



DATENSCHUTZ & E-GOVERNMENT JUDIKATUR

DATENSCHUTZRECHT

EuGH: Keine Vorratsdatennutzung für verwaltungsstrafbehördliche Untersuchungen

» jusIT 2023/115

§ GRC: Art 7, 8, 11, 52
DSGVO: Art 95

RL 2002/58/EG: Art 1, 15 Abs 1

EuGH 7. 9. 2023, C-162/22 (Lietuvos Respublikos generalinė prokuratūra)

1. Verwaltungsstrafbehördliche Disziplinar- oder Dienstvergehen im Zusammenhang mit Korruption im öffentlichen Sektor können zwar eine wichtige Rolle bei der Kriminalitätsbekämpfung spielen. Dennoch dient eine Rechtsvorschrift, die solche Untersuchungen vorsieht, nicht tatsächlich und strikt den Zielen der Verfolgung und Ahndung von schweren Straftaten iSv Art 15 Abs 1 Satz 1 RL 2002/58/EG (ePrivacy-RL), welche ausschließlich die Strafbarkeit von besonders schweren Kriminaldelikten erfassen.
2. (Personenbezogene) Daten über elektronische Kommunikationsvorgänge, die von Betreibern elektronischer Kommunikationsdienste im Rahmen der entsprechenden Rechtsvorschriften nach Art 15 Abs 1 ePrivacy-RL auf Vorrat gespeichert und den zuständigen Behörden zur Bekämpfung schwerer Kriminalität zur Verfügung gestellt wurden, dürfen daher – im Lichte von Art 7, 8, 11 und 52 GRC – keineswegs für Untersuchungen wegen Dienstvergehen im Zusammenhang mit Korruption (hier: gegen einen Staatsanwalt) genutzt werden.

Anmerkung des Bearbeiters:

Dem aus Litauen stammenden Ausgangsfall lagen Ermittlungen der zuständigen Disziplinarbehörden gegen einen dortigen Staatsanwalt zugrunde, der einem Verdächtigen und dessen Anwalt rechtswidrig Informationen weitergegeben haben soll und der deswegen seinen Dienst quittieren musste. Das Dienstvergehen war (zunächst) mittels Gesprächsdaten nachgewiesen worden, die von Betreibern elektronischer Kommunikationsdienste in Litauen gemäß den dortigen Vorschriften auf Vorrat gespeichert worden waren.

Der Staatsanwalt wurde von der litauischen Generalstaatsanwaltschaft seines Amtes enthoben und bekämpfte diese Dis-

ziplinarstrafe vor Gericht. Er machte ua geltend, die Nutzung der „Vorratsdaten“ in Verfahren wegen Dienstvergehen stellte (generell) einen ungerechtfertigten Eingriff in die im Unionsrecht verankerten Grundrechte, insb Art 7 GRC, dar. Das Oberste Verwaltungsgericht von Litauen als Rechtsmittelinstanz unterbrach sein Verfahren und wollte vom EuGH im Wesentlichen wissen, ob die Nutzung personenbezogener Daten elektronischer Kommunikationsvorgänge, die von Betreibern elektronischer Kommunikationsdienste auf Vorrat gespeichert und in der Folge den zuständigen Behörden zur Bekämpfung schwerer Kriminalität zur Verfügung gestellt wurden, im Rahmen einer Untersuchung wegen Dienstvergehen im Zusammenhang mit Korruption mit Art 15 Abs 1 ePrivacy-RL vereinbar ist.

Die Erste Kammer bestätigte zunächst erneut, dass mit der Speicherung von Verkehrs- und Standortdaten schwere Eingriffe in die Grundrechte auf Achtung des Privat- und Familienlebens und auf Schutz der personenbezogenen Daten verbunden sind. Daher wäre eine solche Vorratsdatenspeicherung nur gerechtfertigt, um schwere Kriminalität zu bekämpfen oder schwere Bedrohungen der öffentlichen Sicherheit abzuwenden. Die nach den Vorgaben von Art 15 ePrivacy-RL gewonnenen Daten elektronischer Kommunikation dürfen ausschließlich zu Zwecken der strafgerichtlichen Verfolgung besonders qualifizierter Delikte verwertet werden. Dazu zählt die Nutzung bei Ermittlungen wegen eines Dienstvergehens keineswegs.

Der EuGH hält es in stRsp (vgl zuletzt Urteil vom 26. 1. 2023, C-205/21 [Ministerstvo na vatreshnite raboti], jusIT 2023/48, 119 [Thiele] = ÖJZ 2023/49, 318 [Fuchs] mwN) für unzulässig, wenn die Vorratsdaten, die eine Telekommunikationsbetreiber:in den zuständigen Behörden zur Bekämpfung von schwerer Kriminalität zur Verfügung gestellt hat, anschließend an andere Behörden weitergegeben werden, um Dienstvergehen im Zusammenhang mit Korruption aufzudecken.

