Bernemann, Julian; Kneuper, Ralf

Article — Published Version

Personal Information Management Systems nach TTDSG

HMD Praxis der Wirtschaftsinformatik

Provided in Cooperation with:
Springer Nature

Suggested Citation: Bernemann, Julian; Kneuper, Ralf (2023) : Personal Information Management Systems nach TTDSG, HMD Praxis der Wirtschaftsinformatik, ISSN 2198-2775, Springer Fachmedien Wiesbaden GmbH, Wiesbaden, Vol. 60, Iss. 2, pp. 308-321, https://doi.org/10.1365/s40702-023-00946-4

This Version is available at:
https://hdl.handle.net/10419/308877

HMD Praxis der Wirtschaftsinformatik (2023) 60:308–321
https://doi.org/10.1365/s40702-023-00946-4

SCHWERPUNKT

Personal Information Management Systems nach TTDSG

Julian Bernemann · Ralf Kneuper

Eingegangen: 21. September 2022 / Angenommen: 30. Januar 2023 / Online publiziert: 21. Februar 2023

Zusammenfassung Viele Webpräsenzen nutzen Cookies, um die Interessen der Besucher zu ermitteln und Komfortfunktionen anbieten sowie individualisierte Werbung anzeigen zu können. Rechtliche Voraussetzung für derartige Cookies ist meist eine Einwilligung der Besucher. Die aktuell vorherrschende Praxis zur Einholung von Einwilligungen bei Webpräsenzen in Form von Cookie-Bannern wird aber von den Besuchern oft als nervend angesehen und verfehlt daher das eigentliche Ziel einer informierten und freiwilligen Entscheidung.

Um diese Schwierigkeit zu adressieren, wurde 2021 mit dem Telekommunikation-Telemedien-Datenschutz-Gesetz das Konzept der „anerkannten Dienste zur Einwilligungsverwaltung", meist als PIMS bezeichnet, eingeführt. Der vorliegende Beitrag analysiert dieses Konzept und arbeitet die wesentlichen Herausforderungen bei seiner Umsetzung sowie mögliche Lösungsansätze heraus. Dabei zeigen sich eine Reihe von Herausforderungen aus technischer, rechtlicher und wirtschaftlicher Sicht, für die überzeugende Lösungen derzeit nicht absehbar sind. Insbesondere erscheint der Nutzen der PIMS aus Sicht der Betreiber von Webpräsenzen und Werbenetzwerken, aber auch der Nutzer, unter den derzeitigen rechtlichen Rahmenbedingungen nicht ausreichend, dass derartige Dienste sich in der Breite durchsetzen können.

Schlüsselwörter Personal Information Management System · PIMS · TTDSG

Julian Bernemann
Nußloch, Deutschland

✉ Ralf Kneuper
IU Internationale Hochschule, Erfurt, Deutschland
E-Mail: ralf.kneuper@iu.org

Personal Information Management Systems According to the German Telecommunications Telemedia Privacy Act

Abstract Many websites use cookies to determine the interests of visitors and to offer convenience functions and to display individualized advertising. However, the legal prerequisite for such cookies is usually the consent of the visitor. However, the current practice of obtaining consent for web presences via cookie banners is often seen as annoying by visitors and therefore misses the actual goal of an informed and voluntary decision.

To address this difficulty, the Telecommunications Telemedia Privacy Act, which came into force in 2021, introduced the concept of "recognized consent management services", usually referred to as PIMS. This paper analyzes this concept and elaborates on the main challenges in its implementation as well as possible solutions. This reveals several challenges from a technical, legal and economic perspective, for which convincing solutions are currently not foreseeable. In particular, the benefits of PIMS from the point of view of operators of web presences and advertising networks, but also of users, do not seem sufficient under the current legal framework for such services to become widely accepted.

Keywords Personal Information Management System · PIMS · TTDSG

1 Ausgangssituation und Zielsetzung

1.1 Ausgangssituation

Die Nutzung digitaler Medien nimmt mittlerweile in vielen Lebensbereichen einen wachsenden Stellenwert ein. Der damit verbundene Austausch digitaler Informationen findet meist über das Internet mit Hilfe eines Browsers oder einer entsprechenden App statt. Allerdings findet neben der direkten, für die Nutzer sichtbaren Kommunikation oftmals auch ein kaum sichtbarer Informationsaustausch statt mit dem Ziel, das Verhalten der Nutzer aufzuzeichnen („Tracking") und Profile für Marketing- und ähnliche Zwecke zu bilden

Sowohl die Bereitstellung vieler Komfortfunktionen als auch das Tracking erfolgen meist mittels Cookies über Zugriffe auf die Endgeräte der Nutzer, die zur Wahrung des Datenschutzes und der Systemintegrität in der EU zumeist eine Einwilligung erfordern (Art. 5 Abs. 3 RL (EU) 2002/58/EG in der Fassung 2009/136/EG sowie Art. 6 Abs. 1 lit. a DSGVO). Daher begegnen den Internetnutzern beim Aufruf von Webseiten regelmäßig Einwilligungsabfragen, die allerdings oft als „nervend" empfunden werden und daher auch oft ohne genaues Lesen einfach akzeptiert werden („consent fatigue"), ihren Schutzzweck also verfehlen. Hierfür gibt es viele anekdotische Belege, aber auch systematische Studien wie beispielsweise von Web.de und GMX (Friemel 2020). Wünschenswert wäre daher eine nutzerfreundliche und gleichzeitig rechtskonforme Alternative zu Cookie-Bannern, beispielsweise als zentraler Dienst zur Einwilligungsverwaltung.

