Umsetzung von EU-Datenrecht

Der 18. Österreichische IT-Rechtstag war von der Umsetzung datenrechtlicher Vorgaben der Europäischen Union und deren Auswirkungen in der Praxis geprägt.

Der europäische Gesetzgeber hat den Rahmen vorgegeben, in dem sich die Informationstechnologie im EU-Raum künftig entwickeln soll", führte Universitätsprofessor Andreas Wiebe, Obmann des Forschungsvereins Infolaw, bei der Eröffnung des 18. Österreichischen Rechtstags aus, der am 25. und 26. April 2024 im Haus des Sports in Wien stattfand. Ziel der Veranstaltung war es, diesen Rahmen auszuloten und die Vorgaben in die Praxis umzusetzen.

IT-Rechtstag 2024: Umsetzung von EU-Informations- und Datenrecht

Künstliche Intelligenz – AI-Act. Julia Fuith vom Finanzministerium berichtete einleitend über den Inhalt der zum damaligen Zeitpunkt noch nicht veröffentlichten EU-Verordnung über künstliche Intelligenz (AI-Act). Die Veröffentlichung im Amtsblatt der EU ist nunmehr am 12. Juli 2024 erfolgt. Sie gilt ab dem 2. August 2026, die Kapitel I (Allgemeine Bestimmungen) und II (Verbotene Praktiken im IT-Bereich) bereits ab dem 2. Februar 2025 (Art. 113).

Als *KI-System* (Art 3 Z 1) wird, verkürzt dargestellt, ein maschinengestütztes System bezeichnet, das für einen autonomen Betrieb ausgelegt ist, anpassungsfähig sein kann und aus den erhaltenen Eingaben Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erstellt, die physische oder virtuelle Umgebungen beeinflussen können.

Verbote. Anwendungen, die mit einem unannehmbaren Risiko einhergehen, sind verboten (Kapitel II, Art 5). Darunter fallen beispielsweise Techniken der unterschwelligen Beeinflussung oder der Bewertung oder Klassifizierung von Personen auf Grund ihres Sozialverhaltens oder persönlicher Merkmale (social scoring). Ebenso verboten sind unter anderem KI-Systeme, die ausschließlich auf der Grundlage eines Profiling das Risiko bewerten, dass eine Person eine Straftat begeht (predictive policing) sowie zur Emotionserkennung einer Person am Arbeitsplatz. Verboten ist die Verwendung biometrischer Echtzeit-Fernidentifizierungssysteme in öffentlichen Räumen zu Strafverfolgungszwecken, außer zur gezielten Suche nach bestimmten Opfern von Entführung, Menschenhandel oder sexueller Ausbeutung sowie bei der Suche nach vermissten Personen oder bei Gefahr eines Terroranschlags. Ansonsten ist der Einsatz dieser Systeme zulässig zum Aufspüren einer Person, die der Begehung einer im Anhang II aufgeführten Straftaten verdächtig ist, die mit einer Freiheitsstrafe von mindestens vier Jahren bedroht ist.

KI-Systeme mit hohem Risiko (Kapitel III) müssen in einer eigenen EU-Datenbank registriert werden. Die Systeme müssen die CE-Kennzeichnung tragen. Systeme mit geringem Risiko (beispielsweise Chatbots) sind zulässig, unterliegen aber besonderen Transparenzverpflichtungen.

Der Großteil der Anwendungen wird Systeme mit minimalem Risiko betreffen (zum Beispiel Spamfilter). Diese können auf Basis der bestehenden rechtlichen Verpflichtungen ohne zusätzliche Auflagen angewendet werden.

In der Regel besteht für Unternehmen keine Pflicht, KI einzusetzen, doch könnte, worauf Rechtsanwalt Roman Heidinger hinwies, im Schadensfall bei rückblickender Betrachtung das Fehlen von auf KI aufbauender Kontrollsysteme als Verschulden der Leitungsorgane ausgelegt werden.

Das Spannungsverhältnis des Einsatzes von KI im Verhältnis zur DSGVO, insbesondere in Bezug auf LinkedIn-Profile bei Recruiting-Verfahren, beleuchtete Rechtsanwalt Michael M. Pachinger. Von Bedeutung ist das „Schufa-Urteil" des EuGH vom 7.12.2023, C-34/21, wonach ein *Scoring* (Bonitätsprüfung) bei Prüfung der Kreditwürdigkeit verboten ist, sofern der automatisierten Entscheidung im Einzelfall eine maßgebliche Rolle beigemessen wird. Ähnlich auch die rechtliche Bewertung des *AMS-Algorithmus,* mit dem auf der Basis von Faktoren wie Altersgruppe, Geschlecht, Ausbildung, Berufsgruppe, automatisiert die Chancen einer Vermittlung am Arbeitsmarkt bestimmt wurden (VwGH 21.12.2023, Zl 2021/04/0010-11).

