

**Gegenposition zum
Verbändebrief der
Werbewirtschaft aus der
evidenzbasierten
Regulierungsforschung
an die Bundesregierung**

Bundesministerium des Innern
Bundesministerium für Wirtschaft und Energie
Bundesministerium der Justiz und für Verbraucherschutz
Bundesministerium für Digitales und Staatsmodernisierung
Bundeskanzleramt
Der Beauftragte der Bundesregierung für Kultur und Medien
per E-Mail

Berlin, 24. April 2026

Daten als Wettbewerbsvorteil sichern: Für eine echte Stärkung der europäischen Datenökonomie durch einen funktionierenden Wettbewerb

Sehr geehrter Herr Bundesminister Dobrindt,
sehr geehrte Frau Bundesministerin Reiche,
sehr geehrte Frau Bundesministerin Dr. Hubig,
sehr geehrter Herr Bundesminister Dr. Wildberger,
sehr geehrter Herr Bundesminister Frei,
sehr geehrter Herr Staatsminister Dr. Weimer

Wir schließen uns dem Ziel des [offenen Briefs](#) an, den 19 Verbände der deutschen (Werbe-)Wirtschaft am 13. März an Sie adressierten:

„Damit Europa und Deutschland wieder wettbewerbsfähiger werden, müssen wir Daten nicht nur schützen, sondern sie aktiv als Schlüssel für Innovation, Wertschöpfung und Wohlstand begreifen. Und wir müssen sie vor allem nutzen. Der Koalitionsvertrag der Bundesregierung formuliert hierauf die richtige Antwort: ‘Wir wollen eine Kultur der Datennutzung und des Datenteilens, die Datenökonomie etabliert, auf Innovation setzt und Grund- und Freiheitsrechte schützt.’“¹

Wir sehen einen anderen Weg, dieses Ziel zu erreichen: Die Werbewirtschaft argumentiert, es gäbe einen Zielkonflikt zwischen einer Kultur der Datennutzung und datenbasierter Innovation einerseits und dem Schutz von Grund- und Freiheitsrechten andererseits. Beide Interessen schließen sich aber nicht gegenseitig aus, sondern bedingen einander. Nicht nur der Koalitionsvertrag der Bundesregierung sieht das so. Auch die EU-Kommission hat sich für ihren Digitalen Omnibus das Ziel gesetzt, „sicherzustellen, dass die Einhaltung der (europäischen digitalen Rechts-) Vorschriften zu geringeren Kosten erfolgt, die gleichen Ziele erreicht und verantwortungsvollen Unternehmen einen Wettbewerbsvorteil verschafft.“²

Aktuell koordiniert sich die Werbewirtschaft auf eine Weise, die dieses Ziel nicht erreicht. Sowohl die demokratische Schutzidee des Datenschutzgrundrechts gemäß Art. 8 ECFR als auch die liberalen Wirtschaftsordnungen der EU-Mitgliedstaaten bauen auf dem Grundsatz auf, dass Verbraucher:innen informierte Entscheidungen treffen können. Hierfür sind die in

1

https://table.media/assets/berlin/2026-03-13_verbandsübergreifende-papier-zum-digital-omnibus.pdf.

² <https://digital-strategy.ec.europa.eu/de/library/digital-omnibus-regulation-proposal>.

Artikel 88b Digitaler Omnibus-Entwurf eingeführt, von der Werbewirtschaft aber kritisierten Einwilligungsgaganten, die in Wissenschaft und Praxis bisher einzig bekannte Lösung.

Informierte Verbraucherentscheidungen als Voraussetzung für einen funktionierenden Datenmarkt

