Stiemerling, Weiß, Wendehorst

c/o
ecambria systems GmbH
Herzogenrather Str. 11
D-50933 Köln
Telefon +49 (0) 221 595527-0
Fax +49 (0) 221 595527-5

os@ecambria-experts.de
www.ecambria-experts.de

ecambria-Aktenzeichen: p-os376/21

Köln, den 16.12.2021

Forschungsgutachten zum Einwilligungsmanagement nach § 26 TTDSG

Studie im Auftrag des

Bundesministeriums für Wirtschaft und Energie

Inhaltsverzeichnis

1. Zusammenfassung (Executive Summary)

[1] Zentrales Thema dieser Studie sind mögliche Vorgaben zu technischen und organisatorischen Maßnahmen, um das im TTDSG[1] vorgesehene Einwilligungsmanagement umzusetzen. Ziel des TTDSG ist ein nutzerfreundliches und wettbewerbskonformes Einwilligungsmanagement durch anerkannte Dienste, das von Browsern („*Software zum Darstellen und Abrufen von Informationen aus dem Internet*“) und Websites befolgt bzw. berücksichtigt werden kann.

[2] Die derzeitige Praxis der Einwilligungsbanner stellt Anbieter wie Nutzer vor große Herausforderungen. Sie folgt aus dem Bedürfnis der Telemedienanbieter, eine wirksame Einwilligung vor dem Hintergrund der Anforderungen der DSGVO und der Umsetzung der E-Privacy-Richtlinie (E-Privacy-RL) rechtssicher zu erhalten, wird aber allgemein als höchst unbefriedigend empfunden.

[3] Zieht man die Leitlinien[2] des Europäischen Datenschutzausschusses (European Data Protection Board – EDPB) 05/2020 zur Einwilligung gemäß Verordnung 2016/679/EU heran und berücksichtigt man die Position der Datenschutzbehörden, so hat ein Verantwortlicher die Pflicht, eine Einwilligung granular, d.h. einzelfallbezogen von den Nutzerinnen und Nutzern einzuholen.

[4] Vor diesem Hintergrund sollte ein einmaliges „Whitelisting“ bestimmter Verantwortlicher (z.B. Werbeunternehmen) durch den Nutzer möglich sein, sofern zum Zeitpunkt der Erklärung alle von der DSGVO geforderten Informationen, einschließlich hinsichtlich der konkreten Identität der Verantwortlichen, erteilt werden. Dabei wäre es unerheblich, ob die Liste von Verantwortlichen primär vom anerkannten Dienst zusammengestellt wurde oder primär von einem vertrauenswürdigen Dritten, etwa einer NGO. Spätere Veränderungen (z.B. neu hinzukommende Telemedienanbieter, neue konkrete Zwecke) könnten dann aber nicht mehr oder nur noch eingeschränkt nutzerfreundlich berücksichtigt werden, etwa

[1] Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG), am 23. Juni 2021 (BGBl. 2021 I Seite 1982) erlassen, tritt am 1. Dezember 2021 in Kraft.
[2] *Europäischer Datenschutzausschuss*, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679 v. 04.05.2020.

indem der Nutzer in regelmäßigen Abständen zum „Whitelisting“ zusätzlicher Verantwortlicher aufgefordert wird.

[5] Eine Verbesserung der Nutzerfreundlichkeit lässt sich dadurch erreichen, dass man – zumindest nach dem initialen „Whitelisting“ – abstrakte ex-ante Einwilligungen in granular definierte Zwecke und bloße Kategorien von Verantwortlichen zulässt. Dieses Verfahren kann sich gegebenenfalls auf die DSGVO stützen, wenn der anerkannte Dienst zugleich als die Daten erhebender erster Verantwortlicher auftritt, der die Daten dann an dritte Empfänger weiterleitet. Ist der anerkannte Dienst nicht erster Verantwortlicher, bliebe eine teleologische Auslegung der DSGVO in diesem Sinne, der sich möglicherweise in der Zukunft Judikatur und Aufsichtsbehörden anschließen könnten. Ähnliches gilt für Stellvertretungskonstruktionen, bei denen der anerkannte Dienst oder ein vertrauenswürdiger Dritter (z.B. eine NGO) aufgrund einer granular formulierten Vollmacht mit der Erteilung der Einwilligung und/oder der Ausübung von Betroffenenrechten betraut wird.

[6] Generelle Verweigerungen der Einwilligung sind für die Nutzerfreundlichkeit wichtig, aber juristisch schwierig zu erfassen. Um den Mehrwert anerkannter Dienste für Nutzer zu erhalten und zu vermeiden, dass Nutzer wiederum ständig mit Cookie-Bannern konfrontiert werden, wäre zu empfehlen, dass neue Einwilligungsverlangen zumindest über den anerkannten Dienst gestellt werden müssen, wobei die Entwicklungen zur künftigen E-Privacy-Verordnung (E-Privacy-VO) aufmerksam zu beobachten sind.

[7] Auch aus technischer Sicht kann das Problem der „consent fatigue“[3] ggfs. dann zufriedenstellend gelöst werden, wenn die abstrakte ex-ante Definition einer Einwilligung durch den Betroffenen möglich ist, die dann beim Besuch einer passenden Webseite aufgrund von Einstellungen erfolgt, die der Betroffene vorher vorgenommen hat. Es wird dann spürbar weniger Nutzerinteraktionen zur Einwilligung geben, wenn die Einwilligung auf eine oder mehrere der folgenden Arten ohne weitere Nutzerinteraktion wirksam erklärt werden kann:

[3] *Schermer, Bart & Custers, Bart & Van der Hof, Simone*. (2014). The crisis of consent: How stronger legal protection may lead to weaker consent in data protection. Ethics and Information Technology. 16. 10.1007/s10676-014-9343-8.

- Zweckbezogene Einwilligungen ohne explizite Angabe der Verantwortlichen (z.B. generelle Einwilligung in „personalisierte Werbung, solange Daten nur in Europa verarbeitet werden“)
- Einwilligung für Kategorien von Verantwortlichen (z.B. „Blogs“, „Online-Publikationen“)
- Delegierte Einwilligungen (z.B. Einwilligung in alle Inhalte der „Einwilligungsliste von Max“).

[8] Die Mitteilung dieser Einwilligungen bzw. Einwilligungstypen an den Telemediendienst im speziellen Fall würde dann im Moment des Aufrufs der Website bzw. der App durchgeführt werden, wobei es aus technischer Sicht verschiedene Möglichkeiten gibt, diese Kommunikation auszugestalten. Technisch ist denkbar, dass eine Software unter direkter Kontrolle der Nutzerin oder des Nutzers (d.h. der Browser) die Einwilligung gegenüber der Webseite erklärt oder dass eine Software unter Kontrolle eines Dritten (fremdgehosteter „Dienst“) diese Handlung im Auftrag des Nutzers durchführt.

[9] Aus technischer Sicht kann angenommen werden, dass der Grad der Vernetzung und Arbeitsteilung sowie die Durchdringung von Lebens- und Arbeitswelten mit Systemen der Informationsverarbeitung so stark zugenommen hat, dass selbst technik-affine Nutzerinnen und Nutzer heute nicht in der Lage sind, sich über jede einzelne dieser hochkomplexen Datenverarbeitungen in globalen Netzwerken vollständig zu informieren und erst dann eine Einwilligung zu erklären. Allein der Aufruf einer einzigen Seite einer typischen, werbefinanzierten Nachrichtenwebesite führt zu einer Vielzahl global verteilter, vernetzter Verarbeitungsvorgänge bei potentiell über hundert Akteuren (siehe das nachfolgende Beispiel in Ziff. 3).

[10] Die in dieser Studie vorgenommene Ausdifferenzierung der technischen Möglichkeiten der Einbindung von anerkannten Diensten in das Einwilligungsmanagement und die resultierenden technischen und organisatorischen Anforderungen an diese Dienste, aber auch an die Telemediendienste und Software zur Darstellung und zum Abruf von Informationen aus dem Internet wie Browser berücksichtigt sowohl die Möglichkeiten genereller Einwilligungen als auch individuell, für jeden Verantwortlichen eingeholte Einwilligungen.

[11] Hervorgehoben sei zudem, dass die Zukunft von § 26 TTDSG möglicherweise abhängig ist von weiteren Entwicklungen auf EU-Ebene, und zwar im Zusammenhang mit der künftigen E-Privacy-VO, dem Data Governance Act (DGA) und gegebenenfalls auch dem erst angekündigten Data Act.

2. Auftrag

[12] Am 01.10.2021 wurde das Konsortium um Prof. Dr. Christiane Wendehorst, RA Steffen Weiß und ecambria systems GmbH (Dr. Oliver Stiemerling) unter der Konsortialführung von Herrn RA Steffen Weiß mit der Erstellung dieser Studie beauftragt.

[13] Dr. Oliver Stiemerling erstellte[4] die Kapitel 2 (ausgenommen der rechtlichen Darstellungen), 3 und 5 (bis auf 5.8.2). Die anderen Kapitel wurden von den beiden anderen Konsortialpartnern erstellt; diese danken Dr. Sebastian Schwamberger (Wien) für die redaktionelle Durchsicht. Das Kapitel 5.8.3 („Empfehlung und Vorschläge zur Verordnung“) wurde unter den Autoren der Studie gemeinsam abgestimmt. Zu den im Auftrag konkret formulierten Fragen wird wie folgt zusammenfassend Stellung genommen:

[14] *1. Wie kann der Endnutzer, der einen anerkannten Dienst zur Einwilligungsverwaltung nutzt, die Einwilligung unter Nutzung dieses Dienstes granular erteilen, d. h. für den bestimmten Fall, für den der Telemedienanbieter die Einwilligung benötigt, so dass der Telemedienanbieter rechtssicher vom Vorliegen einer wirksamen Einwilligung ausgehen kann?*

[15] **Das in dieser Studie entwickelte Modell geht davon aus, dass der Endnutzer bereits bei der Konfiguration des Dienstes zum Einwilligungsmanagement bestimmte, aufsichtsbehördlich als wirksam erachtete Einwilligungstypen konfiguriert, die dann nach Anfrage eines konkreten Telemediendienstes granular als spezielle Einwilligungen mit operativer Unterstützung der Wahrnehmung der Betroffenenrechte (integrierbare URLs zu Einsicht, Änderung, Widerruf, Löschen etc.) automatisch erteilt werden.**

[16] *2. Wie sollte eine Einwilligungsmaske/Benutzeroberfläche des anerkannten Dienstes gestaltet sein, damit sie die Anforderungen an eine rechtswirksame Einwilligung in nutzerfreundlicher Weise erfüllt (z.B.: Auflistung der angebundenen*

[4] In seiner Rolle als öffentlich bestellter und vereidigter Sachverständiger muss Herr Dr. Stiemerling bei Gemeinschaftsgutachten (und Studien) seine Anteile explizit markieren (Sachverständigenordnung der IHK zu Köln).

Telemedien mit jeweiliger Datenschutzerklärung, Möglichkeiten der Einwilligungserklärung, Zeitpunkt der Einwilligungserklärung, Darstellung der Datenschutzerklärungen, Widerrufsmöglichkeit, Anpassungsoptionen, u.a.)?

[17] **Das in dieser Studie entwickelte Modell gibt eine Mindestmenge von Funktionen vor, die die Benutzerschnittstelle (Oberfläche) des anerkannten Dienstes enthalten muss, damit der Endbenutzer sich einen Überblick über alle erklärten Einwilligungen und den Verantwortlichen verschaffen kann und mit möglichst wenigen „Klicks“ seine Betroffenenrechte wahrnehmen kann. Mögliche konkrete Anforderungen werden detailliert in Abschnitt 5.4 beschrieben.**

[18] *3. Welche Daten über den Endnutzer sind für eine funktionierende Einwilligungsverwaltung von dem anerkannten Dienst zu speichern oder zu verarbeiten?*

[19] **Im Wesentlichen werden die generellen Präferenzen zu Einwilligungstypen und die konkret bzgl. den Verantwortlichen erklärten speziellen Einwilligungen zusammen mit der konkreten Nutzer-ID gespeichert. Hinzu kommen können „Abonnements“ von Listen von delegierten Einwilligungen und andere Features (Synchronisierung von Endgeräten), für die die entsprechenden Daten im Nutzerprofil gespeichert werden müssen.**

[20] *4. Wie erfolgt die Zuordnung des jeweiligen Nutzers zu seinen jeweiligen Nutzereinstellungen durch den Dienst zur Einwilligungsverwaltung (Log-in System, Setzen einer Nutzer-ID, o.ä.)?*

[21] **Grundsätzlich können Einwilligungen, je nach notwendiger Sicherheit der Authentifizierung, an verschieden stark authentifizierten Nutzer-IDs gespeichert werden. Das passende Authentifizierungsverfahren hängt dabei von den konkreten personenbezogenen Daten und den Verarbeitungszwecken ab und muss im Wesentlichen im Telemediendienst anhand von Risikoerwägungen festgelegt werden.**

[22] *5. Wie kann der Telemedienanbieter, der die Einwilligung benötigt, anerkannte Dienste, die der Endnutzer für die Einwilligungsverwaltung nutzt, in die Gestaltung seines Telemedienangebotes rechtssicher einbinden? Es soll insbesondere*

dargestellt werden, was technisch notwendig ist, damit Telemedien erkennen, dass der Endnutzer einen anerkannten Dienst zur Einwilligungsverwaltung nutzt,

- *damit Telemedien die Einstellungen des Endnutzers befolgen können,*
- *damit der Informationsaustausch zwischen anerkannten Diensten und Telemedien erfolgt (z.B. Anforderungen an eine Schnittstelle, an einen allgemeingültigen technischen Standard zur Signalübertragung, o.ä.?),*

[23] **Grundsätzlich ist es technisch machbar, dass der Telemediendienst die Nutzung eines (beliebigen) Dienstes zum Einwilligungsmanagement an technischen Ergänzungen des initialen Aufrufs des Telemediendienstes durch den Browser erkennt, analog zur Übermittlung von „Do not Track"-Signalen in Kopfzeilen (Headers) der HTTP-Anfrage. Der Telemediendienst kann dann mit dem Dienst zur Einwilligungsverwaltung über ein idealerweise global standardisiertes Protokoll interagieren, Einwilligungen abfragen und sich dann entsprechend der Menge der erteilten bzw. auch nicht erteilten Einwilligungen verhalten.**

[24] 6. Was geschieht technisch, wenn eine Einwilligung in Cookies bei einem speziellen Telemediendienst nicht erklärt wurde, dies aber Bedingung für die (kostenfreie) Nutzung des Telemediendienstes ist?

[25] **Aus technischer Sicht ist es für den Telemediendienst im hier vorgestellten Modell einfach machbar, die Nutzung bei fehlender Einwilligung schlicht zu verweigern. Ob er das darf, ist eine Rechtsfrage.**

[26] 7. Welche technischen Anforderungen sind an Software zum Abrufen und Darstellen von Informationen aus dem Internet zu stellen, damit erteilte Einwilligungen befolgt werden und die Einbindung von anerkannten Diensten zur Einwilligungsverwaltung berücksichtigt werden können?

[27] **Im hier vorgestellten Modell müssen Browser einen wirkmächtigen Plugin-/Extension-Mechanismus unterstützen, der die Integration von anerkannten Diensten zum Einwilligungsmanagement erlaubt. Dieser heute bereits in fast allen marktgängigen Browsern unterstützte Mechanismus fördert den Wettbewerb zwischen verschiedenen Anbietern von Einwilligungsdiensten**

und verhindert ein komplett geschlossenes System des Browser-Herstellers als Plattformanbieter.

3. Aktuelle Herausforderungen des Einwilligungsmanagements

[28] Beim Aufruf einer Webseite wird typischerweise zunächst eine HTML-Datei vom Server an den Browser zurückübermittelt. Diese HTML-Datei enthält oft Verweise auf weitere Elemente (zumeist Bilder und JavaScript-Programme), die bei der Darstellung der Webseite von den entsprechenden Servern heruntergeladen und dargestellt (Bilder) oder ausgeführt (JavaScript-Programme) werden. Die Ausführung von JavaScript-Programmen kann auch dazu führen, dass weitere Elemente von weiteren Servern nachgeladen werden.

[29] Insbesondere bei der technischen Betrachtung von werbefinanzierten Webseiten zeigt sich, dass der Aufruf der eigentlichen Webseite dazu führt, dass während der Darstellung der Webseite im Browser eine große Zahl von Elementen direkt von *anderen* Servern nachgeladen wird. Der Aufruf einer werbefinanzierten Webseite kann dazu führen, dass der Browser des Nutzers mit über 50 fremden Servern (d.h. Server unter einer anderen Domäne als die der ursprünglichen Webseite) direkt kommuniziert.

[30] Bei jedem dieser Aufrufe werden die in der Vergangenheit vom entsprechenden Server im Browser gespeicherte Cookies wieder an den Server zurückübertragen. In der Antwort des jeweiligen Servers können – insbesondere bei einem erstmaligen Aufruf – auch neue Cookies im Speicher des Endgeräts abgelegt werden. Bereits beim Aufruf der fremden Server werden auf jeden Fall die IP-Adresse des Rechners an diese Server übertragen. Es gibt auch Aufrufe von Drittservern, bei denen keine Cookies gesetzt werden.

[31] Im Fall von werbefinanzierten Websites werden die auf dem Endgerät gespeicherten Cookies von den Drittservern typischerweise dafür benutzt, den Nutzer (technisch: den Browser) längerfristig identifizieren zu können, damit diese Drittserver bestimmte Tätigkeiten im Bereich der Online-Werbung durchführen können.

[32] Dazu zählt insbesondere die *Profilbildung*, die die Besuche des entsprechenden Nutzers auf verschiedenen Webseiten über den einen (im Endgerät gespeicherten) Identifikator zu einem übergreifenden Interessenprofil aggregieren kann. Ein

anderer Anwendungsfall ist das sogenannte „*Retargeting*“, bei dem z.B. ein betrachtetes Produkt von einer Website dem Benutzer wieder als Anzeige und quasi „Rücksprungmöglichkeit“ auf anderen Webseiten angezeigt wird. Auch in diesem Anwendungsfall werden auf dem Endgerät gespeicherte Cookies verwendet, um den Nutzer auf der anderen Website wiederzuerkennen.

[33] Hinzu kommt oft, dass beim „Schalten“ einer konkreten Anzeige Netzwerkanfragen zur *Leistungsmessung* (audience measuring) an dritte Server gehen, die dem Betreiber der ursprünglichen werbefinanzierten Webseite nicht bekannt sind, da diese direkt aus der im Browser des Nutzers dargestellten Anzeige aufgerufen werden.

[34] Zusammenfassend kann also festgehalten werden, dass insbesondere der Sachverhalt einer werbefinanzierten Webseite aus technischer Sicht hochkomplex ist und viele Kommunikationspartner involvieren kann. Welche Rechtsverhältnisse diese Kommunikationspartner mit dem ursprünglich aufgerufenen Telemediendienst und dem Nutzer sowie untereinander haben und welche rechtlichen Anforderungen an ggf. notwendige Einwilligungen gestellt werden, ist eine Rechtsfrage. Festzuhalten ist aber, dass der Browser des Nutzers mit diesen Akteuren direkt kommuniziert und diese oft auch Cookies in das Endgerät des Nutzers schreiben und lesen.

[35] Aus Sicht der Autoren dieser Studie sind Szenarien wie diese der Maßstab, an dem sich ein Konzept für anerkannte Dienste zum Einwilligungsmanagement technisch messen lassen muss.

4. Rechtliche Bewertung automatisierter Einwilligungserklärungen aufgrund ex-ante definierter Einwilligungstypen

4.1. Allgemeines

4.1.1. Einwilligung und Einwilligungsverwaltung nach dem TTDSG

[36] Die Speicherung von Informationen in Endeinrichtungen von Nutzern oder der nachgelagerte Zugriff hierauf unterliegt gem. § 25 Abs. 1 S. 1 TTDSG grundsätzlich einem Einwilligungsvorbehalt. Erforderliche Einwilligungen können durch anerkannte Dienste zur Einwilligungsverwaltung gem. § 26 TTDSG verwaltet und an Telemedienanbieter weitergegeben werden. Das TTDSG sieht den anerkannten Dienst als einen Intermediär – ohne wohl auszuschließen, dass der Dienst in der bloßen Bereitstellung einer Plugin Software besteht – und formuliert Anforderungen an dessen Neutralität (kein wirtschaftliches Eigeninteresse) hinsichtlich der verwalteten Einwilligung sowie der gespeicherten Nutzerdaten.[5] Neben der Neutralität stellen ein nutzerfreundliches und wettbewerbskonformes Verfahren sowie die Bereitstellung der technischen Anwendungen zur Einholung und Verwaltung der Einwilligung weitere gesetzliche Vorgaben für anerkannte Dienste dar. Im Ergebnis muss der Telemedienanbieter nachweisen können, dass eine Einwilligung vorliegt, die die gesetzlichen Anforderungen an die Wirksamkeit erfüllt. Daher ist es in einem ersten Schritt erforderlich, die gesetzlichen Bedingungen für eine wirksame Einwilligung zu identifizieren und diese auf nutzerfreundliche und wettbewerbskonforme Verfahren und Anwendungen für die Erteilung einer Einwilligung zu übertragen.

4.1.2. Verhältnis von TTDSG und DSGVO

[37] Generell dient die DSGVO (neben dem freien Verkehr personenbezogener Daten) dem Datenschutz iSd Art. 8 der Charta der Grundrechte in der EU (GRC),

[5] Vgl. § 26 Abs. 1 Nr. 2 TTDSG.

während das TTDSG insoweit, als es auf der E-Privacy-RL[6] beruht, sowohl dem Datenschutz iSd Art. 8 GRC[7] als vor allem auch der Vertraulichkeit der Kommunikation iSd Art. 7 GRC dient. Das TTDSG bzw. die E-Privacy-RL konkretisieren und ergänzen dabei die DSGVO für den Bereich der elektronischen Kommunikation. Die wichtigste Erweiterung im personell-sachlichen Anwendungsbereich, die durch das TTDSG im Vergleich zur DSGVO erfolgt, ist dabei die Erweiterung auf Daten juristischer Personen bzw. sonstige nicht-personenbezogene Daten. Insbesondere durch diese Erweiterung, aber auch infolge anders formulierter Rechtsgrundlagen für die Verarbeitung personenbezogener Daten, ist es erforderlich, den Anwendungsbereich des TTDSG und der DSGVO gegeneinander abzugrenzen.

[38] Das TTDSG genießt (nur) insoweit Vorrang vor der DSGVO, als auch die E-Privacy-RL gegenüber der DSGVO *lex specialis* ist.[8] Unter vorsichtiger Interpretation der E-Privacy-RL im Lichte des deutlich klarer formulierten Art. 2 Abs. 1 des Entwurfs für eine E-Privacy-VO in der vom Rat für den Trilog freigegebenen Fassung[9] betrifft der Vorrang des E-Privacy-Rechts (a) die Verarbeitung elektronischer Kommunikationsdaten, also Kommunikationsinhalte und elektronischer Kommunikationsmetadaten (Verkehrsdaten), im Zusammenhang mit der Bereitstellung und Nutzung elektronischer Kommunikationsdienste, (b) Informationen über die Endgeräte der Endnutzer, (c) das Anbieten öffentlich zugänglicher Verzeichnisse der Endnutzer elektronischer Kommunikationsdienste und (d) das Versenden von Direktwerbung an Endnutzer. Während hinsichtlich (c) und (d) keine Abgrenzungsschwierigkeiten bestehen, bleiben die Abgrenzungsschwierigkeiten hinsichtlich (a) und (b). Insbesondere ist zu ermitteln, welche Verarbeitungsvorgänge noch „im Zusammenhang mit“ der Bereitstellung und Nutzung elektronischer Kommunikationsdienste erfolgen.

---

[6] Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation, ABl. L 2002/201, 37.
[7] Charta der Grundrechte der Europäischen Union, ABl. C 2012/326, 391.
[8] Vgl. *Hanloser*, Schutz der Geräteintegrität durch § 25 TTDSG – Neue Cookie-Regeln ab dem 1.12.2021 ZD 2021, 399 (399).
[9] Council Mandate vom 10. Februar 2021, ST 6087/2021 INIT, abrufbar unter https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf (zuletzt abgerufen am 16.12.2021).