KI-Training. Eine generative KI – wie etwa ChatGPT – muss trainiert werden. Sie braucht einen möglichst umfangreicher Vorrat an Daten. Bei der Einspeisung dieser Daten können sich, wie Rechtsanwalt Stephan Winklbauer ausführte, urheberrechtliche Probleme ergeben, die auch schon zu Klagen von Zeitungsverlagen oder Bildagenturen wegen fehlender Lizenzen geführt haben. Urheberrechtlich geschützt ist eine persönliche geistige Schöpfung, die der

FOTO: KURT HICKISCH

KI einerseits wegen fehlender Rechtsfähigkeit nicht zukommt und weil sie andererseits lediglich ein Werkzeug darstellt. Algorithmen sind nicht schutzfähig. Bei entsprechend kreativer Höhe der der KI gestellten Aufgabe könnte eine indirekte Urheberschaft des Benutzers in Frage kommen, analog dem Fragesteller bei einem Interview. Auch sind die Ergebnisse nach derzeitiger Rechtslage nicht patentierbar.

Data Act. Drei Vorträge haben sich mit der EU-VO 2023/2854 vom 13. Dezember 2023 über Vorschriften für einen fairen Datenzugang und eine faire Datennutzung (Data Act) befasst. Mit dieser soll die wirtschaftliche Nutzung jener Datenmengen, die von einer Unzahl an vernetzten Produkten (Autos, Haushaltsgeräte, Maschinen u. a.) erzeugt oder erhoben werden, in dem Dreiecksverhältnis Nutzer, Dateninhaber und Datenempfänger geregelt werden. Die Verordnung ist bereits in Kraft getreten, gilt aber erst ab dem 12. September 2025.

Datenschutz-Judikatur. Aus der von Bernhard Schildberger vom Justizministerium präsentierten Judikatur zum Datenschutzrecht seien die nachfolgenden Entscheidungen herausgegriffen:

Mit Erkenntnis des BVwG vom 27. März 2023, Gz W214 2259197-1/14E, wurde eine Verletzung der Informationspflicht nach Art 13 DSGVO festgestellt, als ohne entsprechenden Hinweis von einem geparkten, unbesetzten Kraftfahrzeug beim Vorbeigehen eines Passanten über eine verbaute Überwachungskamera eine Reaktion in Form eines kurzen Aufblitzens der Diebstahlsicherung ausgelöst wurde. Durch dieses Aufblinken aufmerksam geworden, hatte der Passant Nachforschungen angestellt. Dass Bildaufnahmen gespeichert wurden, hat sich nicht feststellen lassen, doch hat das bloß automatisierte Erfassen der sich nähernden Person durch die im Fahrzeug verbauten Kameras bereits eine Datenverarbeitung dargestellt.

Eine Kreditauskunftei darf Daten über ein Insolvenzverfahren nicht länger speichern, als, nach Erfüllung des rechtskräftig bestätigten Zahlungsplans, Einsicht in die Insolvenzdatei zu gewähren ist (VwGH 1.2.2024, Ro 2020/04/0031-9, unter Bezugnahme auf das Schufa-Holding-Urteil des EuGH vom 7.12.2023, C-26/22 und C-64/22).

Referenten beim IT-Rechtstag 2024: Roman Heidinger, Michael Pachinger, Julia Fuith, Rainer Knyrim, Stephan Winklbauer und Andreas Wiebe

Eine automatisierte Datenverarbeitung – wie Profiling – stellt dann eine „automatisierte Entscheidung im Einzelfall" im Sinne des Art 22 Abs 1 DSGVO dar, wenn das Ergebnis dieser automatisierten Verarbeitung für eine bestimmte – weitere – Entscheidung maßgeblich ist. Nämlich dann, wenn das Handeln des Dritten von dem betreffenden Profiling „maßgeblich geleitet" wird, und so den Betroffenen erheblich beeinträchtigt (VwGH 2.4. 2024, Ro 2021/04/0008-5 bis 0009-4 im Fall einer Bonitätsprüfung, unter Bezugnahme auf das Schufa-Urteil). Art 15 Abs 1 lit h DSGVO verlangt in einem solchen Fall aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

Die Verhängung einer Geldbuße nach Art 83 DSGVO gegen eine juristische Person setzt nicht die Benennung einer natürlichen Person voraus, der der Verstoß gegen die DSGVO zugerechnet werden kann (VwGH 1. 2. 2024, Ra 2020/04/187-20, unter Bezugnahme auf die Vorabentscheidung des EuGH vom 5. Dezember 2023, C-807/21, Deutsches Wohnen SE).