Um hier Abhilfe zu schaffen, wurde das Konzept der „Personal Information Management Services“ (PIMS) vorgeschlagen, beispielsweise von der Stiftung Datenschutz (2017), sowie die eng verwandten „Personal Information Management Systems“ (EDPS 2020) oder, mit einem etwas anderen Ansatz, die in ISO/IEC 27701:2019 standardisierten Privacy Information Management Systems. Auf dieser Basis hat der deutsche Gesetzgeber in § 26 des Telekommunikation-Telemedien-Datenschutz-Gesetzes (TTDSG) das Konzept unter dem Namen der „anerkannten Dienste zur Einwilligungsverwaltung“ auch juristisch eingeführt. Eine bislang nicht vorliegende Rechtsverordnung der Bundesregierung soll die Anforderungen an PIMS und ihre Anerkennung näher definieren (§ 26 Abs. 2 TTDSG). Mit (Stiemerling et al. 2021) wurde allerdings eine Analyse der juristischen und technischen Rahmenbedingungen für PIMS veröffentlicht.

Als Basis der weiteren Diskussion sollen kurz die wichtigsten an der Nutzung von PIMS beteiligten Rollen erläutert werden:

- Telemediendienste (TMD), typischerweise Webpräsenzen. Dabei wird im Folgenden auf die Unterscheidung zwischen dem Betreiber des TMD und dem TMD selbst verzichtet.
- Drittanbieter, die von TMD aufgerufene Tracking-Mechanismen (insbesondere Third-Party-Cookies) bereitstellen, meist zur Bereitstellung individualisierter Werbung beim TMD
- Nutzer, die über einen Browser auf einem Endgerät (PC, Smartphone etc.) auf TMD zugreifen und dabei zur Erteilung einer Einwilligung in eine Verarbeitung, insbesondere die Nutzung von Cookies, aufgefordert werden
- PIMS, mit dem die (erteilten oder verweigerten) Einwilligungen des Nutzers verwaltet werden.

1.2 Zielsetzung

Das Ziel dieses Beitrags ist es zunächst, die existierenden Ansätze zur Einholung von Einwilligungen darzustellen, dabei auf die rechtlichen Anforderungen einzugehen und die Nutzbarkeit (Usability) zu bewerten. Anschließend soll analysiert werden, inwieweit das neue Konzept von PIMS realisierbar ist und einen Beitrag zur Verbesserung der aktuellen Situation liefern kann.

1.3 Cookies

Wichtigster Tracking-Mechanismus sind Cookies, also kurze Texte, die im Browser auf Anforderung einer besuchten Webpräsenz gespeichert und dieser bzw. der Internet-Domäne zugeordnet sind. Wenn der Browser Daten von dieser Domäne abruft, dann sendet er jeweils die zugehörigen Cookies mit und stellt damit die Verbindung zwischen verschiedenen Anfragen des Browsers her. Dadurch kann beispielsweise erkannt werden, dass ein Nutzer bereits angemeldet ist, einen Warenkorb gefüllt hat, oder die zu verwendende Sprache ausgewählt hat.

Eine spezielle Variante der Cookies sind die Drittanbieter-Cookies (Third-Party-Cookies), bei denen neben Nutzern und den Betreibern der Webpräsenzen eine

dritte Partei involviert ist, die diese Cookies setzt und damit typischerweise Informationen über das Verhalten der Besucher über verschiedene Webpräsenzen hinweg sammeln kann. Durch die Kombination dieser Informationen können Drittanbieter sehr viel umfangreichere und konkretere Aussagen über die Nutzer machen (Mayer und Mitchell 2012).

Auf die weiteren zum Tracking eingesetzten Techniken, die funktional dem gleichen Zweck dienen und oft fälschlich ebenfalls als Cookies bezeichnet werden, beispielsweise Web Storage (eingeführt mit HTML5), das Auslesen von Werbe- und Geräte-IDs oder Seriennummern sowie Fingerprinting soll im Folgenden nicht separat eingegangen werden, auch wenn die Aussagen weitgehend übertragbar sind. Entsprechendes gilt für Tracking-Techniken bei Diensten, auf die nicht mit einem Browser, sondern auf anderem Weg zugegriffen wird, beispielsweise über Apps oder IoT-Geräte.

2 Anforderungen und rechtlicher Rahmen

2.1 Rechtliche Rahmenbedingungen für Cookies

Gesetzliche Regelungen zu Cookies und anderen Tracking-Mechanismen gibt es sowohl auf europäischer Ebene als auch auf nationaler Ebene. Mit Art. 5 Abs. 3 der EU-Richtlinie 2002/58/EG (ePrivacy-Richtlinie) wurde eine Einwilligungspflicht für alle Cookies, die nicht unbedingt für einen vom Nutzer explizit gewünschten Dienst erforderlich sind, eingeführt. Als EU-Richtlinie galt diese Regelung nicht direkt (anders als eine EU-Verordnung wie die unten angesprochene DSGVO), sondern musste von den Mitgliedsstaaten in nationales Recht übernommen werden, und es war lange umstritten, ob dies in Deutschland korrekt umgesetzt wurde. Mit dem sogenannten Planet49-Urteil von 2019 des BGH wurde eindeutig geklärt, dass eine solche Einwilligung aktiv erteilt werden muss (Opt-In) und eine vorbelegte Auswahl, die man abwählen kann (Opt-Out), als Einwilligung nicht genügt. Diese Regelung wurde 2021 mit dem TTDSG explizit in das deutsche Recht übernommen, dem gleichen Gesetz, in dem auch die PIMS eingeführt wurden.

