

DATENSCHUTZ & E-GOVERNMENT JUDIKATUR

DATENSCHUTZRECHT

EuGH: Unterschiedslose Vorratsspeicherung von Verkehrs- und Standortdaten unionsrechtswidrig

» jusIT 2022/62

- § GRC: Art 7, 8, 11, 52 Abs 1
EMRK: Art 8
RL 2002/58/EG: Art 15 Abs 1
- # EuGH 5. 4. 2022, C-140/20 (Commissioner of An Garda Síochána)

- Art 15 Abs 1 ePrivacy-RL (RL 2002/58/EG) untersagt nationale Rechtsvorschriften, die präventiv zur Bekämpfung schwerer Kriminalität und zur Verhütung schwerer Bedrohungen der öffentlichen Sicherheit eine allgemeine und unterschiedslose Vorratsspeicherung der Verkehrs- und der Standortdaten vorsehen.
- Demgegenüber kann eine Unionsrechtskonformität nach Art 15 Abs 1 ePrivacy-RL iVm Art 7, 8, 11 und 52 Abs 1 GRC hergestellt werden, wenn die nationalen Rechtsvorschriften Datenspeicherungen determinieren, die zur Bekämpfung schwerer Kriminalität und zur Verhütung schwerer Bedrohungen der öffentlichen Sicherheit
 - auf der Grundlage objektiver und nicht-diskriminierender Kriterien anhand von Kategorien betroffener Personen oder mittels eines geografischen Kriteriums für einen auf das absolut Notwendige begrenzten, aber verlängerbaren Zeitraum eine gezielte Vorratsspeicherung von Verkehrs- und Standortdaten vorsehen;
 - für einen auf das absolut Notwendige begrenzten Zeitraum eine allgemeine und unterschiedslose Vorratsspeicherung der IP-Adressen, die der Quelle einer Verbindung zugewiesen sind, vorsehen;
 - eine allgemeine und unterschiedslose Vorratsspeicherung der die Identität der Nutzer elektronischer Kommunikationsmittel betreffenden Daten vorsehen;
 - vorsehen, dass den Betreibern elektronischer Kommunikationsdienste mittels einer Entscheidung der zuständigen Behörde, die einer wirksamen gerichtlichen Kontrolle unterliegt, aufgegeben werden kann, während eines festgelegten Zeitraums die ihnen zur Verfügung stehenden Verkehrs- und Standortdaten umgehend zu sichern.

Diese Rechtsvorschriften müssen durch klare und präzise Regeln sicherstellen, dass bei der Speicherung der

fraglichen Daten die für sie geltenden materiellen und prozeduralen Voraussetzungen eingehalten werden und dass die Betroffenen über wirksame Garantien zum Schutz vor Missbrauchsrisiken verfügen.

- Art 15 Abs 1 ePrivacy-RL steht nationalen Rechtsvorschriften entgegen, nach denen die zentralisierte Bearbeitung von Ersuchen um Zugang zu von den Betreibern elektronischer Kommunikationsdienste auf Vorrat gespeicherten Daten, die von der Polizei im Rahmen der Ermittlung und Verfolgung schwerer Straftaten gestellt werden, einem Polizeibeamten obliegt, der von einer innerhalb der Polizei eingerichteten Einheit, die bei der Wahrnehmung ihrer Aufgaben über einen gewissen Grad an Autonomie verfügt, unterstützt wird und dessen Entscheidungen später gerichtlich überprüft werden können.
- Die Zulässigkeit der durch eine unionsrechtswidrige Vorratsspeicherung erlangten Beweismittel unterliegt nach dem Grundsatz der Verfahrensautonomie der Beurteilung durch die jeweils berufenen Gerichte der Mitgliedstaaten. Diese haben aber jedenfalls die unionsrechtlichen Grundsätze der Äquivalenz und der Effektivität zu berücksichtigen.

