CORE®

To track or not to track

Anforderungen an moderne Tracking-Lösungen

Marc-André Dymala
Johannes von Bonin
Dr. Waldemar Grudzin

September 2019
Blogpost

Neue Marktseitige und regulatorische Spielregeln erhöhen den Druck auf die Werbeindustrie rechtlich sowie technologisch nachhaltige Lösungen zu entwicklen

Key Facts

- Datenschutzgrundverordnung (DSGVO) im Mai 2018 in Kraft getreten, Gesetzgebungsprozess für die neue ePrivacy-Verordnung noch nicht abgeschlossen, weshalb Telemediengesetz (TMG) weiterhin gültig und Vorrangsregelung der DSGVO nicht eindeutig geregelt ist
- Unklarheit über Vorrangsregelung führt zu weiterhin bestehendem Interpretationsspielraum bei Auslegung der Rechtsprechung, die Webseitenbetreiber zur Steigerung der Konversionsrate beim pseudonymen Nutzer-Tracking aktiv ausnutzen
- Durch eine eingeschränkte Teilnahme der Vermarktungs- und Medienindustrie am politischen Diskurs werden kurzfristige Kursänderungen der politischen Meinung nicht frühzeitig wahrgenommen und eine Beeinträchtigung deren Wirtschaftlichkeit riskiert
- Apple, Google sowie Mozilla führen die marktseitige Bewegung durch präzise Marktanforderungen sowie dedizierte Anti-Tracking Policies und erhöhen den Druck auf die Nutzer von Tracking-Lösungen, die in ihrer technischen Nachhaltigkeit eingeschränkt werden
- Existierende Lösungen bieten keine rechtliche und technische Nachhaltigkeit, womit sie ein Implosionsrisiko für die Medien- und Vermarktungsindustrie darstellen
- Dringende Empfehlung zur Aufhebung des politischen Schwebezustands an die Politik und Entwicklung von neuen Einwilligungskonzepten an die Werbeindustrie, um nachhaltiges und nutzerfreundliches Nutzertracking sicherzustellen

Report

Als relativ junge Forschungsdisziplin zeichnet sich der Datenschutz zum einen durch einen fortlaufenden Reifeprozess der Rechtsprechung und zum anderen durch eine nicht final abgeschlossene übergeordnete Meinungsbildung im politischen und marktseitigen Diskurs aus. Am 25. Mai 2018 trat die Europäische Datenschutz-Grundverordnung (EU-DSGVO) als erste supranationale Richtlinie im Bereich Datenschutz in Kraft. Die Verordnung vereinheitlicht die Regeln zur Verarbeitung von personenbezogenen Daten innerhalb der Europäischen Union. Weiter verfolgt die DSGVO den Zweck, dem Nutzer die Kontrolle und Verfügungsgewalt über die eigenen Nutzer- und Nutzungsdaten zurückzugeben, indem sie die intransparente Speicherung und Verarbeitung von personenbezogenen Daten unterbindet.

Speziell für Unternehmen lassen sich aus den Anforderungen der DSGVO eine Vielzahl von prozessualen und IT-seitigen Herausforderungen ableiten. Sie werden z.B. durch veränderte Anforderungen an Datenverarbeitungsprozesse oder die Anforderung zur Umstellung der internen Systemlandschaft repräsentiert (vgl. Abbildung 1).

