Der Consent-Fatigue entgegenwirken

Peter Hense & Franziska Boehm
Arbeitsgruppe DSGVO am TUM Think Tank

1. Kontext

Das Ziel unseres Reformvorschlags besteht darin, der permanenten Konfrontation von Nutzerinnen und Nutzern mit Einwilligungsabfragen über Consent-Management-Plattformen (CMPs), der sogenannten Cookie-Banner-Fatigue, entgegenzuwirken. Das Gesetz soll dazu dienen, den klaren Willen der Nutzerinnen und Nutzer mittels standardisierter technischer Signale verbindlich zu kommunizieren und durch Verantwortliche respektieren zu lassen, ohne dass Irreführung durch „Dark Patterns", Umgehung durch technische Tricks wie Fingerprinting, serverseitiges Tracking, First-Party-Cloaking („Hidden Tracking") oder Belästigung durch permanentes Infragestellen des Nutzerwillens („CMP Burnout") dies deutlich erschweren. Angestrebt wird eine Vorschrift, die das bereits seit Jahrzehnten gewünschte, aber nie konsequent verfolgte Ziel erreicht, nämlich die Einwilligung, die Ablehnung der Einwilligungsanfrage, die Rücknahme der Einwilligung sowie das Widerspruchsrecht gemäß Art. 21 Abs. 2 DSGVO durch browserbasierte oder betriebssystemseitige Präferenzsignale, etwa nach dem Vorbild des Global Privacy Control (GPC), rechtsverbindlich zu ermöglichen.

Gegenüber dem von der EU-Kommission vorgelegten Omnibus-Entwurf des Art. 88b weist dieser Entwurf in mehreren Punkten signifikante Unterschiede auf.

Erstens soll die Kommission befugt sein, Durchführungsrechtsakte zur Festlegung technischer Spezifikationen zu erlassen. Dies erfolgt anstelle einer Delegation der Standardausarbeitung an die europäischen Standardisierungsorganisationen ETSI, CEN oder CLC. Eine solche Delegation könnte potenziell zu einem ineffektiven, langjährigen Prozess mit erheblichen Einflussmöglichkeiten diverser Akteure, insbesondere der Werbewirtschaft und großer Plattformbetreiber, auf die Standardisierungsorganisationen führen, was die zügige und nutzerfreundliche Umsetzung gefährden würde. Die Erfahrungen mit dem Transparency and Consent Framework (TCF) des IAB Europe, das trotz formaler Standardisierung von der belgischen Datenschutzaufsicht als rechtswidrig eingestuft wurde, verdeutlichen die Risiken einer industriedominierten Standardentwicklung. Durch die Verankerung der Spezifikationskompetenz bei der Kommission wird sichergestellt, dass technische Vorgaben zeitnah, einheitlich und im Einklang mit den Schutzzielen der DSGVO entwickelt werden können. Sofern die Kommission dazu willens und in der Lage ist.

Zweitens sollen bei Vorliegen eines aktiven Ablehnungssignals sämtliche Tracking-Technologien, namentlich Cookies, Zählpixel, Browser-Fingerprinting, Local-Storage-Mechanismen, ETags sowie darauf aufbauendes Profiling, automatisch blockiert werden, ohne dass eine weitere Nutzerinteraktion erforderlich ist. Damit wird das Ausweichen auf alternative Nachverfolgungstechnologien praktisch unterbunden und die Wirksamkeit des Nutzerwillens technisch durchgesetzt. Diese automatische Blockierung folgt dem Prinzip „Privacy by Design und Default" gemäß Art. 25 Abs. 1, 2 DSGVO und verhindert, dass Verantwortliche durch ständig neue technische Verfahren die Nutzerentscheidung faktisch aushebeln. Die technische Durchsetzung auf Browserebene stellt

zudem sicher, dass auch bei fehlerhafter oder böswilliger Implementierung auf Serverseite der Nutzerwille gewahrt bleibt, da das Signal bereits vor der Datenübertragung wirksam wird.

