

DATENSCHUTZ & E-GOVERNMENT JUDIKATUR

DATENSCHUTZRECHT

EuGH: Beschränkung von in der Fluggastdaten-Richtlinie (PNR-RL) vorgesehenen Befugnissen auf das absolut Notwendige

» jusIT 2022/78

§ AEUV: Art 67 Abs 2
EUV: Art 3 Abs 2
GRC: Art 7, 8, 11, 45, 52 Abs 1
EMRK: Art 8
VO (EU) 2016/679: Art 2 Abs 2 lit d, Art 23
RL (EU) 2016/681: Art 1 Abs 2, Art 2, 3 Z 1, 4, 8 und 9,
Art 4 Abs 1–3, Art 6, 12 Abs 3 lit b, Anh I und II
RL 2004/82/EG: Art 2 lit a, b und d, Art 3 Abs 1 und 2,
Art 6 Abs 2

EuGH 21. 6. 2022, C-817/19 (Ligue des droits humains)

1. Gem Art 2 Abs 2 lit d und Art 23 DSGVO ist die Verarbeitung von Fluggast- und sonstigen Beförderungsdaten durch nationale Behörden und die nationalen PNR-Zentralstellen zu Zwecken der Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität iSv Art 1 Abs 2 iVm Art 6 Abs 2 lit a, b und c RL (EU) 2016/681 (PNR-RL) vom Anwendungsbereich der DSGVO ausgenommen.
2. Art 7, 8 und 21 iVm Art 52 Abs 1 GRC erfordern eine Beschränkung der in der PNR-RL über die Verwendung von Fluggastdatensätzen vorgesehenen Befugnisse auf das absolut Notwendige. Besteht keine reale und aktuelle oder vorhersehbare terroristische Bedrohung eines Mitgliedstaats, steht das Unionsrecht nationalen Rechtsvorschriften entgegen, die eine Übermittlung und Verarbeitung von PNR-Daten bei EU-Flügen sowie bei Beförderungen mit anderen Mitteln innerhalb der Union vorsehen.
3. Art 6 PNR-RL steht in grundrechtskonformer Auslegung nationalen Rechtsvorschriften entgegen, nach denen die Verarbeitung der Fluggastdaten, die im Einklang mit dieser Richtlinie erhoben wurden, zu anderen als den in Art 1 Abs 2 PNR-RL ausdrücklich genannten Zwecken der Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität zulässig ist.
4. Art 12 Abs 3 lit b PNR-RL steht nationalen Rechtsvorschriften entgegen, wonach die nationale PNR-Zentralstelle zugleich als Behörde über die Genehmigung der

Offenlegung der PNR-Daten nach Ablauf einer Sechsmonatsfrist ab Übermittlung an die PNR-Zentralstelle entscheidet.

5. Art 12 Abs 1 PNR-RL steht iVm Art 7, 8 und 52 Abs 1 GRC nationalen Rechtsvorschriften entgegen, die eine allgemeine, unterschiedslos für alle Fluggäste geltende Speicherfrist der Fluggastdaten von fünf Jahren vorsehen.
6. Die PNR-RL gilt nur für Drittstaatsflüge, nicht für Linien- oder Gelegenheitsflüge einer Fluggesellschaft, die vom Hoheitsgebiet eines Mitgliedstaates aus starten und das Hoheitsgebiet eines oder mehrerer anderer Mitgliedstaaten zum Ziel haben, ohne Zwischenlandungen in einem Drittstaat (EU-Binnenflüge).
7. In Situationen, in denen der betreffende Mitgliedstaat nicht mit einer realen und aktuellen oder vorhersehbaren terroristischen Bedrohung konfrontiert ist, muss die Anwendung des durch die PNR-RL geschaffenen Systems auf die Übermittlung und Verarbeitung der PNR-Daten von Flügen und/oder Beförderungen beschränkt werden, die insb bestimmte Verbindungen, bestimmte Reisemuster oder bestimmte Flughäfen, Bahnhöfe oder Seehäfen betreffen, für die es Anhaltspunkte gibt, die seine Anwendung rechtfertigen können.
8. Art 2 PNR-RL iVm Art 3 Abs 2 EUV, Art 67 Abs 2 AEUV und Art 45 GRC steht nationalen Rechtsvorschriften entgegen, die zum Zweck der Verbesserung der Grenzkontrollen und der Bekämpfung illegaler Einwanderung ein solches System der Übermittlung und Verarbeitung der genannten Daten vorsehen.

