

BREYER LEGAL • Klagenfurter Ring 2FA • 65187 Wiesbaden

Landgericht Berlin II
– 60 S 10/25 –
Littenstraße 12-17
10179 Berlin

Jonas Breyer

Rechtsanwalt
Zert. Datenschutz-
beauftragter (FFD)

Felicia Früchtenicht

Rechtsanwältin
Freie Mitarbeiterin

60 S 10/25

Az.: IP-Speicherung

Sehr geehrte Damen und Herren,

In dem Verfahren

10.10.2025 Klagenfurter Ring 2FA
65187 Wiesbaden
T +49 611 141 056 89
F +49 611 141 056 90

Mainzer Landstraße 69
60329 Frankfurt am Main
T +49 69 247 422 39
F +49 69 247 422 40

jbreyer@kanzlei-breyer.de
www.kanzlei-breyer.de

Breyer ./ BRD

weist der Kläger zum Schriftsatz vom 04.09.2025 auf Folgendes hin:

1. § 9 TDDDG keine Rechtsgrundlage

Die These, § 9 TDDDG sei Rechtsgrundlage für die streitgegenständliche Speicherung von IP-Adressen, ist abwegig und wird an keiner Stelle in Literatur oder Rechtsprechung vertreten.

- a) Art. 6 Abs. 1 Unterabsatz 2 DS-GVO soll es nach Erwägungsgrund 10 DS-GVO den Mitgliedsstaaten zwar ermöglichen, bestehende Rechtsgrundlagen beizubehalten. Der Gesetzgeber hat aber § 15 TMG gerade nicht beibehalten, sondern aufgehoben.
- b) Warum der Gesetzgeber die Vorschrift nicht nur für private, sondern auch für öffentliche Stellen ersatzlos gestrichen hat, ist für den vorliegenden Rechtsstreit unerheblich. Es mag sein, dass der Gesetzgeber rechtsirrig davon ausging, die DS-GVO verdränge die Bestimmungen zum Telemediendatenschutz insgesamt (siehe BT-Drs. 19/27441, S. 36: „Teil 3 enthält die Bestimmungen zum

Telemediendatenschutz, die nicht durch die DS-GVO verdrängt werden.“). Möglicherweise hielt er aber im Hinblick auf öffentliche Stellen auch § 3 BDSG für ausreichend.

- c) Jedenfalls ist es unmöglich, § 9 TDDDG entgegen seinem klaren Wortlaut („Verkehrsdaten“, „Anbieter von öffentlich zugänglichen Telekommunikationsdiensten“) und seiner systematischen Stellung („Kapitel 2 Verkehrsdaten, Standortdaten“) auf Nicht-Telekommunikationsdienste und Nicht-Verkehrsdaten anzuwenden. Es gibt auch keinen eindeutigen Willen des Gesetzgebers dahin gehend.
- d) Die Gesetzesbegründung zu § 9 TDDDG lautet (BT-Drs. 19/27441, S. 35): „§ 9 übernimmt die bisher in § 96 TKG enthaltene Regelung zur Verarbeitung von Verkehrsdaten, die redaktionell angepasst wird aber ansonsten inhaltlich unverändert bleibt. Die Regelung dient der Umsetzung von Artikel 6 der ePrivacy-Richtlinie.“ Der Gesetzgeber wollte also eine nur für Telekommunikationsdienste geltende Vorschrift (§ 96 TKG) inhaltlich unverändert fortschreiben. Sie soll Artikel 6 der ePrivacy-Richtlinie umsetzen, der ebenfalls nur für Telekommunikationsdienste gilt.
- e) Wo der Gesetzgeber Telekommunikations- und digitale Dienste (Telemedien) vergleichbar regeln wollte, hat er auch zwei Regelungen geschaffen – siehe etwa zu Bestandsdatenauskünften § 174 TKG einerseits und § 22 TDDDG andererseits.

2. Auch § 3 BDSG kommt als Rechtsgrundlage hier nicht in Betracht

- a) Zwar hat sich der 6. Senat des Bundesverwaltungsgerichts (Urteil vom 20.3.2024 – 6 C 8.22) nicht der Auffassung angeschlossen, wonach § 3 BDSG unionsrechtswidrig und deshalb nicht anwendbar sei. Dagegen ist aber der 7. Senat des Bundesverwaltungsgerichts der Auffassung, eine derartige Generalklausel als Rechtsgrundlage sei mit der DS-GVO nicht vereinbar (Urteil vom 27.09.2018 – 7 C 5/17, Abs. 26); das Erfordernis einer gesonderten Rechtsgrundlage könne „nicht durch einen umfassenden Auffangtatbestand überspielt werden.“ Dass auch die Literatur dies überwiegend so beurteilt, ist belegt worden (Paal/Pauly-Frenzel, § 3 BDSG, Rn. 1 f.; Sydow/Marsch-Reimer, § 3 BDSG, Rn. 18 f.; Reimer, Verwaltungsdatenschutzrecht, Rn. 165 – beck online). Soweit der 6. Senat befürchtet, ohne § 3 BDSG wären „eine Vielzahl allgemeiner

Ermächtigungsgrundlagen“ erforderlich, kann das nicht nachvollzogen werden. Immerhin existierte § 15 TMG vorher auch und es handelte sich nur um eine einzige Norm.