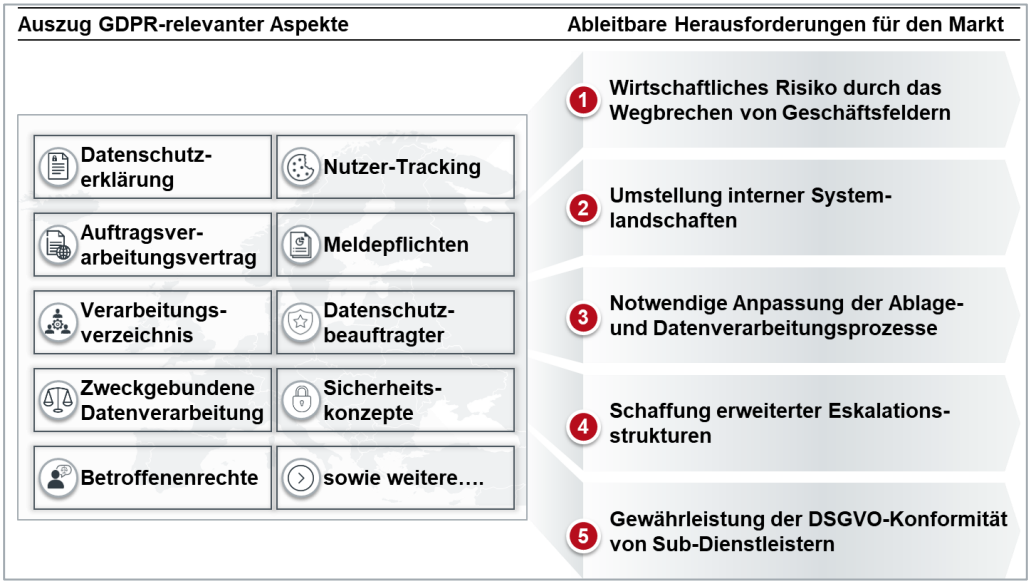


Abbildung 1: Auszug DSGVO-relevanter Aspekte und marktseitiger Herausforderungen

Zeitgleich mit der DSGVO sollte der Entwurf der EU-Kommission zur ePrivacy-Verordnung vom Januar 2017 in Kraft treten und die im Telemediengesetz (TMG) umgesetzte ePrivacy-Richtlinie ersetzen, um die DSGVO im Bereich der elektronischen Kommunikation zu ergänzen sowie zu präzisieren. Allerdings wird der Gesetzgebungsprozess frühestens für Q1 2020 erwartet, was in der Folge dazu führt, dass die Vorschriften des Abschnitt 4 TMG zur Beurteilung der Rechtmäßigkeit von Einwilligungen weiterhin bis voraussichtlich 2021 heranzuziehen sind. Diese Entwicklung eröffnet einen zulässigen Interpretationsspielraum in der Anwendung der DSGVO-Vorschriften, da der Anwendungsvorrang der DSGVO gegenüber dem im TMG umgesetzten nationalen Recht nicht eindeutig geregelt ist.

Weiter wurde mit dem Inkrafttreten der ePrivacy-Verordnung ein Paradigmenwechsel im Einwilligungsmanagement erwartet (vgl. Abb. 2), welcher noch nicht vollständig umgesetzt wurde. Unter Berücksichtigung der bereits erfolgten Unterbindung von impliziten Einwilligungen, die in der Vergangenheit durch die bloße Nutzung einer Webseite erteilt wurden, wird ein Richtungswechsel in drei weiteren Ausprägungen erwartet. Die damit verbundenen Anforderungen sind zum heutigen Zeitpunkt noch nicht vollständig umgesetzt.

i. Sicherstellung Privacy by Default

Einschränkung der intransparenten Bestätigung unterschiedlicher Einwilligungen zur separaten Datenverarbeitung durch das bloße Betätigen des OK-Buttons. Heute wird der volle Umfang der Einwilligung für den Nutzer erst durch das Öffnen der Einstellungsoptionen erkennbar, wo Einwilligungen für separate Datenverarbeitungen per Default eingestellt sind. Dies wird voraussichtlich nach dem Grundsatz von Privacy by Default künftig unterbunden.

ii. Kopplungsverbot von Einwilligungen

Verbot Einwilligungen in Abhängigkeit zueinander zu geben. Abhängigkeiten liegen vor, wenn einzelne Einwilligungen zur separaten Datenverarbeitung nicht unabhängig voneinander gegeben oder abgewählt werden können. Insbesondere, wenn der Einwilligungsumfang mittels Schieberegler angepasst wird, liegt häufig eine derartige Abhängigkeit vor. Nach dem zu erwartenden Kopplungsverbot werden solche Lösungen in ihrer Gültigkeit künftig eingeschränkt, wenn die separaten Einwilligungen nicht zwingend aufeinander aufbauen.