Das Datenschutzrecht stellt sicher, dass Individuen selbstbestimmt entscheiden können. Das ist eine Grundvoraussetzung für eine freiheitlich verfasste Demokratie. Der Skandal um Cambridge-Analytica zeigt exemplarisch, wie politische Akteure personenbezogene Daten nutzen können, um Wähler:innen gezielt zu beeinflussen.³ Aber auch weniger sichtbare Fälle verdeutlichen die Relevanz: Wenn Bürger:innen damit rechnen müssen, dass ihre Mobilfunknummer auf Datenmarktplätzen gehandelt wird, wie es mit der Mobilfunknummer von Friedrich Merz vor seiner Wahl zum Bundeskanzler geschehen ist,⁴ kann das ihre digitale Kommunikation hemmen und ihre Grundrechte untergraben. Negative Auswirkungen können selbst in stabilen Demokratien schneller eintreten, als man erwartet. So kauft und verknüpft die US-Behörde Immigration and Customs Enforcement (ICE) millionenfach Standortdaten mit Einwanderungs-, Finanz- und Social-Media-Daten, um „Zielpersonen“ zu identifizieren – häufig ohne richterliche Kontrolle oder wirksame Schutzmechanismen.⁵ Jüngste Recherchen zeigen, dass detaillierte Standortdaten auch europäischer Bürger durch Datenhändler weltweit zum Kauf angeboten werden.⁶

Auch die freie Marktwirtschaft funktioniert nur, wenn Verbraucher:innen informierte und selbstbestimmte Entscheidungen treffen können. Nur wenn sie in der Lage sind, die (Datenschutz-) Qualität digitaler Dienste einzuschätzen, können sie sich bewusst für bessere oder günstigere Angebote entscheiden. Erst dann können Unternehmen in Wettbewerb miteinander treten. Fehlt diese Transparenz, entsteht ein sogenannter Market for Lemons: Anbieter schlechterer Qualität haben einen Vorteil, weil ihre Angebote für Nutzer:innen nicht klar von besseren zu unterscheiden sind. Dadurch geraten hochwertige Anbieter unter Druck und müssen ihre Qualität senken, um mithalten zu können. So entsteht eine Abwärtsspirale, in der sich die Qualität insgesamt verschlechtert. Zwar versuchen gesetzliche Mindestanforderungen, diese Entwicklung zu begrenzen. Da sie jedoch der ökonomischen Logik entgegenstehen, werden sie in der Praxis umgangen oder nur formal erfüllt – ohne die beabsichtigte Schutzwirkung zu entfalten.

Diese Situation liegt aktuell bei der Verarbeitung personenbezogener Daten vor, vor allem im Bereich der Werbewirtschaft. Die „informierte Einwilligung“ wird in der Praxis oft nur formal umgesetzt und informiert Verbraucher:innen nicht tatsächlich. Ihnen ist es aufgrund der aktuellen Umsetzung der Einwilligung weder möglich, bei digitalen Diensten das jeweilige Datenschutzniveau zu erkennen, noch diese zu unterscheiden. Wir alle klicken jeden Tag Cookie-Banner weg, ohne zu verstehen, wofür der jeweils genutzte Dienst unsere Daten konkret verarbeitet, geschweige denn welche Vorteile und Risiken für uns damit verbunden

³ Siehe unter https://www.bfdi.bund.de/SharedDocs/Pressemitteilungen/DE/2018/03_Facebook.html.

⁴ Siehe unter <https://www.spiegel.de/politik/sicherheitsrisiko-datenhaendler-verkaufen-die-nummern-von-friedrich-merz-oder-seiner-minister-a-bae3b69f-66ba-4fd8-a116-7b183b058db7>.

⁵ Siehe etwa unter <https://www.zeit.de/digital/internet/2026-01/usa-behoerde-ice-ueberwachung-daten>.

⁶ Siehe unter <https://netzpolitik.org/2025/databroker-files-das-wichtigste-zur-spionage-gefahr-durch-handy-standort-daten-in-der-eu/>.

wären. Zahlreiche Studien aus der Wissenschaft bestätigen, dass aktuelle Cookie-Banner nicht verständlich sind.⁷ Demnach ziehen Verbraucher:innen zwar datenschutzfreundliche Dienste solchen mit höheren Risiken vor.⁸ Sie können diese aber nicht erkennen und sich deswegen auch nicht für sie entscheiden. Tatsächlich werden Cookie-Banner so uninformiert weggeklickt, dass man kaum von einer „informierten“ Einwilligung im Sinne des Gesetzes sprechen kann.⁹

Verbraucher:innen sind bei der Nutzung von digitalen Diensten, wie etwa beim Besuch von Websites, vor allem aus folgenden Gründen nicht in der Lage, die Informationen in einer für sie entscheidungsrelevanten Weise zu nutzen:¹⁰

- Aufgrund der extremen Häufigkeit der Anfragen,
- des ungünstigen Augenblicks der Anfrage (sie möchten den Dienst nutzen anstatt das „Kleingedruckte“ lesen),
- des geringen Platzes für die Information und
- der unzureichenden Darstellung der Information.