- b) Der Meinungsunterschied zwischen den Senaten unterstreicht zumindest, dass die Frage nicht offensichtlich zu beantworten und eine Vorlage an den EuGH angezeigt ist.
- c) Selbst wenn man § 3 BDSG für anwendbar hielte, ist im Übrigen allgemeine Auffassung auch des Bundesverwaltungsgerichts, dass die Vorschrift nur „Rechtsgrundlage für die Verarbeitung personenbezogener Daten durch öffentliche Stellen mit geringer Eingriffsintensität“ sein kann (Urteil vom 20.3.2024 – 6 C 8.22, Abs. 28). Das Bundesverwaltungsgericht hat zutreffend eine geringe Eingriffsintensität darin gesehen, wenn eine Behörde die Postanschrift eines Antragstellers erhebt, um ihn identifizieren und ihre Entscheidung an ihn schriftlich bekanntgeben zu können (BVerwG a. a. O.). Die Postanschrift eines Bürgers hat aber offensichtlich eine völlig andere Eingriffsqualität als der Inhalt seiner Internetnutzung.
- d) Zur besonderen Eingriffstiefe der Surfprotokollierung ist bereits umfassend ausgeführt worden. Soweit der BGH im Jahr 2017 in einem obiter dictum in der Protokollierung des Inhalts der Internetnutzung „nach den bisherigen Feststellungen“ nur eine „eher geringe“ Eingriffstiefe erkennen wollte, weil die Person des Internetnutzers nur unter „engen Voraussetzungen“ festgestellt werden dürfe, ist das nicht haltbar. Schließlich sehen Bundesverfassungsgericht und EuGH bereits in der Vorratsspeicherung von Telekommunikations-Verkehrsdaten einen besonders schwerwiegenden Grundrechtseingriff, obwohl sich Verkehrsdatensätze (anhand von Rufnummer oder IP-Adresse) unter denselben Voraussetzungen des § 174 TKG einem Nutzer zuordnen lassen wie die Internet-Nutzungsprotokolle der Beklagten.

3. Schließlich kommt auch Art. 32 DS-GVO als Rechtsgrundlage nicht in Frage

- a) Diese Vorschrift enthält Pflichten zur Gewährleistung der Datensicherheit, stellt aber keine Rechtsgrundlage für die Verarbeitung personenbezogener Daten dar (Simitis/Hornung/

Spiecker gen. Döhmman, Datenschutzrecht, DS-GVO Art. 32 Rn. 69, beck-online). Sie regelt also nicht, ob Daten verarbeitet werden dürfen, sondern wie diese Daten zu schützen sind, wenn eine gültige Rechtsgrundlage für die Verarbeitung existiert.

- b) Dies ergibt sich schon systematisch daraus, dass die „Rechtmäßigkeit der Verarbeitung“ personenbezogener Daten ausdrücklich und abschließend in Artikel 6 DS-GVO geregelt ist. Art. 6 Abs. 1 DS-GVO bestimmt: „Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist...“
- c) Die Pflichten nach Art. 32 DS-GVO entsprechen auch inhaltlich nicht den streitgegenständlichen Verarbeitungszielen der Beklagten. Art. 32 DS-GVO verpflichtet zur Sicherung der personenbezogenen Daten, die vom Verantwortlichen verarbeitet werden. Die amtliche Überschrift der Norm lautet: „Sicherheit der Verarbeitung“. Die Beklagte macht nicht geltend, die personenbezogene Surfprotokollierung auf ihren Webservern diene dem Schutz der bei ihr verarbeiteten personenbezogenen Daten. Soweit die Beklagte geltend macht, Schadsoftware könne bei Dritten zu Datenabflüssen führen, ist dies nicht vom Anwendungsbereich des Art. 32 DS-GVO umfasst.
- d) Art. 6 Abs. 1 UAbs. 1 lit. c i. V. m. Art. 32 DS-GVO kommt als Rechtsgrundlage ebenfalls nicht in Frage. Da diese Vorschrift nur rechtliche Verpflichtungen umfasst, müsste die von der Beklagten teilweise praktizierte unterschiedslose Surfprotokollierung rechtlich verpflichtend sein. Die Beklagte würde also hinsichtlich der Internetportale, bei denen sie keine personenbezogene Protokollierung vornimmt, rechtswidrig handeln. Es dürfte überhaupt keine Internetportale ohne personenbezogene Surfprotokollierung mehr geben. Diese Auffassung vertritt die Beklagte selbst nicht.
- e) Die Beklagte zitiert auch Hoeren/Sieber/Holznagel MMR-HdB/Schmitz, 62. EL Juni 2024, Teil 16.2 Rn. 360, beck-online falsch. Dort heißt es, eine rechtliche Verpflichtung ergebe sich nach Auffassung der Aufsichtsbehörden z. B. bei der „Zugangssicherung“ zu Online-Diensten und erfordere eine Protokollierung und Auswertung der Anmeldungen, Anmeldeversuche, fehlerhafte Anmeldungen, Passwortwechsel und ähnliches. Es ist dort keine Rede von einer Pflicht zur personenbezogenen Protokollierung des Surfverhaltens.