[39] Laut Art. 2 Abs. 2 lit. 3 des Entwurfs für eine E-Privacy-VO in der vom Rat für den Trilog freigegebenen Fassung soll die Zäsur jedenfalls hinsichtlich der Kommunikationsdaten im Sinne von (a) der Empfang durch den Empfänger der Kommunikation sein, d.h. jede weitere Verarbeitung der Daten durch den Empfänger der Kommunikation richtet sich nach der DSGVO. Dagegen untersteht die Verarbeitung von Kommunikationsdaten gerade durch Betreiber von Kommunikationsnetzen und -diensten jedenfalls vorrangig dem E-Privacy-Recht. Die Weitergabe von Kommunikationsdaten durch die Betreiber von Kommunikationsnetzen und -diensten an Dritte wird zwar ohnehin unter die Bedingung der vollen Anonymisierung gestellt,[10] doch wird man bei Weitergabe personenbezogener Kommunikationsdaten davon ausgehen müssen, dass ihre Verarbeitung durch Dritte (z.B. Werbedienstleister) ausschließlich der DSGVO unterliegt. Das TTDSG regelt die Verarbeitung von Kommunikationsdaten daher gleichsam nur „an der Quelle", d.h. nur soweit ein Betreiber eines Kommunikationsnetzes oder -dienstes derartige Daten Dritten zur Verfügung stellt, worunter auch die Ermöglichung der Datenerhebung durch den Dritten (bei Passivität des Betreibers des Kommunikationsnetzes oder Kommunikationsdienstes) zu fassen sein muss.

[40] Bei Endgerätedaten, die (i) auf zur elektronischen Kommunikation verwendeten Endgeräten bereits gespeichert sind, oder (ii) im Zusammenhang mit elektronischer Kommunikation auf dem Endgerät gespeichert werden, oder (iii) vom Endgerät beim Verbindungsaufbau mit anderen Endgeräten verarbeitet oder emittiert werden, ist die Verarbeitung dagegen auch durch andere Akteure als Betreiber von Kommunikationsnetzen und -diensten vorrangig durch das E-Privacy-Recht geregelt. Dies gilt dann nicht nur „an der Quelle", sondern darüber hinaus auch für weitere Verarbeitungsvorgänge betreffend solche Daten. Allerdings stellt sich die Frage, wie weit bei der Verarbeitung von Endgerätedaten die „Ausstrahlungswirkung" des E-Privacy-Rechts reicht (und sich damit z.B. die Rechtsgrundlagen der Datenverarbeitung vorrangig nach dem E-Privacy-Recht zu richten haben). Bedeutung erlangt dies v.a. für umfassende Profile, die ursprünglich mithilfe von Endgerätedaten erstellt wurden, und daraus getroffene Ableitungen.

[10] Vgl. Art. 6b Abs. 2 und 6c Abs. 3 ST 6087/2021 INIT.

4.1.3. Abhängigkeit von Entwicklungen betreffend die E-Privacy-VO

[41] Angesichts der Vorrangigkeit des Unionsrechts vor dem TTDSG, könnte die Zukunft von §§ 25, 26 TTDSG auch von der Neuregelung des E-Privacy-Rechts auf EU-Ebene abhängen. Einen direkten Hinweis auf das Phänomen von „consent fatigue“ und die Möglichkeit einer Einwilligungsverwaltung durch Softwareeinstellungen findet sich im Verhandlungsmandat für den Rat für den Trilog zur E-Privacy-VO im vom Rat neu eingefügten ErwGr 20a:

> *“(20a) End-users are often requested to provide consent to the storage and access to stored data in their terminal equipment, due to the ubiquitous use of tracking cookies and similar tracking technologies. As a result, end-users may be overloaded with requests to provide consent. This can lead to a situation where consent request information is no longer read and the protection offered by consent is undermined. Implementation of technical means in electronic communications software to provide specific and informed consent through transparent and user-friendly settings, can be useful to address this issue. Where available and technically feasible, an end user may therefore grant, through software settings, consent to a specific provider for the use of processing and storage capabilities of terminal equipment for one or multiple specific purposes across one or more specific services of that provider. For example, an end-user can give consent to the use of certain types of cookies by whitelisting one or several providers for their specified purposes. Providers of software are encouraged to include settings in their software which allow endusers, in a user friendly and transparent manner, to manage consent to the storage and access to stored data in their terminal equipment by easily setting up and amending whitelists and withdrawing consent at any moment. In light of end-user’s self-determination, consent directly expressed by an end-user should always prevail over software settings. Any consent requested and given by an end-user to a service should be directly implemented, without any further delay, by the applications of the end user’s terminal. If the storage of information or the access of information already stored in the end-user’s terminal equipment is permitted, the same should apply.”*

[42] Ganz in diesem Sinne finden sich wichtige Bestimmungen des Verhandlungsmandates des Rates für den Trilog zur E-Privacy-VO zur Einwilligung und Einwilligungsverwaltung in deren Art. 4a. Diese machen noch einmal deutlich, dass hier primär an Browser-Einstellungen gedacht ist, und nicht unbedingt an separate

Dienste der Einwilligungsverwaltung. Der vorgeschlagene Art. 4a lautet auszugsweise:

> *"2. Without prejudice to paragraph 1, where technically possible and feasible, for the purposes of point (b) of Article 8 (1), consent may be expressed by using the appropriate technical settings of a software application enabling access to the internet placed on the market permitting electronic communications, including the retrieval and presentation of information on the internet.*
>
> *2aa. Consent directly expressed by an end-user in accordance with Paragraph (2) shall prevail over software settings. Any consent requested and given by an end-user to a service shall be directly implemented, without any further delay, by the applications of the end user's terminal, including where the storage of information or the access of information already stored in the enduser's terminal equipment is permitted.*
>
> *2a. As far as the provider is not able to identify a data subject, the technical protocol showing that consent was given from the terminal equipment shall be sufficient to demonstrate the consent of the end-user according Article 8 (1) (b).*
>
> *3. End-users who have consented to the processing of electronic communications data in accordance with this Regulation shall be reminded of the possibility to withdraw their consent at periodic intervals of [no longer than 12 months], as long as the processing continues, unless the end-user requests not to receive such reminders."*

[43] Diese derzeit in Diskussion befindlichen Vorschläge lösen einerseits eine Reihe von Fragen, die für anerkannte Dienste der Einwilligungsverwaltung derzeit Probleme bereiten (etwa die Frage des Identitätsmanagements, dazu unten 4.5.1), andererseits ist aber auch unklar, inwieweit der vorgeschlagene Art. 4a Abs. 2aa für anerkannte Dienste der Einwilligungsverwaltung zu einer Einschränkung der Funktionen führen kann (dazu unten 4.5.6).

4.1.4. Abhängigkeit vom Data Governance Act (DGA)

[44] Neben der E-Privacy-VO ist es auch der künftige Data Governance Act (DGA)[11], der für anerkannte Dienste der Einwilligungsverwaltung Bedeutung haben dürfte.

[11] ST 14606/2021 INIT.

Bei anerkannten Diensten zur Einwilligungsverwaltung dürfte es sich zumindest in der Regel zugleich um ‘data intermediation services’[12] im Sinne des DGA handeln.

[45] Nach den Bestimmungen von Kapitel 3 DGA (in der Fassung des nach Abschluss des Trilogs vorliegenden Kompromisstextes vom 10. Dezember 2021) wären, neben einem Registrierungserfordernis, Anforderungen, die denen in § 26 Abs. 1 TTDSG ähneln (Unabhängigkeit, Datensicherheit usw.) und auch noch eine Reihe von Anforderungen, die für die technische Ausgestaltung der Einwilligungsverwaltung von Bedeutung sein dürften, anwendbar. Die Fassung des Verhandlungsmandates des Rats für den Trilog zählt in Art. 11 dazu u.a. auch die folgenden Anforderungen auf:

> *“(4) the provider shall facilitate the exchange of the data in the format in which it receives it from the data subject or a data holder and shall convert the data into specific formats only to enhance interoperability within and across sectors or if requested by the data user or where mandated by Union The provider shall offer an opt-out possibility regarding those conversions to data subjects or data holders, unless the conversion is mandated by Union law;*
>
> *[…]*
>
> *(10) the provider offering services to data subjects shall act in the data subjects’ best interest when facilitating the exercise of their rights, in particular by informing and, where appropriate, advising data subjects in a concise, transparent, intelligible and easily accessible form about intended data uses by data users and standard terms and conditions attached to such uses, before data subjects give consent;*
>
> *(11) where a provider of data intermediation services provides tools for obtaining consent from data subjects or permissions to process data made available by data holders, it shall, where relevant, specify the jurisdiction or jurisdictions outside the Union in which the data use is intended to take place and provide data subjects with tools to both give and withdraw consent and data holders with tools to both give and withdraw permissions to process data;*

[12] Article 2(2a) ST 14606/2021 INIT.

(11a) the provider shall maintain a log record of the intermediation activity.

[46] Inwieweit Deutschland vom DGA abweichende bzw. über den DGA hinausgehende Vorschriften für Dienste zur Einwilligungsverwaltung beibehalten kann, bestimmt sich nach Art. 1 DGA:

> *"(2) … Where a sector-specific Union legal act or national law requires … providers of data intermediation services or registered entities providing data altruism services to comply with specific additional technical, administrative or organisational requirements, including through an authorisation or certification regime, those provisions of that sector-specific Union legal act or national law shall also apply. Any additional requirements shall be non-discriminatory, proportionate and objectively justified.*
>
> *(3) Union and national law on the protection of personal data shall apply to any personal data processed in connection with this Regulation. In particular, this Regulation shall be without prejudice to Regulation (EU) 2016/679, Regulation (EU) 2018/1725 and Directive 2002/58/EC,…."*

[47] Das bedeutet zunächst, dass etwa Vorschriften, die ein Anerkennungsverfahren vorsehen, sektorspezifisch sein müssen, was auf das TTDSG zutreffen dürfte. Sie müssen aber auch vor dem Hintergrund der europäischen Harmonisierungsbestimmungen nicht-diskriminierend, verhältnismäßig und objektiv gerechtfertigt sein, was man bei einer Abweichung der Anerkennungsvoraussetzungen nach § 26 TTDSG von den in Art. 11 DGA genannten Voraussetzungen zulasten von Intermediären – die etwa in Bezug auf das Ausmaß der Unabhängigkeit gegeben sein könnte[13] – prüfen müsste. Auch das Verhältnis der zuständigen Stellen sollte beobachtet werden.[14]

---

[13] Dies ist unklar, vgl. die Formulierung „kein wirtschaftliches Eigeninteresse an der Erteilung der Einwilligung und an den verwalteten Daten haben und unabhängig von Unternehmen sind, die ein solches Interesse haben können" im TTDSG einerseits und „shall provide data intermediation services through a legally separate structure" Art. 11 Abs. 1 (der allerdings vor dem Hintergrund von ErwGr 26 zu lesen ist) andererseits.

[14] So stellt sich die Frage, ob die unabhängige Stelle in § 26 TTDSG mit Inkrafttreten des DGA auch als zuständige Behörde iSd Art 12 mit der Überwachung des Art 11 beauftragt wird bzw. beauftragt werden kann. Anders als § 26 TTDSG sieht der DGA nämlich in Art 23 mehrere Kriterien vor, welche die „unabhängige Stelle" möglicherweise nicht erfüllt oder erfüllen kann. Im schlimmsten Fall würde dies zu einer Verdoppelung der Zertifizierung durch zwei zuständige Stellen führen.

[48] Die Vorrangklausel in Art. 1 Abs. 3 DGA bezieht sich ihrem Wortlaut nach nur auf personenbezogene Daten, beansprucht also gegebenenfalls für von § 26 TTDSG erfasste nicht-personenbezogene Daten (z.B. unternehmensbezogene Daten) keine Geltung. Auch soweit man die Vorrangklausel auf das gesamte Unions- und E-Privacy-Recht bezieht, erfasst sie doch keine Dienste der Einwilligungsverwaltung, weil solche Dienste derzeit vom E-Privacy-Recht auf EU-Ebene auch nicht ansatzweise geregelt werden. Auch die Art. 4a Abs. 2 ff des Vorschlags für eine E-Privacy-VO zielen primär auf Browser-Einstellungen ab, und nicht unbedingt auf separate Dienste der Einwilligungsverwaltung.

4.1.5. Abhängigkeit von Entwicklungen betreffend den Data Act (DA)

[49] Die Kommission verfolgt ausweislich eines Inception Impact Assessments für einen noch zu veröffentlichenden Data Act[15] das Ziel, die Vorteile einer Datennutzung gerecht zwischen Unternehmen, Verbrauchern und öffentlichen Einrichtungen aufzuteilen. Hierzu soll der Zugang zu und die Nutzung von Daten zwischen Unternehmen untereinander (B2B) sowie zwischen Unternehmen und Behörden (B2G) erleichtert werden. Die Verwendung von Smart Contracts spielt in den Augen der Kommission hierbei eine bedeutende Rolle, die sich nicht nur auf den Datenteilungsvorgang erstreckt, sondern Portabilitätsansprüche Betroffener automatisiert zu unterstützen vermag, bspw. durch Inhaber eines Endgeräts im Bereich des Internet of Things (IoT). Die Vorteile von Smart Contracts liegen im Bereich des Datenteilens aber auch bei Portierungen von Daten Betroffener in ihrer automatisierten und transparenten Umsetzung, die an vordefinierte Bedingungen eines Nutzers oder eines Unternehmens geknüpft werden kann. Hierzu werden Blockchain-Verfahren und solche einer Distributed Ledger Technology verwendet.

[50] Es wird noch zu prüfen sein, welche Rolle anerkannte Dienste im Bereich der Datenteilung oder der Betroffenenrechte im Rahmen eines Data Act einnehmen

[15] Ares(2021)3527151, abrufbar unter https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13045-Data-Act-&-amended-rules-on-the-legal-protection-of-databases_en (zuletzt abgerufen am 16.12.2021).

werden können. Eine unmittelbare Regulierung von solchen Diensten, einschließlich der Intermediäre, ist nach derzeitigem Kenntnisstand innerhalb eines Data Act nicht bezweckt. Sollten anerkannte Dienste jedoch über die Einwilligungsverwaltung hinausgehende Funktionalitäten anbieten, werden sie sich unter Umständen an den Vorgaben des Data Act zu orientieren haben.

[51] Beispielsweise bezweckt der Data Act, neben der Verwendung von Smart Contracts, in Ergänzung zu Art. 20 DSGVO[16] die Schaffung technischer Spezifikationen, um Betroffenen den Datenumzug zu erleichtern. Hierbei sollen Hersteller insbesondere von IoT-Geräten zur Vorhaltung technischer Programmschnittstellen für eine Datenübertragung in Echtzeit verpflichtet werden. Vertraut ein IoT-Hersteller beispielsweise auf einen anerkannten Dienst zur Umsetzung von Portierungsanfragen, so über die Anbindung an dessen Schnittstellen, werden besagte technisch-organisatorische Vorgaben eines Data Act für einen solchen Dienst von Bedeutung sein.

4.2. Generelle Anforderungen an die Einwilligung bei Zugriffen auf Endeinrichtungen

[52] Die gesetzlichen Anforderungen an die Einwilligung in die Speicherung von Informationen auf Endeinrichtungen und in den Zugriff auf Informationen, die bereits dort gespeichert sind ergeben sich gemäß § 25 TTDSG aus der DSGVO. Art. 4 Nr. 11 DSGVO definiert die Einwilligung *als jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist*. Art. 7 DSGVO sowie die Erwägungsgründe 32, 33, 42 und 43 formulieren weitere

[16] In der DSGVO sind keine technischen Spezifikationen für den Datenportabilitätsanspruch vorgesehen. Vielmehr werden die Verantwortlichen in ErwGr 68 lediglich dazu aufgefordert, interoperable Formate zu entwickeln, die die Datenportabilität ermöglichen. Weitergehend sind bereits die Pflichten in Art. 6 Abs. 1 lit. h des Vorschlags für einen Digital Markets Act (COM(2020) 842 final), welcher Gatekeeper dazu verpflichtet, „für die effektive Übertragbarkeit der Daten sorgen, die durch die Tätigkeit eines gewerblichen Nutzers oder Endnutzers generiert werden, und insbesondere Instrumente bereitstellen, die Endnutzern im Einklang mit der DSGVO die Datenübertragung erleichtern, indem unter anderem ein permanenter Echtzeitzugang gewährleistet wird."

Bedingungen für die Einwilligung. Maßgeblich für das Vorliegen einer wirksamen Einwilligung ist insoweit, dass eine freiwillige, informierte, für den bestimmten Fall unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung vorliegt, womit die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung ihrer personenbezogenen Daten einverstanden ist.[17]

4.2.1. Freiwillig

[53] Die Entscheidung, eine Einwilligung frei zu erteilen, setzt im Wesentlichen eine Souveränität der Nutzer voraus, ein Einverständnis in den Eingriff in die Geräteautonomie zu erteilen oder dies zu unterlassen, ohne Nachteile zu erleiden. Unzulässig ist es insoweit, Druck auf Nutzer auszuüben, um sie zur Erteilung einer Einwilligung verleiten. Betroffene Personen müssen daher eine echte bzw. freie Wahl über die Erteilung einer Einwilligung haben (vgl. ErwGr 42 S. 5 DSGVO) und damit eine Kontrolle hierüber haben.[18] Ein Verweigern oder Zurückziehen einer Einwilligung darf nicht mit Nachteilen für Betroffene verbunden sein.

[54] Die gesetzgeberischen Hinweise in Art. 7 Abs. 4 DSGVO sind ebenso in die Beurteilung der Freiwilligkeit mit einzubeziehen, der die Bedingung der Erteilung einer Einwilligung unter anderem für eine Vertragserfüllung, einschließlich der Erbringung einer Dienstleistung, unter einen besonderen Prüfvorbehalt stellt.

[55] Sollen verschiedene Verarbeitungsvorgänge von personenbezogenen Daten über eine Einwilligung legitimiert werden, setzt ErwGr 43 S. 2 DSGVO bei der Frage der Freiwilligkeit voraus, dass die Einwilligung zwischen verschiedenen Verarbeitungsvorgängen differenziert, wenn dies im Einzelfall „angebracht ist“. Während Teile der Literatur die Granularität der Einwilligung mit Blick auf den Wortlaut von ErwGr 42 S. 2 als nicht die Regel ansehen[19], ist aus aufsichtsbe-

---

[17] Vgl. *Europäischer Datenschutzausschuss*, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679 v. 04.05.2020, Rn. 11.
[18] *Europäischer Datenschutzausschuss*, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679 v. 04.05.2020, Rn. 13.
[19] *Baumann/Alexiou*, Cookie-Walls und die Freiwilligkeit von Nutzereinwilligungen – Wie fest darf die Cookie-Wall stehen? ZD 2021, 349 (351).

hördlicher Sicht die Trennung von verschiedenen Zwecken einer Datenverarbeitung und das Einholen der Einwilligung für jeden Zweck als erforderlich anzusehen.[20]

[56] Bezogen auf einen anerkannten Dienst müssen Nutzer technisch in die Lage versetzt werden, für Telemediendienste ihre Einwilligung frei und souverän zu erteilen oder zu verweigern. Nutzer dürfen insofern nicht technisch dazu gezwungen sein, bei einer Einwilligung zugunsten eines Telemediendienstes, zugleich allen oder bestimmten weiteren Diensten eine Einwilligung erteilen zu müssen oder auf die Einwilligung zugunsten des ausgewählten Dienstes zu verzichten.

4.2.2. Informiert

[57] Eine Einwilligung hat ausweislich der gesetzlichen Definition in „informierter Weise“ zu erfolgen. Diese eng mit dem Datenschutzprinzip der Transparenz der Datenverarbeitung (vgl. Art. 5 Abs. 1 lit. a DSGVO) stehende Vorgabe bezweckt, dass Betroffene Eingriffe in die Geräteautonomie nachvollziehen und die Konsequenzen hieraus abschätzen können.[21] Der Europäische Datenschutzausschuss[22] hat Mindestanforderungen an den Inhalt der Information formuliert, damit die Einwilligung in informierter Weise abgegeben wird:

- die Identität des Verantwortlichen,
- der Zweck jedes Verarbeitungsvorgangs, für den die Einwilligung eingeholt wird,
- die (Art der) Daten, die erhoben und verwendet werden,
- das Bestehen eines Rechts, die Einwilligung zu widerrufen,
- gegebenenfalls Informationen über die Verwendung der Daten für eine automatisierte Entscheidungsfindung gemäß Artikel 22 Absatz 2 Buchstabe c, und

---

[20] *Europäischer Datenschutzausschuss*, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679 v. 04.05.2020, Rn. 44.
[21] Vgl. *EuGH* C-673/17, Rn. 74 – *Planet 49*.
[22] Besagter Ausschuss nimmt iSv Art. 15 Abs. 3 der E-Privacy-RL den Schutz der Grundrechte und der Grundfreiheiten und der berechtigten Interessen im Bereich der elektronischen Kommunikation wahr. Insoweit heißt es in Art. 94 Abs. 2 DSGVO: *„Verweise auf die aufgehobene Richtlinie gelten als Verweise auf die vorliegende Verordnung. Verweise auf die durch Artikel 29 der Richtlinie 95/46/EG eingesetzte Gruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten gelten als Verweise auf den kraft dieser Verordnung errichteten Europäischen Datenschutzausschuss.“*

- Angaben zu möglichen Risiken von Datenübermittlungen ohne Vorliegen eines Angemessenheitsbeschlusses und ohne geeignete Garantien nach Artikel 46.[23]

[58] Die dargelegten Mindestanforderungen decken sich teilweise mit Erwägungsgrund 43 S. 4 DSGVO, der die Angabe des Verantwortlichen und die Zwecke der Datenverarbeitung fordert, damit Betroffene in Kenntnis der Sachlage ihre Einwilligung geben können.

[59] Im Bereich der Cookies wurde seitens des EuGH die Vorgabe aufgestellt, dass die Dauer einer Speicherung von Cookies sowie eine Zugriffsmöglichkeit Dritter auf die darin gespeicherten Informationen bei der Sammlung von Informationen zu Werbezwecken für Produkte der Partner des Veranstalters eines Gewinnspiels zu benennen wären.[24]

[60] In dem Fall, in dem sich mehrere (gemeinsame) Verantwortliche auf die erteilte Einwilligung berufen wollten, oder wenn die Daten an andere Verantwortliche übermittelt oder von anderen Verantwortlichen verarbeitet werden sollten, die sich auf die ursprüngliche Einwilligung stützen möchten, sind nach Auffassung des Europäischen Datenschutzausschusses alle diese Organisationen zu nennen.[25]

[61] Auch wenn sich die datenschutzrechtlichen Informationspflichten gem. Art. 13 und Art. 14 DSGVO mit den Anforderungen an die Informiertheit einer Einwilligung wesentlich überschneiden, sind die Vorgaben an die Transparenz einer Verarbeitung personenbezogener Daten von der Informiertheit der Einwilligung zu trennen.[26] Insofern ist die Erhebung personenbezogener Daten in der Regel

---

[23] *Europäischer Datenschutzausschuss*, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679 v. 04.05.2020, Rn. 64.
[24] *EuGH* C-673/17 Rn. 75 – *Planet 49*.
[25] *Europäischer Datenschutzausschuss*, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679 v. 04.05.2020, Rn. 65.
[26] *Europäischer Datenschutzausschuss*, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679 v. 04.05.2020, Rn. 72; *Paal/Pauly/Paal/Hennemann*, DS-GVO BDSG, Art 13 DSGVO Rn. 9a; vgl. aber *Schmidt-Wudy* in BeckOK DatenschutzR, 37. Edition Stand: 01.08.2021, Art. 13 DS-GVO, Rn. 19; *Stemmer* in BeckOK DatenschutzR, 37. Edition Stand: 01.05.2021, Art. 7 DS-GVO, Rn. 55 ff.

ein der Einwilligung für einen Eingriff in eine Geräteautonomie nachgelagerter Vorgang.

[62] Unbeantwortet bleibt die Frage, *wie* die aufgezeigten Mindestinhalte an die Information den Nutzern zu kommunizieren sind. Nachvollziehbar ist hierbei die aufsichtsbehördlich formulierte Anforderung an eine einfache und klare Sprache, wobei die jeweilige Zielgruppe, so beispielsweise Minderjährige, zu berücksichtigen ist.[27]

[63] Erwägungsgrund 43 S. 3 DSGVO stellt Bedingungen für vorformulierte Einwilligungen auf, welche in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zur Verfügung gestellt werden und keine missbräuchlichen Klauseln gemäß der Richtlinie 93/13/EWG beinhalten sollten. Die Richtlinie 93/13/EWG bezweckt die Kontrolle von nicht im Einzelnen ausgehandelten Vertragsklauseln zwischen Gewerbetreibenden und Verbrauchern. Eine solche Inhaltskontrolle fehlt der Datenschutz-Grundverordnung.[28]

[64] Überträgt man die allgemeinen Anforderungen an die Informiertheit der Einwilligung auf anerkannte Dienste, müssen diese bei der *Gestaltung* von Einwilligungstexten dafür sorgen, dass sie Nutzer eindeutig und unmissverständlich über einen oder mehrere Zwecke einer Datenverarbeitung informieren.