Einwilligungsagenten als bisher einzige Lösung für informierte Entscheidungen

Verantwortlich für die mangelhafte Umsetzung der informierten Einwilligung sind weder die Verbraucher:innen noch der Gesetzgeber, etwa weil er überhaupt das Erfordernis einer Einwilligung eingeführt hat. Denn weitere Studien zeigen, dass sich Verbraucher:innen sehr heterogen entscheiden, sobald sie die verschiedenen Zwecke, für die Dienste ihre Daten verarbeiten, und die damit verbundenen Vorteile und Risiken verstehen.¹¹ Die Einwilligung ist also grundsätzlich das richtige Instrument, weil es den individuellen Bedürfnissen der Verbraucher:innen am besten Rechnung trägt und sie nicht paternalisiert.

Die Werbewirtschaft schlägt in ihrem offenen Brief vor, stattdessen auf das Erfordernis der Einwilligung insgesamt zu verzichten. Zwar könnte der Gesetzgeber in der Tat risikoarme Verarbeitungszwecke privilegieren und einem Opt-Out- statt dem strengen Opt-In-Verfahren bei der Einwilligung unterwerfen. Beim Opt-Out müssen Dienste nicht auf die Einwilligung warten, sondern dürfen die Daten verarbeiten, bis ein/e Verbraucher:in widerspricht. Aber damit Verbraucher:innen eine solche Widerspruchsmöglichkeit wirksam, das heißt einfach,

⁷ Siehe etwa (Un)Informed Consent: Studying GDPR Consent Notices in the Field. Utz, C., Degeling, M., Fahl, M., Schaub, F., and Holz, T. 2019. In Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19). Association for Computing Machinery, New York, NY, USA, 973–990. <https://doi.org/10.1145/3319535.3354212>.

⁸ The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study, Janice Y. Tsai, Serge Egelman, Lorrie Cranor, Alessandro Acquisti, Information Systems Research Vol. 22, No. 2, June 2011, pp. 254–268.

⁹ How Effectively Do Consent Notices Inform Users About the Risks to Their Fundamental Rights? Grassl, P., Gerber, N., & Grafenstein, M. v. (2024). European Data Protection Law Review, 10(1), 96-104. DOI: 10.21552/edpl/2024/1/14.

¹⁰ From consent to control by closing the feedback loop: Enabling data subjects to directly compare personalized and non-personalized content through an On/Off toggle. Smieskol, P., Jakobi, T., & von Grafenstein, M. (2025). Computer Law & Security Review, 59, 1-22, November 2025; Privacy icons as a component of effective transparency and controls under the GDPR: effective data protection by design based on art. 25 GDPR. Grafenstein, M. v., Kiefaber, I., Heumüller, J., Rupp, V., Graßl, P., Kolless, O., & Puzst, Z. (2024). Computer Law & Security Review, 52. DOI: 10.1016/j.clsr.2023.105924.

¹¹ From Cookie Banners to Consent Agents: A Comparative Study on Informed Consent and Consent Rates. Gerber, N., Grassl, P., v. Grafenstein, M. (in review). Computer Law & Security Review.

ausüben können, ist auch diese zu Beginn der Nutzung des Dienstes und damit in einem Cookie-Banner zu ermöglichen. Bei der Frage Opt-In vs. Opt-Out geht es also nur um die Voreinstellung und damit die Wahrscheinlichkeit, ob eine Person einwilligt oder widerspricht. Opt-Out-Verfahren lösen deshalb, anders als es der offene Brief der Werbewirtschaft nahelegt, das Problem uninformatierter Entscheidungen nicht.

