PIMS im TTDSG

Vorschlag zur Regelung von Diensten zur Einwilligungsverwaltung im Telekommunikation-Telemedien-Datenschutzgesetz

Kurzgutachten

im Auftrag der European netID Foundation

vorgelegt von

Professor Dr. Rolf Schwartmann

Leiter der Kölner Forschungsstelle für Medienrecht an der
Technischen Hochschule Köln und
Mitglied der Datenethikkommission
Vorsitzender der Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V.
Mitglied im Stiftungsrat der European netID Foundation

Rechtsanwalt Dr. Stefan Hanloser

Mitglied des Fachbeirats Datenschutz der European netID Foundation

Rechtsanwalt Steffen Weiß, LL.M.

Mitglied der Geschäftsführung für Internationales bei der Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V.

März 2021

Dienste zur Einwilligungsverwaltung

a) Einwilligungserfordernis im TTDSG

Das Telekommunikation-Telemedien-Datenschutzgesetz (TTDSG-Regierungsentwurf, BR-Drs. 163/21 v. 12.2.2021) führt das europarechtliche Einwilligungserfordernis für das Speichern und den Zugriff auf Informationen in Endeinrichtungen von Endnutzern in Deutschland ein. Einwilligungsfrei dürften Informationen fortan nur gespeichert und ausgelesen werden, wenn dies für die Nachrichtenübertragung oder Diensteerbringung erforderlich ist. Die Bundesregierung erstreckt das Einwilligungserfordernis für webbasierte Cookies, das der Bundesgerichtshof in seiner *Planet49*-Entscheidung[5] rechtsfortbildend ins deutsche Recht übernommen hatte, nun auf sämtliche mobilen Anwendungen (Mobile Apps, SmartTV-Apps, etc.) und das gesamte Internet der Dinge (Internet of Things, IoT), von Connected Cars bis Smart Meters.

Die Flut an Einwilligungsabfragen, die Nutzer künftig zu gewärtigen haben, wird entsprechend umfassend, wenn nicht erdrückend sein. Das TTDSG hätte den unbeabsichtigten Negativeffekt, dass der Datenschutz als Folge des unbesehenen Wegklickens von massenhaft abgefragten Einwilligungen zunehmend als lästige Förmelei wahrgenommen wird und mit der Datenschutz-Ermüdung die gesellschaftliche Akzeptanz für den Datenschutz insgesamt schwindet.[6]

b) PIMS als Dienst zur Einwilligungsverwaltung

aa) Bedürfnis einer nationalen Regelung im TTDSG

Abhilfe schaffen hier Dienste zur Einwilligungsverwaltung, sog. Personal Information Management Systeme (PIMS), die den Nutzern eine systematische Verwaltung ihrer Einwilligungen über die von ihnen genutzten Telekommunikationsdienste und Telemedien hinweg ermöglichen. Dieser Ansatz wiederum geht auf eine Empfehlung[7] der Datenethikkommission (DEK) der Bundesregierung aus dem Oktober 2019 zurück. Die Kommission hat sich in ihrem Abschlussgutachten im Rahmen ihrer Überlegungen zu Datentreuhandsystemen mit sog. Privacy Management Tools befasst und eine Regulierung solcher Systeme gefordert.[8] Privacy Management Tools verfügen

[5] Urteil v. 28.5.2020, ZD 2020, 467 m. Anm. *Eckhardt* = BB 2020, 1679 m. Anm. *Hanloser*.
[6] BMJV-Studie „Innovatives Datenschutz-Einwilligungsmanagement“, Abschlussbericht v. 7.9.2020, S. 39 f. zur sog. „*click fatigue*“.
[7] Gutachten der Datenethikkommission (2019), Handlungsempfehlung 21.
[8] Gutachten der Datenethikkommission (2019), Handlungsempfehlung 21.