Schadenersatz. Nach Art 82 Abs 1 DSGVO hat jede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter.

Rechtsanwalt Rainer Knyrim beleuchtete in seinem Referat, welche Auslegung diese Bestimmung mittlerweile durch den EuGH erhalten hat. Im Urteil vom 4. Mai 2023, C-300/21 („Österreichische Post II") stellte der EuGH klar, dass Verstöße gegen Bestimmungen der DSGVO alleine nicht für den Anspruch auf Schadenersatz ausreichen. Erforderlich ist ein kausales Bewirken eines (immateriellen) Schadens, dessen Vorliegen die betroffene Person zu beweisen hat, infolge Verstoßes gegen die Verordnung. Der Anspruch auf Schadenersatz setzt das Erreichen einer Schwelle der Erheblichkeit nicht voraus. Im vorliegenden Fall war die Klägerin durch eine durch die Österreichische Post erfolgte Erhebung und Weitergabe der Parteiaffinität massiv verärgert und hatte ein Gefühl der Bloßstellung erlitten.

Im Fall der bulgarischen Abgabenbehörde NAP, deren Daten durch einen Cyber-Angriff im Internet veröffentlicht wurden und Klage auf Ersatz des durch die Offenlegung angeblich eingetretenen immateriellen Schadens eingebracht wurde, urteilte der EuGH (C 340/21 vom 14. Dezember 2023), dass der Verantwortliche die Beweislast trägt, dass die von ihm getroffenen Sicherheitsmaßnahmen geeignet waren und er nachzuweisen hat, dass er in keinerlei Hinsicht für das Eintreten des Schadens verantwortlich ist. Der Kläger hat den Schaden, den Verstoß gegen die DSGVO und den Zusammenhang zwischen Schaden und Verstoß zu beweisen. Als immaterieller Schaden reicht bereits die Angst oder die Befürchtung aus, dass in Zukunft eine missbräuchliche Verwendung erfolgen könnte. Als Konsequenz aus diesem Urteil folgerte der Vortragende, dass Unternehmen geeignete Sicherheitsmaßnahmen zu setzen und deren Geeignetheit regelmäßig und in einem ständigen Prozess zu evaluieren hätten. Eine Dokumentation der Sicherheitsmaßnahmen sei essenziell.

FOTOS: KURT HICKISCH

Das „Freibeweisen“ des Verantwortlichen sei möglich, habe aber große Hürden zu überwinden.

Dem Urteil C-456/22 vom 14. Dezember 2023 („Gemeinde Ummendorf“) liegt zu Grunde, dass ein Urteil, einschließlich des Namens und der Adresse des Klägers, auf der Website der Gemeinde veröffentlicht wurde. Das Urteil war vier Tage lang abrufbar. Als immaterieller Schaden wurde im Verfahren vor dem EuGH der Verlust der Hoheit über die personenbezogenen Daten geltend gemacht.

Was die Beweislast betrifft, wurde die bisherige Judikatur (Fall „Österreichische Post“) aufrechterhalten und ein Anspruch auf Schadenersatz auch bei minimaler Beeinträchtigung der betroffenen Person anerkannt. Die Beweisführung sei, so Rechtsanwalt Knyrim, für die betroffene Person allerdings nicht trivial.

Das Urteil des EuGH C-667/21 vom 25 Jänner 2024 („Krankenkasse Niederrhein“) betrifft ein Gutachten, das vom Dienstgeber, der Krankenkasse Nordrhein, hinsichtlich eines seit langer Zeit ununterbrochen arbeitsunfähig erkrankten Dienstnehmers erstellt wurde und in dem die Diagnose der Krankheit enthalten war. Der Beschwerdeführer begehrte die Zahlung von Schadenersatz.

Der EuGH stellte fest, dass sich die Schwere des Verstoßes gegen die DSGVO nicht auf die Höhe des (immateriellen) Schadenersatzes auswirkt, sondern dieser einen vollständigen und wirksamen Ausgleich für den konkret erlittenen Schaden bewirken soll. Weiters bestehe keine Haftung des Verantwortlichen, wenn dieser nachweist, dass ihm die gegen die DSGVO verstoßende Handlung nicht zurechenbar ist.