Das Problem der Uninformiertheit beruht vielmehr darauf, wie Entscheidungen herbeigeführt werden. Sogenannte Einwilligungsagenten sind die bisher in Wissenschaft und Praxis einzig bekannte Lösung, um die zuvor aufgezählten Probleme zu lösen. Die Behauptungen der Werbewirtschaft in ihrem offenen Brief sind insofern nicht richtig. Durch die Einbindung von Einwilligungsagenten findet sehr wohl eine individuelle und kontextspezifische Interaktion zwischen digitalem Dienst und seinen Nutzer:innen statt:

In einem Agenten können Verbraucher:innen zentral und vorab die typischen Informationen einsehen und auf dieser Basis Vorentscheidungen treffen. Sobald sie eine konkrete Website besuchen oder einen anderen digitalen Dienst nutzen, gibt der Agent diese Voreinstellungen an den Dienst weiter, wobei Verbraucher:innen ihre Voreinstellungen über eine dynamische Schaltfläche anpassen können. Der Dienst hat dabei die Gelegenheit, die Verbraucher:innen über sein konkretes Datenschutzniveau zu informieren.

Das Neue bei Einwilligungsagenten ist, dass sich Verbraucher:innen mit Hilfe des durch ihn gestuften Informations- und Entscheidungsprozesses auf das Wesentliche konzentrieren können und nicht mehr bei jedem Dienst zum Wegklicken gezwungen werden, weil die dynamische Schaltfläche nach gewisser Zeit von selbst verschwindet.

Auch die Behauptung, es sei "im offenen Internet technisch faktisch nicht realisierbar", die Ablehnung einer Einwilligungsanfrage für sechs Monate zu speichern, ist nicht richtig. Denn diese Pflicht bezieht sich nur auf den jeweiligen Browser, mit dem Verbraucher:innen eine Website besuchen und in dem die Ablehnung der Einwilligungsanfrage über ein Cookie gespeichert wird. Diese Pflicht stellt sicher, dass Websites und andere Dienste nicht, wie heute häufig allgemeine Praxis, immer wieder nach der Einwilligung fragen, obwohl man sie längst abgelehnt hat. Eine erneute Nachfrage ist indes dann erlaubt, wenn der Dienst seit dem letzten Besuch der/s Verbraucher:in das Datenschutzniveau verbessert hat. Denn dann liegt eine neue Entscheidungsgrundlage vor, aufgrund derer sie/er ihre Einwilligung doch erteilen könnte. Andersherum gilt es genauso: Hat sich das Datenschutzniveau seit dem letzten Besuch verschlechtert, etwa weil die Daten jetzt nicht mehr innerhalb der EU, sondern außerhalb gespeichert werden, ist dies den Verbraucher:innen anzuzeigen, gerade wenn sie zuvor ihre Einwilligung erteilt hatten. Auch in diesem Fall hat sich dadurch die Entscheidungsgrundlage geändert, so dass Verbraucher:innen ihre Einwilligung widerrufen können müssen. Insofern ist Art. 88a Abs. 4 Digitaler Omnibus zu schärfen, aber nicht, wie es die Werbewirtschaft in ihrem offenen Brief schlussfolgert, abzuschaffen.

Einwilligungsagenten ermöglichen also gestufte Prozesse, über die Verbraucher:innen mehr Möglichkeiten, Zeit und vor allem mehr Aufmerksamkeit für eine informierte Entscheidung zur Verfügung haben. Studien zeigen, dass Verbraucher:innen unter diesen Bedingungen – anders als in aktuellen Cookie Bannern, wo fast alle Verbraucher:innen entweder auf den "Alles akzeptieren"- oder "Alles ablehnen"-Knopf klicken – granulare Entscheidungen für die verschiedenen Zwecke treffen. Dabei fällt die Zustimmung umso häufiger aus, je niedriger die Risiken bzw. je höher die Vorteile für sie sind. Zudem können Dienste die Chance einer

Zustimmung erhöhen, indem sie Verbraucher:innen bei der Nutzung des Dienstes über ein hohes Datenschutzniveau informieren – vorausgesetzt, es ist vorhanden.¹²

Einwilligungsagenten sind zudem die bisher einzig bekannte Lösung, um Verbraucher:innen einen Überblick über die von ihnen erteilten Einwilligungen zu geben. Man stelle sich die *aktuelle* Situation in Bezug auf Rechtsgeschäfte der Offline-Welt vor: Man schließt einen Vertrag ab, aber bekommt kein eigenes Exemplar ausgehändigt. In der digitalen Welt weiß niemand, welchen Diensten sie wann welche Einwilligungen gegeben hat. Auf dieser Basis werden jedoch massenhaft Informationen über uns gesammelt und in diversesten Kontexten genutzt. Hierüber keinen Überblick zu haben, es nicht bestreiten zu können, wenn ein Dienst das Vorliegen einer Einwilligung behauptet, ist unter rechtsstaatlichen Gesichtspunkten absurd. Dagegen ist es nicht “absurd”, wie es die Werbewirtschaft formuliert, wenn der Gesetzgeber diesen Zustand beseitigen möchte.