über großes Potential, sofern diese „praxisgerecht, robust und datenschutzkonform“ ausgestaltet sind.[9]

bb) Keine Alternative auf europäischer Ebene

Ein künftiger Data Governance Act (DGA)[10] bietet keine Alternative zu einer Regelung von Diensten zur Einwilligungsverwaltung hier und jetzt im TTDSG. Der DGA hat eine ganz andere Zielrichtung: einen echten europäischen Markt für Daten zu schaffen und gemeinsame europäische Datenräume entstehen zu lassen, um die digitale Souveränität Europas im Bereich der Daten zu stärken. Die Regelung zu Datenintermediären in Art. 9 Abs. 1 lit. b des Kommissionsentwurfs erfasst zwar nominal auch Dienste zur Einwilligungsverwaltung, hat aber den Fokus auf Betroffenen, die ihre Daten einem Datennutzer aktiv zur Verfügung stellen. Zudem ist der DGA bereits zeitlich keine Alternative für das akute Problem der „click fatigue“ unter dem TTDSG, weil der DGA für Bestandsdienste wegen der zweijährigen Übergangsfrist frühestens 2024 gelten würde.[11]

Auf europäischer Ebene verfolgt die Kommission das Ziel der gesetzlichen Regelung einer „European e-identity“ (e-ID)[12]. Mit einer solchen digitalen Identität sollen Bürgerinnen und Bürger im europäischen Binnenmarkt auf sicherem und vertrauensvollem Weg Produkte und Dienstleistungen online erwerben können. Im Fokus steht der sichere Zugang zu Produkten und Diensten, nicht das Verwalten von persönlichen Informationen über entsprechende Datenschutzeinstellungen.

[9] Gutachten der Datenethikkommission (2019), Handlungsempfehlung 21.
[10] Kommissionsvorschlag für eine Verordnung über europäische Daten-Governance (Daten-Governance-Gesetz), Komm-Dok. (2020) 767 final v. 25.11.2020.
[11] *Hanloser*, ZD 2021, 121, 122.
[12] https://ec.europa.eu/digital-single-market/en/news/building-trusted-and-secure-european-digital-identity-brochure.

cc) Anwendungs- und Regulierungsbereiche von PIMS

Die erklärten Einwilligungen sind im PIMS für den Nutzer übersichtlich dokumentiert und können mit Wirkung für die Zukunft widerrufen werden.[13] Eine Regelung von Diensten zur Einwilligungsverwaltung im TTDSG, wie sie im Referentenentwurf v. 14.7.2020[14] in § 3 bereits vorgesehen war[15], wäre *sedes materiae* auf Einwilligungstatbestände im TTDSG, insbesondere den sog. Cookie-Consent nach § 24 TTDSG beschränkt. Das schließt jedoch nicht aus, dass eine nutzerschützende Regelung im TTDSG eine positive faktische Ausstrahlungswirkung auf das Management datenschutzrechtlicher Einwilligungen (Art. 6 Abs. 1 lit. a DSGVO) und Widersprüche (Art. 21 DSGVO) hätte.

dd) Empfehlung: PIMS im TTDSG jetzt nutzerschützend regulieren

Dienste zur Einwilligungsverwaltung sind allerdings wirkmächtige Mittler, die zwischen die Diensteanbieter und ihre Nutzer treten. Eine *nutzerschützende* Regulierung der Dienste zur Einwilligungsverwaltung ist entsprechend geboten, um die spezifischen Gefahren, die von ihnen für die Entscheidungsautonomie der Nutzer ausgehen, zu adressieren. Aber auch eine *anbieterschützende* Regulierung ist erforderlich, um die aktuelle Vielfalt an Informations-, Unterhaltungs- und Bildungsangeboten im Bereich der Telemedien dem beherrschenden Einfluss marktmächtiger PIMS-Anbieter zu entziehen.