4.2.3. Für den bestimmten Fall

[65] Art. 6 Abs. 1 lit. a DSGVO stellt klar, dass Betroffene ihre Einwilligung für einen oder mehrere bestimmte Zwecke bei einer Verarbeitung ihrer personenbezogenen Daten geben. Dies geht auf das Datenschutzprinzip des Art. 5 Abs. 1 lit. b DSGVO zurück, das wiederum fordert, dass personenbezogene Daten für *festgelegte*, *eindeutige* und *legitime* Zwecke zu erheben sind. Dies ist Ausdruck der sog. „Granularität“ der Einwilligung, die für jeden Verarbeitungszweck gegeben werden muss (vgl. ErwGr 32 S. 4 u. 5 DSGVO).

---

[27] *Europäischer Datenschutzausschuss*, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679 v. 04.05.2020, Rn. 70.
[28] Vgl. *Simitis/Hornung/Spiecker* gen. *Döhmann/Klement*, Datenschutzrecht, Art. 7 DSGVO, Rn. 80.

[66] Betroffene können durch eine Willensbekundung in verschiedene Vorgänge einwilligen, solange diese demselben Zweck zugeordnet werden können.[29] Pauschale Einwilligungen scheiden mit Blick auf die gesetzlich geforderte Zweckbindung aus.[30]

[67] Bei mehreren Zwecken, die ein Verantwortlicher verfolgt, wären entsprechend gesonderte Einwilligungen einzuholen und hierbei sollten Informationen über Daten gegeben werden, die für jeden Zweck verarbeitet werden.[31]

[68] Stehen Zwecke einer Verarbeitung personenbezogener Daten im Rahmen der Datenerhebung noch nicht fest, ist die Verarbeitung mithin ergebnisoffen, erscheint die Einwilligung nicht möglich. Abhilfe könnte hier die Generaleinwilligung schaffen, die im Bereich der wissenschaftlichen Forschung durch den Gesetzgeber berücksichtigt wurde (vgl. ErwGr 33 DSGVO). Der diesem Modell zugrunde liegende Gedanke ist, dass Betroffene eine gestufte Einwilligung erteilen, indem in bestimmte Bereiche einer Datenverarbeitung oder differenziert in eine bestimmte Datenverwendung eingewilligt wird. Diese Möglichkeit der Einwilligungserteilung ist jedoch auf einen bestimmten Verarbeitungskontext begrenzt und erfordert nach aufsichtsbehördlicher Maßgabe weiterhin einen „gut beschriebenen Zweck“[32], so dass Betroffene beispielsweise in einen allgemein beschriebenen Forschungszweck und spezielle, avisierte Phasen des Forschungsprojekts einwilligen. Im Fortgang des Forschungsvorhabens würde dann in weitere Projektabschnitte eingewilligt werden[33] (sog. „dynamic consent“).

[69] Wie konkret ein Zweck zu bestimmen ist, ergibt sich nicht aus der DSGVO. Insoweit bestehen unterschiedliche Ansätze bei Telemedienanbietern, wie granular eine Datenerhebung oder ein Eingriff in ein Endgerät beschrieben wird. Hierbei bestehen unterschiedliche, branchenspezifische Ansätze für die Beschreibung

---

[29] *Europäischer Datenschutzausschuss*, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679 v. 04.05.2020, Rn. 57.
[30] *Gola*/*Schulz*, DSGVO, Art. 7 DSGVO, Rn. 34 m.w.N.
[31] *Europäischer Datenschutzausschuss*, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679 v. 04.05.2020, Rn. 61.
[32] *Europäischer Datenschutzausschuss*, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679 v. 04.05.2020, Rn. 155.
[33] *Europäischer Datenschutzausschuss*, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679 v. 04.05.2020, Rn. 158.

von Datenverwendungen. Eine Anschauung hierzu bieten beispielsweise die IAB Europe Transparency & Consent Framework Policies, die Hinweise für eine Aufklärung in bestimmter Datenverarbeitungszwecke vorsehen.[34]

[70] Da anerkannte Dienste Einwilligungserklärungen aus verschiedenen Branchen verwalten werden, wird sich ein Standardisierungsgrad im Rahmen der Zweckbeschreibung schwerlich über eine autonome Darstellung beim anerkannten Dienst selbst erreichen lassen. Ein anerkannter Dienst sollte jedoch zumindest Differenzierungen in seinen Nutzerpräferenzen zulassen, damit Nutzer ihre Einwilligungen in unterschiedliche Verarbeitungszwecke geben können. In Unterverarbeitungen, die einem übergeordneten Zweck dienen, muss dabei nicht gesondert eingewilligt werden. Es wäre jedoch als besonders nutzerfreundlich anzusehen, wenn Nutzern Unterverarbeitungen in Form eines Entscheidungsbaumes nachträglich angezeigt werden, damit eine Einwilligung in diese Unterverarbeitungen entzogen werden kann.

4.2.4. Unmissverständlich abgegebene Willensbekundung und deren Form

[71] Ausweislich der Definition der Einwilligung hat diese in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung zu erfolgen. Erwägungsgrund 32 konkretisiert diese Vorgaben um beispielhafte Szenarien für eine solche Handlung in Gestalt des Anklickens eines Kästchens beim Besuch einer Internetseite oder durch die Auswahl technischer Einstellungen für Dienste der Informationsgesellschaft. Aber auch andere Erklärungen und Handlungen sollen zulässig sein, mittels derer die betroffene Person ihr Einverständnis in die beabsichtigte Verarbeitung ihrer personenbezogenen Daten signalisiert (vgl. ErwGr 32 S. 2 DSGVO). Die Erteilung der Einwilligung ist grundsätzlich formfrei möglich, was mit Blick auf die anerkannten Dienste die elektronische Form mit einschließt.[35] Dies bedeutet, dass sowohl eine Einwilligung per Softwareeinstellung, als auch über einen anerkannten Dienst mit Authentifizierungssystem mit Blick

[34] *IAB Europe,* Transparency & Consent Framework Policies, Appendix A: Purposes and Features Definitions, abrufbar unter https://iabeurope.eu/iab-europe-transparency-consent-framework-policies/ (zuletzt abgerufen am 16.12.2021).
[35] Vgl. ErwGr 32 S. 1 DSGVO.

auf die Formvorgaben grundsätzlich wirksame Einwilligungserteilungen darstellen. Im Bereich des Widerspruchsrechts gegenüber Diensten der Informationsgesellschaft sieht die Datenschutz-Grundverordnung eine Ausübung mittels automatisierter Verfahren in Art. 21 Abs. 5 DSGVO im Übrigen ausdrücklich vor.

[72] Stillschweigen, bereits angekreuzte Kästchen oder Untätigkeit der betroffenen Person stellen hingegen keine wirksame Einwilligung dar (vgl. ErwGr 32 S. 3 DSGVO). Opt-Out-Lösungen sind daher nicht im Einklang mit der Datenschutz-Grundverordnung, da sie ein Handeln der betroffenen Person erforderlich machen, um die avisierte Verarbeitung personenbezogener Daten zu verhindern.[36]

[73] Wird eine betroffene Person auf elektronischem Weg zur Abgabe einer Einwilligung aufgefordert, so muss die Aufforderung gem. ErwGr 32 S. 6 DSGVO in klarer und knapper Form und ohne unnötige Unterbrechung des Dienstes, für den die Einwilligung gegeben wird, erfolgen. Besagte „klare und knappe Form" ist als eine Vorgabe an die verwendete Sprache sowie den Umfang der Darstellung zu verstehen. Dies bezieht sich zum einen auf eine Reduktion des Informationsgehaltes auf das Wesentliche.[37] Zum anderen ist eine unnötige Unterbrechung des Dienstes dann naheliegend, wenn durch übermäßige Pop-Up-Fenster eine Einwilligung eingeholt wird, was durch eine weniger den Telemediendienst überdeckende Darstellung gleichsam möglich wäre.[38]

[74] Bezogen auf einen anerkannten Dienst zur Einwilligungsverwaltung bedeuten die vorstehenden Ausführungen zumindest, dass in einer Grundeinstellung keine erteilten Einwilligungen vorhanden sein dürfen, es sei denn der Nutzer hat dies selbst veranlasst.

4.3. Besondere Anforderungen in besonderen Situationen

4.3.1. Ausdrücklichkeit

[75] Für besondere Verarbeitungskonstellationen ist es erforderlich, dass die Einwilligung ausdrücklich erteilt wird. Dies gilt für die Einwilligung in die Verarbeitung

[36] Vgl. *EuGH* C-673/17, Rn. 59 – *Planet 49*.
[37] So auch *Gola/Schulz,* DS-GVO, Art. 7 DSGVO, Rn. 47.
[38] In eine ähnliche Richtung argumentierend *Härting*, Datenschutz-Grundverordnung, Rn. 363.

besonderer Kategorien personenbezogener Daten (vgl. Art. 9 Abs. 2 lit. a DSGVO), im Kontext einer automatisierten Einzelentscheidung einschließlich Profiling (vgl. Art. 22 Abs. 2 lit. c DSGVO) sowie bei der Übermittlung personenbezogener Daten in Drittländer (vgl. Art. 49 Abs. 1 lit. a DSGVO). Da bereits im Rahmen der allgemeinen Anforderungen an die Einwilligung eine Erklärung oder eindeutige bestätigende Handlung vorgeschrieben ist, stellt sich die Frage, wie die Ausdrücklichkeit hier einzuordnen ist. Eine stillschweigende oder konkludente Einwilligung ist zunächst mit einer Ausdrücklichkeit nicht gleichzusetzen und scheidet aus.[39] Es wird aufgrund des höheren Risikos einer Verarbeitung personenbezogener Daten in den aufgezeigten Bereichen zu fordern sein, dass die Einwilligung der Betroffenen sich ausdrücklich auf die besonderen Zwecke der Verarbeitung bzw. die verarbeiteten Daten einer besonderen Kategorie bezieht.[40]

[76] Bezogen auf das Einwilligungsmanagement bedeutet dies, dass anerkannte Dienste über Mechanismen verfügen müssen, die Nutzern das erhöhte Risiko der Datenverarbeitung im Einwilligungstext bewusst machen. Dazu gehört, dass im Falle einer Verarbeitung besonderer Kategorien personenbezogener Daten solche Daten ausdrücklich zu benennen sind.

4.3.2. Einwilligung bei Kindern

[77] Besondere Anforderungen an die Einwilligung gelten, wenn ein Angebot von Diensten der Informationsgesellschaft einem Kind direkt gemacht wird und im Zuge dessen eine Verarbeitung der personenbezogenen Daten des Kindes erfolgen soll, die nicht durch einen gesetzlichen Rechtfertigungsgrund gedeckt ist. In diesem Fall ist die Verarbeitung der personenbezogenen Daten des Kindes nur rechtmäßig, wenn das Kind ein bestimmtes Alter erreicht hat oder sofern und soweit die Einwilligung durch den Träger der elterlichen Verantwortung für das Kind oder mit dessen Zustimmung erteilt wird.[41]

[78] Die Mitgliedstaaten haben bei der Festlegung der Altersgrenze bestimmte Freiheiten, wobei die Altersgrenze bei der Vollendung von mindestens dem 13. und

---

[39] *Jaspers/Schwartmann/Mühlenbeck*, DSGVO/BDSG, Art. 9 DSGVO, Rn. 123.
[40] Vgl. *Kühling/Buchner/Weichert*, DSGVO BDSG, Art. 9 DSGVO, Rn. 47.
[41] AA *Schrader*, Datenschutz Minderjähriger (2021) 149 ff, welcher bei Umgehung des gesetzmäßig funktionierenden Systems von einer wirksamen Einwilligung ausgeht.

höchstens dem 16. Lebensjahr zu ziehen ist. Erlässt ein Mitgliedstaat – so wie Deutschland – keine eigene Regelung, liegt die Altersgrenze bei 16 Jahren.[42] Vollkommen ungeklärt ist derzeit noch die kollisionsrechtliche Situation bei grenzüberschreitenden Sachverhalten. Vertreten wird hier sowohl eine analoge Anwendung von Art. 3 DSGVO[43] (und damit idR die Geltung des Zielstaates, in dem das Kind lebt) als auch eine analoge Anwendung von ErwGr 153 Satz 6 DSGVO[44] (und damit die Geltung des Rechts, dem der Verantwortliche unterliegt) als auch eine Außerachtlassung mitgliedstaatlicher Sonderregelungen bei grenzüberschreitenden Sachverhalten (und damit die Geltung einer Altersgrenze von 16 Jahren). Ein anerkannter Dienst der Einwilligungsverwaltung wird sich – auch außerhalb Deutschlands – zur Sicherheit auf eine Altersgrenze von 16 Jahren einstellen müssen.

[79] Nach Art. 8 Abs. 2 DSGVO muss der Verantwortliche unter Berücksichtigung der verfügbaren Technik angemessene Anstrengungen unternehmen, um sich bei unter 16-Jährigen zu vergewissern, dass die Einwilligung durch den Träger der elterlichen Verantwortung für das Kind oder mit dessen Zustimmung erteilt wurde. Bei der Ermittlung, welche Anstrengungen „angemessen“ sind, müssen u.a. der finanzielle und organisatorische Aufwand, Art und Bedeutung der Datenverarbeitung sowie der Grundsatz der Datensparsamkeit berücksichtigt werden.[45] Bei anerkannten Diensten der Einwilligungsverwaltung, bei denen typischerweise einmalig im Voraus bestimmte Präferenzen definiert werden, die dann für eine Vielzahl von Datenverarbeitungen Bedeutung erlangen, werden die Anforderungen eher hoch einzuschätzen sein.

[80] Dem vorgelagert und fast noch wichtiger ist die Frage der Altersüberprüfung, die in der DSGVO nicht explizit geregelt ist. Dennoch wird zu Recht angenommen, dass angemessene Anstrengungen unternommen werden müssen, um das Alter

---

[42] Anders als Deutschland hat aber ein Großteil der Mitgliedstaaten von der Öffnungsklausel gebraucht gemacht: siehe https://www.ugent.be/re/mpor/law-technology/en/research/childrens-rights.htm (zuletzt abgerufen am 16.12.2021).
[43] MüKoBGB/*Wendehorst,* 8. Aufl., EGBGB Art. 43, Rn. 285.
[44] *Thon,* Transnationaler Datenschutz: Das Internationale Datenprivatrecht der DS-GVO, RabelsZ 84 (2020), 24 (38 ff.).
[45] *Europäischer Datenschutzausschuss,* Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679 v. 04.05.2020, Rn. 136; siehe zu den Maßnahmen im Einzelfall *Schrader*, Datenschutz Minderjähriger 151ff; Ehmann/Selmayr/*Heckmann/Paschke*, DS-GVO, Art. 8 DSGVO, Rn. 29 f.

zu überprüfen.[46] Dabei soll ein risikobasierter Ansatz gelten, d.h. bei Datenverarbeitungen mit niedrigem Risiko kann eine Selbstdeklaration des Nutzers genügen, während bei Datenverarbeitungen mit hohem Risiko weitere Maßnahmen erforderlich werden können.[47] Bei anerkannten Diensten der Einwilligungsverwaltung ist einerseits davon auszugehen, dass potenziell in sehr viele Datenverarbeitungen ganz verschiedenen Risikos eingewilligt werden kann, andererseits aber auch davon, dass Minderjährige unter 16 Jahren sich eher selten eines anerkannten Dienstes der Einwilligungsverwaltung bedienen werden (was aber angesichts des zu erwartenden Vorteils, „Cookie-Banner" loszuwerden, auch anders sein kann).

4.3.3. Einwilligung bei schutzbedürftigen Erwachsenen

[81] Keinerlei Regelungen in der DSGVO existieren für schutzbedürftige Erwachsene, denen die Einwilligungsfähigkeit fehlt.[48] Es muss davon ausgegangen werden, dass diejenige Person zur Erteilung der Einwilligung zuständig ist, welche auch in Bezug auf derartige persönliche Dinge die Vertretungsmacht zukommt.[49] Rein praktisch gesehen wird ein anerkannter Dienst zur Einwilligungsverwaltung die Möglichkeit, dass dem Nutzer des Dienstes die Einwilligungsfähigkeit fehlt, ausblenden müssen, weil praktisch keine verhältnismäßige Möglichkeit besteht, sich der Einwilligungsfähigkeit bzw. der Identität der Person, welche die Einstellungen vornimmt (zB Angehörige einer demenzkranken Person), zu versichern.

---

[46] Siehe nur *Schrader*, Datenschutz Minderjähriger 149; *Karg* in BeckOK Datenschutzrecht, 37. Edition, Art 8 DSGVO, Rn. 55 ff.
[47] *Europäischer Datenschutzausschuss*, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679 v. 04.05.2020, Rn. 137.
[48] *Funke*, Dogmatik und Voraussetzungen der datenschutzrechtlichen Einwilligung im Zivilrecht (2017) 219.
[49] Vgl. *Funke*, Dogmatik und Voraussetzungen der datenschutzrechtlichen Einwilligung im Zivilrecht 225 ff.

4.4. Begleitende Anforderungen an Einwilligung und Einwilligungsverwaltung

4.4.1. Nachweisführung und Dokumentation

[82] Teil der Bedingungen für eine wirksame Einwilligung bildet die Pflicht gem. Art. 7 Abs. 1 DSGVO, diese nachweisen zu können. Im Kontext des TTDSG trifft besagte Nachweispflicht anerkannte Dienste *unmittelbar* nur dann, wenn diese im Anschluss an das Speichern oder den Zugriff auf Informationen in der Endeinrichtung des Nutzers als Verantwortliche im Sinne von Art. 4 Nr. 7 DSGVO selbst über Zwecke und Mittel einer Verarbeitung personenbezogener Daten entscheiden. Bezogen auf den E-Privacy-Bereich findet sich in Art. 4a des Verhandlungsmandates des Rats für den Trilog ebenfalls ein Hinweis auf eine Nachweisführung bei Providern:

> *2a. As far as the provider is not able to identify a data subject, the technical protocol showing that consent was given from the terminal equipment shall be sufficient to demonstrate the consent of the end-user according Article 8 (1) (b).*

[83] Unabhängig von der Frage, ob ein anerkannter Dienst selbst als Provider im Sinne der E-Privacy-Regelungen agiert oder als Verantwortlicher gem. Art. 4 Nr. 7 DSGVO, muss ein solcher Dienst Telemedienanbieter zum einen in die Lage versetzen, den Nachweis über eine gültige Einwilligung überhaupt führen zu können. Dies erfordert die Übermittlung einer Datenstruktur, welche die rechtlichen Anforderungen an eine Einwilligung abbildet (zu den hierbei technisch übermittelten Informationen vgl. Abschnitt 5.2).

[84] Zum anderen darf ein anerkannter Dienst nicht übermäßige Daten an einen Anbieter von Telemedien übermitteln, um nicht in Konflikt mit dem Grundsatz der Datenminimierung gem. Art. 5 Abs. 1 lit. c DSGVO zu gelangen.[50] Neben dem Grundsatz der Datenminimierung gilt es auch, Einwilligungen nur so lange aufzubewahren, wie es für den jeweiligen Zweck erforderlich ist (vgl. Art. 5 Abs. 1 lit. e DSGVO). Der jeweils Verantwortliche benötigt eine Einwilligung grundsätzlich

[50] *Europäischer Datenschutzausschuss*, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679 v. 04.05.2020, Rn. 106.

so lange, wie eine Verarbeitung personenbezogener Daten andauert. Entsprechend wird der Verantwortliche den vom anerkannten Dienst erhaltenen Inhalt der Einwilligung für diese Zeit aufbewahren. Der anerkannte Dienst selbst hat jedoch einen wesentlich weiter gefassten Verarbeitungsauftrag der Nutzer, indem der Dienst Einwilligungen für unterschiedliche Verantwortliche verwalten soll. Entsprechend wird der Zweckverbrauch einer konkreten Datenverarbeitung eine Löschverpflichtung nur unter bestimmten Voraussetzungen auslösen können. Eine Löschung von Einwilligungen beim anerkannten Dienst wird geboten sein, wenn Nutzer dies veranlassen, so beispielsweise über das Löschen eines Accounts insgesamt oder das Entfernen einzelner Einwilligungsparameter. Ein anerkannter Dienst wird daher über einen technischen Mechanismus verfügen müssen, der Nutzeranforderungen für das Löschen einer Einwilligung oder von Einwilligungsparametern unverzüglich umsetzt und die damit verbundenen Daten datenschutzkonform löscht. Ausnahmen von der Löschverpflichtung sind grundsätzlich im Bereich gesetzlicher Aufbewahrungsfristen (Art. 17 Abs. 3 lit. b DSGVO) oder hinsichtlich der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen gemäß Artikel 17 Abs. 3 lit. e DSGVO denkbar.

4.4.2. Gültigkeitsdauer

[85] Die Datenschutz-Grundverordnung enthält keine Hinweise, wie lange eine Einwilligung gültig sein soll. Da eine Einwilligung für einen Verarbeitungskontext abgegeben wird, zu dem auch ein Zweck der Verarbeitung gehört, wäre eine Erneuerung regelmäßig dann geboten, wenn sich Zwecke einer Verarbeitung personenbezogener Daten ändern. Die Besonderheit einer Einwilligungsverwaltung durch anerkannte Dienste besteht darin, dass sich deren Aufgaben in einer Speicherung und Verwaltung von Einwilligungen erschöpfen, mithin der konkrete Verarbeitungszweck für den Dienst nicht ohne weiteres erkennbar ist.

[86] Aus Benutzersicht, so insbesondere mit Blick auf ein nutzerfreundliches Verfahren, erscheint es nichtsdestoweniger sachgerecht, verwaltete Einwilligungen regelmäßig zu erneuen.[51] Dies würde für einen anerkannten Dienst bedeuten, dass

[51] *Riechert* Rechtliche Aspekte eines Einwilligungsassistenten, in Stiftung Datenschutz (Hrsg), Neue Wege bei der Einwilligung im Datenschutz – technische, rechtliche und ökonomische Her-

erteilte und gespeicherte Einwilligungen in regelmäßigen Abständen entweder gelöscht oder Nutzer über das Bestehen einer Einwilligung erinnert werden. Letzteres erscheint das nutzerfreundlichere Verfahren zu sein, da durch eine automatisierte Löschung der Einwilligung Nutzer wiederum zu einer Vielzahl von Einwilligungserteilungen gezwungen sind, was in eine unerwünschte Consent Fatigue münden kann. Die Erinnerung an eine bestehende Einwilligung sollte alle Elemente der ursprünglichen Information beinhalten.[52] Der Zyklus eines Erinnerungsverfahrens sollte so gewählt werden, dass Nutzer ein solches als nicht störend empfinden. Hierbei erscheint eine jährliche Erinnerung über erteilte Einwilligungen sachgerecht.

[87] In diesem Zusammenhang ist auch zu erwähnen, dass Art. 4a Abs. 3 des Trilog-Entwurfs für die E-Privacy-VO eine entsprechende Erneuerungspflicht vorsieht:

> "*End-users who have consented to the processing of electronic communications data in accordance with this Regulation shall be reminded of the possibility to withdraw their consent at periodic intervals of [no longer than 12 months], as long as the processing continues, unless the end-user requests not to receive such reminders.*"

4.4.3. Verhältnis der Einwilligung zu den Betroffenenrechten

[88] Der endgültige Entwurf für einen DGA sieht eine Rolle der Intermediäre in der Unterstützung Betroffener bei der Wahrnehmung ihrer Rechte nach der DSGVO. Insofern heißt es in Erwägungsgrund 23:

> *A specific category of data intermediation services includes providers of services that offer their services to data subjects within the meaning of Regulation (EU) 2016/679. Such providers seek to enhance individual agency, and in particular the individuals' control over the data relating to them. They would assist individuals in exercising their rights under Regulation (EU) 2016/679, in particular giving and withdrawing their consent to data processing, the right of access to their own data, the right to the rectification of inaccurate personal data, the right of erasure*

---

ausforderungen (2017), Stellungnahme B Anhang 1 S. 72, abrufbar unter: https://stiftungdatenschutz.org/fileadmin/Redaktion/Bilder/PIMS-Abschluss-Studie-30032017/stiftungdatenschutz_broschuere_20170611_01.pdf (zuletzt abgerufen am 16.12.2021).

[52] *Europäischer Datenschutzausschuss*, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679 v. 04.05.2020, Rn. 111.