Die von Art. 88b Digitaler Omnibus vorgesehene Lösung ist kein unausgereiftes Konzept. Auch das behauptet die Werbewirtschaft in ihrem offenen Brief. Die Lösung ist nicht nur technisch machbar, sondern in unterschiedlichen Projekten bereits entwickelt worden. Zu nennen sind die technischen Kernkonzepte, die in den Projekten EMIDD und DaSKITA an der TU Berlin entwickelt wurden;¹³ die Spezifikation Advanced Data Protection Control (ADPC), die die Nichtregierungsorganisation NOYB mit der Universität Wien entwickelt hat;¹⁴ bereits existierende und funktionsfähige Anwendungen wie der Consent-O-Mat der Aarhus Universität,¹⁵ der “Super Agent” der portugiesischen Design-Agentur OCD,¹⁶ der Agent “Taste” der französischen Consent Management Plattform Axeptio;¹⁷ oder der “Consenter” der akademischen Ausgründung Law & Innovation, der auf vielen der vorgenannten Konzepte aufbaut. Es hat sich also längst ein Ökosystem entwickelt, das diese Lösungen vorantreibt. Digitale Dienste können solche Lösungen bereits heute bei sich integrieren oder auf Basis der zugrunde liegenden und frei zugänglichen Veröffentlichungen nachbauen.

Informierte Entscheidungen fördern Vertrauen und damit auch Einwilligungsraten und Wettbewerbsvorteile

Über die Transparenz, die agenten-gestützte Einwilligungsprozesse ermöglichen, realisiert sich für rechtskonforme Dienste zum ersten Mal der Wettbewerbsvorteil, der mit Einführung der DSGVO und auch jetzt wieder mit dem Digitalen Omnibus versprochen wird. Dienste mit einem hohen Datenschutzniveau können sich von Diensten mit einem niedrigeren Niveau erfolgreich abgrenzen. Dabei profitieren selbst solche Verarbeitungssysteme, die aufgrund ihrer Komplexität mit grundsätzlich höheren Datenschutzrisiken einhergehen, wie vor allem das Online-Werbenetzwerk. Eine quantitative Langzeitfeldstudie mit ca. 1.000 Nutzern zeigt, dass die Einwilligungsraten auch für personalisierte Werbung bei fast allen verglichenen

¹² Evidence-based regulation: Article 88b Digital Omnibus – Increasing Consumer Awareness and Consent Rates through the Appropriate Design of Agent-Based Consent. Gerber, N., Grassl, P., Jakobi, T., v. Grafenstein, M. (pre-publication) available at <https://zenodo.org/records/19332894>.

¹³ <https://github.com/EMIDD-Projekt> sowie <https://www.tu.berlin/ise/projekte/daskita>.

¹⁴ <https://www.dataprotectioncontrol.org/>.

¹⁵ <https://consentomatic.au.dk/>.

¹⁶ <https://super-agent.com/>.

¹⁷ <https://taste.axept.io/>.

agenten-gestützten Einwilligungsmechanismen höher waren als beim Status Quo-Cookie Banner.¹⁸

Diese Studie zeigt freilich auch, dass es hierbei entscheidend darauf ankommt, wie diese Mechanismen konkret ausgestaltet werden. So erreichte der von der Forschungsgruppe favorisierte Mechanismus nicht nur die qualitativ beste Nutzungserfahrung, sondern auch die höchsten Einwilligungsraten mit einem Zuwachs von bis zu 20 % gegenüber dem Status Quo-Cookie Banner. Demgegenüber fiel die Einwilligungsrate bei einer anderen Testgruppe deutlich hinter die Einwilligungsrate des bisherigen Status Quo-Cookie Banners zurück. Bei dieser Testgruppe mussten die Teilnehmer ihre Voreinstellungen aus dem Agenten auf der besuchten Webseite noch einmal aktiv bestätigen. Diese Lösung erforderte also mehr Klicks als das bisherige Cookie Banner. Das führte dazu, dass – wohl aus Frustration – nur wenige Testpersonen erneut klickten und damit kaum Einwilligungen an die besuchte Testwebsite übergeben wurden. Es kommt also entscheidend darauf an, wie diese Einwilligungsprozesse konkret ausgestaltet werden.

