

Datenschutz am Mittag, 20.4.2024:

Die Bestandsdatenauskunft im TTDSG

Dr. Matthias Lachenmann

Rechtsanwalt, Datenschutzbeauftragter (UDISzert)

Agenda



Überwachungskameras von Ring Amazon gibt Aufnahmen ohne richterlichen Beschluss an deutsche Polizei

Mit seinem weit verbreiteten Heim-Überwachungssystem sammelt Amazon auf seinen Servern umfangreiches Videomaterial. Ohne Rechtsgrundlage gibt das Unternehmen die Daten an die Polizei weiter, wenn diese danach fragt.

[Ingo Dachwitz](#) - 20.09.2022 um 12:59 Uhr - [10 Ergänzungen](#)



Überwachungskameras von Ring Amazon gibt Aufnahmen ohne richterlichen Beschluss an Polizei

Schon lange steht Überwachungshersteller Ring wegen einer zu großen Nähe zur Polizei in der Kritik. Jetzt zeigt sich: Die Amazon-Tochterfirma gab Videoaufnahmen aus privaten Kameras nicht nur ohne Einverständnis der Nutzer:innen, sondern teilweise auch ohne richterliche Anordnung weiter.

[Ingo Dachwitz](#) - 18.07.2022 um 18:59 Uhr

Fake-Notfallanfragen: Apple und Meta gaben angeblich Nutzerdaten preis

Durch Zugriff auf Mail-Adressen von Strafverfolgern konnten Hacker offenbar Nutzerdaten bei Diensten abfragen. In Notfällen werden Daten schnell herausgegeben.

Lesezeit: 2 Min. [In Pocket speichern](#)

[🔊](#) [🖨️](#) [💬 39](#)



(Bild: bluesroad/Shutterstock.com)

31.03.2022 17:39 Uhr | Mac & i

Von Leo Becker

Kriminelle haben durch Schwachpunkte bei der Bearbeitung von Behördenanfragen offenbar Zugriff auf Nutzerdaten populärer Dienste erhalten.

<https://www.sueddeutsche.de> › panorama › kita-toniebox-einbruch-halver-1.5419482

Kita in Halver: Toniebox überführt Einbrecher - Panorama - SZ.de

Nach dem Einbruch in einer Kindertagesstätte in Halver ist der Dieb gefunden - Dank der gestohlenen Toniebox. Erzieher Marcel Rau erzählt.

19.
Jan.
2023



DATENSCHUTZ AM MITTAG

DATENSCHUTZ UND STRAFRECHT
mit Dr. Eren Basar

Was Datenschützer über das Strafrecht wissen sollten



DETAILS

14.
Mär.
2023



DATENSCHUTZ AM MITTAG

**NEUES ZUM CCPA UND ZUM
DATENTRANSFER IN DIE USA**
Barbara Schmitz und Dr. Axel Spies

Natürlich gibt es auch in den USA Gesetze für den Datenschutz.



DETAILS



Bestandsdatenauskunft

Große Koalition plant das nächste verfassungswidrige Gesetz

Schon zwei Mal hat das Bundesverfassungsgericht Gesetze zur Bestandsdatenauskunft als verfassungswidrig eingestuft. Jetzt hat der Bundestag ein Gesetz zur Neuregelung auf den Weg gebracht. Doch die Regierungsparteien haben wenig gelernt: Auch dieses Gesetz dürfte so in Karlsruhe scheitern.

15.01.2021 um 11:24 Uhr - Gastbeitrag, Mayeul Hiéramente - in Überwachung - eine Ergänzung

- I. Anwendungsbereich der Bestands- und Nutzungsdatenauskunft
- II. Exkurs: BMJ-Pläne zum Gesetz gegen digitale Gewalt
- III. Übermittlung der Daten im Rahmen des Doppeltürmodells
- IV. Konkrete Pflichten für Anbieter von Telemedien
- V. Vergleich mit dem US-Amerikanischen Recht
- VI. Fazit und Ausblick

I. Anwendungsbereich der Bestands- und Nutzungsdatenauskunft

grundlegendes Ziel der Bestands- und Nutzungsdatenauskunft:

- verschiedene Behörden aus den Bereichen Strafverfolgung, Sicherheit und Nachrichtendienste dürfen
- von Anbietern von Telemedien verlangen
- Auskunft über Informationen zu den Nutzern/Kunden zu erteilen
- Ziele z.B.: Verhinderung erheblicher Straftaten, Auffinden Vermisster

➤ frühere Regelungen:

- Telekommunikation: § 113 TKG a. F. (§ 174 TKG) für Telekommunikationsanbieter, und automatisierte Auskunftsverfahren nach § 112 TKG a. F. (§ 173 TKG)
- Telemedien: Auskünfte an Sicherheitsbehörden im Einzelfall zum Schutz gewichtiger Rechtsgüter, § 14 und § 15 Abs. 5 Satz 4 TMG a. F.

I. Anwendungsbereich der Bestands- und Nutzungsdatenauskunft

Entwicklung des Gesetzes in der aktuellen Fassung

- Maßgeblich: BVerfGE 130, 151 – Bestandsdatenauskunft I
- Verantwortlich für die jetzige Fassung: BVerfGE 155, 119 – Bestandsdatenauskunft II
- **Gesetzgebungsverfahren zur aktuellen Gesetzesfassung:**
 - 1. Entwurf im nicht ausgefertigten „Gesetz zur Bekämpfung des Rechtsextremismus und der Hasskriminalität“ (BT-Drs. 19/7741)
 - Aufteilung nach Bestands- und Nutzungsdaten in BT-Drs. 19/27900, 19 ff.
 - Neuregelung im „Gesetz zur Anpassung der Regelungen über die Bestandsdatenauskunft“ (BT-Drs. 19/25294)

I. Anwendungsbereich der Bestands- und Nutzungsdatenauskunft

Von §§ 22 – 24 TTDSG erfasste Unternehmen:

- Anbieter von Telemedien = „wer geschäftsmäßig Telemediendienste erbringt, daran mitwirkt oder den Zugang zur Nutzung daran vermittelt“
 - §§ 22 Abs. 1 S. 1, 23 Abs. 1 S. 1 und § 24 Abs. 1 S. 1 TTDSG
 - Beispiele: Website-/App-Betreiber, Cloud-Anbieter usw.

Definition Bestandsdaten (§ 2 Abs. 2 Nr. 2 TTDSG):

- Daten zu Kunden, die im Zusammenhang mit dem Abschluss oder der Durchführung von Verträgen stehen, z. B. Name, IP-Adresse oder Passwörter

Definition Nutzungsdaten (§ 2 Abs. 2 Nr. 3 TTDSG):

- Information, dass eine betroffene Person Interesse an bestimmten Inhalten hat, z.B. bei Aufruf einer Website zu einem bestimmten Thema

§§ 21 – 24 TTDSG

Bestandsdaten
(an private
Stellen)

Bestandsdatenauskunft
(an staatliche Stellen)

Nutzungs-
datenauskunft
(an staatliche
Stellen)

bei geistigem
Eigentum oder
rechtswidrigen
Inhalten, § 21

reguläre
Bestandsdaten,
§ 22

Passwörter und
Zugangsdaten,
§ 23

Nutzungsdaten,
§ 24

II. Exkurs: BMJ-Pläne zum Gesetz gegen digitale Gewalt

- vorgestellt im April 2023: „Eckpunkte des Bundesministeriums der Justiz zum Gesetz gegen digitale Gewalt“
- benannter Fokus des BMJ: „Rechtsdurchsetzung durch die Betroffenen von digitaler Gewalt“
- tatsächlicher Umfang:
 - *„Betroffene sollen sich künftig gegen alle Verletzungen ihrer Rechte zur Wehr setzen können [...]. Das können zum Beispiel wahrheitswidrige geschäftsschädigende Äußerungen sein (z.B. auf Bewertungsseiten), [...]“*
- vorgeschlagene Lösung:
 - *„Künftig sollen auch Nutzungsdaten wie z. B. die IP-Adresse herausgegeben werden müssen, [...]. Bisher beschränkt sich die Regelung auf die Herausgabe von Bestandsdaten wie Name oder E-Mail-Adresse.“*