Drittens sollen die Regeln für alle Verantwortlichen gelten, einschließlich Medienanbieter und sonstiger Inhalteanbieter, und nicht nur für Anbieter von Webbrowsern. In Konsequenz dessen werden beispielsweise auch In-App-Browser, proprietäre Anwendungsumgebungen, Smart-TV-Oberflächen sowie eingebettete Webviews in mobilen Applikationen erfasst. Diese umfassende Adressierung ist notwendig, da Tracking längst nicht mehr auf klassische Webbrowser beschränkt ist, sondern zunehmend in geschlossenen Ökosystemen stattfindet, die sich einer effektiven Nutzerkontrolle entziehen. Eine Ausnahme für kleine und mittlere Unternehmen (KMU) ist nicht vorgesehen, um eine einheitliche Durchsetzung des Nutzerwillens unabhängig von der Unternehmensgröße sicherzustellen. Die Unternehmensgröße ist kein geeigneter privilegierender Faktor, sondern ein Einfallstor für Umgehungskonstruktionen. Dies ist auch aus Gründen der technischen Praktikabilität geboten, da die Signalverarbeitung keine aufwendige Implementierung erfordert und regelmäßig durch Standardsoftware, SDKs, Content-Management-Systeme oder Hosting-Anbieter automatisiert bereitgestellt werden kann.

2. Reformvorschlag

Vor diesem Hintergrund hat die Arbeitsgruppe den folgenden Vorschlag eines Artikels zu technischen Signalen erarbeitet.

(1) Die betroffene Person hat das Recht, ihr Recht auf informationelle Selbstbestimmung/Datenschutz/Privatsphäre durch technische Signale auszuüben, die auf internationalen Standards oder von der Kommission ausgearbeiteten technischen Spezifikationen nach Abs. 2 beruhen.

(2) Die Europäische Kommission kann Durchführungsrechtsakte zur Festlegung technischer Spezifikationen für die Anforderungen nach Abs. 1 erlassen, um die:

i. Interoperabilitätsanforderungen für die Übertragung des Signals zu definieren,

ii. Mindestanforderungen an Anbieter von Endnutzer-Software festzulegen, insbesondere die Bereitstellung einer technischen Möglichkeit zur Aktivierung und Übermittlung des Signals, eine klare und leicht auffindbare Option zur Aktivierung des Signals, die optische Kennzeichnung des aktiven Status des Signals für Nutzer.

(3) Verantwortliche sind verpflichtet:

i. ein nach Absatz 1 gesendetes Signal als wirksamen Widerspruch gegen Verarbeitungen gemäß Art. 21 Abs. 2 (Direktwerbung inklusive Profiling), als Einwilligung, als Ablehnung oder Widerruf einer Einwilligung zu behandeln,

ii. gegenüber Empfängern durch technisch-organisatorische Maßnahmen sicherzustellen, dass das nach Absatz 1 gesendete Signal durch diese effektiv beachtet und umgesetzt wird,

iii. solange ein aktives Signal nach Abs. 1 vorliegt, keine weitere Einwilligung zu Zwecken der Direktwerbung oder Profilbildung einzuholen. Insbesondere darf keine Consent-Management-Plattform

(Cookie-Banner oder vergleichbares Einwilligungsinterface) für diese Zwecke angezeigt werden, außer zur Bestätigung des aktiven Signals,

iv. bei der technischen Umsetzung Manipulationssicherheit nach dem Stand der Technik zu gewährleisten, Priorität gegenüber anderen Tracking- oder Profiling-Mechanismen sicherzustellen sowie zu gewährleisten, dass bei aktivem Signal Tracking-Technologien (z. B. Cookies, Pixel, Fingerprinting) und Profiling automatisch blockiert werden, ohne dass eine Nutzerinteraktion erforderlich ist,

v. Nutzer mit aktiviertem Signal nicht zur Deaktivierung des Signals auffordern, z.B. durch Banner, Pop-ups oder Dark Patterns.

3. Einordnung

Nachfolgend findet sich eine zusammenfassende Übersicht der Vor- und Nachteile des Vorschlags zur weiterführenden Diskussion.