Neben dem TTDSG ist für den Umgang mit Cookies noch die Datenschutz-Grundverordnung (DSGVO) der EU zu berücksichtigen, die u. a. die Anforderungen an Einwilligungen genauer definiert. Die genaue Abgrenzung zwischen den Anwendungsbereichen von ePrivacy-Richtlinie bzw. TTDSG einerseits und DSGVO andererseits ist für die hier beschriebenen PIMS von geringer Bedeutung und wird nicht weiter diskutiert.

Zu berücksichtigen ist in diesem Zusammenhang, dass derzeit an einer ePrivacy-Verordnung der EU gearbeitet wird, die die ePrivacy-Richtlinie in naher Zukunft ablösen soll und bei der PIMS-ähnliche Lösungen zumindest diskutiert werden.

2.2 Anforderungen an Einwilligungen

Aus §§ 25, 26 Abs. 1 TTDSG in Verbindung mit den allgemeinen Anforderungen der DSGVO an Einwilligungen lassen sich für PIMS folgende Anforderungen zur ordnungsgemäßen Umsetzung ableiten.

2.2.1 Freiwilligkeit der Einwilligung (Koppelungsverbot)

Eine Einwilligung ist formfrei möglich, muss aber freiwillig, also ohne Zwang und mit einer echten Wahlmöglichkeit, erfolgen. Dabei ist es nicht zulässig, Einwilligungen so zu bündeln, dass der Nutzer alle Einwilligungen nur gemeinsam annehmen oder ablehnen kann. Dies bedeutet für ein PIMS, dass es den Nutzern ermöglichen muss, frei granulare Einwilligungen oder Ablehnungen zu wählen (Stiemerling et al. 2021, Rn. 53–56).

2.2.2 Informiertheit der Einwilligung

Sowohl DSGVO als auch TTDSG sehen vor, dass „betroffene Personen", hier also die Nutzer, ausreichend über ihre Entscheidungen informiert werden müssen, um deren Konsequenzen korrekt abschätzen zu können (Art. 4 Abs. 11 sowie Art. 7 Abs. 2 DSGVO; § 25 Abs. 1 TTDSG). Dazu gehören u. a. Angaben zur Identität des Verantwortlichen und zu Art und Zweck der Verarbeitung sowie die Dauer der Speicherung und die Zugriffsmöglichkeit Dritter (Drittanbieter-Cookies). Auch wenn Nutzer die gesetzten Cookies grundsätzlich lesen können, ist deren Bedeutung oft nur dem Betreiber der Webpräsenz bekannt. Nutzer können aus Namen und Werten von Cookies deren Bedeutung häufig nicht erkennen, insbesondere nicht, welche Einwilligungen dort festgehalten sind. All diese Informationen müssen auch von einem PIMS bereitgestellt werden (Salemi 2022, Kap. 3.1).

2.2.3 Einwilligung für den bestimmten Fall

Einwilligungen müssen sich jeweils auf einen bestimmten Fall beziehen, der durch festgelegte, eindeutige und legitime Zwecke spezifiziert ist (Stiemerling et al. 2021, Rn. 65). Das bedeutet für PIMS, dass pauschalisierte Einwilligungen nicht möglich sind – eine erhebliche Einschränkung für den gewünschten Zweck.

2.2.4 Unmissverständlich abgegebene und ausdrückliche Willensbekundung

Die Anforderungen der Unmissverständlichkeit und Ausdrücklichkeit der Willensbekundung setzen voraus, dass keine Einwilligung bereits ausgefüllt ins PIMS integriert werden darf. Dies führt dazu, dass ein PIMS-Dienst grundsätzlich keine Einwilligungen geben darf, soweit der Nutzer nicht explizit zugestimmt hat (Stiemerling et al. 2021, Rn. 74).

Ob und unter welchen Rahmenbedingungen es möglich ist, dass eine Einwilligung vom Betroffenen/Nutzer delegiert wird, beispielsweise an ein PIMS, ist umstritten.

Gerade im Fall eines vom Nutzer gewählten PIMS erscheint dies wünschenswert (Stiemerling et al. 2021, Rn. 115–120).

2.3 Weitere Anforderungen an Einwilligungsverwaltung

2.3.1 Dokumentations- und Nachweispflichten

Zur Umsetzung der Dokumentations- und Nachweispflichten der DSGVO muss ein PIMS alle notwendigen Details einer Einwilligung speichern, und darüber hinaus dem Telemedienanbieter genug Informationen bereitstellen, damit dieser die Einwilligung korrekt dokumentieren kann (aber auch nicht mehr).

Zum Nachweis einer erteilten Einwilligung reicht deren Speicherung als Cookie (das dann technisch erforderlich ist und keine Einwilligung benötigt), sofern der TMD anhand seiner Software nachweisen kann, dass diese korrekt gesetzt und ausgewertet werden.