Anmerkung des Bearbeiters:

In dem aus Belgien stammenden Ausgangsfall erhob die Ligue des droits humains (Liga für Menschenrechte, kurz: LDH), ein gemeinnütziger Verein, im Juli 2017 beim belgischen Verfassungsgerichtshof eine Nichtigkeitsklage gegen das zugehörige belgische Gesetz aus Dezember 2016, das ua die PNR-RL der EU über die Erhebung von Fluggastdatensätzen (PNR-Daten – *Passenger Name Record Data*) umgesetzt hatte. Das belgische Gesetz und die PNR-RL sehen zur Bekämpfung von Terrorismus und schwerer Kriminalität die systematische Verarbeitung einer großen Zahl von PNR-Daten (Buchungsdaten der Fluggäste gemäß den Anhängen der PNR-RL) von Flügen zwischen der EU und Drittstaaten (Drittstaatsflüge) bei der Einreise in die bzw der Ausreise aus der EU vor. Darüber hinaus können die Mitgliedstaaten diese Vorschriften nach Art 2 PNR-RL auch auf Flüge innerhalb der Union (EU-Binnenflüge) anwenden. Nach belgischem Recht waren Flug-, Bahn-, Bus-, Fähr- und Reiseunternehmen dazu verpflichtet, die Daten ihrer Passagiere, die über die Landesgrenzen



hinaus unterwegs waren, an eine Zentralstelle weiterzugeben, in der ua Polizei und Geheimdienste vertreten sind. Zu diesen PNR-Daten zählten die Anschrift und Kontaktangaben der Fluggäste, die Zahl und Namen von Mitreisenden sowie alle Arten von Zahlungsinformationen (vgl Anh I PNR-RL). Das belgische Verfassungsgericht legte die Rechtssache dem EuGH vor, um vorab durch zehn Fragen klären zu lassen, ob die beiden unionsrechtlichen Rahmenregelungen überhaupt grundrechtskonform (auszulegen) wären.

Die Große Kammer führte aus, dass einzelne PNR-Daten zwar keine näheren Informationen über das Privatleben der Fluggäste enthielten, die Informationen bei einer Verknüpfung jedoch den ganzen Reiseablauf, die finanzielle Situation und Beziehungen zwischen zwei oder mehreren Menschen offenbaren könnten. Die PNR-RL stellte also einen schwerwiegenden Eingriff in das Grundrecht auf Schutz personenbezogener Daten nach Art 8 GRC dar (vgl bereits EuGH 26. 7. 2017, Gutachten 1/15 [PNR-Daten Kanada], ECLI:EU:C:2017:592 = jusIT 2018/27, 77 [Jahnel]). Dieser schwerwiegende Eingriff wäre nur dann als verhältnismäßig zu beurteilen, wenn er zur Bekämpfung schwerer Kriminalität erforderlich wäre. Die Anwendung des durch die PNR-RL geschaffenen Systems müsse daher auf schwere Straftaten mit einem objektiven Zusammenhang mit der Beförderung von Fluggästen beschränkt sein. Mitgliedstaaten, die beabsichtigten, die Befugnisse auf EU-Flüge auszuweiten, müssten zudem prüfen, ob dies zur Gewährleistung des Schutzes des Lebens und der Sicherheit von Personen absolut notwendig ist. Dies wäre nur dann der Fall, wenn der Mitgliedstaat mit einer realen und aktuellen terroristischen Bedrohung konfrontiert wird.