Vorteile

- **Effektive Durchsetzung des Nutzerwillens:** Entlastung der Betroffenen durch das Wegfallen von wiederholten Einwilligungsabfragen über Consent-Management-Plattformen (CMPs). Durch die automatische Blockierung von Tracking-Technologien bei Vorliegen eines Ablehnungssignals wird der Nutzerwille technisch durchgesetzt, anstatt lediglich auf die freiwillige Compliance der Verantwortlichen zu vertrauen. Dies entspricht dem Grundsatz „Privacy by Design&Default" gemäß Art. 25 Abs. 1, 2 DSGVO und macht die Einwilligungsentscheidung erstmals technisch wirksam.

- **Entgegenwirken der sogenannten Cookie-Banner-Fatigue:** Die standardisierte Signalübermittlung auf Browser- oder Betriebssystemebene ermöglicht eine einmalige, zentrale Präferenzfestlegung, die gegenüber allen Verantwortlichen gilt. Nutzerinnen und Nutzer werden nicht länger auf jeder Website erneut mit manipulativen Einwilligungsdialogen konfrontiert, was die Nutzerfreundlichkeit erheblich steigert und die informierte Selbstbestimmung stärkt.

- **Technologieneutrale Erfassung aller Tracking-Methoden:** Der Vorschlag adressiert nicht nur klassische Cookies, sondern auch Fingerprinting, Zählpixel, Local-Storage-Mechanismen und weitere Nachverfolgungstechnologien. Damit wird verhindert, dass Verantwortliche durch technische Innovation die Regelung unterlaufen, und es entsteht ein zukunftsfähiger Rechtsrahmen.

- Schnelle und einfach skalierbare **Überprüfung durch Datenschutzbehörden** bei technischem Sachverstand möglich.

- **Rechtsklarheit und einheitliche Anwendung ohne Fragmentierung für Betroffene und Verantwortliche:** Einheitliche rechtliche und technische Regelung für alle Verantwortlichen. Die Zuständigkeit der Kommission für technische Spezifikationen sowie der Verzicht auf wirkungslose KMU-Ausnahmen gewährleisten eine harmonisierte Umsetzung im gesamten Binnenmarkt. Dies schafft Rechtssicherheit für Unternehmen und verhindert regulatorische Arbitrage zwischen Mitgliedstaaten.

- **Umfassender Anwendungsbereich über klassische Browser hinaus:** Die Einbeziehung von In-App-Browsern, IoT, Smart-TV-Oberflächen, eingebetteten Webviews und proprietären Anwendungsumgebungen trägt der technischen Realität Rechnung, dass Tracking längst in geschlossenen Ökosystemen stattfindet. Damit wird eine effektive Nutzerkontrolle auch außerhalb des klassischen Webs ermöglicht.

Nachteile

- **Abhängigkeit von der Handlungsfähigkeit der Kommission:** Die Verlagerung der Spezifikationskompetenz auf die Kommission setzt deren Widerstandsfähigkeit gegenüber Lobbyeinflüssen sowie ausreichende technische Expertise voraus. Die bisherigen Erfahrungen mit Art. 12 Abs. 8 DSGVO, der seit über sieben Jahren keine standardisierten Icons für Datenschutzinformationen hervorgebracht hat, mahnen zur Skepsis hinsichtlich der zeitnahen Umsetzung. Ohne politischen Druck und klare Fristen besteht das Risiko, dass auch diese Spezifikationen auf unbestimmte Zeit ausbleiben.

- **Weitreichende Auswirkungen auf Produktdesign und Softwareentwicklung:** Der Vorschlag adressiert nicht nur datenverarbeitende Verantwortliche nach Art. 24 DSGVO, sondern stellt auch neue Anforderungen an Browser-Hersteller, Betriebssystementwickler und Anbieter von Anwendungsumgebungen. Dies erfordert eine grundlegende Anpassung von Softwarearchitekturen und Entwicklungsprozessen, was höhere Implementierungsaufwände und mehr regionsspezifische Versionierungen von Software und Produkten bedeuten kann.

- **Eingeschränkte Flexibilität für mitgliedstaatliche Sonderinteressen:** Die einheitlichen Regeln ohne Ausnahmen für bestimmte Branchen oder Unternehmensgrößen reduzieren den Spielraum für mitgliedstaatliche Anpassungen, die möglicherweise aus protektionistischen Motiven gewünscht werden. Allerdings ist das Datenschutzrecht systematisch der falsche Ort für Journalismus- oder Mediensubventionen, die über andere Instrumente wie Beihilfen oder Steuerrecht adressiert werden sollten.