Anmerkung des Bearbeiters:

In dem aus Irland stammenden Ausgangsfall verurteilte ein Strafgericht im März 2015 eine Person wegen Mordes zu einer lebenslangen Freiheitsstrafe. In der Berufungsinstanz (Court of Appeal) warf der Betroffene dem erstinstanzlichen Gericht ua vor, es hätte zu Unrecht Verkehrs- und Standortdaten im Zusammenhang mit Telefonanrufen als Beweismittel zugelassen. Um die Zulässigkeit der verwendeten Beweismittel wirksam bekämpfen zu können, leitete der Betroffene parallel dazu ein Zivilverfahren vor dem High Court mit dem Ziel ein, bestimmte Vorschriften des irischen Gesetzes von 2011 über die Speicherung und Nutzung dieser Daten (Data Retention Act of 2011) als unvereinbar mit dem Unionsrecht feststellen zu lassen. Mit Entscheidung vom 6. 12. 2018 gab der High Court der Zivilklage des Betroffenen statt. Die Republik Irland legte gegen diese Entscheidung Rechtsmittel beim Supreme Court ein. Dieser wandte sich daraufhin nach Art 267 AEUV an den EuGH und wollte von diesem zusammengefasst wissen, welche Anforderungen das Unionsrecht an die Vorratsdatenspeicherung zum Zweck der Bekämpfung schwerer Kriminalität stellt und welche notwendigen Garantien den Zugang zu den Daten, einschließlich deren Verwertung im Strafverfahren, regulieren müssten.

Die Große Kammer festigte mit dem Urteil ihre bisherige Entscheidungspraxis weiter (vgl. EuGH 6. 10. 2020, C-511/18, 512/18, 520/18 [La Quadrature du Net ua]; siehe auch EuGH



31. 10. 2017, C-623/17 [Privacy International]; dazu *Thiele*, EuGH: Vorratsdatenspeicherung reloaded, jusIT 2020/84, 224 mwN; zuletzt EuGH 2. 3. 2021, C-746/18 [Prokuratuur], jusIT 2021/29, 87 [Thiele]). Demzufolge steht die ePrivacy-RL (Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation [Datenschutzrichtlinie für elektronische Kommunikation], ABL L 2002/201, 37) nationalen Rechtsvorschriften entgegen, die zur Bekämpfung schwerer Straftaten präventiv eine allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs- und Standortdaten vorsehen und elektronische Kommunikationen betreffen (so bereits *Seiser*, Zur [neuerlichen] Speicherung von Daten auf Vorrat – alles auf Anfang?, ZIIR 2016, 18 [21 f] mwN).

Der EuGH betont in seiner Urteilsbegründung, dass eine anlasslose Vorratsdatenspeicherung überhaupt unzulässig sei und anlassbezogene Datenspeicherungen bei schweren Straftaten nur in sehr engen Grenzen zulässig sein können. Der EuGH liefert einige Klarstellungen, wann die Vorratsdatenspeicherung erlaubt sein könnte (Rz 101 ff des Urteils). So müsste ein mittelbarer Zusammenhang zwischen der Speicherung der Daten und dem damit verfolgten Ziel bestehen. Um nicht von vornherein der ePrivacy-RL zuwiderzulaufen, müsste die Speicherung daher gezielt, also etwa anhand von Kategorien betroffener Personen oder eines geografischen Kriteriums, erfolgen. Für das geografische Kriterium könnte zB die durchschnittliche Kriminalitätsrate in einem Gebiet herangezogen oder auf Orte und Infrastrukturen („hot spots“) wie zB Flughäfen oder Bahnhöfe abgestellt werden, an denen sich regelmäßig viele Personen aufhalten. Für die Bekämpfung schwerer Kriminalität und zur Verhütung schwerer Bedrohungen der öffentlichen Sicherheit dürfe auf IP-Adressen allgemein und unterschiedslos zurückgegriffen werden, wenn die Speicherung zeitlich auf das absolut Notwendigste begrenzt werde. Auch eine umgehende Sicherung der Verkehrs- und Standortdaten (sogenannter „quick freeze“) komme in Betracht (Rz 67 des Urteils; näher dazu bereits *Thiele*, jusIT 2020/84, 224 [226]), auch wenn diese keinen gleichwertigen sicherheitstechnischen Ersatz bieten. Der EuGH bleibt seiner sehr restriktiven Haltung und dem – unterstützenswerten – Misstrauen gegen die Vorratsdatenspeicherung durch öffentliche Stellen treu.