iii. Keine Einschränkung von Webseiten

Häufig schränken bestehende Lösungen sowohl die Nutzung als auch die Einsicht der Inhalte auf Webseiten ein, sofern keine Einwilligung vom Nutzer zur Verwendung von Cookies zum pseudonymen Tracking vorliegt. Mehr noch: Um die Konversionsrate zur Nutzung von Cookies zu maximieren, verwehren einige Seiten den Seitenzugriff, sofern der Nutzer seine Einwilligung zur Verwendung von Cookies, einer Personalisierung oder auch dem damit verbundenen Tracking verweigert. Künftig ist zu erwarten, dass die aktuell angewendete Methode zur Einschränkung der Webseite von den Behörden geahndet wird, was viele Marktteilnehmer vor weitreichende Herausforderungen stellt und die Konversionsrate maßgeblich beeinträchtigen wird.

Abbildung 2: Paradigmenwechel Einwilligungsmanagement nach DSGVO

Mut zur Lücke – Aktuelle Tracking-Lösungen nutzen regulatorischen Interpretationsspielraum

Exemplarisch für die Ausnutzung von Interpretationsspielräumen kann die Speicherung der IP-Adresse betrachtet werden, welche gängige Tracking-Lösungen als Identifier zur Ausspielung personalisierter Angebote speichern. Konkret nutzen Lösungen die IP-Adresse als Identifier, um pseudonym erhobene Nutzungsdaten einem Webseitenbesucher zuzuordnen und mittels dieser pseudonym erhobenen Nutzungsdaten Angebote für den Nutzer zu personalisieren. Da die Speicherung der IP-Adresse eine eindeutige Zuordnung der pseudonym erhobenen Nutzungsdaten auf eine Person erlaubt, wird die IP-Adresse bereits heute von einigen Browseranbietern wie z.B. Apple als personalisierte Information eingestuft. Weiter sind pseudonym erhobene Nutzungsdaten in diesem Fall nach Art. 4 Nr. 5 DSGVO nicht als pseudonyme Informationen einzustufen. Allerdings besteht diesbezüglich eine noch unklare Rechtsprechung und fortlaufende Meinungsbildung, weshalb die Speicherung der IP-Adresse aktuell noch als pseudonyme Information eingestuft werden kann. Tracking-Lösungen nutzen diesen Interpretationsspielraum aktiv aus, anstatt nachhaltige Einwilligungs-, Speicherungs- sowie Zuordnungsverfahren erhobener Nutzungsdaten sicherzustellen.

Weiter kann dieser Mut zur Lücke anhand des zu erwartenden Paradigmenwechsels betreffend gängiger Einwilligungslösungen verdeutlicht werden, wonach diese Lösungen mit der zu erwartenden Verbindlichkeit der Anforderungen der ePrivacy-Verordnung eingeschränkt werden. Die Anforderung zur Datenverarbeitung pseudonym erhobener Daten im Sinne einer nach DSGVO informierten Einwilligung ist in Bezug auf die noch umzusetzenden Anforderungen hinsichtlich Privacy by Default, das Kopplungsverbot sowie die Vermeidung zur Einschränkung von Webseiten noch nicht erfüllt.

Fehlende Anteilnahme an politischer Diskussion führt zu einer potentiellen Beeinträchtigung der Wirtschaftlichkeit von Unternehmen der Vermarktungs- und Medienindustrie