III. Übermittlung der Daten im Rahmen des Doppeltürmodells

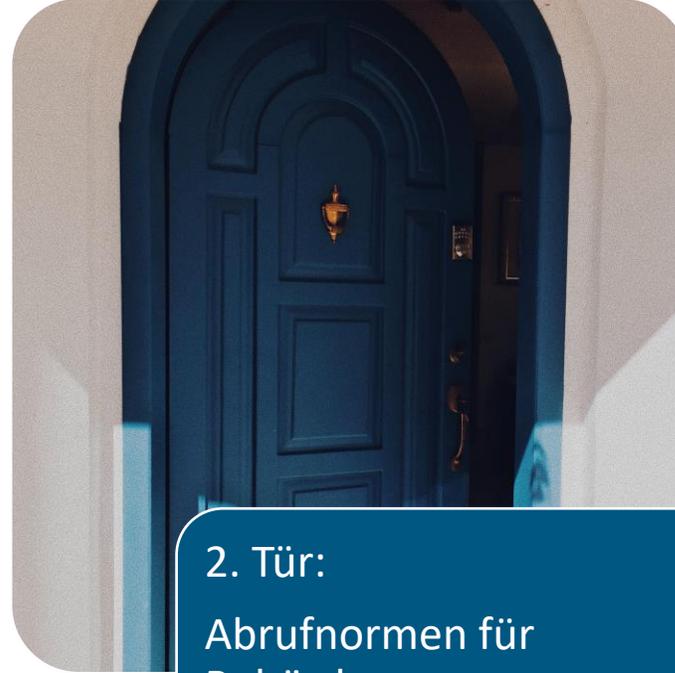
- „Doppeltürmodell“ des BVerfG: Unterscheidung zweier korrespondierender Normen:
 - Datenübermittlung durch auskunftserteilende Stelle („erste Tür“)
 - Datenabruf/Erhebung durch auskunftersuchende Stelle („zweite Tür“)
- Zusammenwirken der Normen durch die Gesetzgeber (Bund und Länder) lässt Recht zur Übermittlung und Verarbeitung entstehen:
 - korrekte Festlegung der Übermittlungsbefugnis und
 - konkrete Festlegung der korrespondierenden Abrufbefugnis
- **Verbot der Übermittlung, wenn die „zweite Tür“ weiter geöffnet wird als die „erste Tür“**

III. Übermittlung der Daten im Rahmen des Doppeltürmodells



1. Tür:
Übermittlungsnormen
für
Telemedienanbieter

- Katalog des § 22 Abs. 3 und 4 TTDSG



2. Tür:
Abrufnormen für
Behörden

- z. B. § 100j Abs. 2 S. 1 Nr. 1 StPO
- z. B. § 10 BKAG

! Türe 2 darf
höchstens so
weit wie Türe 1
geöffnet sein !

IV. Konkrete Pflichten für Anbieter von Telemedien

Pflichten aller Telemedienanbieter – Sicherstellung Rechtsgrundlage:

- **Einschränkung durch Gesetzgeber: nur formelle Prüfung, § 22 Abs. 2 S. 5:**
 - „Die Verantwortung für die Zulässigkeit der Auskunft tragen die um Auskunft ersuchenden Stellen.“
- **BVerfGE 155, 119, Rn. 202: Erfüllung der Pflichten der Übermittlungsregelung**
 - „liegt allein in der Verantwortung des abfrageberechtigten Stellen“
- **Gesetzgeber, BT-Drs. 19/25294, 53: Telemedienanbieter haben**
 - „allein die formalen Voraussetzungen des Auskunftsverlangens zu prüfen“
- **Telemediendienst ist datenschutzrechtlich Verantwortlicher, Art. 4 Nr. 7 DSGVO**
- **→ Rechtsgrundlage: Art. 6 Abs. 1 S. 1 lit. c i. V. m. Abs. 3 DSGVO i. V. m. der Einzelnorm aus § 22 – 24 TTDSG**

IV. Konkrete Pflichten für Anbieter von Telemedien

Verteilung der Pflichten (?):