> *or right 'to be forgotten', the right to restrict processing and the data portability right, which allows data subjects to move their personal data from one controller to the other.*

[89] Die Unterstützung Betroffener bei der Verwaltung einer Einwilligung nach dem TTDSG wäre demnach nur ein Teil eines größeren Aufgabenspektrums eines Datenintermediärs im Sinne des DGA. Das Wesen der Rolle eines Intermediärs liegt in einem umfassenderen Sinn darin, Betroffene bei der Ausübung ihrer Rechte zu unterstützen. Eine solche Unterstützung kann in der Verwaltung von Anfragen zu Betroffenenrechten und deren Umsetzung durch Verantwortliche gesehen werden. Insgesamt erscheint eine solche Funktionalität bei anerkannten Diensten wichtig zu sein, da personenbezogene Daten von Betroffenen regelmäßig bei einer Vielzahl von Verantwortlichen verarbeitet werden, was es der individuellen Person erschwert, hierüber einen Überblick zu behalten und hinsichtlich einer Datenverarbeitung zu intervenieren, mithin diese kontrollieren zu können. Es gilt zu beachten, ob die Speicherung von personenbezogenen Daten zur Wahrnehmung von Betroffenenrechten bei einem Dritten, hier der Intermediär, erfolgen soll oder im Endgerät des Nutzers selbst, so beispielsweise im Browser.

[90] Besonders nah an der Einwilligungsverwaltung und von dieser unter keinen Umständen zu trennen, ist, die Verwaltung des Widerrufs von Einwilligungen. Das Widerspruchsrecht nach Art. 21 DSGVO, das bei bestimmten gesetzlichen Rechtsgrundlagen der Datenverarbeitung gegeben ist, steht wiederum dem Widerruf der Einwilligung funktional nahe und ist prinzipiell auch im Anwendungsbereich der E-Privacy-VO gegeben, wie Art. 6b Abs. 1 lit. f in der Fassung des Verhandlungsmandates des Rates für den Trilog deutlich macht. Beide stehen in engem funktionalem Zusammenhang mit dem Löschungsverlangen gemäß Art. 17 DSGVO, aber auch mit vorgelagerten Rechten, wie dem Datenzugangs- bzw. Informationsanspruch des Art. 15 DSGVO.

[91] Bei der Ausgestaltung von anerkannten Diensten zur Einwilligungsverwaltung besonders zu berücksichtigen ist – gerade im Hinblick auf die Verbesserung des Datenzugangs – auch das Verhältnis von Einwilligung und Datenportabilität. Zumindest soweit personenbezogene Daten betroffen sind, steht dem Betroffenen

das Datenportabilitätsrecht nach Art. 20 DSGVO zu, das durch den Digital Markets Act (DMA)[53] noch einmal indirekt gegenüber Plattformanbietern mit Torwächterfunktion eine erhebliche Erweiterung erfahren soll. Datenintermediäre im Sinne des DGA werden mindestens in gleichem Maße die Ausübung des Portabilitätsrechts verwalten wie die datenschutzrechtliche Einwilligung. Damit anerkannte Dienste der Einwilligungsverwaltung ihre Funktion in vollem Umfang erfüllen können, und zugleich um die Schutzmechanismen der DSGVO betreffend die Einwilligung nicht durch das Portabilitätsrecht zu unterlaufen, erscheint es angezeigt, dass anerkannte Dienste zur Einwilligungsverwaltung zugleich die Verwaltung von Portabilitätsanfragen und Portabilitätsbewilligungen übernehmen.

[92] Insgesamt erscheinen anerkannte Dienste der Einwilligungsverwaltung nur dann den Nutzerbedürfnissen in vollem Umfang gerecht zu werden, wenn sie zugleich die Betroffenenrechten verwalten. Abgesehen vom Widerruf der Einwilligung, der von der Einwilligung selbst nicht zu trennen ist, wird man in der Rechtsverordnung nach § 26 TTDSG aber keine Verpflichtung aussprechen können.

4.4.4. Technische und rechtliche Anforderungen an die Widerruflichkeit

[93] Betroffene Personen haben das Recht, ihre Einwilligung jederzeit zu widerrufen.[54] Dem Einzelnen steht es frei, ob und in welchem Umfang er seine Einwilligung widerrufen möchte.[55] Der Widerruf muss so einfach wie die Erteilung der Einwilligung sein.[56] Die fehlende Möglichkeit, die Einwilligung ohne Nachteile zu widerrufen, führt zur Unfreiwilligkeit der Einwilligung (ErwGr 42 S. 5 DSGVO). Im Bereich der elektronischen Einwilligungserteilung hat dies aus aufsichtsbehördlicher Sicht zur Folge, dass der Widerruf über dieselbe Benutzerschnittstelle erfolgen können muss, wie die Erteilung der Einwilligung.[57] Dies würde entsprechend für die anerkannten Dienste gelten, deren Wesensmerkmal in der elektronischen

---

[53] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über bestreitbare und faire Märkte im digitalen Sektor, COM(2020) 842 final.
[54] Art. 7 Abs. 3 S. 1 DSGVO.
[55] *Kühling/Buchner/Buchner/Kühling,* DSGVO, Art. 7 DSGVO, Rn. 35.
[56] Art. 7 Abs. 3 S. 4 DSGVO.
[57] *Europäischer Datenschutzausschuss*, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679 v. 04.05.2020, Rn. 114.

Einwilligungsverwaltung liegt. Ausgehend von der Prämisse, dass betroffene Personen entscheiden können, in welchem Umfang eine Einwilligung widerrufen wird, so beispielsweise auszugsweise, kann dies einen anerkannten Dienst vor besondere Herausforderungen stellen. Immerhin ist solchen Diensten ein Standardisierungsgrad hinsichtlich gespeicherten Informationen zu einer Einwilligung und den Widerrufsmöglichkeiten mit Blick auf die Vielzahl möglicher Datenverarbeitungen durch Telemedienanbieter immanent.

[94] Um Nutzerinteressen zu wahren und einen erforderlichen Standardisierungsgrad zu berücksichtigen, sollten anerkannte Dienste grundsätzlich dieselben Benutzeroberflächen[58] für das Einholen und den Widerruf einer Einwilligung verwenden. Dies kann beispielsweise dadurch erreicht werden, indem das Häkchen einer „Tick-Box“ gesetzt und zugleich wieder entfernt werden kann. Schwierigkeiten einer Standardisierung eines anerkannten Dienstes mit Blick auf den Widerruf einer Einwilligung können dann entstehen, wenn Betroffene auf anderem Weg (z.B. per Email) Teile ihrer Einwilligung widerrufen möchten, die möglicherweise beim anerkannten Dient über die Benutzerschnittstelle als ein Zweck dargestellt wird.

[95] Art. 7 Abs. 3 S. 3 DSGVO verpflichtet zu einer Information betroffener Personen über das Bestehen eines Widerrufsrechts. Besagte Belehrung muss nicht nur über das Bestehen des Widerrufsrechts, sondern auch über die Voraussetzungen der Ausübung informieren. [59] Auch ErwGr 18 des Verhandlungsmandates des Rats für den Trilog zur E-Privacy-VO[60] geht von einer Unfreiwilligkeit der Einwilligung aus, wenn diese nicht ohne Nachteile widerrufen werden kann und verpflichtet den Verantwortlichen zusätzlich in Art. 4a Abs. 3, den Endnutzer alle zwölf Monate an die Möglichkeit eines Widerrufs der Einwilligung zu erinnern.[61] Anerkannte Dienste der Einwilligungsverwaltung werden solche möglichen künftigen Entwicklungen zu beachten haben.

---

[58] Benutzerschnittstellen und Benutzeroberflächen sind synonym zu verstehen.
[59] *Europäischer Datenausschuss*, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679 v. 04.05.2020,Rn. 88.
[60] ST 6087/2021 INIT.
[61] Für eine Erinnerung auch nach Datenschutzrecht *Riechert* in Stiftung Datenschutz, Stellungnahme B Anhang 1 S. 72.

4.4.5. Auswirkungen des Widerrufs auf dritte Datenempfänger

[96] Die DSGVO ordnet zwar nicht unmittelbar die Weiterleitung des Widerrufs an dritte Datenempfänger an, denen der Verantwortliche die Daten offengelegt hat. Allerdings muss ein Verantwortlicher nach Art. 17 Abs. 1 lit. b DSGVO die Daten löschen, wenn die betroffene Person ihre Einwilligung widerruft, auf die sich die Verarbeitung stützte und es an einer anderweitigen Rechtsgrundlage für die Verarbeitung fehlt. Kommt es dergestalt zur Löschung, muss der Verantwortliche diese gemäß Art. 19 DSGVO allen Empfängern, denen personenbezogene Daten offengelegt wurden, mitteilen, es sei denn, dies erweist sich als unmöglich oder ist mit einem unverhältnismäßigen Aufwand verbunden. Ferner muss der Verantwortliche die betroffene Person über diese Empfänger unterrichten, wenn die betroffene Person dies verlangt. Es stellt sich die Frage, inwieweit anerkannte Dienste der Einwilligungsverwaltung auch diese Aufgaben mindestens teilweise übernehmen bzw. zumindest die technischen Voraussetzungen dafür schaffen sollten, dass die Weiterleitung an Datenempfänger erfolgt.

4.5. Spezialprobleme bei Diensten zur Einwilligungsverwaltung

4.5.1. Identitätsmanagement

[97] § 25 TTDSG knüpft die Zulässigkeit eines Eingriffs in die Privatsphäre bei Endeinrichtungen an die Einwilligung des *Endnutzers*. Art. 2a) der E-Privacy-Richtline definiert den "Nutzer" *als eine natürliche Person, die einen öffentlich zugänglichen elektronischen Kommunikationsdienst für private oder geschäftliche Zwecke nutzt, ohne diesen Dienst notwendigerweise abonniert zu haben*. Eine Identifizierungspflicht von Nutzern ist der E-Privacy-RL ebenso fremd wie der Fassung des Verhandlungsmandates des Rates zur E-Privacy-VO.

[98] Sollte die Identifizierung eines Endnutzers nicht möglich sein, sieht Art. 4a Abs. 2a des Verhandlungsmandates des Rats für den Trilog zur E-Privacy-VO eine Erleichterung in der Nachweisführung der Einwilligung vor: „*2a.As far as the provider **is not able to identify a data subject**, the **technical protocol showing that consent was given** from the terminal equipment shall be sufficient to demonstrate the consent of the end-user according Article 8 (1) (b).“*

[99] Dieser Fall liegt regelmäßig dann vor, wenn die Einwilligung über eine Browser-Einstellung erteilt wird, ohne dass ein zusätzlicher Authentifizierungsmechanismus gegenüber dem Telemediendienst genutzt würde.

[100] Im Bereich der elektronischen Kommunikation ist ein Identitätsmanagement darauf ausgelegt, auch eine „schwache" Authentifizierung und Einwilligungserteilung über den Besitz eines Endgeräts zu ermöglichen. Andernfalls hätte es der Formulierung strengerer Anforderungen an die Nachweisführung bedurft. Insofern wird ein Telemediendienst jeweils entscheiden, welchen Schutzbedarf er der von der Einwilligung umfassten Daten beimisst. Darauf werden sich Anforderungen an die Identifizierung von Nutzern ergeben (zu den technischen Ausgestaltungen s. nachfolgend Ziff. 5.1).

[101] Die Datenschutz-Grundverordnung regelt verschiedene sog. „Identifizierungsmängel" im Bereich der Betroffenenrechte. Gem. Art. 12 Abs. 2 S. 2 DSGVO kann der Verantwortliche einem Antrag von Betroffenen zur Wahrnehmung ihrer Rechte nicht nachgehen, wenn er nachweisbar nicht in der Lage ist, die betroffene Person zu identifizieren.[62] Art. 12 Abs. 6 DS-GVO ermöglicht es dem Verantwortlichen, erforderliche zusätzliche Informationen von der betroffenen Person anzufordern, sollten Zweifel an ihrer Identität bestehen. Eine solche Überprüfungsmöglichkeit besteht im Einzelfall und ermöglicht keine routinemäßige Identitätsprüfung.[63]

[102] Agiert ein anerkannter Dienst als Verantwortlicher iSv Art. 4 Nr. 7 DS-GVO, wird er im Falle eines Betroffenenantrags Maßnahmen zur Identitätsprüfung in Abhängigkeit von einer Identifizierbarkeit der Person vollziehen und über entsprechende Prozesse verfügen müssen.

[103] Sollten über eine Benutzerschnittstelle beim anerkannten Dienst Betroffenenrechte unmittelbar gegenüber anderen Verantwortlichen wahrgenommen werden können (vgl. Betroffenenrechteprotokoll A: Einsicht in den Datenbestand, Korrekturmöglichkeiten, Ziff. 5.6.4), stellt sich die Frage, ob generell erhöhte Anforderungen an die Feststellung einer Identität eines Nutzers angebracht sind (zu den

---

[62] Die englische Sprachfassung der DSGVO spricht insoweit von *„unless the controller demonstrates"*, während die deutsche Sprachfassung auf eine Glaubhaftmachung verweist.
[63] Vgl. *Kühling/Buchner/Bäcker,* DS-GVO, Art. 12 DSGVO, Rn. 30.

unterschiedlichen technischen Ansätzen eines Identitätsmanagements siehe auch Ziff. 5.1). Einerseits besteht beispielweise bei einer Authentifizierung lediglich über das Endgerät der Nutzer und ohne gesondert geschützte Profile auf dem Gerät die Gefahr, dass beispielsweise personenbezogene Daten im Falle einer Auskunftsanfrage nicht an den Betroffenen, sondern an Dritte übermittelt werden, die im Besitz dieses Endgeräts sind. Andererseits hat der Verantwortliche der betroffenen Person die Ausübung ihrer Rechte zu erleichtern (vgl. Art. 12 Abs. 2 S. 1 DSGVO). Anforderungen an die Authentifizierung von Nutzern und die dem vorgelagerte Identifizierung werden sich wohl an den beim Telemediendienst gespeicherten personenbezogenen Daten zu orientieren haben, um hier einen angemessenen Interessensausgleich zu ermöglichen.

[104] Bei einem reinen Verweis auf einen Telemediendienst zur Wahrnehmung der Betroffenenrechte (z.B. über eine URL in der Benutzerschnittstelle des anerkannten Dienstes zu einem Kontaktformular), sind erhöhte Anforderungen an die Identifizierung der Nutzer durch den anerkannten Dienst mit Blick auf die Wahrnehmung von Betroffenenrechten per se nicht ersichtlich.

[105] Aufgrund des Abhängigkeit des anerkannten Dienstes von den zuvor dargestellten unterschiedlichen Rahmenbedingungen und Kriterien erscheinen allgemeine technisch-organisatorische Anforderungen hinsichtlich der Art eines zu verwendenden Identitätsmanagement bei diesem Diensten zu diesem Zeitpunkt wenig sinnhaft. Vielmehr wird es wichtig sein, dass anerkannte Dienste sich auf die Bedürfnisse von Telemedienanbietern einstellen können und entsprechende Funktionalitäten anbieten ohne zu einer bestimmten Authentifizierung verpflichtet zu werden.

4.5.2. Generelle Einwilligungen mittels „Whitelisting“ bei prinzipiell bestimmten Zwecken und bestimmten Verantwortlichen

Die mit den Vorgaben der DSGVO am zwanglosesten vereinbare Form der generellen Vorab-Einwilligung mittels anerkannter Dienste, die auch in ErwGr. 20a der in der Fassung des Verhandlungsmandates des Rates für den Trilog zur E-

Privacy-VO angedeutet ist, stellt das „Whitelisting“ bestimmter Zwecke der Datenverarbeitung durch bestimmte Verantwortliche dar[64]:

> *“…Where available and technically feasible, an end user may therefore grant, through software settings, consent to a specific provider for the use of processing and storage capabilities of terminal equipment for one or multiple specific purposes across one or more specific services of that provider. For example, an end-user can give consent to the use of certain types of cookies by whitelisting one or several providers for their specified purposes. Providers of software are encouraged to include settings in their software which allows endusers, in a user friendly and transparent manner, to manage consent to the storage and access to stored data in their terminal equipment by easily setting up and amending whitelists and withdrawing consent at any moment. …”*

Bestimmte Telemedienanbieter würden sich danach für bestimmte Verarbeitungszwecke bei einem anerkannten Dienst der Einwilligungsverwaltung registrieren. Sobald der Nutzer bestimmte Spezifikationen vorgenommen hat, anhand derer er seine Einwilligung erteilen möchte, würde der anerkannte Dienst dem Nutzer noch einmal eine Zusammenstellung derjenigen Verantwortlichen einschließlich ihrer Verarbeitungszwecke zukommen lassen, die nach den Informationen, die dem anerkannten Dienst zur Verfügung stehen, den Nutzerspezifikationen entsprechen. Der Nutzer würde sodann zu einer (vermutlich sehr umfangreichen) Liste von Verantwortlichen und Verarbeitungszwecken jeweils samt allen sonstigen Pflichtinformationen nach Art. 13 DSGVO seine aktive Einwilligung erteilen.[65] Ob der Nutzer sich die Zeit nehmen wird, die Informationen tatsächlich zur Kenntnis zu nehmen, oder ob er dem anerkannten Dienst vertrauen und in die gesamte Liste einwilligen wird, ist unerheblich, da man sich auch bislang schon mit der bloßen Möglichkeit eines selbstbestimmten Handelns des Betroffenen zufriedengibt.

---

[64] Vgl. *Ketter/Thorun/Spindler*, Innovatives Datenschutz-Einwilligungsmanagement (2020) S. 41 f, abrufbar unter https://www.bmjv.de/SharedDocs/Downloads/DE/Service/Fachpublikationen/090620_Datenschutz_Einwilligung.pdf?__blob=publicationFile&v=1 (zuletzt abgerufen am 16.12.2021).

[65] In diese Richtung auch *Riechert* in Stiftung Datenschutz, Stellungnahme B Anhang 1 S. 73, welche einen „One-Pager“ als zusätzliche transparente Zusammenfassung der erteilten Einwilligung erwägt.

Der Nachteil des „Whitelisting“ bereits registrierter Anbieter besteht darin, dass die Einwilligung sich stets nur auf einen bestimmten Moment bezieht – kommen später neue Anbieter hinzu, oder ändern sich geringfügig die Verarbeitungszwecke (während sie sich weiterhin im Rahmen dessen bewegen, was der Nutzer anfänglich vorgegeben hat), muss eine zusätzliche Einwilligung erteilt werden. Je nachdem, wie häufig sich neue Anbieter beim anerkannten Dienst registrieren, wird der Nutzer also wiederholt mit Einwilligungsverlangen seitens des anerkannten Dienstes konfrontiert. Zwar kann ein anerkannter Dienst solche Aktualisierungen der Einwilligung bündeln, z.B. nur einmal im Monat vornehmen, doch bleibt aus Nutzersicht das Problem der dauernden Befassung und dauernden Verunsicherung. Es stellt sich daher die Frage, ob der Nutzer nicht auf das aktive Ansuchen um erneute Einwilligung nach Information betreffend die Identität der (neu hinzutretenden) Verantwortlichen usw. verzichten kann.

4.5.3. Generelle Einwilligungen für bestimmte Zwecke und bloß der Kategorie nach bestimmte Verantwortliche

[106] Ein Anwendungsbereich der Einwilligung per Softwareeinstellung oder über einen Telemediendienst mit Authentifizierungsmechanismus könnte aus technischer Sicht darin bestehen, im Vorfeld einer Speicherung oder eines Abrufes von Informationen auf Endgeräten von Nutzern für bestimmte Verwendungszwecke eine Einwilligung zu erteilen, ohne die Identität eines Verantwortlichen zu kennen. Der Vorteil eines solchen Systems läge darin, dass sich der Nutzer idealerweise nur ein einziges Mal – nämlich bei der initialen Festlegung der Spezifikationen – mit seinen Einwilligungspräferenzen auseinandersetzen muss. Andererseits bestehen Abstriche bei der Informiertheit der Nutzer, die ihre Einwilligung in Unkenntnis eines Verantwortlichen erteilen.

[107] Solche Varianten einer Einwilligungserteilung müssen die Bedingungen der DSGVO an die Einwilligung erfüllen, so insbesondere hinsichtlich der Merkmale „für den bestimmten Fall“ (oben 4.2.3) und „in informierter Weise“ (oben 4.2.2). Der Europäische Datenschutzausschuss hat in seinen Leitlinien 05/2020 diesbezüglich zur Einwilligung durch Browsereinstellungen formuliert: „*Diese Einwilligungen sollten im Einklang mit den Bedingungen der DSGVO für eine gültige Einwilligung entwickelt werden, beispielsweise so, dass die Einwilligung für jeden*

geplanten Zweck gesondert erfolgt und dass der Name des Verantwortlichen zu den bereitzustellenden Informationen gehört.“[66] Aus aufsichtsbehördlicher Sicht – wie auch bei einem vom BMWi einberufenen Gesprächskreis am 17. November 2021 deutlich wurde – ist die Einwilligung in Kenntnis der Identität des Verantwortlichen zu geben und eine generelle *ex ante*-Erteilung von Einwilligungen nur in bestimmte Zwecke und Kategorien von Verantwortlichen nicht ausreichend.

[108] Auch im Bereich der E-Privacy-VO sollen nach dem Trilog-Entwurf gem. ErwGr. 20a Einwilligungen über Browsereinstellungen gegenüber einem “spezifischen Dienst” erteilt werden[67]: *“Where available and technically feasible, an end user may therefore grant, through software settings, consent to a* ***specific provider*** *for the use of processing and storage capabilities of terminal equipment for one or multiple specific purposes across one or more specific services of that provider.”*

[109] Weshalb bei Einschaltung anerkannter Dienste der Einwilligungsverwaltung bezüglich der Verantwortlichen eine Bestimmung bloß der Kategorie nach nicht ausreichend sein sollte, überzeugt indessen nicht.[68] Vielmehr ist im Hinblick auf die klare Regelung der DSGVO, wonach betreffend eine Weitergabe von Daten durch den Verantwortlichen an Dritte eine Angabe der Kategorien von Empfängern ausreichen soll (Art. 13 Abs. 1 lit. e, Art. 14 Abs. 1 lit. e, 15 Abs. 1 lit. c, Art. 30 Abs. 1 lit. d DSGVO), nicht einsichtig, warum dies nicht auch bei Einschaltung anerkannter Dienste der Einwilligungsverwaltung gilt. Zwar ist die Konkretisierung der genannten Bestimmungen der DSGVO Gegenstand eines Vorlageverfahrens vor dem EuGH und die korrekte Auslegung daher noch nicht in allen Details geklärt.[69] Bei diesem Vorlageverfahren geht es aber lediglich um Fälle, in denen eine Datenweitergabe an konkrete Empfänger schon erfolgt ist oder die konkreten Empfänger schon feststehen, während es unbestritten ist, dass der Verantwortliche bei noch unbekannten Empfängern bloß über Kategorien von

---

[66] *Europäischer Datenausschuss*, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679 v. 04.05.2020, Rn. 89.
[67] ST 6087/2021 INIT.
[68] Vgl. auch *Kühling*, ZfDR 2021, 1 (10).
[69] *OGH* 6 Ob 159/20f. Siehe dazu *Schwamberger*, Auskunft über konkrete Empfänger oder Kategorien von Empfängern personenbezogener Daten? ecolex 2021, 598.

Empfängern zu informieren hat oder wenn eine Angabe der konkreten Empfänger nur mit unverhältnismäßigem Aufwand möglich ist. Zwar heißt dies immer noch nicht, dass die genannten Bestimmungen der DSGVO unmittelbar auf anerkannte Dienste der Einwilligungsverwaltung anwendbar sind, weil anerkannte Dienste nicht unbedingt „Verantwortliche" im Sinne der DSGVO sein müssen. Selbst wenn sie keine „Verantwortlichen" sind, ist die Situation doch wesentlich vergleichbar. Insbesondere hat der DSGVO-Gesetzgeber die genannten Regelungen ersichtlich in der Annahme getroffen, dass der Betroffene mit dem ursprünglich die Daten erhebenden Verantwortlichen einen Ansprechpartner hat, dem die genaue Identität der dritten Empfänger jedenfalls bekannt ist.[70] Dies müsste dann aber erst recht bei Einschaltung eines anerkannten Dienstes der Einwilligungsverwaltung gelten, bei dem die Wahrung von Betroffenenrechten viel wahrscheinlicher ist als bei einem beliebigen Verantwortlichen, selbst wenn der anerkannte Dienst konkret nicht selbst Verantwortlicher sein sollte.

[110] **Bei den technischen und organisatorischen Anforderungen an anerkannte Dienste wäre unter Zugrundelegung dieser Rechtsauffassung – vorbehaltlich anders lautender Entscheidungen des EuGH oder einer anders lautenden Regelung in der E-Privacy-VO – anzunehmen, dass eine Einwilligung in bestimmte Zwecke und bloß der Kategorie nach bestimmte Verantwortliche selbst dann genügt, wenn der anerkannte Dienst konkret nicht die Daten erhebender „Verantwortlicher" im Sinne der DSGVO sein sollte. Es wäre gegebenenfalls zu hoffen, dass sich Aufsichtsbehörden und Gerichte dieser Meinung anschließen werden.**

4.5.4. Übernahme fremder Einwilligungsentscheidungen (abonnierte Listen)

[111] Damit stellt sich die weitere Frage, ob Nutzer nicht nur ihre generelle Vorab-Einwilligung in bestimmte Verarbeitungszwecke und bloß der Kategorie nach bestimmte Verantwortliche erteilen können, sondern ob sie auch (statisch oder dynamisch) fremde Listen als vertrauenswürdig eingestufter Verantwortlicher und

[70] Zur Frage, ob der Verantwortliche dann zu einem späteren Zeitpunkt nach Art. 15 DSGVO auf Auskunft betreffend die genaue Identität der Empfänger in Anspruch genommen werden kann, hat der österreichische OGH eine Vorlage an den EuGH formuliert, vgl. OGH 6 Ob 159/20f.