Zum aktuellen Zeitpunkt bleibt festzuhalten, dass sich diverse Vertreter der Vermarktungs- und Medienindustrie sowie auch Webseitenbetreiber wie z.B. von Webshops, deren Absatz durch ein fehlendes Nutzer-Tracking beeinträchtigt werden könnten, nicht ausreichend am politischen Diskurs sowie der generellen Meinungsbildung beteiligen, um diese im Rahmen ihrer eigenen Interessen positiv zu beeinflussen. Zurückzuführen ist die aktuelle Situation auf die Erwartung, dass die derzeit eingesetzten Lösungen unberührt bleiben würden. Dabei gehen die Marktteilnehmer von zwei Annahmen aus: einerseits von der Vermutung, dass die ePrivacy-Verordnung nicht in Kraft treten wird; andererseits bestehen Zweifel an der Durchsetzungsfähigkeit der Datenschutzaufsicht. Allerdings stellt diese Zurückhaltung voraussichtlich einen Trugschluss dar, der dazu führen kann, dass Anforderungen einer kurzfristigen politischen Kursänderung nicht frühzeitig wahrgenommen werden und aktuelle Tracking-Lösungen somit in ihre Legitimität eingeschränkt werden. Dass diese Gefahr Realität ist, kann anhand der Positionsbestimmung der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 26. April 2018 aufgezeigt werden, in welcher eine unerwartete Vorrangsregelung der DSGVO gegenüber dem TMG kommuniziert wurde. Bis kurz vor Inkrafttreten der DSGVO sind insbesondere Vertreter der Vermarktungs- und Medienindustrie von der Annahme ausgegangen, dass selbst nach Inkrafttreten der Verordnung die neuen Anforderungen im Rahmen einer Übergangsphase vorerst nicht gültig sein würden. Da ein Großteil der Unternehmen bis zu diesem Zeitpunkt keine neue Einwilligungslösung implementiert oder noch nicht mal geplant hatte, wurden sie von der Entwicklung der politischen Meinungsbildung überrumpelt. Wird die Legitimitätsgrundlage gespeicherter Einwilligungen durch einen solchen Kurswechsel gefährdet, hat dies umfangreiche Folgen für Werbetreibende. Sämtliche Einwilligungen, die auf Basis einer früheren Rechtsauslegung erhoben wurden, würden ihre Gültigkeit verlieren und erhobene Nutzungsdaten dürften nicht mehr verwendet oder gespeichert werden. Legitime Einwilligungen müssten zunächst eingeholt und Nutzungsdaten neu erhoben werden. Die Problematik dieser Herausforderung liegt darin, dass der Prozess zur Sicherstellung des alten Personalisierungsgrads einen Zeitraum von bis zu drei Monaten oder länger umfassen kann und in der Zwischenzeit nur schwach bis keine personalisierten Angebote auf betroffenen Webseiten ausgespielt werden könnten. Die damit verbundenen Auswirkungen auf die Wirtschaftlichkeit einzelner Unternehmen können am Beispiel der Vermarktungs- und Medienindustrie illustriert werden, deren Umsätze zu ca. einem Drittel von der Fähigkeit zur Personalisierung von Angeboten abhängen.

Marktseitige Realität erhöht Datenschutzanforderungen und erhöht Druck auf die Vermarktungs- und Medienindustrie

Auch wenn die rechtliche Situation aktuelle Lösungen zum Nutzer-Tracking toleriert, werden Tracking-Lösungen künftig durch marktseitige Anforderungen eingeschränkt und die Umsetzung der DSGVO aktiv gefordert. Tool-Anbieter wie Google positionieren sich klar in Hinblick auf Datenschutz und legen die Anforderungen in diesem Bereich tendenziell strenger und proaktiv aus. So hat Google beispielsweise angekündigt, dass die Nutzung ihrer Tools zum Tracking oder Analysieren den Marktteilnehmern bei nicht DSGVO-konformen Einwilligungen nicht mehr zur Verfügung stehen werden. Dies erhöht den Druck auf einzelne Marktteilnehmer - neben existierenden rechtlichen Konsequenzen - deutlich. Ein weiteres Beispiel ist Apple, die die Einschränkung zur Speicherung der IP-Adresse als pseudonyme Information einwerten, die Entwicklung von Diskussionspunkten, zu denen die EU-Kommission bislang keine klare Position beziehen konnte. Apple agiert als Innovationstreiber und forciert allgemein eine erweiterte Einschränkung des pseudonymen Trackings zum Schutz der Privatsphäre der Nutzer. Bereits im letzten Jahr hat Apple mit Mojave OS Transparenz und Kontrolle bezüglich ihrer Nutzungsdaten geschaffen und Werbetreibende damit stark unter Druck gesetzt. Konkret hat das Unternehmen aus Cupertino damals einen verbesserten Tracking-Schutz angekündigt, der durch die Teilung von vereinfachten Systemprofilen das Device-Fingerprinting durch Werbetreibende einschränken bzw. verhindern sollte. Darüber hinaus möchte Apple die unerlaubte Nachverfolgung der Nutzer durch eingebettete "Gefällt mir"-Buttons oder solche zum Teilen von Kommentaren unterbinden. Weiter war auf Basis von Apples damaliger Positionierung mittelfristig die Unterbindung von Third Party Cookies in Browsern sowie eine Einschränkung der Kompatibilität von iframes in Safari zu erwarten. Mit der Veröffentlichung der neuen Anti-Tracking Policy vom 14.08.2019 hat Apple seine Position nun deutlich verschärft und weitere Regeln definiert. Konkret soll die Umgehung von Apples Anti-Tracking durch Webseiten erschwert sowie geahndet werden, beispielsweise durch die Einschränkung solcher Webseiten. Zusätzlich ist mit iOS 13 und MacOS Catalina für dieses Jahr eine neue Safari-Version geplant, die die Möglichkeit bietet, Tracking-Cookies gänzlich abzuschalten. Durch dieses Vorgehen kommt der Markt mit Vertretern wie Apple, Mozilla oder Google der EU-Kommission in Brüssel zuvor und schafft voraussichtlich nachhaltige, den Markt beeinflussende Standards.