- **Fortbestehende Durchsetzungsdefizite trotz klarer Regeln:** Auch technisch verbindliche Compliance-Vorgaben können durch Umgehungstechniken ausgehebelt werden, etwa durch Ignorieren der Signale, serverseitiges Tracking vor der Signalauswertung oder durch Consent Signal Fraud wie bei beim Industriestandard TCF beobachtet. Recht ist nicht gleich Rechtsdurchsetzung, und ohne effektive Aufsichtsmechanismen sowie technische Kontrollmöglichkeiten bleibt die Gefahr systematischer Nichteinhaltung bestehen.

- **Schwierige Abstimmung mit internationalen Standards:** Eine Harmonisierung mit internationalen Projekten wie dem Global Privacy Control (GPC) ist wünschenswert, aber strukturell herausfordernd, da insbesondere US-amerikanische Vorgaben und Standards auf anderen rechtlichen Grundlagen basieren und teilweise abweichende Schutzkonzepte verfolgen. Zugleich dürfen die von der Kommission erlassenen Spezifikationen nicht konsensorientierte Standardisierungsprozesse bei europäischen Standardisierungsorganisationen wie CEN oder ETSI verdrängen oder langfristig obsolet machen, um die technische Innovationsfähigkeit und internationale Anschlussfähigkeit zu wahren.

ARBEITSGRUPPE DSGVO

Die Arbeitsgruppe DSGVO am TUM Think Tank bringt Expertinnen und Experten aus Wissenschaft, Praxis, Aufsicht und Zivilgesellschaft zur Weiterentwicklung der DSGVO zusammen. Dies ist einer von vier konkreten, rechtlich anschlussfähigen Reformbausteinen, die sowohl Datenschutz wirksamer machen als auch verantwortliche Datennutzung für Wirtschaft und Gesellschaft erleichtern.

Der TUM Think Tank bietet die organisatorische Plattform. Initiiert wurde die Arbeitsgruppe von Kai Zenner, Max Schrems, Boris Paal und Markus Siewert.

INSTITUTION

TUM Think Tank | Hochschule für Politik München |
Technische Universität München

DISCLAIMER

Der vorliegenden Reformvorschlag (Version 1.0) wird von einer Mehrheit der Arbeitsgruppe mitgetragen, auch wenn nicht alle Mitglieder allen Teilen gleichermaßen zustimmen und durchaus auch abweichende Meinungen existieren.

Die Vorschläge verstehen sich nicht als Endpunkt, sondern als Ausgangspunkt für weiterführende Diskussionen. In den kommenden Wochen und Monaten wird die Arbeitsgruppe diese Vorschläge – insbesondere vor dem Hintergrund der derzeit teilweise kontrovers geführten Debatten zum Digital Omnibus – weiterentwickeln und zusätzliche Reformbausteine ausarbeiten.

Die in diesem Bericht geäußerten Inhalte und Ansichten geben ausschließlich die Meinung der Autoren wieder und sind nicht dem TUM Think Tank als Institution oder seinen Mitgliedern zuzuschreiben.

KONTAKT

tumthinktank@hfp.tum.de
https://tumthinktank.de

Mitglieder der Arbeitsgruppe DSGVO

Christoph Bausewein | Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V.

Linda Bienemann | Persönliche Referentin Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI)

Franziska Boehm | FIZ-Karlsruhe & Karlsruher Institut für Technologie (KIT)

Stefan Brink | Wissenschaftliches Institut für die Digitalisierung der Arbeitswelt (WIDA) / Berlin

Thomas Fuchs | Hamburgischer Beauftragter für Datenschutz und Informationsfreiheit (HmbBfDI)

Niko Härting | HÄRTING & Deutscher Anwaltverein

Peter Hense | Spirit Legal Rechtsanwaltsgesellschaft mbH

Boris Paal | Technische Universität München

Frederick Richter | Stiftung Datenschutz

Max Schrems | noyb

Louisa Specht-Riemenschneider | Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI)

Christiane Wendehorst | Universität Wien

Michael Will | Bayerisches Landesamt für Datenschutz (BayLDA)

Kai Zenner | MEP Axel Voss, Europäisches Parlament & TUM Think Tank