



Munich Personal RePEc Archive

Identifying Challenges in the Use of Cookie Banners and Privacy Policies in Websites and Applications

Gündoğan, Ennis

FOM Hochschule für Oekonomie Management Düsseldorf,
Deutschland

26 October 2024

Online at <https://mpra.ub.uni-muenchen.de/123255/>
MPRA Paper No. 123255, posted 25 Jan 2025 01:56 UTC

Identifizierung von Herausforderungen beim Einsatz von Cookie-Bannern und Datenschutzerklärungen auf Webseiten und in Anwendungen

Ennis Gündoğan 
FOM Hochschule für Oekonomie & Management
Düsseldorf, Deutschland
ennis.guendogan@fom-net.de

26. Oktober 2024

Zusammenfassung Mittels der im Rahmen dieser Arbeit durchgeführten quantitativen Befragung wird verifiziert, dass Komponenten wie Cookie-Banner und Datenschutzerklärungen in Webseiten und Anwendungen während der Nutzung des jeweiligen Onlinedienstes als Störfaktor wahrgenommen werden. Zudem liest die Mehrheit der befragten Personen die Datenschutzerklärung eines Dienstes nicht, um Informationen über verwendete Cookies zu erhalten. Nach einer Unterteilung der technisch nicht notwendigen Cookies in neun Cookie-Typen werden mithilfe der Befragung zusätzliche cookierelevante Erfahrungswerte eingeholt. Die Befragten nehmen Cookie-Daten vom Typ ‚Kartendienst‘ am häufigsten an, während sie Tracking-Cookies am häufigsten ablehnen. Weiterhin lehnt die Mehrheit der Befragten die Übertragung von Cookie-Daten an Systeme in Drittländer ab. Die Übertragung von Cookie-Daten an Systeme in Deutschland und in der EU findet gemäß der Befragung eine größere Akzeptanz.

Von diesen Evaluierungen ausgehend lässt sich schließen, dass bisherige Methoden wie Cookie-Banner und Datenschutzerklärungen auf Webseiten und in Anwendungen nachgebessert werden müssen. Für die Erstellung von Telemediendiensten sind Unternehmen konkrete Hilfswerkzeuge wie Textgeneratoren anzubieten, die die rechtskonforme Erstellung cookierelevanter Informationen unterstützen.

Schlüsselwörter Cookies · Cookie-Einwilligung · Datenschutz · Onlinedienste · EU-DSGVO

Identifying Challenges in the Use of Cookie Banners and Privacy Policies in Websites and Applications

Abstract The quantitative survey conducted as part of this work verifies that components such as cookie banners and privacy policies on websites and applications are perceived as distracting when using the respective online services. Moreover, most respondents do not read the privacy policy of a service to obtain information about the cookies being used. The survey also seeks to gather additional cookie-related empirical data by subdividing technically unnecessary cookies into nine different types. Respondents most frequently accept cookie data of the “map services” type, while they most often reject tracking cookies. Furthermore, most respondents are opposed to the transfer of cookie data to systems outside the EU. However, the survey indicates that the transfer of cookie data to systems within Germany and the EU is more widely accepted.

Based on these evaluations, it can be concluded that existing methods, such as cookie banners and privacy policies on websites and applications, need to be improved. Companies should be provided with specific tools, such as text generators, to assist in creating legally compliant cookie-related information for online services.

Keywords Cookies · Cookie consent · Data privacy protection · Online services · EU GDPR

1 Einleitung

Der Gesetzgeber reglementiert u. a. den Umgang mit personenbezogenen Daten im europäischen Raum bspw. durch die Datenschutz-Grundverordnung der Europäischen Union (EU-DSGVO). Ein wesentlicher Bestandteil dieser Verordnung ist, dass personenbezogene Daten auf einem Endgerät nur nach ausdrücklicher Einwilligung des Nutzers gespeichert oder ausgelesen werden dürfen (Europäisches Parlament 2016). Im Bereich der Onlinedienste und Anwendungen führte dies zum Einsatz