Fehlende Nachhaltigkeit aktueller Tracking-Lösungen – die Kernkompetenz der Vermarktungs- und Medienindustrie wird bedroht

Im Ergebnis der Entwicklungen in Form einer Kombination aus a) Mangel an regulatorischem Rahmen und b) Tatsachen schaffendem sowie dabei tendenziell strenger auslegenden Rechtsrahmen der Technologiekonzerne besteht das Potential, das Nutzer-Targeting im Online-Geschäft durch die stattfindende marktseitige Bewegung sowie eine mögliche Verschärfung der rechtlichen Anforderungen nachhaltig zu verändern und eine Implosion in der Medien- und Vermarktungsindustrie herbeizuführen. Grund dafür ist die Tatsache, dass gängige Tracking-Lösungen im Kontext der aktuellen und prognostizierbaren Entwicklung über keine rechtliche sowie technische Nachhaltigkeit verfügen. Konkret lässt sich diese Beobachtung anhand zweier Methoden zum pseudonymen Tracking verdeutlichen:

I. Device Finger Printing

Wie bereits ausgeführt, ist die Speicherung der IP-Adresse im Rahmen des pseudonymen Trackings umstritten und wird dennoch von einzelnen Tracking-Anbietern verwendet. Weiter wird die technische Nachhaltigkeit dieser Lösungsoption durch die Positionierung von Apple gefährdet. Es ist davon auszugehen, dass die Kompatibilität der Lösungen mit dem Release des neuen Safari Browsers bereits in diesem Jahr weiter eingeschränkt wird. Die Realität dieser Gefahr kann in dem Kontext verdeutlicht werden, dass diese Lösungsoption von Anbietern am Markt vertrieben wird und sich Kundenunternehmen auf die rechtliche sowie technische Nachhaltigkeit der Lösung verlassen. Dabei bauen einige Anbieter bewusst Vertrauen hinsichtlich der rechtlichen Nachhaltigkeit ihrer Lösungen auf, indem Gütesiegel oder Zertifizierungen zur Bestätigung ihrer DSGVO-Konformität kommuniziert werden, um jeglichen Zweifel an der Legitimität der Lösungen aus dem Weg zu räumen. Auf den ersten Blick scheinen diese Konformitätsbestätigungen verlässlich, wie so oft, steckt der Teufel in den Details einzelner Absätze dieser Bestätigungen, welche für Kundenunternehmen in der Regel nicht ersichtlich sind. Diese Details geben Aufschluss darüber, dass die vermeintlich gesetzeskonformen Lösungen nur im Kontext des zulässigen Interpretationsspielraums und der andauernden Meinungsbildung betreffend die Speicherung der IP-Adresse als gesetzeskonform gelten. Sobald sich die Diskussion dazu verschärft und die Speicherung der IP-Adresse flächendeckend von der Rechtsprechung als personalisierte Information angesehen wird, werden die kommunizierten Bestätigungen zur DSGVO-Konformität in ihrer Gültigkeit eingeschränkt und der Zugriff sämtlicher Kundenunternehmen auf die von ihnen erhobenen Nutzungsdaten entfällt.