Im Fall des Urteils C-687/21 vom 25. Jänner 2024 („MediaMarkt Saturn“) waren beim Kauf eines Elektrohaushaltsgerätes Kauf- und Kreditvertrag, die die personenbezogenen Daten des Käufers enthielten, zusammen mit einem anderen Gerät irrtümlich einem anderen Käufer ausgehändigt worden. Der Irrtum wurde rasch bemerkt. Innerhalb einer halben Stunde wurden Gerät und Dokumente, ohne dass der Dritte von deren Inhalt Kenntnis genommen hätte, zurückgegeben. Es wurde der Ersatz des immateriellen Schadens auf Grund des Risikos des Verlustes der Kontrolle über die personenbezogenen Daten begehrt. Diese Befürchtung könne, so der EuGH, zwar einen immateriellen Schaden darstellen, doch führe das rein hypothetische Risiko der missbräuchlichen Verwendung nicht zu einem Schadenersatzanspruch. Die Beweislast eines eingetretenen Schadens treffe den Kläger.

Entscheidung des Bundesverwaltungsgerichts: Das bloße automatisierte Erfassen einer sich nähernden Person durch die im Fahrzeug verbauten Kameras stellt bereits eine Datenverarbeitung dar

Knyrim gab in der Folge einen Überblick über Fälle, in denen in Österreich immaterieller Schadenersatz zugesprochen wurde, samt der Höhe des jeweiligen Betrages.

750 Euro wurden zugesprochen für einen unrichtigen Vermerk in einer Bonitätsdatenbank (OGH 17.12.2009, 6 Ob 247/08d), 8.000 Euro für die Veröffentlichung der Aufzeichnung sexueller Aktivitäten im Internet (OLG Wien 25.8.2015, 11 R 119/15y). Für monatelanges Stalking wurden 5.000 Euro zugesprochen (OGH 15.12.2015, 8 Ob 129/15a) und für öffentliche Bloßstellung (kreditrelevante Daten wurden rechtswidrig nicht aus der Bonitätsdatenbank gelöscht) 1.000 Euro (LG Feldkirch 7.8.2019, 57 Cg 30/19b).

Für unerlaubte GPS-Überwachung durch ein GPS-Ortungssystem am Dienstfahrzeug wurde ein Ersatz des immateriellen Schadens in Höhe von 2.400 Euro zugesprochen (OGH 22.1.2020, 9 ObA 120/19s), für Verletzung des Auskunftsrechts und des dadurch ausgelösten „massiven Genervtseins“ 500 Euro (OGH 23.6.2021, 6 Ob 56/21k).

Der immaterielle Schaden durch die Verbreitung unwahrer Tatsachenbehauptungen (es wurden Vorwürfe wegen sexueller Belästigung erfunden) wurde mit 10.000 Euro bewertet (OLG Wien 27.11.2023, 33 R 109/23a) und der durch die Verwendung des Standbildes eines Politikers für Facebook-Postings einer politischen Partei, verbunden mit dessen massiver Genervtheit, mit 500 Euro (OGH 20.12.2023, 6 Ob 206/23x). In Deutschland, so Knyrim, seien die Fälle derartiger Schadenersatzansprüche in den vergangenen Jahren stark angestiegen, auf monatlich zwischen 220 und 300 Fälle.

Erörtert wurde auch die neue Entwicklung der Judikatur, dass Datenschutzbestimmungen vom OGH einer konsumentenschutzrechtlichen Klauselkontrolle im Hinblick auf deren Transparenz unterworfen und dabei geradezu „durch den Fleischwolf gedreht“ werden. Etwa im Zusammenhang mit einer Aktualisierung von Nutzungsbedingungen (hierzu ein Urteil des OGH vom 21.2.2023, 2 Ob 11/23s) und der Informationen über das Nutzungsrecht (OGH 17.5.2023, 6 Ob 222/23y).

Bemerkenswert ist, dass bei der Beurteilung derartiger Klauseln als Basis von der kundenfeindlichsten Auslegung auszugehen ist. Verarbeitungsvorgänge sollten daher so konkret wie möglich beschrieben werden. Knyrim rät dazu, keine Kästchen zum Ankreuzen der Datenschutzinformationen zu verwenden und im Text keine zustimmungsähnliche Wirkung zu suggerieren.

Kurt Hickisch

FOTO: WERNER SABITZER