Diese Ergebnisse sind nicht nur übertragbar auf ähnliche Fälle. Die Studienlage zeigt auch, dass sich die Informiertheit, das Vertrauen und damit auch die Einwilligungsraten mithilfe von agenten-gestützten Einwilligungsmechanismen weiter steigern lassen. Die Warnung der Werbewirtschaft, dass die wirtschaftlichen Folgen von Art. 88b Digitaler Omnibus gravierend wären, ist deshalb irreführend. Tatsächlich ist das Gegenteil der Fall: Art. 88b schafft nicht nur Vertrauen in die Verarbeitung personenbezogener Daten, es birgt auch ein sehr großes wirtschaftliches Potential.

Hintergründe der Kritik der Werbewirtschaft an Art. 88b Digitaler Omnibus

Worum geht es also bei der Kritik, die die Werbewirtschaft an Art. 88b Digitaler Omnibus übt? Wieso möchte sie die Einführung von agenten-gestützten Einwilligungsmechanismen verhindern, obwohl diese zu teils deutlich höheren Einwilligungsraten führen?

Drei Gründe erscheinen plausibel: Zum einen schafft Art. 88b ein Level Playing Field, indem Verbraucher:innen die Vorteile und Risiken der Verarbeitung ihrer Daten nicht nur verstehen, sondern die Dienste auch vergleichen können. Diese Transparenz stellt für Unternehmen einen Vorteil dar, die teils erheblichen Aufwand in die datenschutzkonforme Ausgestaltung ihrer Systeme investieren, sich aber mangels Transparenz nicht von anderen Diensten mit einem niedrigeren Datenschutzniveau abgrenzen können. Spiegelbildlich stellt die höhere Transparenz einen Nachteil für solche Unternehmen dar, deren Datenverarbeitungspraxis überdurchschnittlich hohe Datenschutzrisiken verursacht. Zu denken ist etwa an die großen Plattformen wegen der hohen Komplexität ihrer Systeme oder an die bereits genannten Data Broker, die personenbezogene Daten an beliebige Dritte verkaufen. Solange solche Risiken nicht offen gelegt werden, profitieren diese Unternehmen von derselben Einwilligungsrate wie Unternehmen, die einen hohen Aufwand betreiben, um ein hohes Datenschutzniveau zu gewährleisten. Es liegt nahe, dass Dienste, die von der bisherigen Intransparenz profitieren, nicht nur auf dem Markt sehr mächtig sind, sondern auch im offenen Brief zu Art. 88b ihre Handschrift hinterlassen.

¹⁸ Evidence-based regulation: Article 88b Digital Omnibus – Increasing Consumer Awareness and Consent Rates through the Appropriate Design of Agent-Based Consent. Gerber, N., Grassl, P., Jakobi, T., v. Grafenstein, M. (pre-publication) available at <https://zenodo.org/records/19332894>.

Ein weiterer Grund mag sein, dass mit den Anbietern von Einwilligungsagenten eine weitere Akteursgruppe hinzu kommt und dies den Interessenausgleich innerhalb des ohnehin schon komplexen Online-Werbenetzwerks noch komplizierter macht. Darauf scheint der Brief der Werbewirtschaft abzielen, wenn er davor warnt, dass Art. 88b "komplexe Verfahren zu schaffen" droht. Denn die Technik von Einwilligungsagenten ist – zumindest im Gegensatz zur Komplexität des Online-Werbesystems – keineswegs komplex. Aber in der Tat wird das Online-Werbesystem durch den zusätzlichen Akteur "Anbieter von Einwilligungsagenten" aus Sicht der Werbewirtschaft noch komplizierter. Diese Komplexitätszunahme scheint der Werbewirtschaft vor allem deshalb ein Dorn im Auge zu sein, weil dieser Akteur nicht primär wirtschaftliche Interessen, sondern zunächst die Interessen der Verbraucher wahrnimmt. Zu einem fairen Interessenausgleich gehören aber beide: die Werbenden und die Umworbenen. Das gilt erst recht, wenn eine konstruktive Zusammenarbeit ökonomische Werte eben nicht nur von der Wirtschafts- auf die Verbraucherseite schiebt, sondern zusätzlichen Mehrwert für alle erzeugt – wie die oben beschriebenen Studien zeigen.