Das vorliegende Urteil beantwortet die durchaus praxisnahe Frage, ob die aus einem Strafverfahren gewonnenen Beweismittel, vor allem durch eine genehmigte Telefonüberwachung, in einem parallel geführten (aber idR unterbrochenen) Disziplinarverfahren verwendet werden dürfen. Der EuGH verweist auf die bisherige Rsp zu Art 15 ePrivacy-RL, die bereits an dieser Stelle ausführlich referiert und erörtert wurde (vgl Thiele, EuGH: Vorratsdatenspeicherung reloaded, jusIT 2020/84, 224 mwH). Als weiterer, ergänzungsbedürftiger Aspekt erscheint, dass im Einklang mit dem Grundsatz der Verhältnismäßigkeit nur die Bekämpfung schwerer Kriminalität und die Verhütung schwerer Bedrohungen der öffentlichen Sicherheit geeignet sind, die mit der Speicherung von Verkehrs- und Standortdaten verbundenen schweren Eingriffe in die Grundrechte zu rechtfertigen. Gestützt auf seine Rsp zu den dem Gemeinwohl dienenden Zielen, die eine Beschränkung der Rechte rechtfertigen können, fügt das EU-Höchstgericht hinzu, dass die Bekämpfung schwerer Krimi-

nalität und die Verhütung schwerer Bedrohungen der öffentlichen Sicherheit zwar von geringerer Bedeutung als der Schutz der nationalen Sicherheit sind, dass ihre Bedeutung aber die der Bekämpfung von Straftaten im Allgemeinen übersteigt (Rz 35 f und 38 des Urteils).

Ausblick: Verkehrs- und Standortdaten, die von Betreibern elektronischer Kommunikationsdienste in Anwendung einer nach Art 15 Abs 1 ePrivacy-RL erlassenen Rechtsvorschrift auf Vorrat gespeichert und den zuständigen Behörden zu diesem Zweck zur Verfügung gestellt wurden, dürfen anschließend nicht an andere Behörden übermittelt und (dort) zur Bekämpfung von Verwaltungsstraftaten oder Dienstvergehen eingesetzt werden. Insofern besteht ein Verarbeitungsverbot, das etwa über ein bloßes Weiterverarbeitungsverbot iSv § 45 DSGVO (dazu *Thiele/Wagner*, DSGVO² § 45 Rz 33 ff) hinausgeht und nach §§ 38, 39 DSGVO von den Sicherheitsbehörden jedenfalls zu beachten ist.

Zusammenfassend hat der EuGH entschieden, dass elektronische Kommunikationsdaten, die zur Bekämpfung schwerer Kriminalität – soweit zulässig, auch auf Vorrat – gesammelt wurden, nicht für Untersuchungen der Disziplinar- und Verwaltungsbehörden wegen Korruptionsvorwürfen im öffentlichen Sektor genutzt werden dürfen.

Bearbeiter: Clemens Thiele

EuGH: Anforderungen des Art 88 DSGVO an nationale Bestimmungen zum Beschäftigtendatenschutz

» jusIT 2023/116

§ VO (EU) 2016/679: Art 88 Abs 1 und Abs 2, Art 6 Abs 2 und Abs 3

EuGH 30. 3. 2023, C-34/21 (Hauptpersonalrat der Lehrerinnen und Lehrer)

1. Art 88 DSGVO ist dahin auszulegen, dass eine nationale Rechtsvorschrift keine „spezifischere Vorschrift“ iSv Abs 1 dieses Artikels sein kann, wenn sie nicht die Vorgaben von Abs 2 dieses Artikels erfüllt.
2. Art 88 Abs 1 und 2 DSGVO ist dahin auszulegen, dass nationale Rechtsvorschriften zur Gewährleistung des Schutzes der Rechte und Freiheiten von Beschäftigten hinsichtlich der Verarbeitung ihrer personenbezogenen Daten im Beschäftigungskontext unangewendet bleiben müssen, wenn sie nicht die in Art 88 Abs 1 und 2 vorgegebenen Voraussetzungen und Grenzen beachten, es sei denn, sie stellen eine Rechtsgrundlage iSv Art 6 Abs 3 DSGVO dar, die den Anforderungen dieser Verordnung genügt.

Anmerkung des Bearbeiters:

Siehe dazu den Besprechungsaufsatz von *Warter* in diesem Heft der jusIT 2023/113, 234 ff.

Bearbeiter: Johannes Warter

EuGH: Keine Beschränkung von Betroffenenrechten aus wirtschaftlichen Interessen

» jusIT 2023/117

§ VO (EU) 2016/679: Art 12, 15, 23

EuGH 26. 10. 2023, C-307/22 (FT – Kopie einer Krankenakte)

1. Das Recht der betroffenen Person auf eine unentgeltliche erste Kopie ihrer verarbeiteten personenbezogenen Daten besteht auch, wenn der betreffende Antrag mit einem anderen als den in Satz 1 des ErwGr 63 DSGVO genannten Zwecken begründet wird.
2. Eine nationale Regelung, die vor dem Inkrafttreten der DSGVO erlassen wurde, kann in den Anwendungsbereich des Art 23 DSGVO fallen.
3. Art 23 Abs 1 lit i DSGVO erlaubt keine nationale Regelung, die der betroffenen Person zum Schutz der wirtschaftlichen Interessen des Verantwortlichen die Kosten für eine erste Kopie ihrer personenbezogenen Daten auferlegt.
4. Im Rahmen eines Arzt-Patienten-Verhältnisses umfasst das Recht auf Erhalt einer Kopie der personenbezogenen Daten iSd Art 15 Abs 3 Satz 1 DSGVO eine originalgetreue und verständliche Reproduktion aller Daten. Sofern es für die Überprüfung der Richtigkeit und Vollständigkeit der Daten und die Verständlichkeit erforderlich ist, setzt dieses Recht eine vollständige Kopie der Dokumente voraus.

Anmerkung des Bearbeiters:

Siehe dazu den Besprechungsaufsatz von *Kröpfl* in diesem Heft der jusIT 2023/114, 239 ff.

Bearbeiter: Maximilian Kröpfl