Zwecke übernehmen können, die etwa von NGOs bereitgestellt werden könnten. Hierbei müsste die Wettbewerbskonformität allerdings gewährleistet sein, etwa indem seitens Telemediendiensteanbietern ein Anspruch darauf besteht, zu fairen, billigen und nicht-diskriminierenden Bedingungen in die Liste aufgenommen zu werden.

[112] Was eine statische Übernahme fremder Listen anbelangt, so können dieser – sofern vom anerkannten Dienst technisch und organisatorisch ermöglicht – rechtliche Hindernisse dann nicht entgegenstehen, wenn dem Betroffenen bei Erteilung der Einwilligung theoretisch alle Informationen nach Art. 13 DSGVO zur Verfügung gestellt werden (auch wenn er diese realistischerweise nicht lesen wird) und er daraufhin aktiv die Einwilligung erklärt (klassisches Whitelisting, siehe oben 4.5.2).

[113] Eine dynamische Übernahme fremder Einwilligungsentscheidungen trifft dagegen auf ähnliche Bedenken seitens der Aufsichtsbehörden wie bereits die Einwilligung in bloße Kategorien von Verantwortlichen (dazu oben 4.5.3). Nach hier vertretener Auffassung müsste die Übernahme fremder Listen dagegen konsequenterweise möglich sein, allerdings nur, soweit bei der aktiven Einwilligung in die fremde Liste die Zwecke der Datenverarbeitung bestimmt und die Verantwortlichen zumindest der Kategorie nach bestimmt sind. Eine „Blanko-Einwilligung“ in beliebige Zwecke und beliebige Kategorien von Verantwortlichen dürfte die DSGVO dagegen tatsächlich nicht zulassen.[71]

[114] **Sofern anerkannte Dienste der Einwilligungsverwaltung die Übernahme fremder Listen vertrauenswürdiger Telemedienanbieter und akzeptabler Verarbeitungszwecke ermöglichen wollen, müssen sie daher sicherstellen, dass dem Nutzer bei Treffen der Übernahmeentscheidung alle Informationen zur Verfügung stehen, die ihm auch zur Verfügung stehen müssen, wenn er die Einwilligung nach Vorschlag des anerkannten Dienstes selbst erteilt. Ferner muss der anerkannte Dienst sicherstellen, dass dem Nutzer**

[71] Vgl. *Stemmer* in BeckOK Datenschutzrecht, 37. Edition, Stand: 01.05.2021, Art. 7 DSGVO, Rn. 76; *Paal/Pauly/Frenzel*, DSGVO BDSG, Art. 7 DSGVO, Rn. 8; *Ernst*, Die Einwilligung nach der Datenschutzgrundverordnung – Anmerkungen zur Definition nach Art. 4 Nr. 11 DSGVO, ZD 2017, 113.

eine stets aktuell gehaltene Übersicht über die Empfänger und alle Pflichtinformationen nach der DSGVO zur Verfügung steht.

4.5.5. Stellvertretung bei Einwilligungsentscheidungen und der Ausübung von Betroffenenrechten

[115] Angesichts der verschiedenen Schwierigkeiten, die mit der Erteilung genereller Einwilligungen verbunden sind, wäre auch zu prüfen, ob anerkannte Dienste nicht im konkreten Einzelfall bestimmte Erklärungen (Einwilligungen, Widerruf der Einwilligung, Ausübung von Betroffenenrechten) im Namen von und mit Wirkung für die Betroffenen erklären können. Während es bei der Übernahme fremder Einwilligungslisten letztlich nur um die Modalität geht, wie der Gegenstand der Einwilligung initial formuliert wird (d.h. durch Vorschlag des anerkannten Dienstes oder einer dritten NGO etc.), geht es hier um die Frage, ob bei der Einwilligung und/oder der Ausübung von Betroffenenrechten auch eine echte Stellvertretung (etwa im Sinne der §§ 164 ff. BGB) möglich ist. Dies würde bedeuten, dass auch die Pflichtinformationen nach der DSGVO nicht mehr dem Betroffenen, sondern nur noch seinem Stellvertreter zugehen müssen und der Stellvertreter im Rahmen der ihm erteilten Vollmacht eigene Entscheidungen treffen kann.

[116] Während eine Botenschaft im Datenschutzrecht nach hA bejaht wird,[72] ist die Möglichkeit einer Stellvertretung bis heute umstritten.[73] Gesetzliche Vertretung

---

[72] Siehe nur *Stemmer* in BeckOK Datenschutzrecht, 37. Edition, Stand: 01.05.2021, Art. 7 DSGVO, Rn. 31; *Ernst*, ZD 2017, 110 (111).

[73] Dafür etwa *Specht-Riemenschneider/Blankertz/Sierek/Schneider/Knapp/Henne*, Datentreuhand – Ein Beitrag zur Modellbildung und rechtlichen Strukturierung zwecks Identifizierung der Regulierungserfordernisse für Datentreuhandmodelle, MMR-Beil. 2021, 25 (41 f.); *Hoffmann*, Einwilligung der betroffenen Person als Legitimationsgrundlage eines datenverarbeitenden Vorgangs im Sozialrecht nach dem Inkrafttreten der DSGVO, NZS 2017, 807 (808); dagegen etwa *Ernst*, ZD 2017, 110 (111); Freiherr von Ulmenstein, Datensouveränität durch repräsentative Rechtswahrnehmung, DuD 2020, 528; *Funke*, Die Vereinbarkeit von Data Trusts mit der Datenschutzgrundverordnung (DSGVO), Dezember 2020, 5, abrufbar unter: https://algorithmwatch.org/de/wp-content/uploads/2020/11/Die-Vereinbarkeit-von-Data-Trusts-mit-der-DSGVO-Michael-Funke-AlgorithmWatch-2020-1.pdf (zuletzt abgerufen am 16.12.2021). Zur Notwendigkeit von Regelungen zur Zulässigkeit und Grenzen rechtsgeschäftlicher Mandate siehe *Verbraucherzentral Bundesverband e.V.*, Neue Datenintermediäre – Anforderungen des vzbv an „Personal Information Management Systems“ (PIMS) und Datentreuhänder (2020) S. 7, abrufbar unter https://www.vzbv.de/sites/default/files/downloads/2020/09/17/20-09-15_vzbv-positionspapier_datenintermediaere.pdf (zuletzt abgerufen am 16.12.2021).

bei Einwilligungen (z.B. durch Eltern in Bezug auf Kinder) muss jedenfalls möglich sein, anderenfalls Art. 8 DSGVO kaum verständlich wäre. Auch gewillkürte Vertretung muss mindestens in dem von Art. 80 DSGVO bestimmten Umfang möglich sein, darüber hinaus – aufgrund von Überlegungen effektiven Rechtsschutzes – aber wohl auch bei Beauftragung z.B. eines Rechtsanwalts mit der Vertretung in einem konkreten Rechtsstreit.[74] Darüber hinaus ist die Möglichkeit, datenschutzrechtliche Rechtspositionen zu delegieren, allerdings nicht geklärt.

[117] Der endgültig ausverhandelte Entwurf zum DGA (dazu oben 4.1.4) hat die ursprünglich extrem zurückhaltende Formulierung der Europäischen Kommission in ErwGr 24 etwas abgeschwächt. Die Fassung lautet nun: „In this context it is important to acknowledge that the rights under Regulation (EU) 2016/679 ~~can only be exercised by each individual and cannot be conferred or delegated to a data cooperative~~ **are personal rights of the data subject and that data subjects cannot waive such rights.**“

[118] Auch wenn der DGA die DSGVO unberührt lässt,[75] kann aus dem ErwGr geschlossen werden, dass der europäische Gesetzgeber offensichtlich von einer Unmöglichkeit der Abtretung datenschutzrechtlicher Positionen ausgeht (was in der Tat angesichts der persönlichkeitsrechtlichen Natur geradezu auf der Hand liegt). Jedoch ist insbesondere seit der Neuformulierung durch den Rat nicht mehr klar zum Ausdruck gebracht, dass auch deren Ausübung nicht mehr an einen Stellvertreter delegiert werden kann. Zwischen beidem ist allerdings ein großer Unterschied, da die bloße Delegation der Ausübung an einen Stellvertreter eine jederzeitige Rückholmöglichkeit (durch Widerruf der Vollmacht) beinhaltet.

[119] Auf der einen Seite erscheint die Ermöglichung von Stellvertretung gerade bei der Ausübung von weiteren, über die Einwilligung hinausgehenden Betroffenenrechten als einzige Möglichkeit, den Nutzer effektiv von ständigen, ihn tendenziell überfordernden Entscheidungen zu entlasten.[76] Auf der anderen Seite ist nicht

---

[74] Siehe nur *Stemmer* in BeckOK Datenschutzrecht, 37. Edition, Stand: 01.05.2021, Art. 7 DSGVO, Rn. 31.
[75] Art. 1 Abs. 3 ST 12124/2021 INIT.
[76] In diese Richtung auch *Specht-Riemenschneider/Blankertz/Sierek/Schneider/Knapp/Henne*, MMR-Beil. 2021, 25 (42 f.).

zu verkennen, dass die Delegation – etwa der Ausübung von Portabilitätsrechten – auch eine Reihe von Gefahren für den Betroffenen mit sich bringt.[77] **Wo hier die Grenzen liegen, kann nur vom EuGH oder vom europäischen Gesetzgeber definiert werden. Nach Auffassung der Gutachter sollte auch dies eine Frage des Vorhandenseins „angemessener Garantien" für die Rechte und berechtigten Interessen des Betroffenen sein.** Dazu sollte neben der jederzeitigen Widerruflichkeit der Vollmacht und der jederzeitigen Offenlegung getroffener Entscheidungen auch gehören, dass die Vollmacht jedenfalls zur Ausübung von Portabilitätsrechten in ähnlichem Maße bestimmt ist, wie die Einwilligung.[78] Dagegen besteht betreffend die Ausübung anderer Betroffenenrechte (z.B. Löschungsverlangen) kein entsprechender Schutzbedarf, und sind die Anforderungen hier deutlich niedriger anzusetzen.[79]

[120] **Angesichts der bestehenden Rechtsunsicherheit ist für die Ausgestaltung anerkannter Dienste derzeit noch zu empfehlen, dass die Bedingungen für die Ausübung von Betroffenenrechten vom Nutzer selbst *ex ante* festgelegt werden, so dass eine Stellvertretungskonstruktion nicht nötig wird (z.B. Löschungsverlangen immer, wenn bestimmte Voraussetzungen eintreten).**

4.5.6. Generelle Verweigerungen der Einwilligung

[121] Je nach Ausgestaltung eines anerkannten Dienstes kann es vorkommen, dass ein solcher Dienst in einer Grundeinstellung an Telemediendienste kommuniziert, dass ein Eingriff in das Endgerät zu unterbleiben hat (so z.B. konkret bezogen auf ein Nutzertracking[80]).

---

[77] Siehe nur Gutachten der *Datenethikkommission* (2019) 136 f., abrufbar unter https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.pdf (zuletzt abgerufen am 16.12.2021).

[78] *Kühling*, Der datenschutzrechtliche Rahmen für Datentreuhänder, ZfDR 2021, 1 (8 ff.); *Wendehorst/Schwamberger/Grinzinger*, Datentreuhand – wie hilfreich sind sachenrechtliche Konzepte?, in *Pertot* (Hrsg.), Rechte an Daten (2020) 103 (114 f.); *Buchner*, Informationelle Selbstbestimmung und Privatrecht (2006) 293 f.

[79] Für die Möglichkeit der Stellvertretung beim Auskunftsbegehren nach Art 15 DSGVO jüngst *OLG Stuttgart* BeckRS 2021, 6282, Rn. 32. Weitergehend *Kühling*, ZfDR 2021, 1 (12): Möglichkeit der Geltendmachung sämtlicher Betroffenenrechte.

[80] Vgl. hierzu auch der Do-Not-Track-Mechanismus in Browsern, https://de.wikipedia.org/wiki/Do_Not_Track_(Software) (zuletzt abgerufen am 16.12.2021).

[122] Dabei ist zunächst zu fragen, wie eine derartige pauschale Vorweg-Ablehnung rechtlich zu qualifizieren ist. Die E-Privacy-RL kennt eine solche pauschale Vorweg-Ablehnung in Bezug auf unerbetene Werbe-Nachrichten in Art. 13 Abs. 2 (und dementsprechend das deutsche Recht in § 15 Abs. 3 TMG), und die gleiche Regelung findet sich in Art. 16 Abs. 2 des Entwurfs zur E-Privacy-VO. Allgemeiner gestattet Art. 21 Abs. 5 DSGVO im Zusammenhang mit Diensten der Informationsgesellschaft, dass die betroffene Person ihr Widerspruchsrecht mittels automatisierter Verfahren ausüben kann, bei denen technische Spezifikationen verwendet werden. Zwar bezieht sich das Widerspruchsrecht nach Art. 21 DSGVO lediglich auf Datenverarbeitungen, die auf eine der gesetzlichen Generalklauseln öffentlicher Interessen oder privater berechtigter Interessen in Art. 6 Abs. 1 lit. e oder f gestützt werden, doch erschiene eine analoge Anwendung auf Fälle der Einwilligung im Wege eines *argumentum a fortiori* begründbar.[81]

[123] Da eine Einwilligung nach dem EuGH[82] und dem BGH[83] ohnehin im Wege aktiven Tuns erteilt werden muss, ist das Problem allerdings weniger, ob der Betroffene diese auch durch technische Voreinstellungen allgemein verweigern kann – bloße Untätigkeit würde genügen um die Wirkungen einer Einwilligung zu verhindern – sondern vielmehr, in welchem Verhältnis eine im Voraus erklärte generelle Ablehnung der Einwilligung zu einer speziell durch aktives Tun (z.B. Anklicken einer Schaltfläche „OK“) erteilten Einwilligung steht. Diesbezüglich positioniert sich die Fassung des Verhandlungsmandates des Rates für den Trilog zur E-Privacy-VO in Art. 4a klar zugunsten eines Vorrangs der individuell erteilten Einwilligung: *„2aa. Consent directly expressed by an end-user in accordance with Paragraph (2)* ***shall prevail over software settings****.[…]”* (siehe näher schon oben 4.1.3), wobei sich diese Fassung im Laufe der weiteren Verhandlungen natürlich noch ändern kann.

[124] In Ermangelung einer Art. 4a Abs. 2aa des Trilog-Entwurfs entsprechenden Regelung dürfte es allerdings auch jetzt bereits allgemeinen Rechtsgrundsätzen entsprechen, dass sich eine Person nicht selbst ihrer eigenen Privatautonomie

---

[81] AA etwa *Schwartmann/Jaspers/Thüsing/Kugelmann/Atzert*, Art. 21 DSGVO Rn. 17.
[82] *EuGH*, C-673/17 – *Planet49*.
[83] *BGH*, I ZR 7/16 – *Cookie-Einwilligung II*.

begeben kann. Insoweit ist die Situation derjenigen beim gewillkürten Formzwang vergleichbar – so, wie Parteien eines Vertrages theoretisch formfrei von einem einmal vereinbarten Formzwang wieder abgehen können, so kann auch eine einzelne Person bei der Einwilligung theoretisch jederzeit von einer einmal erklärten Ablehnung der Einwilligung wieder abgehen. Hier wie dort ist aber die generelle Vereinbarung bzw. Erklärung nicht vollends wirkungslos, sondern begründet eine widerlegliche Vermutung, dass die spätere Erklärung ohne Bindungswillen erfolgte. Mit anderen Worten sind an den Nachweis, dass es sich bei der später erteilten speziellen Einwilligung tatsächlich um eine bewusste Entscheidung gehandelt hat, deutlich erhöhte Anforderungen zu stellen und besteht eine Vermutung, dass etwa eine entsprechende Schaltfläche eher aus Nachlässigkeit oder Ermüdung angeklickt wurde.

[125] Da die Bedingungen einer wirksamen Einwilligung – vorbehaltlich der Rolle einer auf der Grundlage der RL 93/13/EG bzw. ihrer Umsetzung in den §§ 307 ff BGB erfolgenden Klauselkontrolle[84] – durch die DSGVO (und künftig die E-Privacy-VO) grundsätzlich abschließend geregelt sind, kann hier auch der nationale Verordnungsgeber wenig ausrichten. **Damit anerkannte Dienste der Einwilligungsverwaltung ihr volles Potential zugunsten der Nutzer entfalten können, wäre es aber wünschenswert, dass an die Unmissverständlichkeit einer speziellen Einwilligung, die einer generellen Ablehnung widerspricht, deutlich erhöhte Anforderungen zu stellen sind und Anbieter, welche sich für generelle Einwilligungen auf einen anerkannten Dienst bzw. eine Software-Einstellung berufen, auch spezielle Einwilligungsansuchen über denselben anerkannten Dienst bzw. dieselbe Software stellen müssen.**

[126] Je nach gesetzgeberischer Entscheidung auf europäischer Ebene sollten anerkannte Dienste technisch-organisatorisch sicherstellen, dass sowohl eine gene-

[84] Siehe dazu ErwGr 42 DSGVO und allgemein *Wendehorst/v. Westphalen*, Das Verhältnis von Datenschutz-Grundverordnung und AGB-Recht, NJW 2016, 3745 mwN. Dass die Klauselkontrolle stattfindet, akzeptiert auch der BGH, siehe etwa *BGH* I ZR 7/16 – *Cookie-Einwilligung II*, Rn. 26. Allerdings ist umstritten, ob der Maßstab der Klauselkontrolle über dasjenige hinausgehen (d.h. das Gesamtgefüge der Rechte und Pflichten der Parteien berücksichtigen) kann, was ohnehin im Datenschutzrecht als zugunsten der betroffenen Person zwingendes Recht normiert ist.

relle Ablehnung eines Endgeräteeingriffs als auch eine spezielle Einwilligungserteilung in ihrer Grundarchitektur möglich sind. Nutzer sollten sowohl über die Bedeutung und Auswirkungen einer ablehnenden Grundeinstellung als auch über die Umstände der Datenverarbeitung im Zuge einer speziellen Einwilligung informiert werden.

4.6. Zwischenergebnis

[127] Anerkannte Dienste müssen - aus rechtlicher Sicht - in der Lage sein, wirksame Einwilligungen von Nutzern einzuholen und in deren Auftrag zu verwalten. Dies bedeutet hinsichtlich der Anforderungen an anerkannte Dienste Folgendes:

[128] **Freiwilligkeit:** Anerkannte Dienste müssen Nutzer technisch in die Lage versetzen, ihre Einwilligungen für Telemedienanbieter frei und souverän zu erteilen oder zu verweigern. Nutzer dürfen insofern nicht technisch dazu gezwungen sein, bei einer Einwilligung zugunsten eines Telemediendienstes, zugleich allen oder bestimmten weiteren Diensten eine Einwilligung erteilen zu müssen oder auf die Einwilligung zugunsten des ausgewählten Dienstes zu verzichten.

[129] **Informiertheit:** Anerkannte Dienste müssen bei der Gestaltung von Einwilligungstexten dafür sorgen, dass sie Nutzer eindeutig und unmissverständlich über einen oder mehrere Zwecke einer Datenverarbeitung informieren. Weitere Vorgaben an eine Informationstiefe beim anerkannten Dienst erscheinen aufgrund der unterschiedlichen Verarbeitungskontexte einer Einwilligung nicht geboten.

[130] **Für den bestimmten Fall**: Ein anerkannter Dienst muss Differenzierungen in seinen Nutzerpräferenzen zulassen, damit Nutzer ihre Einwilligungen in unterschiedliche Verarbeitungszwecke geben können. Es wäre als besonders nutzerfreundlich anzusehen, wenn anerkannte Dienste Nutzern Unterverarbeitungen, die einem Verarbeitungszweck zuzuordnen sind, in Form eines Entscheidungsbaumes zumindest nachträglich anzeigen, damit Nutzer ihre Einwilligung für solche Unterverarbeitungen entziehen können.

[131] **Unmissverständlich abgegebene Willensbekundung und deren Form:** Ein anerkannter Dienst darf in seiner Grundeinstellung keine Einwilligungen enthalten, es sei denn der Nutzer hat dies selbst veranlasst.

[132] **Ausdrücklichkeit:** Anerkannte Dienste müssen technisch in der Lage sein, Nutzern das erhöhte Risiko einer Datenverarbeitung, wo einschlägig, bewusst zu machen. Dazu gehört, dass besondere Kategorien personenbezogener Daten in einem Einwilligungstext technisch dargestellt werden.

[133] **Nachweisführung und Dokumentation:** Anerkannte Dienste müssen Telemedienanbieter in die Lage versetzen, den Nachweis über eine gültige Einwilligung führen zu können. Dies erfordert die Übermittlung einer Datenstruktur, welche die rechtlichen Anforderungen an eine Einwilligung abbildet. Ferner wird ein anerkannter Dienst über einen technischen Mechanismus verfügen müssen, der Nutzeranforderungen für das Löschen einer Einwilligung oder von Einwilligungsparametern unverzüglich umsetzt und die damit verbundenen personenbezogenen Daten datenschutzkonform löscht.

[134] **Gültigkeitsdauer:** Es wäre als nutzerfreundlich anzusehen, wenn ein anerkannter Dienst Nutzer in regelmäßigen Abständen über das Bestehen einer Einwilligung erinnern. Hier erscheint ein Zyklus von 12 Monaten sachgerecht.

[135] **Widerruflichkeit:** Anerkannte Dienste sollten dieselbe Benutzeroberfläche für das Einholen und den Widerruf einer Einwilligung verwenden.

[136] **Identitätsmanagement:** Die Pflicht, ein Identitätsmanagement bei Nutzern durchzuführen, ist hinsichtlich der anerkannten Dienste von verschiedenen Faktoren abhängig. Zum einen von den Anforderungen der Telemedienanbieter selbst an die Authentifizierung (vgl. nachfolgend Ziff. 5.1). Zum anderen ist ein Identitätsmanagement abhängig von der Stellung des anerkannten Dienstes als Verantwortlicher iSv Art. 4 Nr. 7 DSVO und bestehender „Identifizierungsmängel“. Sollen Betroffenenrechte unter Verwendung eines anerkannten Dienstes gegenüber Telemedienanbietern unmittelbar wahrgenommen werden, ist von einem Zusammenhang zwischen möglichen besondere Anforderungen an ein Identitätsmanagement mit den beim Telemedienanbieter gespeicherten personenbezogenen Daten auszugehen. Aufgrund des Abhängigkeit des anerkannten Dienstes von unterschiedlichen Rahmenbedingungen und Kriterien erscheinen allgemeine technisch-organisatorische Anforderungen an ein zu verwendendes Identitätsmanagement zu diesem Zeitpunkt daher wenig sinnhaft.

[137] **Einwilligung in Listen von Zwecken und Verantwortlichen**: Zentrale Herausforderung für das Einwilligungsmanagement ist das Einholen von Einwilligungen im Voraus. Möglich ist jedenfalls ein einmaliges „Whitelisting“ bestimmter dritter Verantwortlicher durch den Nutzer, sofern zum Zeitpunkt der Erklärung alle von der DSGVO geforderten Informationen, einschließlich hinsichtlich der konkreten Identität der Verantwortlichen, erteilt werden. Dabei wäre es unerheblich, ob die Liste von Verantwortlichen primär vom anerkannten Dienst zusammengestellt wurde oder von dritter Stelle.

[138] **Generelle ex ante-Einwilligungen**: Eine Verbesserung der Nutzerfreundlichkeit lässt sich dadurch erreichen, dass man – zumindest nach dem initialen „Whitelisting“ – abstrakte ex-ante Einwilligungen in granular definierte Zwecke und bloße Kategorien von Verantwortlichen zulässt. Dieses Verfahren kann sich gegebenenfalls auf die DSGVO stützen, wenn der anerkannte Dienst zugleich als die Daten erhebender erster Verantwortlicher auftritt, der die Daten dann an dritte Empfänger weiterleitet. Ist der anerkannte Dienst nicht erster Verantwortlicher, bliebe eine teleologische Auslegung der DSGVO in diesem Sinne, der sich möglicherweise in der Zukunft Judikatur und Aufsichtsbehörden anschließen könnten. Ähnliches gilt für Stellvertretungskonstruktionen, bei denen der anerkannte Dienst oder ein vertrauenswürdiger Dritter mit der Erteilung der Einwilligung und/oder der Ausübung von Betroffenenrechten betraut wird und dabei granular formulierte Anweisungen befolgt.

