

Datenschutz-Newsletter 2025 / III

Aktuelles rund um den Datenschutz

Microsoft kann US-Zugriff auf EU-Cloud nicht verhindern

Anton Carniaux, Chefjustiziar von Microsoft Frankreich, wurde im Juni 2025 vor dem französischen Senat zur sogenannten „souveränen Microsoft-Cloud“ befragt. Dabei räumte er unter Eid ein, dass Microsoft nicht garantieren könne, dass Daten von EU-Bürgern, die in dieser Cloud gespeichert sind, nicht ohne Zustimmung europäischer Behörden an die US-Regierung weitergegeben werden. Auf die konkrete Frage, ob etwa Daten, die öffentliche Stellen über die französische Beschaffungsstelle UGAP an Microsoft übermitteln, absolut sicher seien, musste er verneinen. Zwar betonte er, dass ein solcher Fall bislang noch nicht eingetreten sei, doch zeigte die Aussage klar die Grenzen einer europäischen Datensouveränität auf. Microsoft prüfe zwar jede Anfrage von US-Behörden sehr genau und lehne unbegründete Gesuche ab. Falls möglich, würden diese Anfragen an die Kunden weitergeleitet und nur in Ausnahmefällen komme es zu einer Herausgabe. Das Unternehmen strebe stets an, die Betroffenen zu informieren, wenn Daten übermittelt werden müssen, garantieren könne es dies jedoch nicht. Eine „souveräne EU-Cloud“ ist demzufolge rechtlich nicht vollständig abgesichert. Für Behörden und öffentliche Einrichtungen, die besonderen Wert auf Datenschutz und Kontrolle legen, hat dies einen erheblichen Vertrauensverlust zur Folge. Wie tragfähig sind demnach die Schutzmechanismen des aktuellen Data Privacy Frameworks zwischen der EU und den USA tatsächlich?

Data Privacy Framework: EU-Gericht weist Klage ab

Gegen den Angemessenheitsbeschluss der EU-Kommission zum EU-US Data Privacy Framework (DPF) wurde Klage zum Gericht der Europäischen Union erhoben. Ziel der Klage war es, das Abkommen für nichtig erklären zu lassen, da es keinen ausreichenden Datenschutz garantiere. Kritisiert wurde insbesondere, dass der Data Protection Review Court (DPRC), der Beschwerden von EU-Bürgern prüfen soll, weder unabhängig noch unparteiisch sei. Auch würden US-Nachrichtendienste personenbezogene Daten in großem Umfang ohne ausreichende rechtliche Grundlage sammeln. Ein mit der EU vergleichbares Schutzniveau bestehe keineswegs. Das Gericht wies die Klage allerdings ab und stellte fest, dass die USA zum Zeitpunkt des Beschlusses ein angemessenes Datenschutzniveau gewährleistete. Der DPRC verfüge über institutionelle und verfahrensrechtliche Garantien, die seine Unabhängigkeit sicherstellen, etwa Schutz vor unrechtmäßiger Einflussnahme und klare Regeln für die Amtsenthebung von Richtern. Auch bei Sammelabrufen gebe es nachträgliche Rechtsschutzmöglichkeiten, da Beschwerden von Betroffenen geprüft werden können. Zudem sei die EU-Kommission verpflichtet, die praktische Umsetzung des DPF kontinuierlich zu überwachen und den Angemessenheitsbeschluss bei Bedarf anzupassen, einzuschränken oder aufzuheben. Das Urteil bringt Unternehmen und Organisationen, die Daten in die USA übermitteln, zunächst Rechtssicherheit, da sie sich weiterhin auf das DPF stützen können. Die Belastbarkeit der zugesicherten Schutzmechanismen in der Praxis stehen allerdings weiter in Frage.

Datenschutz in Pflegeeinrichtungen

Im Gesundheits- und Pflegebereich ist der Schutz personenbezogener Daten von besonderer Bedeutung. Überwiegend handelt es sich um Gesundheitsdaten, die einem besonderen Schutz der Datenschutzgrundverordnung (DSGVO) unterliegen. Beschwerden über Verstöße mehrten sich allerdings in der Vergangenheit. Daher hat die Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (LDI NRW) im September 2025 eine Initiativprüfung gestartet, die den Datenschutz in Pflegeeinrichtungen beleuchtet und Schwächen offenlegen will.