2.3.2 Gültigkeitsdauer der Einwilligung und Möglichkeit des Widerrufes

Es gibt keine explizit definierte Gültigkeitsdauer für Einwilligungen, aber länger als zwei Jahre nicht genutzte Einwilligungen sollten laut DSK erneuert werden (DSK 2022, Kap. 3.5). Auch das Gutachten von Stiemerling et al. empfiehlt, Einwilligungen „regelmäßig zu erneuern“ (Stiemerling et al. 2021, Kap. 4.4.2). Damit wird einerseits unterstützt, dass eine Einwilligung noch den bewussten Willen des Nutzers widerspiegelt, andererseits wird das Problem des „consent fatigue“ dadurch weiter verschärft.

Für ein PIMS bedeutet das, dass auch hier festgehalten werden muss, wann eine Einwilligung erteilt wurde, um nach Bedarf eine Bestätigung anzufordern.

Daneben muss ein PIMS auch die Möglichkeit eines Widerrufes von Einwilligungen unterstützen und diesen Widerruf ggf. an den TMD weitergeben.

3 Anwendungsfälle für PIMS

3.1 Überblick über die Einbindung eines PIMS

Abb. 1 gibt einen Überblick, wie ein PIMS in den Ablauf der Einwilligungsanfragen eingebunden werden. Variante 1 beschreibt den bislang üblichen Ablauf ohne Nutzung eines PIMS. Varianten 2 und 3 beschreiben jeweils den Ablauf mit Nutzung eines PIMS, wobei zwei technische Möglichkeiten unterschieden werden (vgl. Abschn. 5): Das PIMS kann lokal im Browser implementiert werden (Variante 2; vgl. Abschn. 5.2), oder es kann als Serverdienst implementiert werden (Variante 3; vgl. Abschn. 5.3).

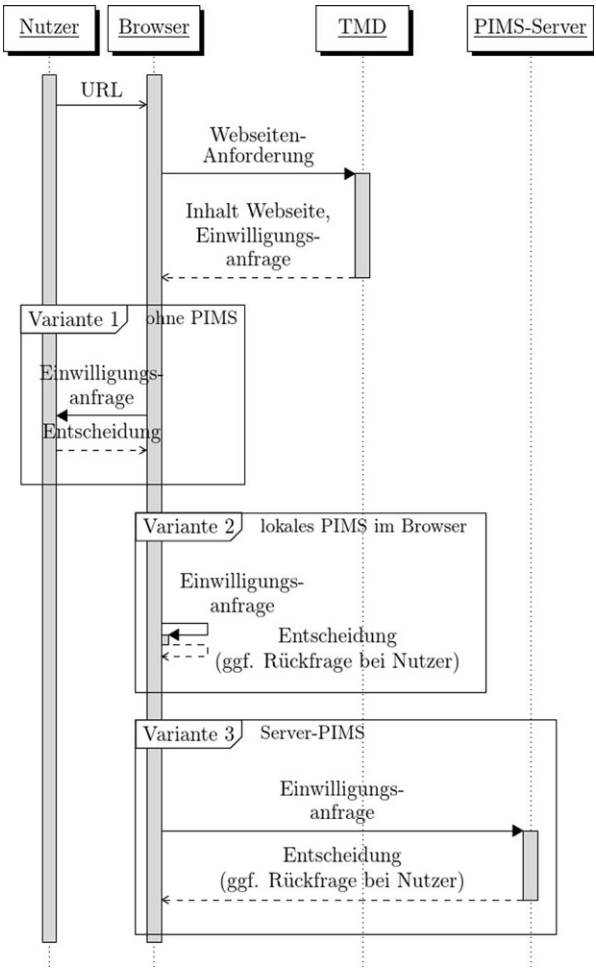

Abb. 1 Einbindung von PIMS in Einwilligungsabfragen

3.2 Anwendungsfälle

In Anlehnung an (Stiemerling et al. 2021, Rn. 140) sollte ein PIMS die folgenden Anwendungsfälle abdecken:

1. Ex-ante-Einwilligung erstellen: Eine essentielle Funktion eines PIMS ist die Definition genereller, dienstübergreifender Einwilligungen im Vorhinein bzw. deren Übernahme aus vordefinierten Einwilligungslisten. Das Management solcher dienstübergreifender Einwilligungen erfordert ein entsprechendes Datenmodell in PIMS sowie die Möglichkeit, diese Einwilligungen dienstunabhängig zu speichern. Wie bereits in Abschn. 2.2.3 erläutert, besteht hierbei aber die Herausforderung, dass solche generellen Einwilligungen ausreichend bestimmt sein müssen, und es ist jeweils im Einzelfall zu betrachten, inwieweit das der Fall ist.