Im zu berichtenden, lesenswerten (299 Randzahlen umfassenden) Urteil standen die PNR-RL (Richtlinie [EU] 2016/681 des Europäischen Parlaments und des Rates vom 27. April 2016 über die Verwendung von Fluggastdatensätzen [PNR-Daten] zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität, ABL L 2016/119, 132) und die API-RL (Richtlinie 2004/82/EG des Rates vom 29. April 2004 über die Verpflichtung von Beförderungsunternehmen, Angaben über die beförderten Personen zu übermitteln, ABL L 2004/261, 24) auf dem unionsinternen, rechtlichen Prüfstand. Die Fluggastdaten-Rahmenregelungen haben den „*datenschutzrechtlichen Stresstest*“ eher nicht bestanden. Der EuGH hält zwar fest, dass die PNR-RL in einer mit dem Unionsrecht vereinbaren Weise auszulegen ist und nicht *per se* mit dem (primären) Unionsrecht unvereinbar ist. Gleichzeitig betont aber die Große Kammer, dass die Regelungen der PNR-RL einen schwerwiegenden Eingriff in das Recht auf Achtung des Privatlebens und den Schutz personenbezogener Daten darstellen, und zwar insb bei Anwendung auf EU-Flüge, der Verarbeitung nach Art 6 PNR-RL und für die Speicherfrist und Depersonalisierung nach Art 12 PNR-RL (vgl Rz 115–118 sowie Rz 244 f und 247 des Urteils). Daher sind die darin den Mitgliedstaaten eingeräumten Befugnisse, personenbezogene Daten zu verarbeiten, restriktiv auszulegen (vgl Rz 169–175, 218 ff und Rz 225–228 des Urteils).

Bemerkenswert sind die Ausführungen zur Abgrenzung der Anwendungsbereiche von DSGVO einerseits sowie PNR-RL und API-RL samt deren nationalen Umsetzungsregelungen andererseits. Nach Art 2 Abs 2 lit d DSGVO hat die Verarbeitung der Fluggastdaten durch private Wirtschaftsteilnehmer, dh va die Fluggesellschaften, ebenso wie jene durch die Behörden nach der API-RL-Umsetzung dem Regime der DSGVO zu folgen. Die Verarbeitungstätigkeiten der PNR-Zentralstelle und der (zuständigen) nationalen Behörden zur Bekämpfung terroristischer Straftaten und schwerer Kriminalität iSv Art 1 Abs 2 PNR-RL fällt hingegen nicht in den Anwendungsbereich der DSGVO (vgl *Thiele/Wagner*, DSG² § 36 Rz 11 ff).

Durch ein kontinuierliches, nicht zielgerichtetes und systematisches Überwachungsregime kommt es nach dem Urteil des EuGH zu schweren Eingriffen in die Rechte auf Datenschutz und Privatsphäre (so bereits EuGH 5. 4. 2022, C-140/20 [Commissioner of An Garda Síochána], jusIT 2022/62, 155 [Thiele]). Dies bedeutet für die in Art 6 Abs 3 lit b PNR-RL vorgesehene Vorabüberprüfung der Fluggastdaten (im Sinne der Anhänge zur PNR-RL) und deren Weitergabe an Polizei und Justiz, dass dafür im Voraus exakte Kriterien festgelegt sein müssen. Die konkrete Erörterung dieser Anforderungen an diese Verarbeitung der PNR-Daten (vgl Rz 194–201 des Urteils) erscheinen durchaus verallgemeinerungsfähig und für den Einsatz von Künstlicher Intelligenz zu beachten, worauf bereits GA Pitruzzella, SA 27. 1. 2022, C-817/19 [Ligue des droits humains/Kommission] Rz 228, ECLI:EU:C:2022:65) hingewiesen hat. Die Grenzen, die der EuGH für die Verarbeitung durch die Zentralstelle und die Behörden definiert hat, lassen sich folgendermaßen zusammenfassen:

- *Festlegung der Kriterien im Vorhinein*, dh, dieses Erfordernis der Prädetermination steht der Heranziehung von Technologien der Künstlichen Intelligenz im Rahmen selbstlernender Systeme („machine learning“) entgegen, die – ohne menschliche Einwirkung und Kontrolle – den Bewertungsprozess und insb die Bewertungskriterien, auf denen das Ergebnis der Anwendung dieses Prozesses beruht, sowie die Gewichtung der Kriterien ändern können (Rz 194 des Urteils);
- Erfordernis eines *wirksamen Rechtsbehelfs* iSv Art 47 GRC, insb zur Prüfung allfällig diskriminierender Ergebnisse (Rz 195 des Urteils);
- *Ausschluss* besonders kategorisierter, dh *sensibler* (ErwGr 51 DSGVO) Daten als Grundlage für die Verarbeitungskriterien (Rz 196 des Urteils);
- *Ausschluss* von unmittelbarer oder mittelbarer *Diskriminierung*, dh, die Anwendung der im Voraus bestimmten Verarbeitungskriterien, auch wenn sie neutral formuliert sind, darf nicht geeignet sein, Personen mit sensiblen Merkmalen besonders zu benachteiligen (Rz 197 des Urteils);
- *Bestimmtheit, Zielgerichtetheit und Verhältnismäßigkeit*, dh, die bei der Vorabüberprüfung herangezogenen Kriterien sind so festzulegen, dass sie speziell auf Personen abzielen, bei denen der begründete Verdacht einer Beteiligung an terroristischen Straftaten oder schwerer Kriminalität besteht (Rz 198 des Urteils);

- *Zuverlässigkeit*, dh, die im Voraus festgelegten Kriterien sind so zu bestimmen, dass sowohl „belastende“ als auch „entlastende“ Gesichtspunkte berücksichtigt werden (Rz 200 des Urteils);
- Regelmäßige *Überprüfung* der festgelegten Kriterien unter Berücksichtigung der gemachten Erfahrungen, insb um die Zahl „falsch positiver“ Ergebnisse so weit wie möglich zu verringern (Rz 201 des Urteils).

Schließlich betont die Große Kammer, dass die PNR-RL und die API-RL nicht dazu genutzt werden dürfen, die Grenzkontrollen zu verbessern und den Kampf gegen illegale Einwanderung zu stärken (Rz 266–269 des Urteils).

Ausblick: Das vorliegende Urteil dürfte weitreichende Folgen für die weitgehend erfolgte Umsetzung der PNR-RL durch die anderen Mitgliedstaaten haben. In Österreich setzt das PNR-Gesetz (PNR-G, BGBl I 64/2018) die Richtlinie um. § 2 Abs 5 PNR-G enthält eine Verordnungsermächtigung des BMI zur Erweiterung auf EU-Binnenflüge. Die PNR-Verordnung (PNR-VO, BGBl II 208/2018 idF II 28/2020) ist bereits in Geltung.

Gleichmaßen hat die deutsche Regelung des Gesetzes über die Verarbeitung von Fluggastdaten (FlugDaG, dBGBI I 2017, 1484) die PNR-RL auf alle innereuropäischen Flüge ausgeweitet. Ein deutsches Verwaltungsgericht (VG Wiesbaden 15. 5. 2020, 6 K 806/19.WI [Fluggastdatengesetz I], JurPC Web-Dok 83/2020; anhängig beim EuGH zu C-222/20 [OC/BRD]; VG Wiesbaden 13. 5. 2020, 6 K 805/19.WI [Fluggastdatengesetz II], JurPC Web-Dok 82/2020; anhängig beim EuGH zu C-215/20 [JV/BRD]), und ein Amtsgericht (AG Köln 20. 1. 2020, 142 C 328/19 [Fluggastdatengesetz III], JurPC Web-Dok 44/2020, anhängig beim EuGH zu C-148/20, C-149/20 und C-150/20 [Deutsche Lufthansa]) haben dem EuGH insgesamt fünf Vorabentscheidungsersuchen zur Übermittlung von Fluggastdaten im Zusammenhang mit der PNR-RL vorgelegt. In diesen Verfahren soll das Europäische Höchstgericht ua klären, ob die jeweiligen Regelungen einschließlich des FlugDaG mit dem Unionsrecht vereinbar sind. Die weitere Rechtsentwicklung bleibt dynamisch und spannend.