- Verantwortung der datenanfragenden Sicherheitsbehörden: Richtigkeit der Angaben in ihrem Auskunftersuchen (Zulässigkeit)
 - insbesondere Vorliegen der Erforderlichkeit der Daten für die konkreten Zwecke
- Verantwortung der Telemediendienste als übermittelnde Stelle: Prüfung der weiteren normierten Voraussetzungen
- keine Verantwortung der Telemediendienste: Bewertung, ob eine aus dem Ausland drohende Gefahr von internationaler Bedeutung tatsächlich vorliegt
- Pflicht zur Übermittlung nur, wenn die formellen und materiellen Voraussetzungen der §§ 22-24 TTDSG eingehalten werden (wohl m. M.)

IV. Konkrete Pflichten für Anbieter von Telemedien

Abrufverlangen
einer
Sicherheitsbehörde,
Abs. 3 und 4



Voraussetzungen
der Absätze 1, 2, 5
und 6 eingehalten



Befugnis und
Verpflichtung zur
Übermittlung

IV. Konkrete Pflichten für Anbieter von Telemedien

Pflichten der Behörden – zugleich Prüfpflicht der Telemediendienste:

- **Anforderungen an die Abfrage der Sicherheitsbehörden (Absatz 3 und 4):**
 - Angabe der gesetzlichen Bestimmung für die Übermittlung
 - Abfrageberechtigung durch die in der Norm benannten Sicherheitsbehörde
 - erfolgt jeweils in Bezug auf den konkreten Einzelfall (§ 22 Abs. 2)
 - Nennung der Erforderlichkeit der Daten sowie der Zweck des Ersuchens (§ 22 Abs. 2)
 - Abfrage bewegt sich im Rahmen der Voraussetzungen der Norm
- **Beispiele für Fehler bei den Abfragen:**
 - keine Nennung der korrekten Rechtsgrundlagen (z. B. § 14 TMG a.F.)
 - Anfrage der Polizei ohne Klarstellung, ob und inwiefern Bezug zu Strafverfolgung oder Gefahrenabwehr besteht

IV. Konkrete Pflichten für Anbieter von Telemedien

Pflichten aller Telemedienanbieter – Implementierung der Prüfung:

- Ernennung einer verantwortlichen Fachkraft, die die Einhaltung der formalen Voraussetzungen prüft (Abs. 6 S. 2)
 - Fachkraft soll im Vorfeld über die ggf. nötigen Schritte geschult sein
 - Ziel: schnelle Reaktion des Telemedienanbieters
- Prüfung der Auskunftsverlangen und Freigabe der Daten bei positivem Prüfergebnis durch die verantwortliche Fachkraft (Abs. 6 S. 3)

Pflichten aller Telemedienanbieter – Pflichtenrahmen:

- Berücksichtigung sämtlicher unternehmensinternen Datenquellen für die Auskunftserteilung (Abs. 1 S. 4)
- Dokumentation von Prüfung und Ergebnis (Art. 24, Art. 5 Abs. 2 DSGVO)
 - vertiefte Prüfung insbesondere bei einer Anfrage in elektronischer Form

IV. Konkrete Pflichten für Anbieter von Telemedien

Pflichten aller Telemedienanbieter – Stillschweigen:

- Stillschweigen gegenüber den Betroffenen sowie Dritten über das Auskunftersuchen und die Auskunftserteilung, § 22 Abs. 5 S. 3 TTDSG
- Pflicht zur Information kann durch die Sicherheitsbehörden nach den fachgesetzlichen Auskunftsnormen bestehen (nach Abschluss der Maßnahmen)
- → hohe Bedeutung von Transparenzberichten

Last Updated: January 1, 2022

Type of Request Received	Number of Requests	Number of Users Impacted
Subpoenas	0	0
Search Warrants	0	0
Court Orders	0	0
International Requests	0	0
National Security Requests	0	0

Law Enforcement Requests Report

Explore law enforcement requests by country dating back to 2013.