Ausblick: Die Zulässigkeit von Beweismitteln, die durch eine – wie im Anlassfall – unzulässige Vorratsspeicherung erlangt werden, unterliegt nach dem Grundsatz der Verfahrensautonomie der Mitgliedstaaten dem nationalen Recht. Der EuGH beschränkt sich daher bloß auf den Hinweis auf die Grundsätze der Äquivalenz und der Effektivität (Rz 127 f des Urteils), die von den nationalen Instanzen zu beachten sind (siehe EuGH 17. 12. 2015, C-419/14 [WebMindLicenses], ECLI:EU:C:2015:832). Aus dem Datenschutzgrundrecht des § 1 DSG leitet die österreichische Rechtspraxis kein Beweismittelverwertungsverbot ab (*Thiele/Wagner*, DSG² § 1 Rz 196 mwN). Ein besonderes Beweismittelverbot enthält lediglich § 31 MedienG, der auch in datenschutz- und

zivilrechtlichen Verfahren zu beachten ist (vgl *Thiele*, Grenzen der Transparenz: Redaktionsgeheimnis und Datenschutz, in Berkaß/Holoubek/Leitl-Staudinger [Hrsg], Transparenz im Medienbereich [2021] 47 [57 ff] mwH).

Zusammenfassend hat der EuGH entschieden, dass Rechtsvorschriften, die eine allgemeine und unterschiedslose Vorratspeicherung von Verkehrs- und Standortdaten der elektronischen Kommunikation zum Zwecke der Bekämpfung schwerer Straftaten erlauben, mit dem Unionsrecht schon vom Grundsatz her nicht vereinbar sind.

Bearbeiter: Clemens Thiele

EuGH: Arbeitsrechtlicher Kündigungsschutz für DSBA unionsrechtskonform

» jusIT 2022/63

§ VO (EU) 2016/679: Art 37 Abs 1 und Abs 6, Art 38 Abs 3 und Abs 5, Art 39 Abs 1 lit b
BDSG (Deutschland): § 6 Abs 6 Satz 2, § 38 Abs 2
DSG: §§ 5, 57

EuGH 22. 6. 2022, C-534/20 (Leistriz)

1. Art 38 Abs 3 Satz 2 DSGVO gilt gem Art 37 Abs 6 leg cit gleichermaßen für Datenschutzbeauftragte, die Beschäftigte des Verantwortlichen oder des Auftragsverarbeiters sind, und für diejenigen, die ihre Aufgaben auf der Grundlage eines mit dem Verantwortlichen oder dem Auftragsverarbeiter geschlossenen Dienstvertrags erfüllen.
2. Daher gilt Art 38 Abs 3 Satz 2 DSGVO im Verhältnis zwischen einem Datenschutzbeauftragten und einem Verantwortlichen oder einem Auftragsverarbeiter, und zwar unabhängig von der Art des sie verbindenden Beschäftigungsverhältnisses.
3. Interne und externe Datenschutzbeauftragte sollen nach ErwGr 97 iVm Art 38 Abs 3 Satz 2 DSGVO ihre Pflichten und Aufgaben in vollständiger Unabhängigkeit ausüben können.
4. Art 38 Abs 3 Satz 2 DSGVO steht einer nationalen Regelung grundsätzlich nicht entgegen, nach der ein Datenschutzbeauftragter, der bei einem Verantwortlichen oder einem Auftragsverarbeiter beschäftigt ist, nur aus wichtigem Grund gekündigt werden kann, auch wenn die Kündigung nicht mit der Erfüllung seiner Aufgaben zusammenhängt.
5. Der auch für Mitarbeiter in der Probezeit gültige Sonderkündigungsschutz nach § 6 Abs 6 Satz 2 iVm § 38 Abs 3 BDSG verstärkt die unabhängige Stellung des Datenschutzbeauftragten in Erfüllung seiner Aufga-