II. iframes

Weitere Lösungen, die als Open Source am Markt erhältlich sind, nutzen die Option von iframes zum Tracking der Nutzer und zur Umgehung von Third Party Regelungen. Selbst wenn diese Lösungen im Rahmen einer rechtskonformen Einwilligung angewendet werden, wird die Nachhaltigkeit dieser Lösungen ebenfalls durch Browser-Provider eingeschränkt. Mozilla oder Apple forcieren in ihren Anti-Tracking Policies die Unterbindung solcher Angebote, um ein intransparentes Tracking der Nutzer zu unterbinden.

Lösungsrahmen

Zur Aufhebung des politischen Schwebezustands und zur Sicherstellung eines nachhaltigen Nutzertrackings lassen sich im Wesentlichen folgende Handlungsempfehlungen auf Seiten der Politik und des Marktes ableiten:

Politische Handlungsempfehlungen

I. Die Politik ist dazu angehalten, existierende Interpretationsspielräume zu schließen und Klarheit angesichts der Vorrangsregelung der DSGVO gegenüber dem TMG zu schaffen. Dazu empfiehlt es sich, unter Anbetracht der Gefahr einer weiteren Verzögerung oder des Ausbleibens des Gesetzgebungsprozesses der ePrivacy-Verordnung, eine Synchronisation des TMGs vorzunehmen.

II. Abstimmung mit Vertretern der Industrie und des Marktes hinsichtlich der Ausdehnung einzelner Anforderungen sind erforderlich, um die andauernde Meinungsbildung abzuschließen. Gerade unter Berücksichtigung der technischen Umsetzbarkeit einzelner Anforderungen, um einen Verlust erfolgskritischer Einnahmequellen durch eine zu starke Einschränkung des Nutzer-Trackings zu vermeiden.

Marktseitige Handlungsempfehlungen

I. Kontinuierliches Screening des Marktes hinsichtlich Repositionierungs-bestrebungen von Software-, Tracking-, und Browseranbietern wie Mozilla, Google oder Apple als Basis für eine informierte Beteiligung am politischen Diskurs und um auf variierende Anforderungen frühzeitig zu reagieren.

II. Unabhängig von der aktuellen Gesetzeslage sollten Lösungskonzepte eine proaktive Erhebung von Einwilligungen nach den Anforderungen einer künftigen Rechtsprechung forcieren. Damit kann sichergestellt werden, dass die Gültigkeit dieser Einwilligungen zur Erhebung und Speicherung von Nutzungsdaten auch mit der Verbindlichkeit einer künftigen Rechtsprechung unberührt bleibt.

III. Entwicklung nachhaltiger Lösungskonzepte auf Basis der erzielten Regelungen und Leitlinien aus der Teilnahme am politischen Diskurs sowie unter Berücksichtigung der marktseitigen Entwicklungen:

Lösungsansätze könnten beispielsweise auf persistente und SSO-gebundene Einwilligungen setzen, die unabhängig von der Verfügbarkeit von Cookies über eine geräteübergreifende Gültigkeit verfügen. Dazu erlaubt ein SSO-gebundenes Einwilligungsprinzip eine kollektive Einwilligungsabfrage von Webseiten, die im Rahmen des SSO-Prinzips kollektiv miteinander agieren. Dem folgend fördert die kollektive Einwilligungsabfrage eine Steigerung der Conversion und wirkt der Gefahr einer sinkenden Conversion, die mit der Umsetzung zunehmender Transparenzanforderungen gegenüber dem Nutzer einhergeht, aktiv entgegen. Als weiteren Vorteil kann mittels des kollektiven