2. Einwilligungsanfrage bearbeiten: Bei diesem Anwendungsfall ruft der Nutzer einen TMD auf, der daraufhin prüfen muss, ob für die durchzuführenden Zugriffe eine Einwilligung vorliegt. Hierzu muss der TMD zunächst identifizieren, welches PIMS der Nutzer verwendet, und bei diesem die gewünschten Einwilligungen anfragen. Wenn dort bereits für alle Einwilligungen eine Zustimmung oder Ablehnung hinterlegt ist, beantwortet das PIMS die Anfrage ohne weitere Interaktion mit dem Nutzer. Andernfalls fordert es für die nicht vorliegenden Einwilligungsanfragen eine Antwort vom Nutzer an.
3. Einwilligung bearbeiten oder widerrufen: Der Nutzer bearbeitet im PIMS eine oder mehrere Einwilligungen und erlaubt beziehungsweise widerruft diese. Im Falle eines Widerrufs muss der Zugriff unmittelbar gestoppt und gespeicherte Daten gelöscht werden. Sofern das PIMS hierzu keinen direkten Zugriff auf das Endgerät des Nutzers hat, erfordert dies die Unterstützung der betreffenden TMD.
4. Bericht erstellen: Mit einem Bericht erhalten Nutzer eine Übersicht darüber, welche Einwilligungen aktuell erteilt bzw. abgelehnt sind und nachvollziehen, inwieweit die aufgerufenen TMD diese Entscheidungen befolgt haben. Dieser Anwendungsfall wird in 3.2 noch näher betrachtet.
5. PIMS-Nutzung beenden: Nutzer müssen jederzeit die Möglichkeit haben, ihre Nutzung des PIMS zu beenden. In diesem Falle muss das PIMS die gespeicherten Daten des Nutzers löschen und die Einwilligungen analog zu Anwendungsfall 3 widerrufen.
6. Dienst-Registrierung starten, ändern oder beenden: Der TMD muss ein vertragliches Verhältnis mit dem PIMS besitzen, um zum einen sicherzustellen, dass das PIMS korrekt seine Anfragen akzeptiert und dass er auch darauf vertrauen kann, dass das PIMS diese Einwilligung rechtsgültig einholt.
7. Nutzer-Registrierung starten. Vor der Nutzung eines PIMS müssen die rechtlichen Grundlagen für die Nutzung des PIMS zwischen Nutzern und dem PIMS-Dienst geklärt und die Nutzer über die Funktionsweise des PIMS informiert werden.

Damit das Konzept der PIMS ein Erfolg werden kann und auch einen Mehrwert für Nutzer und TMD bietet, ist eine gute Nutzbarkeit notwendig. Der aktuell verbreitete Ansatz der Cookie-Banner erfüllt durchaus die rechtlichen Anforderungen zur Einholung und Dokumentation der Einwilligungen, aber mit schlechter Nutzbarkeit. Dementsprechend gibt es die Herausforderung, aber auch die Chance für PIMS, sich über eine gute Nutzbarkeit durchzusetzen.

3.3 Überprüfung und Widerruf erteilter Einwilligungen

Mit Hilfe geeigneter Berichte müssen Nutzer nachvollziehen können, welche Entscheidungen sie getroffen und ob diese Entscheidungen wie erwünscht umgesetzt wurden, insbesondere auch welche Cookies mit welcher Bedeutung gesetzt wurden („Recht auf Auskunft“). Daher ist eine Kooperation des PIMS mit den TMD erforderlich: Die TMD könnten dem PIMS ausreichend Informationen zu dem jeweiligen Cookie und Zweck übermitteln, die dann vom PIMS für die Nutzer angemessen aufbereitet werden.

Eine weitere Schwierigkeit ist, dass das Konzept der Cookies technisch keinen Zugriff Dritter auf die von einem TMD gesetzten Cookies erlaubt. Diese Einschränkung, die dem Schutz der Nutzer und ihrer Privatheit dient, macht im Fall eines PIMS die Umsetzung deutlich schwieriger. Ein solcher Zugriff erfordert ein Plug-in beziehungsweise geeignete Software direkt auf dem Endgerät, was aber nicht bei allen Endgeräten und Browsern möglich ist.

Als Alternative zu einer solchen Plug-in-Schnittstelle ist es möglich, eine Auskunft oder einen Widerruf über eine abgespeicherte URL beim TMD zu realisieren. Diese URL muss der TMD beim Senden der Anfrage übermitteln und das PIMS speichert diese zusammen mit der Einwilligung ab. Mit Hilfe dieser URL soll der Nutzer dann seine Einwilligungen überprüfen und Modifikationen oder einen Widerruf vornehmen (Stiemerling et al. 2021, Rn. 222–223). Voraussetzung ist, dass die URL zumindest immer dann verfügbar ist, wenn auch der TMD verfügbar ist.

4 Standardisierung von Einwilligungen

Ein wesentlicher potenzieller Nutzen eines PIMS ist die Vereinfachung des Umgangs mit Einwilligungen durch deren einheitliche Darstellung. Dazu muss ein PIMS Einwilligungen gruppieren und zusammenfassen. Dies gestaltet sich einerseits aufgrund der Vielzahl von verschiedenen Einwilligungsformen schwierig, bietet andererseits aber auch die Möglichkeit, einen echten Nutzen für die Nutzer des Dienstes zu generieren.

Der Bedarf an einer einheitlichen Darstellung wird beispielsweise deutlich, wenn man sich die verschiedenen Cookie-Banner und den deutlich unterschiedlichen Detaillierungsgrad betrachtet, mit denen verschiedene Webpräsenzen die Nutzung gleicher Dienste wie beispielsweise Google Analytics beschreiben und die entsprechende Einwilligung einholen. Zwar können auch gleiche Dienste unterschiedlich parametrisiert sein, was zu Unterschieden in den Beschreibungen führt, aber die tatsächlich zu findenden Unterschiede gehen weit darüber hinaus.

Darüber hinaus gestaltet sich eine Standardisierung auch deshalb schwierig, weil die Einwilligungen für die TMD möglichst global, also auch außerhalb des Geltungsbereiches der DSGVO, gültig sein sollten.