Im Einzelnen sind folgende Bereiche regelungsbedürftig:

Interessenkonflikte vermeiden – Um Interessenkonflikte zu Lasten der Nutzer zu vermeiden, sollte es Anbietern von Diensten zur Einwilligungsverwaltung untersagt sein, die Informationen über erteilte oder verweigerte Einwilligungen eines Nutzers für andere Geschäftszwecke als die Erbringung des Dienstes zur Einwilligungsverwaltung zu nutzen. Eine Begünstigung anderer eigener Geschäftszwecke durch dieses Sonderwissen ist mit dem Rollenbild des treuhänderischen Datenmittlers unvereinbar

---

[13] Verbraucherzentrale Bundesverband – vzbv, Positionspapier „Personal Information Management Systems (PIMS) – Chancen, Risiken und Anforderungen“ v. 19.2.2020 in der Fassung der Überarbeitung v. 15.9.2020, S. 6.
[14] Dazu Schwartmann/Benedikt/Reif, Datenschutz bei Websites – Aktuelle Rechtslage und Ausblick auf das TTDSG, RDV 2020, 231 ff.
[15] Kritisch zur Streichung der PIMS-Regelung, vgl. Schwartmann/Benedikt/Reif, Entwurf zum TTDSG: Für einen zeitgemäßen Online-Datenschutz?, MMR 2021, 99 ff.

(Synergieverbot). Die Indifferenz des Dienstes zur Einwilligungsverwaltung gegenüber dem Treugut, also den verwalteten Einwilligungen muss durch eine strenge Zweckbindung gewährleistet sein.

Entscheidungsautonomie sichern – Nutzer müssen *technisch* in der Lage sein, ihre Einwilligungen für bestimmte Telekommunikationsdienste oder Telemedien zu erteilen oder zu verweigern sowie diese Einwilligungen auf bestimmte Zweckkategorien zu beschränken. Ein souveränes Einwilligungsmanagement setzt voraus, dass die Dienste zur Einwilligungsverwaltung entsprechend granulare Einwilligungsentscheidungen technisch ermöglichen. Der Nutzer, der einem vertrauenswürdigen Dienst eine Einwilligung erteilen möchte, darf nicht technisch dazu gezwungen sein, zugleich allen Diensten eine Einwilligung zu erteilen oder auf die Einwilligungserteilung an den vertrauenswürdigen Dienst zu verzichten.

Normtext TTDSG

§ 2 TTDSG - Begriffsbestimmungen

(2) Im Sinne dieses Gesetzes ist oder sind

7.(neu) „Dienst zur Einwilligungsverwaltung“ jeder Dienst und jedes informationstechnische Produkt für die Erteilung von Einwilligungen nach diesem Gesetz, insbesondere für die Einwilligung in die Verarbeitung von Verkehrs- und Standortdaten sowie in das Speichern von Informationen in der Endeinrichtung des Endnutzers und den Zugriff auf Informationen, die bereits in der Endeinrichtung gespeichert sind.

8.(neu) „Anbieter eines Dienstes zur Einwilligungsverwaltung“ jeder, der einen Dienst zur Einwilligungsverwaltung für nicht selbst bereitgehaltene Telekommunikationsdienste und Telemedien geschäftsmäßig anbietet.

Kapitel 2

Teil 4 (neu)

Dienste zur Einwilligungsverwaltung

§ 25 (neu) Dienste zur Einwilligungsverwaltung

(1) Endnutzer können ihre Rechte nach diesem Gesetz durch Dienste zur Einwilligungsverwaltung ausüben.

(2) Anbieter von Diensten zur Einwilligungsverwaltung dürfen die Informationen über die Einwilligungsentscheidungen der Nutzer für keine anderen Zwecke als die Einwilligungsverwaltung verwenden.

(3) Vereinbarungen zwischen Endnutzern und Anbietern von Diensten zur Einwilligungsverwaltung sind nur wirksam, wenn die Endnutzer freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich erklären oder sonst eindeutig bestätigen, dass sie mit der Ausübung ihrer Rechte durch den Anbieter einverstanden sind.

(4) In Verkehr gebrachte Software, die das Speichern von Informationen in den Endeinrichtungen der Endnutzer und den Zugriff auf Informationen, die bereits in den Endeinrichtungen gespeichert sind, steuert, muss Schnittstellen für Dienste zur Einwilligungsverwaltung diskriminierungsfrei zur Verfügung stellen und das Speichern und das Auslesen entsprechend der Einwilligungsentscheidungen der Endnutzer nach § 24 unverzüglich ermöglichen oder verhindern.