[Download the current report >](#)

V. Vergleich mit dem US-Amerikanischen Recht

verletztes Unionsrecht	bemängelte Rechtslage in USA u. a.	Rechtslage in Deutschland u. a.
<ul style="list-style-type: none">• Art. 7 EuGRCh: Schutz Privat- und Familienleben, Wohnung und Kommunikation• Art. 8 Abs. 1 EuGRCh: Schutz personenbezogener Daten• Art. 52 Abs. 1 EuGRCh: Gesetzesvorbehalt, Wesensgehaltsgarantie (S. 1) und VHMK-Grundsatz (s. 2)	<p>Keine Verhältnismäßigkeit bei Abfragen</p> <ul style="list-style-type: none">• konkrete Gefahr für nationale Sicherheit nicht erforderlich: Datenerhebungen nur „as tailored as feasible“ (PPD-28; Rn. 64, 181 Schrems II)• Datensammeln muss nicht verhältnismäßig sein: FISA ermächtigt zur Durchführung von Überwachungsprogrammen; keine Aufsicht, ob Zielpersonen vorschriftmäßig für Beschaffung von Auslandsaufklärungsdaten ausgewählt wurden (nur Überprüfung Überwachungszweck) (Rn. 179, 180, 184 Schrems II)	<p>Teilweise Verhältnismäßigkeit bei Abfragen</p> <ul style="list-style-type: none">• konkretisierte Gefahren können ausreichend sein (z. B. § 22 Abs. 3 Nr. 2 lit. b TTDSG), teils keine konkreten Gefahren erforderlich (z. B. für BND, §§ 22 Abs. 3 Nr. 8 TTDSG)• Datensammeln muss verhältnismäßig sein, aber praktische Umsetzung durch die Behörden fraglich

V. Vergleich mit dem US-Amerikanischen Recht

verletztes Unionsrecht	bemängelte Rechtslage in USA u. a.	Rechtslage in Deutschland u. a.
<p>Art. 47 Abs. 1 EuGRCh: Recht auf einen wirksamen Rechtsbehelf</p>	<p>kein Rechtsschutz gegen Zugriffe</p> <ul style="list-style-type: none">• Rechtsbehelfe gegen Zugriffe auf Basis von FISA scheitern praktisch daran, dass Einzelpersonen Klagebefugnis nicht nachweisen können (Rn. 115 DSS-Beschluss der EU-Kommission)• Rechtsbehelfe gelten nicht für andere Rechtsgrundlagen (Rn. 115 DSS-Beschluss und Rn. 192 Schrems II)	<p>kein Rechtsschutz gegen Zugriffe</p> <ul style="list-style-type: none">• auch gegen Maßnahmen deutscher Sicherheitsdienste muss eine Betroffenheit in eigenen Rechten nachgewiesen werden• faktisch kein Rechtsschutz möglich, da bereits keine Information des Betroffenen über den Eingriff erfolgt, bzw. erst nachträglich (§ 22 Abs. 5 S. 3 TTDSG)

VI. Ergebnis und Ausblick

- die Bestands- und Nutzungsdatenauskunft betrifft alle Anbieter von Telemedien bzw. Telemediendienste → (fast) alle deutschen Unternehmen
- komplexe rechtliche Bewertung wird teilweise den Telemediendiensten auferlegt
- Benennung einer Fachkraft sinnvoll, insbesondere bei Unternehmen mit erwarteten regelmäßigen Anfragen
- Transparenzberichte in größerem Umfang wünschenswert
- mögliche Auswirkungen auf die Diskussion mit den USA über ein angemessenes Datenschutzniveau?
- geplant: europaweite Ausweitung durch die E-Evidence VO

Kontakt

BHO Legal

Hohenstaufenring 29-37
50674 Köln

Tel.: + 49 (0) 221 270 956 0

Fax: + 49 (0) 221 270 956 222

cologne@bho-legal.com

Dr. Matthias Lachenmann

Rechtsanwalt | Partner

Telefon: + 49 (0) 221 270 956 180

E-Mail: matthias.lachenmann@bho-legal.com

Gierschmann/Baumgartner

TTDSG

Telekommunikation-
Telemedien-Datenschutz-
Gesetz

Kommentar