[139] **Generelle Verweigerungen der Einwilligung**: Generelle Verweigerungen der Einwilligung sind für die Nutzerfreundlichkeit wichtig, aber juristisch schwierig zu erfassen, da sich Betroffene nicht für die Zukunft ihrer eigenen Autonomie begeben können. Um den Mehrwert für Nutzer zu erhalten und zu vermeiden, dass Nutzer wiederum ständig mit Cookie-Bannern konfrontiert werden, sollte darauf geachtet werden, dass neue Einwilligungsverlangen zumindest über den anerkannten Dienst gestellt werden müssen, wobei die Entwicklungen zur künftigen E-Privacy-VO aufmerksam zu beobachten sind.

5. Elemente des Einwilligungsmanagements

[140] Grundsätzlich muss ein Einwilligungsmanagement unabhängig von konkreten Implementierungsalternativen aus technischer Sicht die folgenden Nutzungsfälle (Funktionen aus Sicht des Benutzers) unterstützen, um den durch das Gesetz intendierten Zweck zu erfüllen:

1. Feststellung der **Identität** des Einwilligenden (Authentifizierung)
2. Ex ante Definition von **generellen Einwilligungen bzw. Einwilligungstypen bzw. Whitelisting von einzelnen Verantwortlichen/Verfahren**
3. **Automatische Erteilung von speziellen Einwilligungen (d.h. Einwilligungen für ausdrücklich genannte Verantwortliche)** auf Basis von grundlegenden Einwilligungen zu Beginn der Nutzung eines Telemediendienstes
4. **Abfrage von speziellen Einwilligungsentscheidungen** auf Anfrage eines Telemediendienstes
5. **Anzeige** bereits manuell und automatisch erteilter spezieller Einwilligungen inklusive der Möglichkeit, alle Betroffenenrechte für einzelne oder Mengen von Einwilligungen wahrzunehmen
6. Ex post **Widerruf** zu bereits erteilten speziellen und definierten generellen Einwilligungen

[141] Die angestrebte Verringerung der Anzahl der Interaktionen mit Cookie-Bannern o.ä. ergibt sich dabei, wie bereits in der Einleitung thematisiert, durch die Benutzungsfälle 2 und 3, die eine „automatisierte Erklärung“ von Einwilligungen im Einzelfall auf Basis von generischen, ex ante definierten Einwilligungstypen erlauben. Die Machbarkeit eines Cookie-Banner vermindernden Einwilligungsmanagements steht und fällt dabei mit der Rechtskonformität der über diese beiden Nutzungsfälle erteilten Einwilligungen.

[142] Bei der Umsetzung dieser Anforderungen müssen vier wesentliche technische Gestaltungsentscheidungen getroffen werden, deren jeweilige Alternativen den Lösungsraum aufspannen, der hier betrachtet wird:

A. **Art der Authentifizierung** des Einwilligenden

B. **Datenmodell** für generische und spezielle Einwilligungen

C. **Ort der Speicherung** von generischen und speziellen Einwilligungen

D. **Gestaltung und Betrieb der Benutzeroberfläche** für die interaktiven Nutzungsfälle.

[143] Die Anforderungen an die technischen Protokolle zum Datenaustausch zwischen den technischen Komponenten der beteiligten Akteure ergeben sich im Wesentlichen aus den Gestaltungsentscheidungen bezüglich dieser vier Elemente. Des Weiteren sind noch querschnittliche Fragen der IT-Sicherheit zu klären, die ebenfalls einen Einfluss auf die Interaktionsprotokolle haben.

5.1. A. Identitätsmanagement für Einwilligende

[144] Internetnutzer können mit verschiedenen Methoden[85] authentifiziert werden, die die einwilligende Person mit unterschiedlichen Graden von Sicherheit und Bestimmtheit identifizieren. Die in diesem Kapitel durchgeführten Differenzierungen sind sowohl für die technische Architektur eines Einwilligungsmanagements als auch für die Bewertung der Rechtskonformität einer konkreten Einwilligung wichtig. Die konkrete Auswahl des Verfahrens wird typischerweise vom Telemediendienst getroffen, da dessen Anbieter selbst abschätzen muss, wie genau und sicher die Identität eines Einwilligenden in Bezug auf die konkreten Zwecke und Daten festgestellt werden sollte. Eine Online-Bank hat naturgemäß weitergehende Anforderungen an die Authentifizierung als eine werbefinanzierte Website.

5.1.1. Reine Endgeräteidentifizierung

[145] Die **unterste Stufe der Authentifizierung** in Bezug auf die Sicherheit und Bestimmtheit liegt bei einer quasi **anonymen, gemeinsamen Nutzung von Endgeräten** vor. Im Endeffekt wird dabei nicht der Nutzer, sondern das Gerät authentifiziert, häufig über im Browser abgelegte „Cookies“ mit von Telemediendiensten bzw. Werbenetzwerken vergebenen, global eindeutigen Identifikatoren. Diese Art der Authentifizierung ist nicht trennscharf und führt beispielsweise bei

[85] *Laue/Stiemerling,* Identitäts- und Zugriffsmanagement für Cloud Computing Anwendungen – Technisch-organisatorische Probleme, rechtliche Risiken und Lösungsansätze, DuD 10/2010, 692-697.

einem offenen „Familien-IPad“ dazu, dass die Tochter morgens in einen Verarbeitungsvorgang einwilligt, von dem abends der Sohn der Familie betroffen ist. Das Gleiche gilt für gemeinsam genutzte, mit dem Internet konnektierte Fahrzeuge. Einwilligungen werden bei dieser Methode entweder im Telemediendienst verknüpft mit dem (auch im Cookie abgelegten) Identifikator gespeichert oder direkt zusammen mit dem Identifikator in einem Cookie o.ä. im Browser.

5.1.2. Lokale Benutzerprofile auf dem Endgerät

[146] Eine **bessere Trennung der betroffenen Personen** wird durch **lokale Profile auf dem jeweiligen Endgerät** erreicht. Dabei wird über eine Benutzeridentifizierung auf dem Endgerät (ggf. auch nur schwach authentifiziert, z.B. durch einfache Auswahl aus einer Namensliste) dafür gesorgt, dass die persönliche Datenhaltung und Konfiguration des Geräts für jeden identifizierten Benutzer individualisiert wird. In solchen Fällen hat z.B. ein Browser getrennte Cookie-Speicher, so dass es für einen Telemediendienst so aussieht, dass er mit verschiedenen Ausprägungen des Endgeräts kommuniziert. Willigt beispielsweise morgens die Tochter der Familie auf ihrem Profil in einen Verarbeitungsvorgang ein und der Telemediendienst setzt einen Cookie mit einem eindeutigen Identifikator, so ist der Sohn der Familie, der abends unter seinem eigenen Profil den Telemediendienst nutzt, von dieser Einwilligung nicht „betroffen“, da der Cookie aus dem Profil der Tochter für den Telemediendienst nicht sichtbar ist. Das gleiche Prinzip gilt bei gemeinsam genutzten Fahrzeugen, bei denen die Identifizierung des Fahrers oder der Fahrerin über einen individuellen Fahrzeugschlüssel erfolgt. Auch dabei werden die individuellen Einstellungen für jeden identifizierte Benutzer einzeln gespeichert (z.B. die Sitzeinstellung und die Konfiguration der Konnektivität des Fahrzeugs und der Fahrassistenzsysteme).

5.1.3. Authentifizierung als Besitzerin oder Besitzer einer konkreten E-Mail-Adresse

[147] Eine weit verbreitete Methode der Authentifizierung der einwilligenden Person funktioniert über die **E-Mail-Adresse**. Quasi jeder Internet-Nutzer hat heute eine private oder dienstliche E-Mail-Adresse, die ihm oder ihr eindeutig und persönlich zugeordnet ist, d.h. nur diese Person kann auf die eingehenden E-Mails zugreifen

und von der E-Mail-Adresse Nachrichten verschicken. Durch den Versand eines Verifizierungslinks an die E-Mail-Adresse kann ein Telemediendienst deshalb den Besitzer einer E-Mail-Adresse relativ sicher authentifizieren, so dass entsprechende Verfahren (z.B. Double Opt-in für Newsletter o.ä.) heute anerkannte Methoden zur Authentifizierung von Einwilligenden sind.

[148] Typischerweise kann sich ein Internetnutzer oder eine Internetnutzerin so spezifische Credentials (d.h. Kombination von Benutzername und Passwort) pro Telemediendienst auswählen, mit denen er oder sie sich dann in der Folge direkt – d.h. ohne weiteren Versand einer E-Mail – beim Telemediendienst anmelden kann. Einwilligungen werden dann typischerweise direkt an der Credential-ID im Telemediendienst gespeichert. Meldet sich die Benutzerin oder der Benutzer mit denselben Credentials über ein anderes Endgerät an (z.B. Mobiltelefon), so ist er auch im Rahmen dieser Benutzersitzung eindeutig identifiziert und authentifiziert, so dass der Telemediendienst eine z.B. bei einer Nutzungssitzung auf dem PC abgegebene Einwilligung auch auf dem Mobiltelefon eindeutig identifizieren und sich darauf berufen kann.

[149] Eine Authentifizierung über die E-Mail-Adresse kann zusätzlich über andere Faktoren als nur das Passwort als Teil der „Credentials“ abgesichert werden. Beispielsweise kann dieser Zugang zu einem Telemediendienst auch mit einem konkreten Smartphone oder einer bestimmten SIM-Karte im Smartphone verknüpft werden, so dass einem Angreifer nicht nur das „Wissen“ um das Passwort zum Zugriff ausreicht. Der Angreifer muss sich auch noch den Faktor „Besitz“ aneignen, um zugreifen zu können. Dies ändert jedoch nichts an der Bestimmtheit der Authentifizierung des E-Mail-Besitzers bzw. der E-Mail-Besitzerin. Selbst wenn der Zugang zum Mobiltelefon durch einen Fingerabdruck oder eine Gesichtserkennung als dritten Faktor (es handelt sich insoweit um ein biometrisches Merkmal) abgesichert ist, wird immer nur der „Besitzer“ bzw. die „Besitzerin“ der E-Mail-Adresse bestimmt.

5.1.4. Authentifizierung als natürliche Person

[150] Die **höchste Stufe der Authentifizierung** der einwilligenden Person erreicht man durch den tatsächlichen Abgleich eines staatlichen Ausweisdokuments inkl. biometrischer Merkmale (Foto, Fingerabdrücke, Irisdaten, …) beim Einrichten

des Zugangs zum Telemediendienst. Diese Verfahren sind aus dem Online-Banking oder anderen stark regulierten Bereichen bekannt.

[151] Der elektronische Personalausweis inkl. „Ausweisapp“ ist eine abgeschwächte Variante dieser „Bürgerauthentifizierung“, da keine biometrischen Merkmale abgeglichen werden, sondern lediglich der „Besitz“ des Ausweises und das „Wissen“ um die vergebene PIN genügen, um sich als Bürger oder Bürgerin gegenüber einem Telemediendienst zu authentifizieren.

[152] In diesen Fällen ist eine gespeicherte Einwilligung direkt mit der einwilligenden, sicher identifizierten natürlichen Person verknüpft.

5.1.5. Kombinierte Authentifizierung

[153] Die meisten Telemediendienste nutzen kombinierte Methoden der Authentifizierung. So können z.B. Online-Publikationen zumeist ohne ausdrückliche Anmeldung genutzt werden, wobei Einwilligungen dann nur mit einem geräte- bzw. profilgebundenen Identifikator verknüpft werden. Nutzt man denselben Telemediendienst auf einem anderen Endgerät, so muss eine Einwilligung typischerweise erneut erteilt werden.

[154] Meldet sich der Benutzer oder die Benutzerin zusätzlich mit einem E-Mail-basierten Zugang an (z.B. um Artikel hinter einer „Paywall“ nutzen zu können), so kann der Telemediendienst diese Person auch endgeräteübergreifend identifizieren. Insbesondere kann der Telemediendienst dann auch eine Verknüpfung zwischen verschiedenen, vorher vergebenen endgeräte- bzw. profilbasierten Identifikatoren herstellen. Wenn sich eine Person also auch nur ein einziges Mal mit demselben Zugang auf zwei Endgeräten eingeloggt hat, weiß der Telemediendienst sofort, dass das Smartphone und der PC von derselben Person genutzt werden. Durch die Verknüpfung der beiden verschiedenen geräte- bzw. profilgebundenen Identifikatoren im Nutzerdatensatz auf Seiten des Telemediendienstes kann dieser Telemediendienst diesen Zusammenhang später auch dann herstellen, wenn die Person sich nicht explizit mit den E-Mail-basierten Credentials anmeldet. Auch in diesem Fall könnte der Telemediendienst Einwilligungen, die auf einem Endgerät abgegeben wurden, einem anderen Endgerät zuordnen.

5.1.6. Föderative Authentifizierung

[155] Ein Sonderfall der Authentifizierung ist die sogenannte „föderative Authentifizierung“[86], im Fall von sozialen Netzwerken auch „social login“ genannt. Auch Dienste wie „NetID“[87] oder „Verimi“[88] bieten Telemediendiensten eine föderative Authentifizierung an. Dabei delegiert ein Telemediendienst die Authentifizierung an den Partner (z.B. „NetID“, „Verimi“ oder das soziale Netzwerk), bei dem der Internetnutzer bzw. die Internetnutzerin bereits einen typischerweise E-Mail-basierten Zugang hat.

[156] Der Telemediendienst vertraut bei diesem Verfahren auf die technischen und organisatorischen Maßnahmen des Partners. Falls es zum Streit über eine Einwilligung käme, müsste der Telemedienanbieter sinngemäß argumentieren: „*Ich habe dem Social Network A vertraut, dass es den Nutzer korrekt authentifiziert hat*.“

5.1.7. Fazit zu den Gestaltungsvarianten der Authentifizierung

[157] Im Hinblick auf das übergreifende Ziel der Nutzerfreundlichkeit und der Vermeidung eines Übermaßes von Einwilligungsinteraktionen sollte ein Dienst zum Einwilligungsmanagement die Möglichkeit bieten, Endgeräte bzw. Nutzerprofile auf diesen Endgeräten so zu verknüpfen, dass Einwilligungen automatisch für alle von der betreffenden Person verwendeten Endgeräte funktionieren, wenn die Person das wünscht. Diese Art der Verknüpfung würde eine geräteübergreifende Authentifizierung zumindest per E-Mail-Verfahren erfordern.

[158] Es sollte einem Telemediendienst vor dem Hintergrund der Nutzerfreundlichkeit freistehen, die Methode der Authentifizierung selbst entsprechend der Kritikalität der von der jeweiligen Einwilligung umfassten Datenkategorien zu wählen und ggf. auch selbst umzusetzen oder an einen Dritten im Sinne eines föderativen Logins auszulagern. Es sollte kein Zwang bestehen, nur eine über einen Dritten authentifizierte Einwilligung verwenden zu dürfen.

---

[86] https://de.wikipedia.org/wiki/F%C3%B6derierte_Identit%C3%A4t (zuletzt abgerufen am 16.12.2021).
[87] https://netid.de/ (zuletzt abgerufen am 16.12.2021).
[88] https://verimi.de/ (zuletzt abgerufen am 16.12.2021).

[159] Zudem muss der Telemediendienst im Zweifelsfall (d.h. insbesondere im Streitfall) die Gültigkeit einer konkreten Einwilligung z.B. für einen Datentransfer in die USA nachweisen.

[160] Konkrete Vorgaben zu bestimmten Arten der Authentifizierung erscheinen aus technischer Sicht in der vorgesehenen Verordnung deshalb nicht nötig.

5.2. B. Datenmodelle und Standards zur technischen Abbildung von Einwilligungen

[161] Essentiell für die angestrebte Verringerung der Einwilligungsinteraktionen ist – wie in der Einleitung beschrieben – die *Definition* von generellen Einwilligungstypen, insbesondere zu bestimmten Verarbeitungsvorgängen und bestimmten Kategorien von Verantwortlichen. Diese Einwilligungstypen können dann beim Aufruf eines Telemediendienstes von diesem angefragt und vom Einwilligungsmanagement „im Namen“ und „im Auftrag“ des Betroffenen speziell für den anfragenden Telemediendienst (und ggf. nachgelagerte getrennte und gemeinsame Verantwortliche) automatisch erklärt werden. Sowohl für die Definitionen der generellen Einwilligungstypen als auch die konkret erklärten, speziellen Einwilligungen muss der Dienst zum Einwilligungsmanagement passende Datenmodelle vorsehen. Dabei sind die „speziellen Einwilligungen“ konkretisierte Ausprägungen von generellen Einwilligungstypen.

5.2.1. Ein Datenmodell für spezielle Einwilligungen

[162] Die rechtlichen Elemente einer speziellen Einwilligung sind für die EU durch die DSGVO vorgegeben und z.B. durch die Leitlinie des EDPB konkretisiert worden. Auch internationale Standards wie die ISO/IEC 29184[89] geben – jurisdiktionsübergreifend – Empfehlungen zu den Informationsinhalten als Basis für eine gültige Einwilligung ab. Über diese rechtlichen Inhalte hinaus, muss ein Einwilligungsmanagementsystem ggf. auch noch zusätzliche Informationen zu einer konkret erteilten Einwilligung speichern, wie z.B. den DNS-Namen des Servers, an den die konkrete Einwilligung übermittelt wurde.

[89] Siehe: https://www.iso.org/standard/70331.html (zuletzt abgerufen am 16.12.2021).

[163] Die ISO/IEC 29184 *empfiehlt* folgende grundsätzliche Inhalte für die Datenschutzinformation, auf der eine konkrete Einwilligung basiert:

- Zweck („purpose description“)
- Verantwortlicher („identification of PII controller“)
- Personenbezogene Daten (“PII collection”)
- Art der Erhebung („collection method“)
- Zeit und Ort der Erhebung („timing and location of the PII collection”)
- Art der Verarbeitung („method of use“)
- Ort und Jurisdiktion der gespeicherten Daten („geo-location of, and legal jurisdiction over, stored PII“)
- Weitergabe an Dritte („third-party transfer“)
- Aufbewahrungsfrist („retention period“)
- Betroffenenrechte („participation of PII principal“)
- Informations- und Beschwerdemöglichkeit („inquiry and complaint“)
- Information über Zugriff auf Einwilligungsdaten („information about the choices made for consent“)
- Risiken („risks“).

[164] Als internationaler Standard deckt die ISO/IEC 29184 nicht alle datenschutzrechtlichen Anforderungen an die Information Betroffener im Rahmen der Erhebung personenbezogener Daten ab (vgl. Art. 13/14 DSGVO). Dies ist für die hier durchgeführte technische Betrachtung allerdings nicht entscheidend, da der resultierende, beschreibende Text im unten vorgeschlagenen Datenobjekt auch ggf. zusätzliche Informationen zur Erfüllung der DS-GVO enthalten kann, ohne dass dies Einfluss auf die Datenstruktur hat.

[165] Die Informationen müssen aus technischer Sicht nämlich nicht strukturiert als einzelne Datenfelder vorliegen, sondern können in einem klaren und knappen Informationstext als ein einzelnes Text-Datenobjekt gesehen werden, das vom Einwilligungsmanagementsystem für die nutzende Person auf dem Bildschirm dargestellt bzw. barrierefrei vorgelesen oder vergrößert dargestellt wird. Vorstellbar sind auch alternative Beschreibungen in verschiedenen Sprachen und ggf. sogar verschiedenen Schwierigkeits- und Zusammenfassungsgraden. Technisch

könnte man diese Informationstexte in einzelnen Objekten pro Landessprache beispielsweise mit folgenden Datenfeldern abbilden:

- ☐ Technische ID
- ☐ „Locale“ (Fachbegriff für Sprach- und Landinformation, z.B. „de_AT“)
- ☐ Bezeichnung
- ☐ Kurzbeschreibung (überblicksartige Beschreibung)
- ☐ Langbeschreibung (alle notwendigen Informationen inkl. Zweck).

[166] Technisch-operativ können im Rahmen eines Einwilligungsmanagements auch die folgenden Datenfelder für eine spezielle Einwilligung im Internet relevant sein. Diese Einzelinformationen werden technisch nicht unbedingt alle benötigt, erlauben aber die Unterstützung von datenschutzförderlichen Funktionen wie zum Beispiel einem Widerruf mit einem Klick:

- ☐ Technische ID des Einwilligungstyps (d.h. des generellen Einwilligungstyps, auf dem die spezielle Einwilligung basiert) inklusive genauer Version des Einwilligungstyps
- ☐ Hashwert der Datenschutzinformation (Langbeschreibung + Kurzbeschreibung + Bezeichnung + „Locale“)
- ☐ Verantwortlicher (bzw. Liste von Verantwortlichen)
- ☐ Kontaktinformationen des/der Verantwortlichen
- ☐ DNS-Name des Servers, gegenüber dem die Einwilligung abgegeben wurde
- ☐ IP-Adresse des Clients, der die Einwilligung geschickt hat
- ☐ URL zur Einsicht in den betroffenen Datenbestand und Korrekturmöglichkeit
- ☐ URL zum Widerruf der Einwilligung und Löschung aller Daten
- ☐ Zeitpunkt der Einwilligung (Datum und Zeitstempel in UTC[90])
- ☐ Gültigkeitszeitraum der Einwilligung / Verfallsdatum
- ☐ Status („erteilt“ oder „widerrufen“)
- ☐ Zeitpunkt des Widerrufs (Datum und Zeitstempel in UTC)

[90] https://de.wikipedia.org/wiki/Koordinierte_Weltzeit (zuletzt abgerufen am 16.12.2021).

- ☐ Art der Einwilligung („automatisch“, „nach Abfrage auf Website“, „andere“)
- ☐ Identifikation der einwilligenden Person (ID im Cookie, E-Mail-Adresse, Account-ID, …)
- ☐ Authentifizierung (Device, Passwort, Ausweisdokument, föderiertes Login)
- ☐ Identity Provider bei föderiertem (social) Login
- ☐ Security Token des Identity Providers (Beglaubigung des Logins durch Identity Provider)
- ☐ Beglaubigung der Einwilligung durch einen neutralen Dritten (z.B. durch Zeitstempeldienst).

[167] Diese Daten dienen der Dokumentation der Einwilligung (ggf. sogar bis hin zu einer kryptografischen „Beglaubigung“ durch einen neutralen Dritten) und der operativen Ermöglichung der Betroffenenrechte in Bezug auf Information, Korrektur, Löschung, Beschwerde, sowie manueller und zeitgesteuerter Widerruf der eigentlichen Einwilligung.

[168] Insbesondere die Daten für die operative Ermöglichung der Betroffenenrechte sind hier für einen Dienst zum Einwilligungsmanagement von zentraler Bedeutung, da diese einem Betroffenen die Durchsetzung seiner Rechte effektiv möglich machen. Die Daten zur Dokumentation der Einwilligung sind eher für die Telemediendienste von Interesse, die damit die Existenz und Gültigkeit einer konkreten Einwilligung nachweisen können.

[169] In der angedachten Verordnung könnte man diese Datenfelder zur Einwilligung ggf. in etwas technologieneutralerer Form fassen. Im Kern geht es darum, dass man über das Einwilligungsmanagement die tatsächlich gespeicherten personenbezogenen Daten einfach einsehen, ggf. korrigieren oder löschen kann. Auch muss ein Widerruf der Einwilligung und eine Gesamtlöschanforderung einfach auslösbar sein.

5.2.2. Definition von generellen Einwilligungstypen

[170] Eine Möglichkeit, das Ziel einer Verringerung der regulatorisch induzierten Nutzerinteraktionen mit einem System zum Einwilligungsmanagement zu erreichen, ist es, dem Betroffenen zu ermöglichen, generelle Typen von Einwilligungen zu

definieren (bzw. aus einer Liste von z.B. durch die Aufsichtsbehörden „anerkannten“ Typen von Einwilligungen auszuwählen), die der Dienst zum Einwilligungsmanagement dann im Namen und im Auftrag des Betroffenen automatisch und ohne weitere Nachfrage an konkrete Telemediendienste übergeben kann.

[171] Aus technischer Sicht ist es dabei unerheblich, ob der Rechtsakt der „Einwilligung“ bereits mit der *manuellen Auswahl* des generellen Einwilligungstyps oder erst mit der *automatischen Übermittlung in Sinne einer Erklärung* an einen konkreten Telemediendienst im Namen und im Auftrag des Betroffenen erfolgt. Wichtig für das Ziel des TTDSG ist die Ermöglichung von rechtsgültigen Einwilligungen bei effektiver Vermeidung von ständigen Nachfragen durch jeden einzelnen Telemediendienst.