Teil 5 (ex-4)

Straf- und Bußgeldvorschriften und Aufsicht

§ 27 (ex-26) Bußgeldvorschriften

(1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

14. entgegen § 25 Absatz 2 Informationen über die Einwilligungsentscheidungen der Nutzer für einen anderen Zweck als die Einwilligungsverwaltung verwendet.

§ 28 (ex-27) Zuständigkeit, Aufgaben und Befugnisse der oder des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

(1) Soweit für die geschäftsmäßige Erbringung von Telekommunikationsdiensten Daten von natürlichen oder juristischen Personen verarbeitet werden ***sowie für Dienste zur Einwilligungsverwaltung hinsichtlich ihrer Pflichten aus § 25****, ist der oder die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit die zuständige Aufsichtsbehörde.*

Zu § 2 TTDSG

„Dienst zur Einwilligungsverwaltung“

Ein Dienst zur Einwilligungsverwaltung ermöglicht Nutzern die Speicherung und Verwaltung von Einwilligungserklärungen im Geltungsbereich des TTDSG. Dienste zur Verwaltung von Datenschutzeinstellungen bedienen sich allgemein den Funktionalitäten eines Privacy Information Management Systems (PIMS), wobei gem. § 2 Abs. 2 Nr. 7 TTDSG die Einwilligung als individuelle Datenschutzeinstellung im Fokus steht. Die erklärten Einwilligungen sind im PIMS für den Nutzer übersichtlich dokumentiert und können mit Wirkung für die Zukunft widerrufen werden. Hauptanwendungsbereich für Dienste zur Einwilligungsverwaltung ist der Cookie Consent nach § 24 TTDSG. Primäres Ziel der gesetzlichen Regelung solcher Dienste ist die Unterstützung von Nutzern bei der Wahrnehmung ihrer Rechte mittels Datenschutzeinstellungen (PIMS). Relevante Einwilligungsverwaltung trifft die Nutzung von

- Verkehrsdaten, TTDSG-RegE 9(2);
- Standortdaten, TTDSG-RegE 13(1),(2)
- Cookie/ MAID-Consent, TTDSG-RegE 24

„Anbieter eines Dienstes zur Einwilligungsverwaltung“

Ein Anbieter eines Dienstes zur Einwilligungsverwaltung erbringt seine Dienste nicht für eigene Telekommunikations- oder Telemediendienste, sondern bietet die Speicherung und Verwaltung von Einwilligungserklärungen bezogen auf Dienste Dritter an.

Die Einschränkung auf nicht selbst erbrachte Telemediendienste bringt den Gedanken eines Datentreuhändermodells zum Ausdruck. Eine Bündelung von Daten, die im Rahmen der Nutzung eines elektronischen Kommunikationsdienstes anfallen (Verkehrs- und Standortdaten) und den persönlichen Datenschutzeinstellungen der einzelnen Nutzer (so insbesondere die Einwilligungserklärung) bei ein und demselben Diensteanbieter, wird so vermieden.

Zu § 25 TTDSG

Abs. 1 u. 3 – Anforderungen an eine freiwillige Nutzung

Die Nutzung von Diensten zur Einwilligungsverwaltung basiert regelmäßig auf einer Vereinbarung zwischen Diensteanbieter und Nutzer. Hierbei ist sicherzustellen, dass der Anbieter seine Leistungen im Bereich der Verwaltung von Datenschutzeinstellungen transparent gegenüber den Nutzern beschreibt, damit diese solche treuhänderischen Dienste in informierter Weise auf Basis ihres Einverständnisses in Anspruch nehmen. Die Freiwilligkeit des Einverständnisses verdient besondere Beachtung, damit insbesondere Anbieter mit einer markbeherrschenden Stellung ihre Position gegenüber Nutzer nicht missbrauchen. Hierzu gehört auch eine Bündelung von eigenen erbrachten Telemediendiensten mit treuhänderischen Diensten zur Verwaltung persönlicher Information durch ein- und denselben Dienst.