Nichtsdestotrotz – und das ist der dritte Grund – verbreiten marktmächtige Akteure aus der Werbewirtschaft die Behauptung, dass die Einführung von Einwilligungsagenten zu einem Absinken der Einwilligungsraten führen würde. So behauptet sie in ihrem offenen Brief, dass Art. 88b "die Finanzierungsgrundlage des freien Internets gefährden" würde. Das ist jedoch in dreierlei Hinsicht falsch: Nicht nur sieht Art. 88b Medienanbieter, die bekanntlich auf Werbeeinnahmen angewiesen sind, eine Ausnahme von der Pflicht vor, die Signale von Einwilligungsagenten zu akzeptieren. Tatsächlich erhalten Medienanbieter durch Agenten einen weiteren Vertriebskanal. Denn der Agent kann seine Nutzer:innen darauf aufmerksam machen, dass bei einem Besuch des Mediums die Erteilung der Einwilligung in Werbung beziehungsweise der Abschluss eines Abonnements zwingend ist; beides kann bereits im Agenten angeboten werden. Nicht zuletzt können Agenten und darauf aufbauende Dienste erheblich zur Kundenzufriedenheit, Kundenbindung und damit, wie gesagt, zu einer höheren Einwilligungsrate bzw. Nutzung des Dienstes beitragen.

Auch der Internetkonzern Alphabet setzt in den Brüsseler Büros der EU-Kommission auf die Angst-Karte, indem er seit wenigen Wochen eine (bisher nicht öffentlich zugängliche) Studie kursieren lässt, wonach die wirtschaftlichen Folgen für Europa verheerend seien. Diese Studie basiert allerdings auf einer irreführenden Prämisse, da sie als Ausgangspunkt Apple's Einführung des App Tracking Transparency-Mechanismus (ATT) nimmt. Mit ATT hat Apple die Einwilligung für die Verarbeitung personenbezogener Daten in mobilen Apps zentral für alle Drittanbieter so gestaltet, dass deren Einwilligungsraten stark gesunken sind;¹⁹ während Apple Einwilligungen für seine eigene Datenverarbeitung über benutzungsfreundlichere Mechanismen bezieht (und sein eigenes Werbegeschäft seitdem deutlich ausgebaut hat).²⁰ Mit ATT legt die Studie von Alphabet also einen Fall zugrunde, wie man Einwilligungen gerade nicht ausgestalten sollte. Sind dagegen agentenbasierte Einwilligungen so gestaltet, dass sie wirklich informativ sind, können – wie oben gezeigt – nicht nur die Informiertheit, sondern auch die Einwilligungsraten deutlich ansteigen.

Notwendiger Anpassungsbedarf in Art. 88b zugunsten eines Level Playing Field

¹⁹ Laub, R., Miller, K., Skiera, B., The Economic Value of User Tracking for Publishers.

²⁰ Siehe die laufenden Wettbewerbsverfahren gegen Apple, etwa des Bundeskartellamts unter <https://www.bundeskartellamt.de/DE/DigitalWirtschaft/VerfahrenGegenGrosseDigitalkonzerne/Apple/Apple.html>.

Art. 88b Digitaler Omnibus bietet also mit der Schaffung eines Level Playing Fields großes wirtschaftliches Potential. Mit einer entsprechenden Klarstellung in Art. 88b wäre Apple nicht mehr in der Lage, die Einwilligungsmechanismen für seine Wettbewerber in einer für diese ungünstigen Weise, für die eigenen Zwecke aber günstigen Weise zu gestalten.

Um tatsächlich informierte Entscheidungen und einen fairen Wettbewerb sicher zu stellen, müssten in Art. 88b freilich einige Aspekte klargestellt werden. Dazu gehört zunächst, dass Anbieter von Browsern, App Stores und Betriebssystemen nicht selbst Einwilligungsagenten anbieten dürfen; zumindest, wenn sie Gatekeeper im Sinne des Digital Markets Acts sind. Denn das würde ihre Marktmacht noch weiter steigern.