Die Beschwerden deuteten auf wiederholte Rechtsverstöße, insbesondere um die rechtswidrige Weitergabe von personenbezogenen Daten an externe Dritte (Mitteilungen zu Todesfällen, zur finanziellen Situation, von Gesundheitsinformationen). Die Behörde sieht häufig wechselnde Beschäftigte wegen mangelnder Schulung als einen Defizitpunkt. Bei der Prüfung der LDI NRW werden verschiedene Betreiber von stationären Pflegeeinrichtungen kontaktiert und insbesondere zur Sicherstellung von datenschutzrechtlichen Kenntnissen der Mitarbeiter befragt. Ein Augenmerk liegt auf den Schulungs- und Sensibilisierungskonzepten. Nach der Überprüfung wird der LDI NRW eine abschließende Bewertung veröffentlichten.

Bereits jetzt werden verschiedene Hinweise für Pflegeeinrichtungen gegeben. Dabei sollten bestehende Datenschutz- und Schulungskonzepte kontrolliert werden. Datenschulungen seien keine einmaligen Maßnahmen, sondern sind als fortlaufender Prozess zu behandeln. Auch bei hoher Personalfuktuation müsse gewährleistet sein, dass alle Mitarbeitenden stets auf dem aktuellen Stand sind: eine gründliche Erstunterweisung bei Arbeitsantritt und regelmäßige Auffrischungen und Sensibilisierungen. Dabei kann an alle Formen einer Wissensvermittlung, wie Präsenzseminare, Online-Schulungen, Informationsmaterialien, Merkblätter oder interne Newsletter gedacht werden. Eine Dokumentation der Maßnahmen ist dabei ebenfalls wichtig. Das notwendige Bewusstsein muss für datenschutzkonformes Handeln entwickelt werden.

Die Initiative der LDI NRW macht deutlich, dass Datenschutz im Pflegebereich kein Randthema sein darf. Das

Risiko von „Missgeschick“ bei der Verarbeitung und Missbrauch sensibler Gesundheitsdaten ist immanent. Das Vertrauen von Bewohnern und Angehörigen darf nicht beschädigt werden. Die Datenschutzkonzepte müssen konsequent auf den Prüfstand gestellt werden.

Illegale Datenweitergabe - Bußgeld

Der Umgang mit personenbezogenen Daten erfordert erhöhte Sorgfalt, insbesondere für Einrichtungen, die mit Kindern und Jugendlichen arbeiten und dabei Gesundheits- und Sozialdaten verarbeiten. Die griechische Datenschutzaufsichtsbehörde verhängte im Juni 2025 gegen eine Vereinigung mit therapeutischen Leistungen für Kinder ein Bußgeld wegen illegaler Datenweitergabe, Missachtung des Auskunftsrechts und mangelnder Kooperation mit der Datenschutzbehörde.

Ausgangspunkt war eine Beschwerde von Eltern wegen Verweigerung ihres Auskunftersuchen. Zudem habe die Vereinigung Daten der Kinder an ein Unternehmen weitergegeben. Eine Einwilligung oder Unterrichtung hat nicht stattgefunden. Besonders schützenswerte Gesundheitsdaten und Gerichtsurteile von Betroffenen waren hiervon umfasst.

Die griechische Aufsicht stellte mehrere Datenschutzverstöße fest und verhängte mehrere Einzelbußgelder: 3.000 Euro wegen der Weigerung des Auskunftsrechts, 3.000 Euro wegen der unzulässigen Weitergabe besonders schützenswerter personenbezogener Daten ohne vorherige Information, 3.000 Euro wegen der umfangreichen Übermittlung eines Gerichtsurteils und 1.000 Euro wegen mangelnder Kooperation mit der Aufsicht.

Der Fall verdeutlicht die besondere Schutzwürdigkeit von Gesundheits- und Sozialdaten und auch die besondere Schutzbedürftigkeit von Kindern. Verantwortliche sind angehalten strenge Vorkehrungen zu treffen, um Missbrauch und unrechtmäßige Offenlegung zu verhindern und schwerwiegende Eingriffe zu vermeiden.

Stand: 30. September 2025

Alle Beiträge sind nach bestem Wissen zusammengestellt. Eine Haftung für deren Inhalt kann jedoch nicht übernommen werden.

Für Fragen zum Thema Datenschutz stehen Ihnen unsere zertifizierten Datenschutzbeauftragten gerne zur Verfügung.

RA/StB Thomas Hesz; WP/StB Marcel Peetz (M.Acc.); Stefan Gräbe
Zertifizierte Datenschutzbeauftragte (TÜV)

Telefon: 09221 / 900 - 0

edsb@firtconsult.de www.firtpartner.de