[172] Grundsätzlich besteht die Datenstruktur eines solchen Einwilligungstyps aus denselben Datenfeldern, wie das Objekt zur Datenschutzinformation:

- ☐ Technische ID
- ☐ „Locale“ (Land- und Sprachinformation)
- ☐ Bezeichnung
- ☐ Kurzbeschreibung
- ☐ Langbeschreibung.

[173] Der Unterschied besteht allerdings darin, dass in den Textfeldern keine konkreten Verantwortlichen genannt werden. Diese werden erst bei der Erteilung der speziellen Einwilligung an einen konkreten Telemediendienst hinzugefügt und zwar in der Datenstruktur der beim Telemediendienst und beim Nutzer gespeicherten speziellen Einwilligung.

[174] Es ist allerdings vorstellbar, dass der Betroffene seinen Auftrag zur automatischen Einwilligung auf bestimmte Kategorien von Verantwortlichen einschränken will. In diesem Fall muss die Datenstruktur des generellen Einwilligungstyps auch noch ein Feld für die Kategorien von Verantwortlichen enthalten:

- ☐ Kategorien von Verantwortlichen

[175] Vorstellbar wären hier Kategorien wie

- * (= alle möglichen Verantwortlichen)

- Betreiber einer Firmeninformationswebseite (z.B. www.volkswagen.de)
- Betreiber einer Nachrichtenwebsite (z.B. www.spiegel-online.de)
- Betreiber eines Forums (z.B. www.netmoms.de)
- Betreiber eines Blogs (z.B. www.einerschreitimmer.com)
- Betreiber Werbenetzwerk (z.B. Tradedesk, inc.)
- Betreiber eines Analytics-Dienstes (z.B. analytics.google.com)
- Betreiber eines Dienstes zur Leistungsmessung
- Betreiber eines Dienstes zur Reichweitenmessung
- Betreiber nur in der EU
- Betreiber nur in Deutschland.

[176] Dabei stellt sich die Frage, wie die Kategorisierung eines Verantwortlichen im Einzelfall zustande kommt. Denkbar wäre eine Selbsteinordnung des Telemediendienstes im Moment der Anfrage, die allerdings ein gewisses Missbrauchspotential eröffnet. Alternativ oder zusätzlich könnte man eine Kategorisierung durch dritte Stellen (z.B. NGOs, Aufsichtsbehörden etc.) vorsehen, die analog zu einem Zertifikat oder einer Whitelist eine neutrale Bestätigung der Kategorie eines Verantwortlichen abgeben.

[177] Eine technische Aufgabe ist eine konsistente, globale Definition und Kodierung von Kategorien von Verantwortlichen. Auch ist zu erwarten, dass im Verlauf der Zeit neue Kategorien hinzukommen.

[178] Des Weiteren könnte der Betroffene noch eine weitergehende Kontrolle ausüben, falls er für einen generellen Einwilligungstyp ein bestimmtes Verhalten des Einwilligungsmanagementsystems vorgeben möchte, beispielsweise „nie erteilen“, „immer erteilen“, „bitte individuelle Nachfrage“. So könnte der Betroffene gemäß seiner persönlichen Privatsphärenpräferenz für seiner Auffassung nach unkritische Verarbeitungen Einwilligungen automatisch erklären lassen, für sicher unerwünschte Dinge immer automatisch eine Absage erteilen und bei Vorgängen, die er gerne fallweise betrachten würde, eine explizite Nachfrage anfordern. Für diese Differenzierung wäre also noch ein zusätzliches Datenfeld notwendig:

- ☐ Einwilligungsentscheidung („nie“, „immer“, „Nachfrage“).

5.2.3. Delegierte Einwilligungen

[179] Eine weitere Möglichkeit, Einwilligungsanfragen von einzelnen Telemediendiensten zu vermeiden, ist die Delegation von Einwilligungen an einen vertrauenswürdigen Dritten. Technisch kann so ein Konzept einfach dadurch umgesetzt werden, dass man eine Liste von speziellen Einwilligungen (und ggf. sogar generellen Einwilligungstypen) bei dem vertrauenswürdigen Dritten referenziert und diese Einwilligungen dann beim Aufruf eines konkreten Telemediendienstes als spezielle, eigene Einwilligungen automatisch an den Telemediendienst kommuniziert werden.

[180] Beispielweise könnte ein Betroffener im Einwilligungsmanagement die URL der Einwilligungsliste einer Organisation seines Vertrauens wie z.B.

[181] `https://www.gdd.de/einwilligungsliste.xml`

[182] angeben. Das Einwilligungsmanagement kopiert diese Liste in den eigenen Datenspeicher und kommuniziert / erklärt nach Anfrage eines Telemediendienstes automatisch eine spezielle Einwilligung an den Telemediendienst, falls die angefragte Einwilligung auf der Einwilligungsliste enthalten ist.

[183] Auch für diese Art von Listen könnte es aus technischer Sicht verschiedene Ausprägungen geben, beispielsweise auch „Blacklists“ mit Einwilligungsanfragen, die das Einwilligungsmanagement auf jeden Fall ablehnen soll. Auch Kombinationen von Listen und Einwilligungen aus mehreren Quellen sind denkbar.

5.3. C. Speicherung der Einwilligungen

[184] Grundsätzlich erscheint es technisch-operativ sinnvoll, spezielle Einwilligungen zu Nachweis- und Kontrollzwecken sowohl unter der Kontrolle des jeweils Verantwortlichen (Telemediendienstes) als auch des Betroffenen zu speichern.

[185] Der Verantwortliche muss im Zweifelsfall nachweisen können, dass er die Daten des Betroffenen im Rahmen einer gültigen Einwilligung verarbeitet. Dafür braucht er naturgemäß nur genau die speziellen Einwilligungen, die für ihn erteilt wurden.

[186] Der Betroffene profitiert im Rahmen der Ausübung seiner Rechte, wenn er alle erteilten und ggf. auch widerrufenen Einwilligungen an einer zentralen Stelle einsehen kann sowie ihm dort weitere Handlungsmöglichkeiten ermöglicht werden (Widerruf, Datenbestand einsehen, etc.).

[187] Da die Liste der Einwilligungen, insbesondere der speziellen Einwilligungen für bestimmte Telemediendienste (`www.onkologie.uniklinik-koeln.de`, `www.seitensprungportal.org`, …), zweifelsfrei einen sehr hohen Schutzbedarf hat, muss insbesondere die vollständige Speicherung unter der Kontrolle des Nutzers genauso sicher sein, wie beispielsweise die Browser-Historie, die Credential-Liste im Passwortspeicher des Browsers oder die Lesezeichen. Für eine Speicherung der Einwilligungen im Klartext bietet sich also beispielsweise der (ggf. sogar profil-bezogene) Speicher des Browsers selbst an. Dieser Speicher ist nur für den Besitzer des Endgeräts bzw. den Inhaber eines konkreten Profils auf dem Endgerät zugänglich. Die Datenhaltung der Einwilligungen profitiert also von denselben Schutzmaßnahmen wie die Browser-Historie mit ähnlichen Inhalten und das Endgerät insgesamt (z.B. Login per Fingerabdruck o.ä.).

[188] Um Anfragen zu Einwilligungen auch geräteübergreifend zu minimieren, sollten die Einwilligungen (und Widerrufe) zwischen allen Endgeräten bzw. Profilen des Betroffenen synchronisiert werden können. Hierfür können bei einer Speicherung im Browser entweder die Standardmechanismen des Browsers zur Ende-zu-Ende-verschlüsselten Synchronisierung zwischen verschiedenen Endgeräten genutzt werden oder es müsste ein zusätzlicher Dienst eines Dritten genutzt werden, um die Einwilligungsdaten (ebenfalls Ende-zu-Ende-verschlüsselt) von einem Endgerät zum anderen Endgerät zu übertragen.

[189] Auch im Falle eines einzigen Geräts ohne Synchronisierungsnotwendigkeit ist eine vollverschlüsselte Speicherung der Einwilligungsdaten außerhalb des Browsers, idealerweise in Form eines „Online-Backups“ bei einem hochverfügbaren, sicheren Dienst im Internet sinnvoll, um bei Verlust oder einem technischen Schaden des Endgeräts die Verfügbarkeit der Einwilligungsdaten auf Seiten des Betroffenen wiederherstellen zu können. Dieses Backup der lokalen Daten auf

dem Endgerät könnte auch im gleichen Zug wie eine grundsätzliche, vollverschlüsselte Sicherung des Endgeräts über die dafür vorgesehenen Mechanismen des Endgeräts erfolgen.

[190] Neben den grundsätzlichen (minimalen) Datenattributen sollte die Verordnung im Sinne der Förderung des Wettbewerbs auch eine effektive Portierbarkeit der Einwilligungsdaten zwischen konkurrierenden Diensten zum Einwilligungsmanagement verlangen, damit ein Betroffener einfach von einem Dienst zu einem anderen Dienst wechseln kann. Diese Portierbarkeit wird typischerweise durch die Möglichkeit des Exports in einem anerkannten Datenformat wie XML sichergestellt. Idealerweise sollte man sich global in einem ISO- oder W3C-Standard (oder einem anderen globalen Gremium) auf ein einheitliches Datenformat zur Speicherung und Übertragung von Einwilligungsdaten einigen. Ob das Datenformat in einer Verordnung des deutschen Gesetzgebers vorgeschrieben oder verlangt werden kann, wäre eine noch zu klärende Rechtsfrage.

5.4. D. Nutzerfreundliche Benutzerschnittstellen zum Management der Einwilligungen

[191] Die Vorteile der im TTDSG vorgesehenen anerkannten Dienste zum Einwilligungsmanagement liegen aus technischer Sicht nicht nur in der Verringerung der notwendigen Nutzerinteraktion durch eine automatisierte Erklärung oder einen automatisierten Widerruf von Einwilligung für konkrete Telemediendienste auf Basis von standardisierten, von Betroffenen wohlverstandenen und von den Aufsichtsbehörden anerkannten Einwilligungstypen.

[192] Ein weiterer Vorteil im Sinne der informationellen Selbstbestimmung besteht in der Möglichkeit des Betroffenen, Einwilligungen für verschiedene Telemediendienste in einer einzigen, ihm wohlbekannten Benutzeroberfläche seines ausgewählten anerkannten Dienstes zu verwalten, anstatt bei jedem Telemediendienst mit einer anderen, mehr oder weniger „nudgy“[91] gestalteten Oberfläche konfrontiert zu werden. Dieser zweite Punkt hat zudem den Vorteil, dass der Betroffene

[91] Als „nudgy“ wird eine Oberfläche bezeichnet, die einen Benutzer mehr oder weniger sanft in eine bestimmte Entscheidung „drängt“ (engl.: to nudge). Viele aktuelle Oberflächen zum Einwilligungsmanagement drängen den Nutzer zu weitgehenden Einwilligungen, beispielsweise indem

immer leicht den Zugang zu den Funktionen zur Ausübung seiner Betroffenenrechte findet und diese bei Bedarf auch übergreifend über eine große Zahl von Telemediendiensten effizient ausüben kann.

[193] Aus funktionaler Sicht sollte die Benutzerschnittstelle des Dienstes zumindest folgende Operationen unterstützen:

[194] **Konfiguration von automatisiertem Verhalten des Dienstes pro Einwilligungstyp**

- Konfiguration des gewünschten Verhaltens in Bezug auf standardisierte, anerkannte Einwilligungstypen (z.B. im Rahmen der Einrichtung des Dienstes).
- Erfassung / Import von neuen Einwilligungstypen und Konfiguration des jeweils gewünschten Verhaltens.

Zum besseren Verständnis wird im Folgenden eine Skizze einer Schnittstelle für das Konzept der Erfassung des Verhaltens in Bezug auf Einwilligungstypen dargestellt (die Texte sind nicht rechtlich abgestimmt und dienen nur der Verdeutlichung):

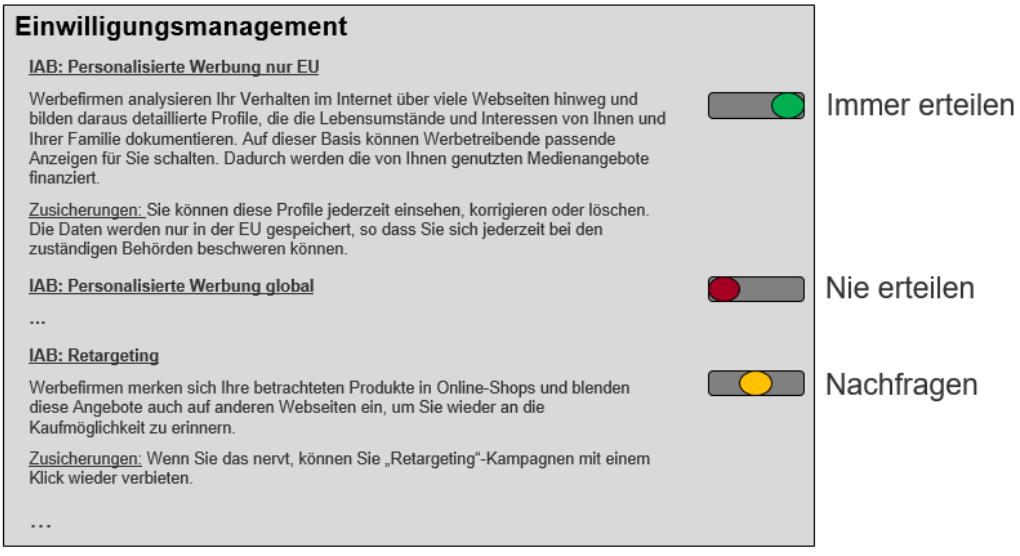

Abbildung 1: Skizze der Konfiguration des gewünschten Verhaltens für bestimmte Einwilligungstypen

die Schaltfläche „Alles akzeptieren" in einer Signalfarbe dargestellt wird, während „Auswahl übernehmen" fast unsichtbar hellgrau auf weiß dargestellt wird.

[195] **Entscheidung bei konkreter Anfrage eines Telemediendienstes**

- Bei notwendiger manueller Entscheidung: Anzeige der Anfrage mit verständlicher Darstellung aller notwendigen Informationen, Entgegennahme der Entscheidung des Betroffenen, Speicherung und Kommunikation an den Telemediendienst. Vorschlag zur Konfiguration des Dienstes für zukünftige automatische Kommunikation der Entscheidung und Umsetzung.
- Bei automatischer Kommunikation der Entscheidung: Einblenden von entsprechenden Symbolen oder Kennzeichen auf dem Endgerät des Nutzers (analog „grünes Schloss“ bei TLS[92]).

[196] **Such- und Navigationsfunktionen für Einwilligungen (Minimalanforderung)**

- Wem habe ich eine konkrete Art von Einwilligungstyp erteilt?
- Welche Einwilligungen habe ich einem konkreten Verantwortlichen erteilt?
- Welche Einwilligungen habe ich Verantwortlichen einer bestimmten Kategorie erteilt?
- Welche Einwilligungen sind älter als X Monate? (ggf. mit automatischer Erinnerung bei Ablauf)

[197] **Handlungen auf Mengen von Einwilligungen (Ergebnisse der Suche / Navigationshierarchie / Auswahl / Alle)**

- Einwilligungen widerrufen.
- Einwilligungen um X Monate verlängern.

[198] **Handlungen in Bezug auf einzelne Verantwortliche**

- Aufruf der Benutzerschnittstelle des Verantwortlichen zur Einsicht, Änderung und (ggf. selektiven) Löschung der nur auf Einwilligung basierenden Daten (bzw. Antrag auf Einsicht etc.).

[92] https://de.wikipedia.org/wiki/Transport_Layer_Security (zuletzt abgerufen am 16.12.2021).

- Gesamtlöschanweisung an den Verantwortlichen für alle auf Einwilligung basierenden Daten.

[199] **Handlungen in Bezug auf einzelne Einwilligungen**

- Detailansicht (alle Textanteile des Informationsdatensatzes).
- Widerruf.
- Verlängerung um X Monate.

[200] Diese grundlegenden (Mindest-)Operationen der Benutzerschnittstelle könnten in der vorgesehenen Verordnung explizit verlangt werden. Die detaillierte grafische bzw. textuelle Gestaltung sollte hier allerdings dem Wettbewerb der verschiedenen Anbieter überlassen werden, da entsprechende Aspekte sich typischerweise nicht „am grünen Tisch“ planen lassen, sondern einem evolutionären, iterativen und partizipativen Entwicklungsprozess unterliegen. Am Ende des Tages werden sich die Anbieter von Diensten zum Einwilligungsmanagement durchsetzen, die die attraktivste und gebrauchstauglichste Benutzeroberfläche und Funktionsmenge haben. Auch ist zu erwarten, dass mittelfristig die besten Ideen und Konzepte zur Interaktionsgestaltung im Sinne der software-ergonomischen Erwartungskonformität von der Mehrzahl der konkurrierenden Einwilligungsmanagementdienste übernommen werden.

[201] Aus software-ergonomischer Sicht würde es zudem Sinn machen, insbesondere vorkonfigurierte Einwilligungstypen in Bezug auf ihre klare Darstellung und Verständlichkeit direkt in Zusammenhang mit der Benutzerschnittstelle durch einen konkreten „Usability Test“ zu evaluieren. Beispielsweise könnte man einer Menge von Testnutzern Kontrollfragen stellen, die prüfen, ob die Konsequenzen der Konfiguration des Verhaltens zu generellen Einwilligungstypen tatsächlich von der überwiegenden Mehrheit verstanden wurden. Konkret könnte man den Betroffenen nach einer Zustimmung zur Profilbildung durch ein Werbenetzwerk auf Basis eines bestimmten Datenschutzinformationstextes fragen, um welche konkreten Daten es geht und was mögliche wahrnehmbare oder sogar negative Effekte der Verarbeitung für ihn sein könnten.

5.5. Mehrwerte durch die Involvierung von Dritten in den Prozess der Einwilligung

[202] Die Analysen in den vorherigen Kapiteln haben bereits eine Reihe von (optionalen) Funktionen ergeben, die notwendigerweise durch Dritte (d.h. nicht den Nutzer mit seinem Browser oder den Telemediendienst) bereitgestellt werden müssen. Konkret waren das die folgenden Funktionen:

- die Synchronisierung von Einwilligungsdaten zwischen Endgeräten bzw. Profilen auf Endgeräten,
- ein Ende-zu-Ende-verschlüsselter Backup außerhalb des Endgeräts,
- die Bereitstellung von Listen von Einwilligungen als Vertrauensstelle und
- die Kategorisierung von Telemediendiensten (ggf. sogar Zertifizierung).

[203] Über die Funktionen dieser Liste hinaus nutzen heute viele Telemediendienste als alternative Authentifizierungsmöglichkeit zu eigenen Credentials ein **föderatives Identitätsmanagement**, dem sie vertrauen, den Betroffenen ausreichend sicher zu authentifizieren, um z.B. Benutzerprofile, Zahlungsdaten oder auch eine erklärte Einwilligung an der entsprechenden Benutzer-ID in der eigenen Datenbank zu speichern. Ein solches zentrales Identitätsmanagement hat für den Benutzer und den Telemediendienst den Vorteil, dass auch bei einem erstmaligen Besuch eines Telemediendienstes keine neuen Credentials (Benutzername / Passwort) erstellt werden müssen, sondern quasi das „Login“ des föderativen Identitätsmanagements verwendet werden kann. In Bezug auf die IT-Sicherheit und den Grad der Authentifizierung vertraut der Telemediendienst dabei dem Identitätsmanagement des Partners.

[204] Dieser Mehrwert eines Identitätsmanagements ist unabhängig von den anderen Funktionen eines Einwilligungsmanagements. Ein Telemediendienst würde – wie bereits ausgeführt – eine über das Einwilligungsmanagement erklärte Einwilligung schlicht an der Identität des Einwilligenden speichern, die er ggf. (aber nicht zwangsläufig) von einem Dienst zum föderativen Identitätsmanagement erhalten hat. Der Telemediendienst könnte die erklärte Einwilligung genauso an einer selbst authentifizierten Identität speichern.

[205] Eine weitere mögliche Rolle für einen Dritten ist die **Erstellung und aufsichtsbehördliche Abstimmung von rechtskonformen, generellen Einwilligungstypen**. Dies würde auch die Erstellung und Prüfung von Texten für die Datenschutzinformationen zur Einwilligung umfassen. Eine verständliche und nicht zu große Menge von rechtskonformen und mit den Aufsichtsbehörden abgestimmten Standardeinwilligungen zu haben, wäre ein wichtiger Schritt auf dem Weg zum Ziel, eine große Zahl von individuellen Einwilligungen pro Telemediendienst in der Nutzerinteraktion zu vermeiden.

[206] Eine weitere Funktion eines Dritten im Rahmen des Einwilligungsmanagements wäre eine **„Beglaubigung" von erklärten Einwilligungen**, um Streitfälle zu vermeiden. Beispielsweise könnte ein Telemediendienst einen elektronischen Fingerabdruck („Hash") einer speziellen Einwilligung von einem neutralen Dritten mit Zeitstempel elektronisch signieren lassen. Damit könnte der Telemediendienst im Streitfall nachweisen, dass eine spezielle Einwilligung zu einem bestimmten Zeitpunkt vorlag. Hier wären auch Blockchain-Lösungen denkbar, wobei der Mehrwert dieser aufwändigen Technik noch zu prüfen wäre.

5.6. Technische Protokolle zwischen den beteiligten Akteuren

[207] Die hier skizzierten technischen Protokolle ergeben sich aus den oben herausgearbeiteten Gestaltungsalternativen und sollen sich möglichst nahtlos in die bestehende Interaktion eines Nutzers mit einem Telemediendienst integrieren, um keine unnötigen Interaktionsschritte („Klicks") zu verursachen. Die folgende Darstellung soll noch keine konkreten technischen Protokolle vorgeben, sondern lediglich die Kommunikationspartner und -inhalte skizzieren, um einen Überblick über den Spezifikationsbedarf zu geben.

5.6.1. Schritt 1: Aufruf des Telemediendienstes, Anzeige der Nutzung eines Einwilligungsmanagements und Übertragung von speziellen Einwilligungen und einem Widerruf

[208] Die Interaktion eines Nutzers mit einem Telemediendienst startet üblicherweise mit dem Anklicken eines Links auf einer anderen Webseite (oder auch Favoritenliste, Suchergebnisseite etc.) oder der Eingabe der Internetadresse in die Adress-

zeile des Browsers. Dadurch wird ein sogenannter „**HTTP-Request**“[93] vom Browser ausgelöst, d.h. der Browser baut eine (ggf. verschlüsselte) Verbindung zu dem Server auf, der im Link genannt ist, und übertragt die Anfrage an den Server. Dieser HTTP-Request kann in allen marktgängigen Browsern von Browser-Plugins[94] bzw. Browser-Extensions um Zusatzinformationen ergänzt werden. Bei HTTP-Requests, die direkt vom Browser des Benutzers gesendet werden, kann der Telemediendienst bei Ende-zu-Ende-Verschlüsselung nach dem Stand-der-Technik im Normalfall (d.h. ohne die Annahme nachrichtendienstlicher oder organisierter, krimineller Eingriffe) davon ausgehen, dass die gesendeten Signale auch tatsächlich unverändert direkt vom Browser der Person kommen, die die Website besucht. Es handelt sich bei der Anfrage um denselben Aufruf aus der derselben Quelle, der durch die Verschlüsselung auch vor Manipulationen geschützt ist.

[209] In diesem HTTP-Request könnte also bereits die Information kodiert werden, dass der Benutzer einen Dienst zum Einwilligungsmanagement verwendet. Dies kann in der Form eines einfachen Flags (Kennzeichens) für einen im Browser laufenden Dienst oder auch in Form einer URL zu einem bei einem Dritten laufenden Dienst für das Einwilligungsmanagement geschehen.

[210] Ebenso könnten auf diesem Weg konkret für diesen Telemediendienst bereits erteilte spezielle Einwilligungen oder ihr Widerruf sofort übermittelt werden, falls diese im Browser vorliegen. Die sichere Identifizierung des Telemediendienstes geschieht dabei über den Servernamen in der URL, analog zur Vorgehensweise bei der Übertragung von Cookies, die von diesem Telemediendienst in der Vergangenheit selbst gesetzt wurden. In diesem Schritt würde der Telemediendienst auch spätestens darüber informiert werden, dass eine vorher erteilte, spezielle Einwilligung widerrufen wurde. Der Telemediendienst muss diesen Widerruf dann berücksichtigen und sich entsprechend verhalten, d.h. die betroffenen einwilligungsbedürftigen Verarbeitungsvorgänge nicht mehr ausführen.

---

[93] Siehe auch: https://de.wikipedia.org/wiki/Hypertext_Transfer_Protocol (zuletzt abgerufen am 16.12.2021).
[94] Siehe z.B. https://developer.mozilla.org/en-US/docs/Mozilla/Add-ons/WebExtensions (zuletzt abgerufen am 16.12.2021).