Auch müsste man in Art. 88b sicher stellen, dass Einwilligungsagenten wirklich informierte Entscheidungen ermöglichen. Sonst ist es wahrscheinlich, dass sie – je nach Stoßrichtung des Anbieters – Verbraucher:innen lediglich befähigen, alle Anfragen möglichst einfach anzunehmen oder abzulehnen, ohne dass sie ihre Entscheidung jeweils verstanden hätten. Hierfür lässt sich jedoch an bereits bestehende gesetzliche Anforderungen anknüpfen. Nach Art. 25 DSGVO müssen alle Anforderungen der DSGVO, wie die informierte Einwilligung, *wirksam* und *unter Berücksichtigung des Stands der Technik* technisch umgesetzt werden. In seinen Guidelines zu Art. 25 DSGVO hat der Europäische Datenschutzausschuss (EDSA) bereits ausgeführt, dass dieser Nachweis empirisch zu erbringen ist. Auch die Methoden zur Feststellung der Risiken hat der EDSA längst geklärt. Sowohl die gesetzliche Vorschrift als auch die empirischen Methoden für die Ausgestaltung wirklich informierender Einwilligungen liegen also bereits vor. Auf ihre Anwendung müsste Art. 88b nur hinweisen.

Um die Einhaltung dieser und weiterer Vorgaben zu gewährleisten, müssen sich schließlich Einwilligungsverwaltungsdienste anerkennen lassen – das heißt, Einwilligungsagenten und Consent Management-Plattformen gleichermaßen, um eine abgestimmte Kommunikation sicherzustellen. Dies sollte aufgrund von Art. 10 ff. Data Governance Act erfolgen, einerseits um gesetzliche Doppelstrukturen zu vermeiden, zum anderen um einen Ausgleich mit den Interessen der Wirtschaft zu gewährleisten.

Die Lösung ist da, wir müssen sie nur anwenden, mit/nicht gegen die Werbewirtschaft

Die Werbewirtschaft verwendet viele ausgefeilte Mittel, um die beste Nutzungserfahrung in Bezug auf das Ausspielen von Online-Werbung zu schaffen und ihren Erfolg an den Verkaufszahlen zu messen. Sie wäre also durchaus in der Lage, ihre empirischen Methoden zu nutzen, um Verbraucher:innen die Vorteile und Risiken ihrer Werbepraktiken transparent zu machen. Sie tun es bisher nicht, vielleicht weil sie den Verbraucher:innen oder ihrem eigenen Produkt misstrauen?

Es würde sich ökonomisch aber auszahlen. Denn dass Verbraucher:innen in personalisierter Werbung prinzipiell mehr Vorteile als Risiken sehen, auch das belegen Studien.²¹ Die Werbewirtschaft hat es also gar nicht nötig, Verbraucher:innen hinters Licht zu führen. Wird Werbung durch Personalisierung wirklich relevanter und bleiben die Datenschutzrisiken hinter den Vorteilen zurück, wird sich das in höherem Vertrauen, höheren Einwilligungsraten und höherer Datenqualität bemerkbar machen. Dafür schafft Art. 88b ein Level Playing Field.

²¹ Smieskol, P., Jakobi, T., & von Grafenstein, M. (2025). From consent to control by closing the feedback loop: Enabling data subjects to directly compare personalized and non-personalized content through an On/Off toggle. *Computer Law & Security Review*, 59, 1-22. DOI: 10.1016/j.clsr.2025.106186.

Unterzeichner:innen Gegenposition zum Verbändebrief der Werbewirtschaft

Dr. Nina Gerber (Technische Universität Darmstadt – Institut für Psychologie)

Prof. Dr. Timo Jakobi (Technische Hochschule Nürnberg – KI-basierte Usability-Evaluation)

Dr. Elias Grünewald (Charité – Institut für Medizinische Informatik)

Prof. Dr. Frank Pallas (Universität Salzburg – Artificial Intelligence and Human Interfaces)

Prof. Dr. Matthias Kettemann (Alexander von Humboldt Institut für Internet und Gesellschaft
– Neue Technologien und Zukunft des Rechts)

Prof. Dr. Max von Grafenstein, LL.M. (Einstein Center Digital Future, Universität der Künste
Berlin – Digitale Selbstbestimmung)