Exemplarisch für einen weit verbreiteten Ansatz zur Standardisierung von Einwilligungen ist das IAB Europe Transparency & Consent Framework zu nennen. Dieses Framework hat das Ziel, allen Parteien, die digitale und personalisierte Werbung schalten, zu helfen, dies DSGVO-konform ausführen zu können (IAB Europe 2022). Auch wenn diese letzte Eigenschaft fraglich ist, könnten PIMS die im Framework definierten Kategorien zur Gruppierung von Einwilligungen nutzen.

Einen deutlich umfassenderen Anspruch beschreiben Bartsch et al. (2022) mit dem Ansatz der Policy Definition Languages (PDLs), um Datenschutzfestlegungen einheitlich zu beschreiben und dadurch die Datensouveränität zu fördern. Hierbei handelt es sich aber derzeit nicht um ein einsetzbares Produkt, sondern eine Studie, die zeigt, dass das Thema trotz einiger existierender Ansätze noch ein weites Forschungsfeld mit vielen offenen Fragen ist.

5 Technische Umsetzung

Basierend auf den beschriebenen Rahmenbedingungen und Voraussetzungen sehen die Autoren die im Folgenden beschriebenen Ansätze zur Umsetzung eines PIMS.

5.1 Datenmodellierung

Aus den beschriebenen Anwendungsfällen ergeben sich folgende Anforderungen an ein PIMS-Datenmodell:

- Speicherung von standardisierten Einwilligungen entsprechend eines branchenübergreifenden Standards
- Dokumentation der Verknüpfungen zwischen TMD und Drittanbietern
- Möglichkeit der Erfassung von nicht standardisierten Einwilligungen
- Bereitstellung zusätzlicher Details, um den Nutzer umfassend zu informieren
- Erfassung von für eine Berichtsfunktion erforderlichen Daten
- Bei Nutzung von Benutzerkonten: Datenspeicherung für ein Nutzermanagement sowie Erfassung von endgerätspezifischen Einwilligungen

Im Gutachten (Stiemerling et al. 2021, Kap. 5.2.1) wird daher eine Verwendung des Standard ISO/IEC 29184 „Information technology—Online privacy notices and consent“ mit einer Erweiterung um PIMS-spezifische Felder empfohlen.

5.2 Lokale Implementierung eines PIMS

Ein mögliches Architekturmodell für PIMS ist die Implementierung als Erweiterung im Endgerät beziehungsweise Browser etwa durch ein Plug-in. Die Installation auf dem Endgerät ist für den Nutzer ausreichend, um das PIMS vollumfänglich zu nutzen, und das PIMS unterliegt der Kontrolle des Nutzers.

Ergänzend könnte der PIMS-Anbieter nach entsprechender Registrierung eine Synchronisation der Einwilligungen über Gerätegrenzen hinweg anbieten.

Dieser lokale Ansatz bietet den Vorteil der Datenminimierung, da der PIMS-Anbieter keine Daten über Nutzer sammeln muss und somit auf eine Authentifizierung verzichten kann (soweit auf die Synchronisation verzichtet wird), da seine Einwilligungen primär an das jeweilige Endgerät gekoppelt sind. Des Weiteren hat eine solche browserbasierte Lösung sowohl technische Vorteile aufgrund der höheren Verfügbarkeit, geringeren Abhängigkeit und einfacheren Implementierung (Stiemerling et al. 2021, Rn. 234) wie auch rechtliche Vorteile aufgrund der besseren Annäherung an Artikel 5 DSGVO (Stiemerling et al. 2021, Rn. 238).

Da eine Plug-in-Lösung auf die auf dem Endgerät gespeicherten Daten zugreifen kann, bietet sie auch den Vorteil, den Nutzer bei der Kontrolle und Modifikation dieser Daten zu unterstützen, etwa im Fall eines Widerrufs einer Einwilligung oder wenn dieses PIMS nicht mehr genutzt werden soll und somit der Widerruf aller Einwilligungen erfolgt.

Neben den oben genannten Vorteilen hat die lokale Lösung aber auch deutliche Nachteile. So ist es erforderlich, auf jedem Endgerät ein entsprechendes Plug-in zu installieren, was aber nicht auf jeder Plattform (Browser) möglich ist. Ferner muss

der Anbieter für jede entsprechende Schnittstelle ein Plug-in entwickeln und pflegen. Zudem kann der Nutzer ohne eine implementierte Synchronisationsmöglichkeit seine Einwilligungen nur auf einem Endgerät nutzen und müsste zur Nutzung auf neuen oder geteilten Endgeräten immer zunächst sein Plug-in installieren und alle Einwilligungen erneut entscheiden.

Die wesentlichen Schritte bei Nutzung einer lokalen PIMS-Implementierung sind:

1. Erkennung durch den TMD, dass der Nutzer ein PIMS nutzt
2. TMD stellt Einwilligungsanfrage, ggf. inkl. URL für spätere Anpassungen oder Widerruf der Einwilligung
3. PIMS beantwortet Anfrage, bei Bedarf nach Rückfrage beim Nutzer
4. TMD verarbeitet die Antwort, legt sie für die weitere Anwendung in einem Sitzungs-Cookie ab, und antwortet mit einem Redirect
5. Der Redirect veranlasst den Browser, erneut die ursprüngliche Seite anzufordern, diesmal jedoch mit dem gesetzten Cookie

Ein Beispiel für ein derartiges lokales PIMS auf Basis eines Plug-ins ist Advanced Data Protection Control (ADPC), welches u. a. von der österreichischen Datenschutz-Initiative NOYB propagiert wird und bisher als Prototyp vorliegt (siehe https://www.dataprotectioncontrol.org/). ADPC ist relativ flexibel und erlaubt beispielsweise den TMD, die Einwilligungsabfragen frei zu formulieren, was natürlich wie angesprochen die Standardisierung erschwert.