5.6.2. Schritt 2: Anfrage von speziellen Einwilligungen durch den Telemediendienst

[211] Benötigt der Telemediendienst spezielle Einwilligungen für sich (oder auch für Dritte, insbesondere in Szenarien der Online-Werbung mit vielen im Hintergrund Beteiligten), so kann er im Falle eines direkt im Browser laufenden Dienstes zur Einwilligungsverwaltung entsprechende Anfragen für spezielle Einwilligungen in der Antwort auf den HTTP-Request direkt zurückgegeben und zwar in der sogenannten „**HTTP-Response**“.

[212] Falls der Dienst zum Einwilligungsmanagement durch einen Dritten betrieben wird, müsste der Telemediendienst die speziellen Einwilligungen von diesem Dienst abfragen, beispielsweise dadurch, dass der Browser des Benutzers durch einen *Redirect* (d.h. einer spezielle HTTP-Response des Telemediendienstes mit einer neuen Ziel-URL) zum Server des Einwilligungsmanagements umgeleitet wird, wo er sich dann ggf. anmelden muss und dann von dort (ggf. wieder mit einem *Redirect*) inklusive der speziellen Einwilligungen (oder den Widerrufen) wieder zum Telemediendienst geleitet wird.

[213] Grundsätzlich findet in diesem Schritt auf Seiten des Dienstes zum Einwilligungsmanagement die für die Zielsetzung der Vermeidung von Nutzerinteraktionen entscheidende Prüfung statt, ob als Antwort auf die Einwilligungsanfrage bestimmte spezielle Einwilligungen automatisch erteilt werden können. Idealerweise kommt die Prüfung in diesem Schritt zu dem Ergebnis, dass alle Einwilligungsanfragen des Telemediendienstes automatisch erteilt werden können. Nur in diesem Fall würden für den Nutzer sichtbare Nachfragen des Telemediendienstes vermieden.

[214] Nur für die Einwilligungen, für die gemäß der Konfiguration des Dienstes zum Einwilligungsmanagement keine automatisierte Erteilung in Frage kommt, müsste der Dienst eine (eigene) Benutzeroberfläche anzeigen, die die konkret benötigte Einwilligung darstellt und die Entscheidung des Nutzers einholt.

[215] Die automatisch oder manuell erklärten Einwilligungen stehen am Ende des Schritts zur Übermittlung an den Telemediendienst bereit.

5.6.3. Schritt 3: Übermittlung spezieller Einwilligungen oder eines expliziten Widerrufs an den Telemediendienst

[216] In diesem Schritt werden die automatisch oder manuell erklärten Einwilligungen an den Telemediendienst übertragen. Dies kann über einen weiteren direkten HTTP-Request vom Browser an den Telemediendienst geschehen oder – im Falle eines von einem Dritten betriebenen Dienstes zum Einwilligungsmanagement – über einen zusätzlichen Aufruf eines Webservices von Server-zu-Server bzw. im Redirect über den Browser des Benutzers zurück zum Telemediendienst.

[217] Nach diesem Schritt kann der Telemediendienst die übermittelten Einwilligungen und Widerrufe auswerten und seine Verarbeitungstätigkeiten nach den Vorgaben des Betroffenen durchführen (oder eben auch nicht).

[218] Zu beachten ist hier auch der Sonderfall der von Telemediendiensten für Dritte eingeholte Einwilligungen. Insbesondere im Szenario der Online-Werbung sind hier die Akteure „im Hintergrund“ relevant, die detaillierte Nutzerprofile über viele Telemediendienste hinweg bilden und auf Basis dieser Profile zielgruppengenaue, personalisierte Werbung vermitteln können. Da diese Werbeplattformen typischerweise nicht direkt sichtbar mit dem Nutzer interagieren, sind die Werbeplattformen darauf angewiesen, dass die Einwilligung in die Profilbildung und -verwendung von den Telemediendiensten für sie eingeholt wird. In diesem Fall müssen sich die Telemediendienste und die diversen Akteure im Hintergrund abstimmen, wer die Einwilligungen speichert und im Konfliktfall die konkrete Einwilligung eines Betroffenen nachweisen kann. Diese Abstimmung ist nicht Gegenstand der hier durchgeführten Untersuchungen.

[219] Nach diesem dritten Schritt ist der zentrale Protokollablauf zur Erteilung (oder Nichterteilung) von Einwilligungen durchgeführt. Die nachfolgenden Zusatzprotokolle dienen der direkten Geltendmachung von Betroffenenrechten.

5.6.4. Betroffenenrechteprotokoll A: Einsicht in den Datenbestand, Korrekturmöglichkeiten

[220] Ein ganz wesentliches Betroffenenrecht bei den komplexen, verteilten und schwer nachvollziehbaren Verarbeitungsvorgängen im Internet, insbesondere im

Anwendungsfall der Online-Werbung, ist das Recht der Auskunft über gespeicherte Daten inklusive der darauf aufbauenden Korrekturmöglichkeiten (dazu gehört ggf. im Sinne von einer erhöhten Nutzerfreundlichkeit auch das selektive Löschen von einzelnen Daten).

[221] Zusammen mit der Anfrage nach einer Einwilligung muss der Telemediendienst eine URL des Verantwortlichen übermitteln, über die (authentifiziert über denselben Mechanismus wie die Einwilligung selbst) dem Betroffenen über eine Benutzerschnittstelle des Verantwortlichen vollständiger Einblick in die gespeicherten Daten gewährt wird, inklusive möglichst feingranularer Korrektur- und Löschmöglichkeiten.

[222] Diese Einsichtsmöglichkeit ist insbesondere auch dann wichtig, wenn ein Telemediendienst eine Einwilligung für einen Dritten (z.B. ein Werbenetzwerk im Hintergrund) eingeholt hat. Durch die bereitgestellte URL und Authentifizierungsmöglichkeit per Cookie o.ä. kann der Betroffene unkompliziert („one click“) Einsicht nehmen und ggf. Korrekturen und selektive Löschungen vornehmen. Beispielsweise könnte ein Betroffener, der sich nach einem einzigen Besuch auf einer Webseite über Bluthochdruck über die vielen Anzeigen zu diesem Thema wundert, direkt im Einwilligungsmanagement nach den verursachenden Einträgen bei den Werbenetzwerken suchen und diese löschen.

5.6.5. Betroffenenrechteprotokoll B: Widerruf und komplette Löschung

[223] Eine Einwilligung sollte aus technischer Sicht genauso einfach und schnell widerrufen werden können, wie sie erteilt wurde. Auch hierfür eignet sich die Lösung, dass der Telemediendienst direkt mit der Einwilligungsanfrage eine URL liefern muss, über die die Einwilligung komplett widerrufen werden kann, inklusive der Löschung der bisher verarbeiteten Daten. Auch dieser Prozess funktioniert mit Einwilligungen, die von einem Telemediendienst für Dritte eingeholt werden. Die URL zeigt in diesem Fall auf die Widerruf- und Löschservices des tatsächlich Verantwortlichen.

5.6.6. Betroffenenrechteprotokoll C: Verlängerung von Einwilligungen

[224] Zusammen mit der Anfrage nach einer Einwilligung kann der Telemediendienst eine URL zur Verlängerung einer bereits erteilten Einwilligung übergeben. Diese

Einwilligungs-URL könnte vom Benutzer ausdrücklich über die Benutzerschnittstelle des Dienstes zum Einwilligungsmanagement aufgerufen werden, oder automatisch im Hintergrund nach allgemeineren Vorgaben des Betroffenen (z.B. eine Konfigurationseinstellung im Sinne von „Einwilligungen bei Nutzung des Telemediendienstes automatisch verlängern“).

5.7. Querschnittsthema IT-Sicherheit

[225] Grundsätzlich besteht die Möglichkeit, dass Einwilligungsdaten ggf. einen sehr hohen Schutzbedarf haben, da aus diesen, neben einer Menge Trivialitäten, auch höchst private Lebensumstände abgelesen werden können. Alle Risiken, die die Vertraulichkeit und Integrität dieser Daten gefährden, sollten vermieden werden. Einwilligungen sollten keinem Dritten zugänglich sein und beim Transport (zwischen Endgeräten oder auch zwischen Telemediendienst und Nutzer) Ende-zu-Ende-verschlüsselt sein.

[226] Die Verfügbarkeit der Einwilligungsdaten ist weniger kritisch, da ein Verlust der bereits erteilten Einwilligungen nur zur Notwendigkeit einer Neueingabe und Neuerteilung führt. Das ist für den Betroffenen zwar ärgerlich aber nicht existentiell kritisch.

[227] Insbesondere beim Einblick eines Betroffenen in über längere Zeit aufgebaute Profile bei Werbenetzwerken spielt die Methode der Authentifizierung dieses Zugriffs eine wichtige Rolle. Typischerweise ist das Profil des Werbenetzwerks mit einer technischen ID verknüpft, die beim Aufruf der URL zur Einsicht direkt, wie beim normalen „Tracking“, z.B. über einen Cookie mitgeliefert wird.

[228] Werden die personenbezogenen Daten an einer per E-Mail authentifizierten Identität gespeichert, so kann auch wieder mit diesen Credentials oder einem an die E-Mail versandten Code auf die Daten zugegriffen werden.

5.8. Bewertungen und Empfehlungen

[229] Die in dieser Studie betrachteten Implementierungsalternativen für anerkannte Dienste zum Einwilligungsmanagement unterscheiden sich im Wesentlichen in der Frage, welche Anteile eines solchen Dienstes im Browser des Nutzers und welche Anteile auf dem Server eines Dritten laufen.

[230] Die im Vorfeld der Studie im Fachkreis des BMWi vorgestellten Lösungen NOYB, netID und usercentric[95] unterscheiden sich konkret dadurch, wo die Einwilligungen gespeichert werden und durch welches System die Benutzeroberfläche zur Einwilligungsverwaltung bereitgestellt wird. Die Lösung von usercentric ist allerdings nicht als webseitenübergreifendes Einwilligungsmanagement konzeptioniert, sondern fokussiert auf die Unterstützung einzelner Telemediendienste bei der Umsetzung der Anforderungen des Datenschutzes, beispielsweise indem es die Integration von Werbediensten und Social-Media-Diensten technisch, je nach Benutzerentscheidung, an- oder abschaltet.

[231] Das von NOYB vorgestellte Konzept ist dahingehend „browserzentriert", dass Benutzeroberfläche und Einwilligungsspeicher im Browser angesiedelt sind. Lediglich Zusatzfunktionen wie die Bereitstellung von delegierten Einwilligungen („bulk consent") involvieren Systeme bei Dritten.

[232] Die von der netID-Foundation angedachte Lösung legt die Benutzerschnittstelle und die Speicherung der erteilten Einwilligungen auf die Server von Dritten (z.B. der „1&1 Mail & Media GmbH") und ist in diesem Sinne „drittserverzentriert". Dort würden dann auch die erteilten Einwilligungen und alle anderen Daten zum Einwilligungsmanagement gespeichert. Bei dieser Lösung stellt sich die Frage, woher der Telemediendienst beim ersten Aufruf durch den Browser des Nutzers weiß, dass dieser einen konkreten Dienst zum Einwilligungsmanagement verwendet. Ggf. würde sich auch hier ein Browser-Plugin von netID anbieten, das einen entsprechenden Hinweis in den Erstaufruf des Telemediendienstes einfügt (ggf. sogar direkt mit einer URL zum Server mit dem Einwilligungsmanagement).

5.8.1. Bewertung der Alternativen aus technischer Sicht

[233] Grundsätzlich erscheinen beide Implementierungsalternativen (serverzentriert und browserzentriert) technisch machbar, d.h. es gibt keine fundamentalen „Unmöglichkeiten" in der Umsetzung. Aus diesem Grund sollte weder die eine noch die andere Möglichkeit in der Verordnung explizit ausgeschlossen werden.

[95] Siehe: https://usercentrics.com/de/ (zuletzt abgerufen am 16.12.2021).

[234] Aus technischer Sicht hat die serverzentrierte Lösung allerdings erhebliche Nachteile, so dass davon auszugehen ist, dass sich eine solche Lösung nicht am Markt durchsetzen wird:

- Die notwendige Abfrage von Einwilligungen beim Server erzeugt eine sogenannte Laufzeitabhängigkeit, die dazu führt, dass das Gesamtsystem bestehend aus Dienst, Browser und Telemediendienst eine **geringere Verfügbarkeit** hat, als eine Lösung, die nur von der Verfügbarkeit des Browsers und Telemediendienstes abhängt.
- Die Speicherung von Einwilligungen in einer für den Betreiber des Servers sichtbaren Form gibt unnötigerweise einem Dritten Zugriff auf diese Daten und eröffnet so eine ganze Reihe von zusätzlichen Angriffsvektoren, so dass das Gesamtsystem in Summe **weniger sicher** ist, als eine Lösung, bei der die Einwilligungsdaten nur im Browser und im Telemediendienst verwaltet werden.
- Zudem ist die Spezifikation der Protokolle zur Interaktion „im Dreieck“ zwischen Browser, Einwilligungsmanagement-Server und Telemediendienst **komplizierter und wird letztendlich aufwändiger und ggf. auch langsamer in der Ausführung** als eine Interaktion nur zwischen Browser und Telemediendienst.

[235] Eine Verlagerung von Aufgaben auf den Server eines Dritten macht aus technischer Sicht eher bei Aufgaben Sinn, die von einer Unabhängigkeit vom Browser des Nutzers (und auch der Telemediendienste) tatsächlich profitieren:

- Ausgelagerter (verschlüsselter) Backup der Einwilligungsdaten auf dem Server eines Dritten
- Synchronisierung von Einwilligungsdaten zwischen Endgeräten (über den Server eines Dritten)
- Unabhängige „Beglaubigung“ von erklärten Einwilligungen durch einen neutralen Dritten
- Bereitstellung von aufsichtsbehördlich abgestimmten Einwilligungstypen

- Bereitstellung von Listen von delegierten Einwilligungen als Vertrauensstelle
- Unabhängige Kategorisierung von Telemediendiensten / Verantwortlichen.

[236] Auch kann es für Telemediendienste vorteilhaft sein, neben eigenen „Credentials“ auch ein Login über einen zentralen Dienst zum föderativen Identitätsmanagement anzubieten. Dadurch muss sich der Benutzer für den Telemediendienst kein eigenes Passwort merken. Diese Entscheidung des Telemediendienstes ist allerdings unabhängig von der Frage der Berücksichtigung eines Dienstes zum Einwilligungsmanagement.

5.8.2. Bewertung der Alternativen aus rechtlicher Sicht

[237] Eine rechtliche Bewertung beider Umsetzungsalternativen führt zu keiner eindeutigen Überlegenheit der einen oder der anderen Alternative. Vielmehr hat jede der beiden Umsetzungsalternativen ganz spezifische rechtliche Hürden zu überwinden.

[238] Zunächst einmal **entspricht die browserzentrierte Lösung eher den Grundprinzipien der Datenverarbeitung nach Art. 5 DSGVO**, insbesondere den Grundprinzipien der Datensparsamkeit und der Datensicherheit. Dies liegt daran, dass keinem Dritten Art und Umfang der Nutzung von Telemediendiensten durch den einzelnen Nutzer bekannt werden und dass – wie oben (5.8.1) dargelegt – weniger Angriffsmöglichkeiten für Dritte bestehen. Ferner liegt die Wahl des Plug-in in der Hand des jeweiligen Nutzers bzw. des datenschutzrechtlich Betroffenen, was ein höheres Maß an Autonomie des Betroffenen mit sich bringt.

[239] Dafür ist es **bei der browserzentrierten Lösung schwieriger zu argumentieren, dass dem Nutzer bei Konfiguration des Plug-in neben bestimmten Zwecken nur Kategorien von Empfängern der Daten zur Auswahl zur Verfügung stehen müssen**. Während bei einer drittserverzentrierten Lösung argumentiert werden kann, dass der anerkannte Dienst die Aufgaben übernimmt, welche nach der DSGVO dem ersten Verantwortlichen obliegen, stellen beim reinen Browser-Plug-in die jeweiligen Datennutzer (z.B. Werbeunternehmen) die ersten Verant-

wortlichen dar und müssen daher – jedenfalls nach der bei den Aufsichtsbehörden vorherrschenden Auffassung – auch im Zeitpunkt der Erteilung der Einwilligung der konkreten Identität nach bekannt sein. Das ist zwar kein absolutes technisches Hindernis gegen die browserzentrierte Lösung, führt aber dazu, dass **bei der browserzentrierten Lösung laufend nachträgliche Befassungen des Nutzers erforderlich werden können, sobald sich die Identität von Verantwortlichen ändert** (sofern sich die herrschende Auslegung der DSGVO nicht ändert bzw. nicht im Rahmen der E-Privacy-VO eine Klarstellung erfolgt).

[240] Die browserzentrierte Lösung basiert teilweise auf der Annahme, dass auch eine versehentlich oder aus Bequemlichkeit erteilte individuelle Einwilligung nicht mehr „unmissverständlich“ und daher nach der DSGVO nicht wirksam sei, wenn über das Plug-in bei jeder Anfrage automatisiert eine generelle Ablehnung mitgesendet wird. Inwieweit diese Vorstellung juristisch haltbar ist oder **inwieweit nicht doch nach allgemeinen rechtsgeschäftlichen Grundsätzen eine individuell und ausdrücklich erteilte Einwilligung (etwa durch Anklicken einer Schaltfläche mit „OK“) eine automatisiert vom Plug-in mitgesendete Ablehnung überlagern muss, erscheint fraglich**.

[241] **Beide Umsetzungsalternativen werden auf Schwierigkeiten stoßen, wenn sich die sich in Art. 4a Abs. 2aa des Verhandlungsmandates für den Rat für den Trilog zur E-Privacy-VO abzeichnende Lösung durchsetzen sollte**. Damit anerkannte Dienste der Einwilligungsverwaltung ihr Potenzial entfalten können, ist erforderlich, dass **nur besonders qualifizierte individuelle Einwilligungen eine generelle Ablehnung überspielen können** und dass **bei Bestehen einer generellen Ablehnung das Ansuchen um eine spezielle Einwilligung über den anerkannten Dienst bzw. die betreffende Software laufen muss**, wenn sich der Telemedienanbieter sonst auch für die Erteilung von Einwilligungen auf den anerkannten Dienst bzw. eine Softwareeinstellung beruft (Argument: wer als Telemedienanbieter die Vorteile anerkannter Dienste für eine erleichterte Einholung von Einwilligungen in Anspruch nehmen will, muss auch konsequent sein, wenn es um die Ablehnung von Einwilligungen geht).

5.8.3. Empfehlung und Vorschläge zur Verordnung

[242] Grundsätzlich halten es die Autoren dieser Studie vor dem Hintergrund der Ziele des TTDSG für am effektivsten, in der Verordnung vorwiegend **Anforderungen an anerkannte Dienste zum Einwilligungsmanagement** und insbesondere auch die dort verwalteten Einwilligungstypen und speziellen Einwilligungen festzulegen. Dass Ziel muss sein, dass die Verwendung von entsprechenden „anerkannten Diensten zum Einwilligungsmanagement“ dadurch attraktiv wird, dass diese den Telemediendiensten eine gewisse Rechtssicherheit und Automatisierung von Einwilligungen auch für komplexe Geschäftsmodelle wie Online-Werbung bieten, insbesondere wenn die Aufsichtsbehörden in den Prozess der „Anerkennung“ der Dienste und Einwilligungstypen involviert werden.

[243] Die konkreten Anforderungen an einen Dienst zur Einwilligung könnten die Folgenden sein:

- Usability-geprüft Benutzeroberfläche ohne „Nudging“ mit allen hier beschriebenen Funktionen (ggf. ohne delegierte Einwilligungen).
- Nur aufsichtsbehördlich als wirksam erachtete Einwilligungstypen werden zur automatisierten Erteilung von Einwilligungen verwendet.
- Verweigerung von Einwilligungsanfragen ohne direkte Einblicks-, Korrektur- und Widerrufsmöglichkeit (URL-Angaben).
- Benutzerschnittstelle zur direkten und effektiven Ausübung von Betroffenenrechten auf Basis der URLs.
- Nachweis der sicheren Verwaltung von erteilten Einwilligungen (sehr hoher Schutzbedarf). Ausschluss des Zugriffs Dritter auf die Einwilligungen.
- Sicherstellung der Portierbarkeit aller Daten zu definierten Einwilligungstypen und erteilten Einwilligungen und Widerrufe.

[244] Die genauen technischen Protokolle zwischen Telemediendienst und Einwilligungsmanagement für die Erteilung von Einwilligungen und die Betroffenenrechte sollten international einheitlich spezifiziert werden. Es können aber auch verschiedene Protokolle parallel existieren. Ein Einwilligungsdienst könnte dann auch mehrere Protokolle parallel unterstützen, um sich am Markt durchzusetzen.

Auch wäre es im Interesse von Telemediendiensten, alle weit verbreiteten, konkurrierenden Protokolle zu unterstützen, um eine möglichst nahtlose Benutzererfahrung zu ermöglichen. Idealerweise wird sich nach einiger Zeit ein Standardprotokoll herauskristallisieren und durch das W3C-Konsortium oder ein vergleichbares Gremium festgelegt werden. Dann müssten Telemediendienste nur dieses eine Protokoll unterstützen, um beliebige Dienste zum Einwilligungsmanagement „zu berücksichtigen".

[245] **Anforderungen an die Browser** reduzieren sich darauf, durch Dritte erstellte Plugins/Extensions mit Zugriff auf den lokalen Browser-Speicher, die Response-Request-Operationen und die Benutzeroberfläche des Browsers zuzulassen. Dieser Schritt öffnet insbesondere die Gestaltung von gebrauchstauglichen Benutzeroberflächen und Zusatzfunktionen dem Wettbewerb, indem nicht nur Browser-Hersteller, sondern auch Dritte direkt im Browser laufende Dienste zum Einwilligungsmanagement erstellen können. Browser-Hersteller könnten auch selbst einen anerkannten Dienst zum Einwilligungsmanagement direkt als Standardfunktion des Browsers implementieren, wobei trotzdem noch der Wettbewerb mit als Plug-in implementierten Alternativen aufrechterhalten werden sollte.

[246] Obwohl die allermeisten Browser die Anforderung der Öffnung für wirkmächtige Plugins/Extensions heute schon umsetzen (die mobile Version vom Googles Chrome-Browser ist eine Ausnahme), ist diese Anforderung wichtig, um in Bezug auf Online-Werbung geschlossene Plattformen zu vermeiden. Aus technischer Sicht ist die „erzwungene" Öffnung von Browsern für Erweiterungen und Veränderungen durch Dritte vergleichbar mit dem Zusammenhang von Betriebssystemen und darauf laufenden Anwendungen. Diesbezüglich sei auf die vergangene kartellrechtliche Diskussion um die enge Verknüpfung von Browsern und Betriebssystemen verwiesen.

[247] **Für Telemediendienste müssen keine speziellen Anforderungen** gestellt werden. Die Motivation der Telemediendienste zur Unterstützung von gemäß der Verordnung anerkannten Diensten zum Einwilligungsmanagement sollte sich alleine durch die durch die Verordnung eröffnete Möglichkeit der rechtskonformen Weiterführung von werbefinanzierten Angeboten ergeben. Aus technischer Sicht ist eine Umsetzung eines (wie auch immer genau ausgestalteten) Protokolls zur

Anfrage und Entgegennahme von automatisiert erteilten Einwilligungen (Schritte 1, 2 und 3) zumindest bei einem im Browser laufenden Dienst zum Einwilligungsmanagement einfach umzusetzen, da es sich in die bereits bestehenden Interaktionen „einklinken“ kann. Es ist zu erwarten, dass Hersteller von Content-Management-Systemen (CMS) und Blog-Plattformen (z.B. Wordpress) bei einem international getragenen Protokoll schnell eigene Erweiterungen und Funktionen herausbringen, die eine Nutzung des Protokolls mit geringem Aufwand ermöglichen.

[248] Aufwändiger ist die Implementierung von telemediendienst-spezifischen Schnittstellen für die Betroffenenrechte, insbesondere die direkte Einsichtnahme in die gespeicherten Daten und die feingranularen Korrektur- bzw. Löschfunktionen. Ggf. könnte diese Aufwände in der Verordnung dadurch abgemildert werden, dass die in der speziellen Einwilligung angegebene URL zunächst auf ein Kontaktformular zeigt, über das die Betroffenen ihre Rechte wahrnehmen können. Eine direkte Einsichtnahme wäre allerdings wesentlich datenschutzfreundlicher.

6. Anlagen

- Keine -

Die Studie umfasst 88 Seiten und 137406 Anschläge.

Köln, Hamburg, Wien, den 16.12.2021

Dr. Oliver Stiemerling
Öffentlich bestellter und vereidigter Sachverständiger für Systeme und Anwendungen der Informationsverarbeitung

RA Steffen Weiß, LL.M.

Prof. Dr. Christiane Wendehorst