

An den Herrn Präsidenten und die Mitglieder des Gerichtshofs

SCHRIFTLICHE ERKLÄRUNG DER REPUBLIK ÖSTERREICH

gemäß Artikel 23 des Protokolls über die Satzung
des Gerichtshofs der Europäischen Union

in der

RECHTSSACHE C-582/14

Zu dem vom Bundesgerichtshof (Deutschland) mit Entscheidung vom 28. Oktober 2014 vorgelegten und am 17. Dezember 2014 beim Gerichtshof eingegangenen Vorabentscheidungsersuchen nimmt die Republik Österreich wie folgt Stellung:

I. Vorlagefragen:

(1) Der Bundesgerichtshof hat dem Gerichtshof folgende Fragen zur Auslegung des Unionsrechts im Wege der Vorabentscheidung vorgelegt:

1. *Ist Art. 2 Buchstabe a der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Abl. EG 1995, L 281/31) - Datenschutz-Richtlinie - dahin auszulegen, dass eine Internetprotokoll-Adresse (IP-Adresse), die ein Diensteanbieter im Zusammenhang mit einem Zugriff auf seine Internetseite speichert, für diesen schon dann ein personenbezogenes Datum darstellt, wenn ein Dritter (hier: Zugangsanbieter) über das zur Identifizierung der betroffenen Person erforderliche Zusatzwissen verfügt?*
2. *Steht Art. 7 Buchstabe f der Datenschutz-Richtlinie einer Vorschrift des nationalen Rechts entgegen, wonach der Diensteanbieter personenbezogene Daten eines Nutzers ohne dessen Einwilligung nur erheben und verwenden darf, soweit dies erforderlich ist, um die konkrete Inanspruchnahme des Telemediums durch den jeweiligen Nutzer zu ermöglichen und abzurechnen, und wonach der Zweck, die generelle Funktionsfähigkeit des Telemediums zu gewährleisten, die Verwendung nicht über das Ende des jeweiligen Nutzungsvorgangs hinaus rechtfertigen kann?*

II. Rechtliche Würdigung:

1. Zu Frage 1:

(2) Nach Art. 2 Buchstabe a der Datenschutz-Richtlinie bezeichnet der Ausdruck „personenbezogene Daten“ alle Informationen über eine bestimmte oder bestimmbare natürliche Person („betroffene Person“). Als bestimmbar wird demzufolge eine Person angesehen, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennnummer oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind. Bei der Entscheidung, ob eine Person bestimmbar ist, sollten zufolge Erwägungsgrund 26 der Richtlinie alle Mittel berücksichtigt werden, die vernünftigerweise entweder von dem Verantwortlichen für die Verarbeitung oder von einem Dritten eingesetzt werden könnten, um die betreffende Person zu bestimmen. Umgekehrt finden nach dem zitierten Erwägungsgrund die Schutzprinzipien der Richtlinie keine Anwendung auf Daten, die derart anonymisiert sind, daß die betroffene Person nicht mehr identifizierbar ist.

(3) Eine Internetprotokoll-Adresse (IP-Adresse) im hier interessierenden Sinne ist eine durch eine Ziffernfolge definierte Adresse, die Rechnern (Endgeräten, Routern etc.) zugewiesen wird, um diese in auf dem Internetprotokoll (IP) basierenden Datennetzen (Bsp.: „Internet“, lokales firmeninternes Netzwerk) adressierbar und damit erreichbar zu machen. Daten können so von ihrem Absender zum vorgesehenen Empfänger transportiert werden. Ähnlich der Postanschrift auf einem Briefumschlag werden Datenpakete mit einer IP-Adresse versehen, die den Empfänger (Endgerät etc.) eindeutig bestimmt.

(4) Dabei gilt es zu berücksichtigen, dass der jeweilige Rechner, welcher etwa im Internet durch eine IP-Adresse adressiert wird, nicht automatisch mit einem bestimmten Nutzer gleichgesetzt werden kann/darf. Bei bestimmten Typen von Rechnern, wie beispielsweise von natürlichen Personen bei einem Diensteanbieter angemeldeten Smartphones, ist es in der Regel möglich, die einem solchen Endgerät für den Betrieb im Internet jeweils zugewiesene IP-Adresse mit einer bestimmten Person in Verbindung zu bringen („Abonnent“ eines Dienstes bzw.

„Anschlussinhaber“). Letztere muss nicht in jedem Einzelfall auch tatsächlicher Nutzer des Gerätes sein. Zu denken ist etwa an die Überlassung an Familienmitglieder oder Freunde etc. Weiters ist zu bedenken, dass im Einzelfall verschiedene Nutzer mit unterschiedlichen Endgeräten über ein und denselben Netzzugang Zugriff zum Internet haben können (Bsp.: öffentliches „Free WIFI“, privates WLAN oder IP-Adresse des Rechners einer größeren Institution). Diesfalls wird aus der Perspektive des Internets, das heißt auf der Netzebene oberhalb eines Netzzugangspunktes im vorstehenden Sinne stets ein und dieselbe IP-Adresse verwendet.