5.3 Serverseitige Implementierung

Alternativ kann ein PIMS auch als eigener serverseitiger TMD realisiert werden, bei dem Nutzer sich über das Internet anmelden. Die Kommunikation mit den TMD erfolgt über übliche Webstandards.

Ein Vorteil eines serverseitigen Ansatzes ist, dass die im PIMS erfassten Einwilligungen für alle Geräte des Nutzers gelten können. Zudem bietet die Nutzung von Webstandards den Vorteil, dass der Anpassungsaufwand für verschiedene Endgeräte sehr gering ist, da die Endgeräte die verwendeten Standards zumeist bereits unterstützen.

Nachteilig sind die geringere Verfügbarkeit eines zentralen Dienstes, das aufwendigere Kommunikationsmodell mit drei beteiligten Parteien (Endgerät, PIMS, TMD), sowie das höhere Sicherheitsrisiko, wenn die Daten von allen Nutzern gesammelt auf einem Server gespeichert sind.

Da eine rein webbasierte Lösung nicht direkt auf das Endgerät zugreifen kann, ist es für ein PIMS schwierig, zwischen verschiedenen Endgeräten eines Nutzers zu unterscheiden. Zwar kann ein PIMS nach der Anmeldung selbst mit Cookies oder ähnlichen Technologien zur Identifizierung arbeiten, aber falls dieses Identifizierungsmerkmal verloren gehen sollte (zum Beispiel durch gelöschte Cookies), ist auch die Gerätezuordnung verloren. Auch kann das PIMS nicht auf die auf dem Endgerät gespeicherten Cookies zugreifen, um Nutzer bei der Kontrolle der Einwilligungen zu unterstützen.

Bei einem serverbasierten PIMS muss der TMD zunächst das vom Nutzer verwendete PIMS erkennen. Beim serverbasierten Ansatz ist dies ein nicht triviales Problem mit folgenden Lösungsansätzen:

- Das PIMS stellt zusätzlich ein lokales Plug-in bereit zur Identifikation des PIMS und des Gerätes sowie den Zugriff auf lokale Cookies
- Der Telemediendienst bietet eine Auswahlseite mit den von ihm unterstützten PIMS an.
- Grundsätzlich denkbar aber relativ aufwändig wäre ein zentraler Verzeichnisdienst aller registrierten PIMS-Anbieter, bei dem Nutzer sich mit dem präferierten PIMS registrieren.

Der Ablauf unterscheidet sich gegenüber einer lokalen Implementierung über ein Plug-in im Wesentlichen in folgenden Punkten:

- Zuerst muss der TMD ermitteln, (ob und) welches PIMS der Nutzer einsetzt.
- Falls der Nutzer noch nicht beim PIMS angemeldet ist, muss zum Login umgeleitet werden.
- Die Prüfung der Einwilligungsanforderung ist weitgehend identisch zum lokalen Ansatz mit der Ausnahme, dass dies serverseitig passiert und die eventuell zusätzlich eingeholte Einwilligung/Ablehnung serverseitig gespeichert wird.

Eine alternative Realisierungsmöglichkeit eines serverbasierten PIMS ist eine Beschränkung darauf, die Einwilligungen zu speichern und dem TMD über eine API (Programmierschnittstelle) Lese- und Schreibzugriff auf diese gespeicherten Einwilligungen zu geben. Die Interaktionen zum Einholen dieser Einwilligungen werden in diesem Fall vom TMD geführt, und das PIMS übernimmt nur deren Speicherung. Die Gestaltung des Einwilligungsprozesses muss nicht angepasst werden, sondern es wird lediglich eine zusätzliche Abfrage über die API beim PIMS notwendig, ob und welche Einwilligungen des Nutzers bereits vorliegen, bzw. eine getroffene Entscheidung muss dort abgelegt werden.

Dieser Ansatz wird beispielsweise von netID verfolgt, das von einer von den deutschen Unternehmen Mediengruppe RTL Deutschland, ProSiebenSat.1 und United Internet gegründeten Stiftung bereitgestellt wird (siehe https://developerzone.netid.dev/).

6 Bewertung und Ausblick

Auch wenn das TTDSG mit der Einführung von PIMS zur Einwilligungsverwaltung ein gravierendes Problem des Datenschutzes adressiert, bleibt fraglich, inwieweit dieses Problem mit PIMS wirklich gelöst werden kann. Es bleibt eine Reihe von Herausforderungen aus technischer, rechtlicher und wirtschaftlicher Sicht, für die Lösungen derzeit nicht absehbar sind.

Aus rechtlicher Sicht besteht insbesondere die Herausforderung, dass Einwilligungen u. a. informiert, für den bestimmten Fall und unmissverständlich eingeholt werden müssen. Generelle oder abstrakte Einwilligungen für eine Klasse von Ein-

zelfällen sind damit kaum möglich, obwohl gerade darin der Hauptnutzen einer Einwilligungsverwaltung bestehen könnte.