Zusammenfassend hat der EuGH entschieden, dass die Erlaubnistatbestände der an sich grundrechtskonformen PNR-RL eng auszulegen sind und sich die Erhebung und Verarbeitung von Fluggastdaten auf das absolut Notwendige, dh auf eine unmittelbare Bekämpfung des Terrorismus, beschränken muss.

Bearbeiter: Clemens Thiele

OGH: Anforderungen an die Entscheidungsanonymisierung im Erwachsenenschutzrecht

» jusIT 2022/79

§ VO (EU) 2016/679: Art 5, 17, 23
OGHG: § 15 Abs 2
GOG: §§ 83, 84, 85
ABGB: §§ 268 ff
AußStrG: § 6 Abs 1, § 140

OGH 27. 7. 2022, 6 Ob 296/03b (Anonymisierungen im Erwachsenenschutzrecht)

1. Höchstgerichtliche Entscheidungen in (ehemals) Sachwalter- und nunmehr Erwachsenenschutzverfahren sind grundsätzlich im RIS zu veröffentlichen. Die Nicht-öffentlichkeit mündlicher Verhandlungen in solchen Verfahren (§ 140 AußStrG) bedeutet nicht, dass darin ergangene Entscheidungen nach § 15 Abs 2 OGHG zwingend von der Veröffentlichung ausgenommen werden müssen.
2. Solange durch die Anonymisierung einer Gerichtsentscheidung ein ausreichender Persönlichkeitsschutz von Parteien, Zeugen und anderen Verfahrensbeteiligten gewährleistet ist, geht das Informationsinteresse der Öffentlichkeit an der Kenntnis vom praktizierten Recht vor.

Anmerkung des Bearbeiters:

Die im Rechtsinformationssystem des Bundes (RIS) bereits 2004 veröffentlichte Entscheidung (vom 29. 1. 2004, 6 Ob 296/03b) in einer (damaligen) Sachwalterschaftssache wies eine Anonymisierung des Nachnamens des Betroffenen (E***) und dessen Geburtsdatums sowie der Adresse (***), nicht jedoch eine solche des Vornamens des Betroffenen („Peter“) und des damaligen einstweiligen Sachwalters (ein Rechtsanwalt) auf. Der Veröffentlichung des Beschlusses war auch zu entnehmen, dass für den Betroffenen erstmals am 2. 2. 2001 eine Rechtsanwältin (ohne jede Namensnennung) als einstweilige Sachwalterin bestellt worden war und ihn im Revisionsrekursverfahren „teilweise“ ein bevollmächtigter Verfahrensvertreter (Ing. Gebhard F***) vertrat. Mehr als 18 Jahre später wandte sich der Betroffene als „Einschreiter“ an den OGH mit dem „Ersuchen“ um weitere Anonymisierung, konkret seinen Vornamen ebenfalls unkenntlich zu machen. Ganz generell wollte der Einschreiter auch wissen, ob Gerichtsentscheidungen aus einem Sachwalterverfahren überhaupt öffentlich dokumentiert werden dürften, handelte es sich doch um nicht-öffentliche Gerichtsverfahren.

Der OGH kam dem Ersuchen des Einschreiters – nach Umdeutung in eine dadurch ausgelöste amtswegige Überprüfung (vgl OGH 2. 2. 2021, 6 Ob 177/20b [Nachträgliche Anonymisierung II]),