- f) Im Übrigen zeigt Erwägungsgrund 49 DS-GVO, dass der Verordnungsgeber die Netz- und Informationssicherheit als mögliches legitimes Interesse im Sinne des Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO angesehen hat und nicht als rechtliche Verpflichtung. Dies hat auch der EuGH so entschieden (EuGH, 04.07.2023 – C-252/21, Meta/Facebook vs. BKartA, Abs. 119 ff.). Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO aber ist auf staatliche Stellen bei der Erfüllung öffentlicher Aufgaben nicht anwendbar.

4.1 Zum Modell „ITZBund“

- a) Auch § 5 Abs. 1 Nr. 1 BSIG deckt nicht die Praxis der Beklagten ab, das völlig unauffällige Surfverhalten des Klägers über die Dauer des Nutzungsvorgangs hinaus auf Vorrat zu speichern. Wie bereits in früheren Schriftsätzen umfassend erläutert, müssen die nach dieser Vorschrift ersterfassten Daten unverzüglich automatisiert ausgewertet und danach sofort und spurlos gelöscht werden (§ 5 Abs. 1 S. 2 BSIG). Dieser automatisierte Vorgang – Prüfung auf Anhaltspunkte für Schadprogramme – kann und muss in Echtzeit erfolgen, so dass im Fall des Klägers und seines unauffälligen Nutzungsverhaltens in Ermangelung jeglicher Anhaltspunkte eine sofortige Löschung noch während des Nutzungsvorgangs zu erfolgen hat.
- b) Dass das BSIG bereits nicht einschlägig ist, hat die Kammer selbst ausgesprochen: Urteil vom 31.01.2013, S. 18–19.
- c) Im Übrigen wurde schon aufgezeigt, dass das BSI auch tatsächlich keine flächendeckende Surfprotokollierung praktiziert. Die beanstandete Surfprotokollierung findet vielmehr (hinsichtlich eines Teils der dort gehosteten Internetportale) beim ITZBund statt.

4.2 Zum Modell „Eigenbetrieb“

Aus denselben Gründen rechtfertigt auch hier der § 5 BSIG die beanstandete Surfprotokollierung nicht.

4.3 Zum Modell „Hostinganbieter“

- a) Die Beklagte kann sich der DS-GVO natürlich auch nicht dadurch entziehen, dass sie einen privaten Anbieter mit der technischen

Bereitstellung ihrer Internetportale beauftragt (Webhosting). Das Webhosting stellt eine klassische Auftragsverarbeitung (AV) nach Art. 28 DS-GVO dar, bei der die Beklagte Zweck und Mittel der Datenverarbeitung auf ihren Internetportalen bestimmt (Anmeldung, Formulare, Cookies, Logfiles...), während der Hostinganbieter diese Daten „für den Verantwortlichen“ ohne eigene Zwecke verarbeitet. Die Auftragsdatenverarbeitung zeichnet sich dadurch aus, dass der Auftraggeber verantwortlich bleibt. Deshalb sind nur die Rechtsgrundlagen einschlägig, die dem Auftraggeber/Verantwortlichen zur Verfügung stehen. Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO ist auf staatliche Stellen bei der Erfüllung öffentlicher Aufgaben nicht anwendbar.

- b) Beim Webhosting bestimmt üblicherweise der Auftraggeber, ob eine personenbezogene, anonymisierte oder keine Protokollierung der Zugriffe auf den Webserver stattfindet. Die Protokollierung erfolgt für den Auftraggeber; die Protokolle sind für diesen zugänglich.
- c) Es wird bestritten, dass die von der Beklagten beauftragten Webhoster daneben eigenmächtig eine Surfprotokollierung zu eigenen Zwecken praktizieren. In diesem Fall wäre die Beklagte unter dem Gesichtspunkt der Datensparsamkeit verpflichtet, einen anderen Webhoster zu wählen, der dies nicht tut.
- d) Im Übrigen ist der Fall der eigenmächtigen Protokollierung durch einen Webhoster für eigene Zwecke nicht Gegenstand dieses Rechtsstreits. Durch Verfolgung eigener Zwecke würde der Webhoster selbst zum Verantwortlichen für diese Datenverarbeitung werden. Im vorliegenden Rechtsstreit verklagt der Kläger nur die Beklagte auf Unterlassung ihrer Datenverarbeitung. Die Klage bezieht sich nur auf die Datenverarbeitung, für welche die Beklagte die Verantwortung trägt, nicht auf eine Datenverarbeitung in Verantwortung Dritter.

Mit freundlichem Gruß

Jonas Breyer
(Rechtsanwalt)