Die wichtigste technische Herausforderung betrifft die einheitliche Darstellung von Einwilligungsanfragen und deren Beantwortung. Umgekehrt liegt in dieser Vereinheitlichung auch gerade ein weiterer wesentlicher Teil des Nutzens eines PIMS.

Die wohl gravierendsten Herausforderungen liegen aber im wirtschaftlichen Bereich: Die Erfahrungen der Vergangenheit, beispielsweise mit der Do-Not-Track-Einstellung im Browser, haben gezeigt, dass in der Werbewirtschaft wenig Bereitschaft besteht, ohne gesetzlichen Zwang auf Tracking zu verzichten, auch in den Fällen, in denen dies der eindeutig formulierte Wille der Nutzer ist. Dazu kommt, dass PIMS bisher nur in Deutschland rechtlich geregelt sind, und auch hier mit verschiedenen PIMS-Anbietern zu rechnen ist. Alle diese Anbieter zu unterstützen, um eine bislang rein deutsche Regelung umzusetzen und damit den eigenen Werbeertrag zu schmälern, scheint auch bei gutem Willen viel verlangt von den Betreibern der Webpräsenzen bzw. den darin verwendeten Werbenetzwerken.

Insgesamt erscheint es daher unwahrscheinlich, dass sich dieses Konzept in der Breite durchsetzen kann, solange nicht einige Erweiterungen vorgenommen werden:

- Es muss eine rechtliche Verpflichtung für Betreiber geben, die in PIMS festgehaltenen Willensbekundungen zu berücksichtigen. Diese muss für einen wesentlich größeren Rechtsraum als nur Deutschland gelten, beispielsweise für die EU. Entsprechende Diskussionen auf EU-Ebene laufen, allerdings ist aktuell auch hier nicht mit einer verpflichtenden Lösung zu rechnen.
- Aus Sicht der Betreiber muss es eine einheitliche Schnittstelle zur Unterstützung der PIMS geben (oder zumindest eine kleine Anzahl unterschiedlicher Schnittstellen, z. B. je eine für lokale und serverbasierte PIMS).
- Aus Sicht der Nutzer muss ein PIMS die Verwaltung von Einwilligungen gegenüber Cookie-Bannern wesentlich vereinfachen, vor allem indem generische, geräteübergreifende Einwilligungen bzw. Ablehnungen möglich werden (z. B. „ich erlaube für alle besuchten Webpräsenzen und alle meine Geräte statistische Auswertungen meiner Aktionen, aber kein Google Analytics“).

Funding Open Access funding enabled and organized by Projekt DEAL.

Literatur

Bartsch J, Dehling T, Lauf F, Meister S, Sunyaev A (2022) Let the Computer Say NO! The Neglected Potential of Policy Definition Languages for Data Sovereignty. In: Friedewald M, Kreutzer M, Hansen M (Hrsg) Selbstbestimmung, Privatheit und Datenschutz: Gestaltungsoptionen für einen europäischen Weg. Springer Vieweg, Wiesbaden, S 449–468 https://doi.org/10.1007/978-3-658-33306-5_22

DSK (Datenschutzkonferenz) (2022) Orientierungshilfe der Aufsichtsbehörden zur Verarbeitung von personenbezogenen Daten für Zwecke der Direktwerbung unter Geltung der Datenschutz-Grundverordnung (DS-GVO). https://www.datenschutzkonferenz-online.de/media/oh/OH-Werbung_Februar%202022_final.pdf. Zugegriffen: 07.02.2023

EDPS (European Data Protection Supervisor) (2020) Personal Information Management Systems. TechDispatch #3/2020. https://edps.europa.eu/sites/default/files/publication/21-01-06_techdispatch-pims_en_0.pdf. Zugegriffen: 07.02.2023

Friemel C (2020) Zwei Jahre DSGVO: 63 Prozent der Deutschen genervt von Cookie-Hinweisen. 1&1 Mail & Media GmbH. https://newsroom.web.de/2020/05/23/zwei-jahre-dsgvo-63-prozent-der-deutschen-genervt-von-cookie-hinweisen/. Zugegriffen: 07.02.2023

IAB Europe (2022) What Is The Transparency & Consent Framework (TCF)? https://iabeurope.eu/transparency-consent-framework/. Zugegriffen: 07.02.2023

Mayer JR, Mitchell JC (2012) Third-party web tracking: policy and technology. In: 2012 IEEE symposium on security and privacy, S 413–427 https://doi.org/10.1109/SP.2012.47

Salemi S (2022) Chancen und Risiken von PIMS nach § 26 TTDSG. Datenschutz Datensicherh 46:505–510

Stiemerling O, Weiß S, Wendehorst C (2021) Forschungsgutachten zum Einwilligungsmanagement nach § 26 TTDSG. Gesellschaft für Datenschutz und Datensicherheit. https://www.gdd.de/downloads/aktuelles/studien/Gutachten-fuer-Bundesministerium-Wirtschaft-und-Energie.pdf. Zugegriffen: 07.02.2023

Stiftung Datenschutz (2017) Neue Wege bei der Einwilligung im Datenschutz – technische, rechtliche und ökonomische Herausforderungen. Handlungsempfehlungen. https://stiftungdatenschutz.org/praxisthemen/abgeschlossene-projekte/einwilligung-und-pims. Zugegriffen: 07.02.2023