und SSO-gebundenen Einwilligungsprinzips eine stetige Aktualisierung der gespeicherten Einwilligung erzielt sowie ein Gültigkeitsablauf der Einwilligung vermieden werden. Eine solche Aktualisierung kann dann erfolgen, sofern der kollektive Verbund nachträglich um weitere Services erweitert wird. Besucht der Nutzer dann einen additiv hinzugefügten Service, kann eine Aufforderung zur Erweiterung und Aktualisierung der vorher gegebenen Einwilligung um den neu hinzugekommenen Service erfolgen. Stimmt der Nutzer dieser Aufforderung zu, wird die Einwilligung um den neuen Service erweitert und das Einwilligungsdatum für alle anderen Services parallel aktualisiert. Darüber hinaus erlauben SSO-gebundene Einwilligungen eine Personalisierung von Angeboten auf Basis verifizierter Nutzerdaten, anstatt ungenauer Nutzungsdaten, die in diesem Fall aus Profilinformationen abzuleiten und systemseitig in pseudonyme Segmentdaten zu übersetzen sind. Illustriert werden kann dieser Vorgang anhand der Segmentbildung auf Basis der im Profil hinterlegten Altersangabe. Dabei erfolgt eine Umwandlung der Altersinformation in eine Altersspanne von beispielsweise fünf bis zehn Jahren, die als pseudonyme Information zur Personalisierung von Angeboten verwendet werden kann. Im Ergebnis resultiert dieses Vorgehen in einer Optimierung des Nutzertargetings, da eine Personalisierung auf Basis korrekter Profildaten, anstatt ungenau erhobener Tracking-Daten erfolgt.

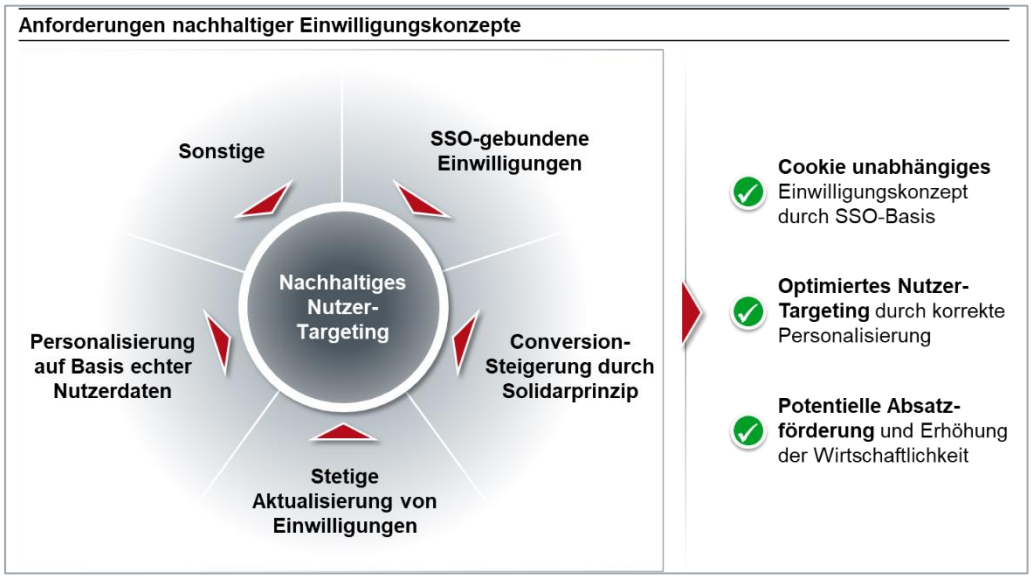


Abbildung 3: Anforderungen künftiger Einwilligungskonzepte

Fazit

Wie zu Beginn des Beitrags erwähnt, stellt das Einwilligungsmanagement nur einen Bereich der durch die EU-DSGVO gestellten Anforderungen dar. Setzt man die genannten Herausforderungen des Einwilligungsmanagements in Beziehung zu sämtlichen Anforderungen der DSGVO, so kann der enorme Umfang der Herausforderungen für Unternehmen verdeutlicht werden.