- (5) Darüber hinaus gilt es zu bedenken, dass IP-Adressen sowohl vorübergehend („dynamische“ Adressen) – beispielsweise nur für eine „Sitzung“ – als auch permanent („statische“ Adressen) zugewiesen werden können. Letzteres kann sowohl Einzelnutzer als auch staatliche Institutionen oder private Organisationen betreffen. Auf der Ebene der Adressverwaltung kann grundsätzlich jede IP-Adresse mittels eines öffentlichen Verzeichnisses („WHOIS“; siehe dazu <https://who.is/> bzw. www.whois.com) einem Internetzugangsdiensteanbieter („access provider“) oder – sofern zutreffend, wie beispielsweise bei größeren Institutionen/Organisationen – auch einem festen Nutzer zugeordnet werden. Ein Internetzugangsdiensteanbieter kann in Bezug auf den von ihm genutzten Bestand an IP-Adressen bzw. bezogen auf seine eigenen registrierten Kunden in der Regel ermitteln, welchem Rechner/Kunden eine bestimmte IP-Adresse in der jüngeren Vergangenheit in welchem Zeitraum zugeordnet war. Bei einer sogenannten dynamischen IP-Adresse ist insofern für eine Identifizierung eines bestimmten Rechners/Kunden/Anschlussinhabers der Zeitpunkt der Benutzung dieser IP-Adresse von wesentlicher Bedeutung.
- (6) Ob nun eine bestimmte IP-Adresse als personenbezogenes Datum im Sinne von Art. 2 Buchstabe a der Datenschutz-Richtlinie zu qualifizieren ist oder nicht, hängt im Lichte der obigen Ausführungen davon ab, ob jener Rechner, dem eine IP-Adresse zugewiesen wird, einer bestimmten oder bestimmbar natürlichen Person zugeordnet werden kann. Diese muss nicht auch tatsächlicher Nutzer des Rechners und damit der IP-Adresse sein.
- (7) Aus Art. 2 Buchstabe a in Verbindung mit Erwägungsgrund 26 der Datenschutz-Richtlinie ergeben sich gewisse Kriterien für die Bestimmbarkeit einer „Person“ im

hier verstandenen Sinn. Dabei ist hervorzuheben, dass Erwägungsgrund 26 auch dann von einer Bestimmbarkeit ausgeht, wenn diese erst durch Einsatz von Mitteln eines Dritten ohne unverhältnismäßigen Aufwand erreicht werden kann.¹ Es kommt somit nicht darauf an, dass der Auftraggeber selbst über alle die für die Bestimmbarkeit einer Person notwendigen Mittel verfügt. Dies bedeutet, dass eine IP-Adresse auch dann als personenbezogenes Datum angesehen werden kann, wenn ein Dritter (wie etwa ein Zugangsdiensteanbieter („access provider“)) über die zur Bestimmbarkeit des Inhabers notwendigen Mittel verfügt und mit Einsatz dieser Mittel die Identität einer Person ohne unverhältnismäßigen Aufwand festgestellt werden kann.

- (8) Die sogenannte „Art. 29-Gruppe“ (nach der Datenschutz-Richtlinie) hat sich mit der Frage, ob eine IP-Adresse als personenbezogenes Datum anzusehen ist, in diversen Stellungnahmen auseinandergesetzt und dies stets bejaht.² Aus diesen ergibt sich, dass eine IP-Adresse – unabhängig davon, ob es sich um eine „statische“ oder „dynamische“ handelt – nur dann nicht als personenbezogenes Datum anzusehen ist, wenn der Zugangsdiensteanbieter mit absoluter Sicherheit darlegen kann, dass der Nutzer nicht identifiziert werden kann. Im Zweifelsfall ist nach Auffassung der „Art. 29-Gruppe“ daher vom Vorliegen eines personenbezogenen Datums auszugehen.
- (9) Ähnlich äußerte sich die International Working Group on Data Protection in Telecommunications (IWGDPT), die so genannte „Berlin Gruppe“. Sie vertritt diese Ansicht seit Jahren, zuletzt in ihrem „Arbeitspapier zu „Big Data und Datenschutz“, Bedrohung der Grundsätze des Datenschutzes in Zeiten von Big-Data-Analysen“.³

¹ Vgl. die Formulierung „[...] sollten alle Mittel berücksichtigt werden, die vernünftigerweise entweder von dem Verantwortlichen für die Verarbeitung oder von einem Dritten eingesetzt werden könnten, um die betreffende Person zu bestimmen.“

² Siehe dazu die Stellungnahmen 4/2007 – WP 136, S. 17; 1/2009 – WP 159, Punkt 4; 9/2014 – WP 224, S. 9; alle abrufbar unter http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm#h2-6).

