicherheitsüberprüfungsmechanismen zu erhalten. Dies schafft erhebliche Risiken für den Datenschutz und die Datensicherheit, insbesondere bei der Übermittlung personenbezogener Daten. Es fehlen Organisationen derzeit sinnvolle Möglichkeiten, Datenportabilitätsanforderungen unter Gewährleistung robuster rechtlicher und technischer Schutzmaßnahmen umzusetzen.

Unsere Kernpunkte

Wir setzen uns ein für die Schaffung eines robusten Rahmens, der Datenportabilität ermöglicht und gleichzeitig angemessenen Schutz personenbezogener Daten gewährleistet, das Vertrauen in digitale Dienste aufrechterhält und Innovation unterstützt. Dieser sollte flexibel genug sein, um sich an entwickelnde Sicherheitsbedrohungen anzupassen und dabei konsistente Schutzstandards aufrechtzuerhalten.

1. Sicherheits- und Datenschutzstandards

Aktuelle Rahmenmängel umfassen:

- Fehlen von Mindestsicherheitsstandards für anfragende Drittparteien
- Keine expliziten Vorgaben für Sicherheitsbewertungen oder Due Diligence
- Mangel an Mechanismen zur Ablehnung risikoreicher Datenübertragungen
- Unzureichender Schutz personenbezogener Daten von EU-Bürgern
- Kein standardisierter Überprüfungsprozess für Sicherheitsmaßnahmen Dritter

Wir setzen uns ein für:

- Entwicklung umfassender Sicherheitsstandards durch europäische Normungsgremien
- Einführung verpflichtender Sicherheitszertifizierungen für Datenanfragende
- Klare Überprüfungsverfahren einschließlich Governance-, Erkennungs-, Präventiv- und Korrekturkontrollen
- Recht zur Verweigerung von Übertragungen aus dokumentierten Sicherheitsbedenken
- Regelmäßige Sicherheitsaudits und Compliance-Überwachung

2. DSGVO-Konformität und internationale Übermittlungen

Herausforderungen sind:

- Unklares Zusammenspiel zwischen DMA und DSGVO-Anforderungen
- Komplexe Einwilligungsvalidierung bei Datenübermittlungen
- Schwierigkeiten bei internationalen Übermittlungen in Länder ohne Angemessenheitsbeschluss
- Begrenzte Optionen für rechtmäßige Übermittlungsmechanismen
- Herausforderungen bei Rechenschaftspflichten

Wir setzen uns ein für:

- Detaillierte Leitlinien zur DSGVO-Konformität im DMA-Kontext
- Entwicklung von Standardvertragsklauseln für internationale Übermittlungen
- Klare Rahmenbedingungen für die Einwilligungsprüfung
- Spezifische Bestimmungen für Übermittlungen in Hochrisikoländer

- Harmonisierten Ansatz für DSGVO- und DMA-Verpflichtungen

3. Verhinderung von Datenkommerzialisierung und -missbrauch

Wesentliche Bedenken bestehen bezüglich:

- Potenzieller Missbrauch von Daten für nicht autorisierte kommerzielle Zwecke
- Mangelnde Transparenz bei Datenverarbeitungszwecken und -praktiken
- Risiken im Zusammenhang mit incentivierter Datenweitergabe
- Unzureichende Kontrollen der Weiterverarbeitung
- Potenzial für irreführende Praktiken bei der Einholung von Einwilligungen

Wir setzen uns ein für:

- Strikte Beschränkungen der kommerziellen Nutzung übertragener Daten
- Verpflichtende Zweckspezifizierungsanforderungen
- Klare Einschränkungen für incentivierte Datenweitergabe
- Erweiterte Transparenzpflichten für Datenempfänger
- Regelmäßige Überwachung der Datennutzungskonformität

4. Technischer Implementierungsrahmen

Aktuelle Herausforderungen in der Implementierung sind:

- Fehlen standardisierter Sicherheitsbewertungsmethoden
- Unzureichende Leitlinien für technische Schutzmaßnahmen
- Unklare Anforderungen für kontinuierliche Überwachung
- Mangel an Incident-Response Protokollen
- Begrenzte Vorgaben für den Umgang mit Sicherheitsverletzungen

Wir setzen uns ein für:

- Entwicklung umfassender technischer Standards
- Implementierung strukturierter Sicherheitsbewertungsrahmen
- Spezifische Anforderungen an die laufende Überwachung
- Verpflichtende Incident-Response-Verfahren
- Klare Protokolle für Sicherheitsverletzungsmeldungen

5. Governance und regulatorische Aufsicht

Ein Rahmenwerk erfordert:

- Klare Zuweisung von Aufsichtsverantwortlichkeiten
- Definierte Durchsetzungsmechanismen über Jurisdiktionen hinweg
- Koordination zwischen mehreren Regulierungsbehörden
- Spezifische Abhilfemaßnahmen bei Nichteinhaltung
- Einheitliche Auslegung der Anforderungen

Wir setzen uns ein für:

- Verstärkten Aufsichtsrahmen mit klarer Kompetenzverteilung
- Koordinierte Durchsetzungsprotokolle zwischen EU-Behörden
- Harmonisierten Ansatz zwischen DMA- und DSGVO-Durchsetzung
- Spezifisches Sanktionsregime für Sicherheitsverstöße
- Regelmäßige Überprüfung und Aktualisierung der Anforderungen

6. Implementierungszeitplan und Unterstützung

Wichtige Voraussetzungen sind:

- Realistische Implementierungszeitpläne
- Klare Compliance-Leitlinien
- Technische Unterstützung bei der Implementierung
- Ressourcenzuweisung für Sicherheitsmaßnahmen
- Schulungs- und Sensibilisierungsprogramme

Wir setzen uns ein für:

- Phasenweisen Implementierungsansatz
- Detaillierte Implementierungsleitlinien
- Technischen Unterstützungsrahmen
- Leitfaden zur Ressourcenzuweisung
- Umfassende Schulungsprogramme