Eine stiefmütterliche Behandlung der Datenschutzanforderungen führt dazu, dass häufig nur die regulatorischen Mindestanforderungen im Rahmen der Abarbeitung eines „Pflichtenhefts“ umgesetzt werden. Zukünftig sollten diese zur Vermeidung von Doppelaufwänden und aufgrund der Gefahr einer non-Compliance auf strategischer Ebene betrachtet werden. Bedenkt man darüber hinaus die ökonomische Tragweite, die das Thema Datenschutz für Unternehmen besitzt, so ist die Verankerung auf strategischer Ebene dringendst zu empfehlen. Wenn Datenschutz nicht als Aufwand, sondern als wettbewerbsdifferenzierender Faktor verstanden wird, können sowohl drohende Verluste abgewendet, als auch strategisch wichtige Positionen am Markt besetzt werden.

Quellen

Düsseldorfer Kreis

Positionsbestimmung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder, Düsseldorf, 26. April 2018: https://datenschutz.saarland.de/fileadmin/datenschutz/dsk_entschliessungen/95/Positionsbestimmung-TMG.pdf Bundesgerichtshof

CORE Techmonitor

Opt-in – Vorrangregelung DSGVO setzt Industrien mit hohem P&L-Anteil in der Drittvermarktung von Nutzerdaten unter Druck: https://core.se/de/techmonitor/opt-in-vorrangregelung-dsgvo-setzt-industrien-mit-hohem-pl-anteil-in-der-drittvermarktung-von-nutzerdaten-unter-druck

heise online

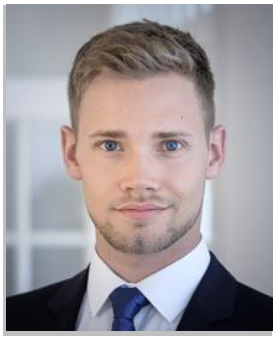
Tracking-Schutz im Browser Safari: Apple warnt Werbefirmen vor Umgehung: https://www.heise.de/mac-and-i/meldung/Tracking-Schutz-im-Browser-Safari-Apple-warnt-Werbefirmen-vor-Umgehung-4498286.html

WebKit

WebKit Tracking Prevention Policy: https://webkit.org/tracking-prevention-policy/

Macwelt

Adtracking: Apple droht der Werbeindustrie: https://www.macwelt.de/news/Adtracking-Apple-droht-der-Werbeindustrie-10648343.html



Marc-André Dymala ist Transformation Manager bei CORE. Er hält zwei Master-Abschlüsse: in International Business Mangement (SWUFE Chengdu, China) und in Chinese European Economics and Business Studies (HWR Berlin). Seine Schwerpunktthemen sind Qualitätsmanagement, Lean Agile Methods (ISO 9001), Geschäftsprozess- und Change Management.

Mail: marc-andre.dymala@core.se

Johannes von Bonin ist Transformation Fellow bei CORE. Er hat seinen Master in Economics of the Middle East an der Lebanese American University & Philipps-Universität in Marburg absolviert. Seine Themen sind wirtschaftliche Entwicklung und quantitative Analysen.

Mail: johannes.bonin@core.se

Dr. Waldemar Grudzien ist Expert Director bei CORE und beschäftigt sich mit den Sicherheitsvorschriften der Finanzindustrie und deren technologischen Auswirkungen auf IT-Infrastrukturen. Während seiner Tätigkeit bei einem nationalen Verband der Finanzindustrie war er Spezialist für Retailbanking und Bankentechnologien. Er hat an der TU Berlin Elektrotechnik studiert.

Mail: waldemar.grudzin@core.se

CORE SE
Am Sandwerder 21-23
14109 Berlin | Germany
https://core.se/
Phone: +49 30 263 440 20
office@core.se

COREtransform GmbH
Am Sandwerder 21-23
14109 Berlin | Germany
https://core.se/
Phone: +49 30 263 440 20
office@core.se

COREtransform GmbH
Limmatquai 1
8001 Zürich | Helvetia
https://core.se/
Phone: +41 44 261 0143
office@core.se

COREtransform Ltd.
Canary Wharf, One Canada Square
London E14 5DY | Great Britain
https://core.se/
Phone: +44 20 328 563 61
office@core.se

COREtransform MEA LLC
DIFC – 105, Currency
House, Tower 1
P.O. Box 506656
Dubai I UAE Emirates
https://core.se/
Phone: +97 14 323 0633