³ „Big Data und Datenschutz, Bedrohung der Grundsätze des Datenschutzes in Zeiten von Big-Data-Analysen“, 55. Sitzung, 5.-6. Mai 2014, Skopje, S. 3 (abrufbar unter <http://www.datenschutzberlin.de/content/europa-international/international-working-group-on-data-protection-intelecommunications-iwgdpt/working-papers-and-common-positions-adopted-by-the-working-group>).

- (10) Auch die Tatsache, dass eine IP-Adresse gegebenenfalls nur unter hohem Aufwand einer Person zugeordnet werden kann, reicht für sich alleine noch nicht aus, um vom Nichtvorliegen eines personenbezogenen Datums auszugehen. Hier ist nach Ansicht der Republik Österreich kein anderer Maßstab als bei anderen Daten anzuwenden, die unter Umständen nur mit großem Aufwand einer Person zugeordnet werden können, deren grundsätzliche Qualität als personenbezogenes Datum aber unstrittig ist (beispielsweise undeutlich erkennbares Autokennzeichen o.ä.).

2. Zu Frage 2:

- (11) Gemäß Art. 7 Buchstabe f der Datenschutz-Richtlinie sehen die Mitgliedstaaten vor, dass die Verarbeitung personenbezogener Daten lediglich erfolgen darf, wenn insbesondere der Fall zutrifft, dass die Verarbeitung zur Verwirklichung des berechtigten Interesses, das von dem für die Verarbeitung Verantwortlichen oder von dem bzw. den Dritten wahrgenommen wird, denen die Daten übermittelt werden, erforderlich ist, sofern nicht das Interesse oder die Grundrechte und Grundfreiheiten der betroffenen Person, die gemäß Art. 1 Abs. 1 der Richtlinie geschützt sind, überwiegen.
- (12) Der Bundesgerichtshof verweist in Rz 34 des Vorabentscheidungsersuchens auf § 12 Abs. 1 TMG, wonach eine Speicherung über den Zugriff hinaus nur zulässig sei, soweit das TMG oder eine andere Rechtsvorschrift, die sich ausdrücklich auf Telemedien bezieht, es erlaubt oder der Nutzer eingewilligt hat. Als mögliche Erlaubnis zieht der Bundesgerichtshof § 15 Abs. 1 TMG in Betracht. Dabei bleibt offen, ob § 15 Abs. 1 TMG die einzige mögliche Rechtsgrundlage ist. Nach dem Wortlaut von § 12 Abs. 1 TMG käme allenfalls auch eine andere Rechtsvorschrift in Betracht, sofern sie sich ausdrücklich auf Telemedien bezieht. Ob es eine derartige innerstaatliche Vorschrift gibt, wäre jedoch vom vorlegenden Gericht zu prüfen.
- (13) Soweit die Auslegung von Art. 7 Buchstabe f der Datenschutz-Richtlinie betroffen ist, vertritt die Republik Österreich die Ansicht, dass eine begrenzte Speicherung einer IP-Adresse auch über die Dauer des Zugriffs auf eine Website hinaus zulässig sein kann. Diese Zulässigkeit kann sich etwa aus der Verpflichtung gemäß

(14) Die Republik Österreich schlägt auf Basis der obigen Erwägungen folgende Antworten auf die Vorlagefragen des Bundesgerichtshofs vor:

1. Art. 2 Buchstabe a der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr ist dahin auszulegen, dass eine Internetprotokoll-Adresse (IP-Adresse), die ein Diensteanbieter im Zusammenhang mit einem Zugriff auf seine Internetseite speichert, für diesen schon dann ein personenbezogenes Datum darstellt, wenn ein Dritter (im Ausgangsverfahren: Zugangsanbieter) über das zur Identifizierung der betroffenen Person erforderliche Zusatzwissen verfügt.
2. Art. 7 Buchstabe f der Datenschutz-Richtlinie steht nicht schlechthin einer Speicherung personenbezogener Daten eines Nutzers ohne dessen Einwilligung entgegen, soweit dies erforderlich ist, um über die Ermöglichung und Abrechnung der konkreten Inanspruchnahme eines Telemediums durch den jeweiligen Nutzer hinaus die generelle Funktionsfähigkeit des Telemediums zu gewährleisten. Dabei ist auf eine strikte Wahrung der Grundsätze des Art. 6 Abs. 1 der Richtlinie zu achten.