Abs. 2 – Verbot der Zweckänderung

Dienste zur Verwaltung von Einwilligungserklärungen dürfen Daten von Endnutzern, die sie im Rahmen der Diensteerbringung erhalten, nicht für andere Zwecke verwenden. Das gesetzliche Verbot der Zweckänderung untermauert die Bedeutung von Datentreuhändern im Bereich der Nutzerdatenverwaltung als eine neutrale Stelle, die unabhängig von Interessen anderer Telekommunikations- und Telemediendiensteanbieter fungiert. Ohne ein materiell-rechtliches Verbot einer Zweckänderung wird der Grundgedanke eines Datentreuhandmodells konterkariert.[19]

Abs. 4 - Technische Umsetzung der Nutzerentscheidung

Die Norm muss gewährleisten, dass insbesondere Browseranbieter auch an die Einstellungen der Datenschutzvorgaben des Nutzers – sei es eine Einwilligung zum Tracking oder der Ablehnung - gebunden und diese nicht beim Ausspielen seiner Angebote ignoriert. Dem kann eine normative Vorgabe Rechnung tragen, die in Verkehr gebrachte Software zum Betrieb von Netzkommunikation dazu verpflichtet, Diensten

[19] Eingehend dazu Schwartmann/Weiß (Hrsg.), Datenmanagement- und Datentreuhandsysteme, Ein Arbeitspapier der Fokusgruppe Datenschutz der Plattform Sicherheit, Schutz und Vertrauen für Gesellschaft und Wirtschaft im Rahmen des Digital-Gipfels 2020.

zur Einwilligungsverwaltung eine Schnittstelle zur Übermittlung der Einwilligungsentscheidung des Nutzers zu bieten.

Im Falle der Einwilligung des Nutzers müssen Speicherung und Zugriff auf Informationen auf dem Endgerät technisch ermöglicht werden. Der Weg über eine verpflichtende Schnittstelle entspricht der Empfehlung der DEK, die in ihrem Abschlussgutachten ausführt: „PMT/PIMS können nur dann verlässlich arbeiten, wenn eine Kooperation mit allen betroffenen Verantwortlichen sichergestellt ist. Dabei ist eine hinreichende Breitenwirkung nur durch eine – unter sachgerechten Bedingungen stehende – rechtliche Verpflichtung für Verantwortliche im Sinne der DS-GVO zu erreichen, die Kontrolle des Zugangs zu personenbezogenen Daten durch PMT/PIMS zu ermöglichen und beispielsweise sicherzustellen, dass jede datenschutzrelevante Information das PMT/PIMS erreicht und das PMT/PIMS in Bezug auf alle personenbezogenen Daten die Interessen der betroffenen Person wahrnehmen kann.“[20]

Sofern der Gesetzgeber vor einer solchen Verpflichtung der Browseranbieter zurückschreckt, müsste er sie über Marktzugangsregeln dazu verpflichten, Browser nur so in den Verkehr zu bringen, dass sie PIMS allgemein und Dienste zur Einwilligungsverwaltung im Speziellen nicht behindern.

Zu § 27 u. 28 TTDSG

§ 28 (ex-27) Abs. 1 TTDSG regelt die Zuständigkeit der oder des BfDI als Aufsichtsbehörde, soweit es sich um Anforderungen handelt, die auf die Verarbeitung personenbezogener Daten natürlicher oder juristischer Personen gerichtet sind. Eine Regelung zur Zuständigkeit hinsichtlich Diensten zur Einwilligungsverwaltung ist davon nicht umfasst und bedarf einer Ergänzung. Durch die Zuständigkeit der oder des BfDI wird gewährleistet, dass die Aufsicht zukünftig umfassend, d. h. auch im Hinblick auf die Verhängung von Sanktionen, durch den oder die BfDI als unabhängiger Datenschutzaufsichtsbehörde erfolgt.

[20] Gutachten der Datenethikkommission, S. 134.