neuer Komponenten, z. B. eines Cookie-Banners und einer Datenschutzerklärung. Zum einen wird durch dieses Verfahren versucht, den Anwender auf bedeutende datenschutzrelevante Informationen mithilfe einer Datenschutzerklärung aufmerksam zu machen. Zum anderen dienen diese Komponenten dazu, das Selbstbestimmungsrecht bezüglich der Verarbeitung personenbezogener Informationen des Anwenders durch Einwilligungsmechanismen wie ein Cookie-Banner zu gewährleisten. Trotzdem werden diese Komponenten während der Nutzung des jeweiligen Dienstes als Störfaktor wahrgenommen (Heine und Wessel 2021; Jakobi et al. 2020). In einigen Fällen werden Cookie-Banner mithilfe von Browser-Plug-ins gänzlich geblockt. Ausgehend von diesen Annahmen soll im Rahmen dieser Arbeit folgende Forschungsfrage (FF) beantwortet werden: Wie werden Cookie-Banner und Cookies im Allgemeinen von Anwendern empfunden? Die Beantwortung dieser Fragestellung ist für die Identifizierung eventueller Hindernisse, die sich negativ auf das Onlinenutzererlebnis auswirken, und für die Ausarbeitung von Handlungsempfehlungen, die die Nutzung von Onlinediensten in Hinblick auf den Cookie-Einwilligungsprozess optimieren, relevant.

2 Theoretische Grundlagen

2.1 Rechtliche Entwicklung

Zu den zum Schutz elektronischer Daten beitragenden ersten Schritten zählt die Annahme der EU-Datenschutzrichtlinie 95/46/EG am 24. Oktober 1995. Mittels dieser Richtlinie sind u. a. die Erhebung und die Verarbeitung sensibler personenbezogener Daten nicht nur nachvollziehbar, sondern auch ausschließlich limitiert erlaubt (Europäisches Parlament 1995). Die EU-Datenschutzrichtlinie 2002/58/EG vom 12. Juli 2002, auch ePrivacy-Richtlinie (ePR) genannt, geht nach Rn. 25 konkret auf Cookies ein. Sie besagt u. a., dass der Anwender über die Platzierung von Cookie-Daten gemeinsam mit dem Nutzungsgrund unterrichtet und den Anwendern die Möglichkeit der Ablehnung von Cookie-Daten geboten werden muss (Europäisches Parlament 2002). Diese Richtlinie wurde durch die Richtlinie 2009/136/EG vom 25. November 2009 ergänzt (Europäisches Parlament 2009). Es wurde konkretisiert, dass nach Art. 5 Abs. 3 der Richtlinie 2009/136/EG die Speicherung und die Auslesung von Cookie-Daten bzw. „Informationen [...] nur gestattet [sind], wenn der betreffende [...] Nutzer [...] seine Einwilligung gegeben hat“ (Europäisches Parlament 2009). Nach dieser Richtlinie ist für das Speichern und das Auslesen von Cookie-Daten eine konkrete Einwilligung vonseiten des Anwenders vorausgesetzt (Opt-in-Verfahren). Dies gilt jedoch nach Rn. 66 nicht für Cookies, deren „technische Speicherung oder [deren] Zugriff unverzichtbar [ist], um die Nutzung eines vom Teilnehmer oder Nutzer ausdrücklich angeforderten Dienstes zu ermöglichen“ (Europäisches Parlament 2009). Auch Cookie-Daten, deren „alleinige[r] Zweck die [...] Übertragung einer Nachricht über ein elektronisches Kommunikationsnetz ist“ (Europäisches Parlament 2002), bedürfen keiner gesonderten Einwilligung.

Nach der Umsetzung der EU-Datenschutzrichtlinie 2009/136/EG in nationales Recht sind die Speicherung und die Auslesung von Cookie-Daten nach § 15 Abs. 3 Telemediengesetz (TMG) erlaubt, „sofern der Nutzer dem nicht widerspricht“ (Bundesministerium der Justiz 2021a). Demnach wird nach dem TMG die Cookie-Verarbeitung so lange gewährleistet, bis ein Widerspruch vonseiten des Anwenders erfolgt (Opt-out-Verfahren). Während somit auf der einen Seite die EU-Richtlinie eine Einwilligung (sog. Opt-in) für die Cookie-Verwendung voraussetzt, erlaubt das TMG auf der anderen Seite die Cookie-Verwendung im Vorhinein, mit der Bedingung, dem Anwender einen Widerspruch (sog. Opt-out) zu ermöglichen.

Nach jahrelangen Diskussionen über die Umsetzbarkeit der Richtlinien und der Reformvorschläge wurde die bis dahin gültige EU-Datenschutzrichtlinie durch die EU-DSGVO vom 27. April 2016 mit einer zweijährigen Übergangszeit abgelöst (EDPS 2018). Durch diese seit dem 25. Mai 2018 geltende Verordnung (Amt für Veröffentlichungen der Europäischen Union 2018) und aufgrund der Präzedenz der europaweiten EU-DSGVO gegenüber dem nationalen TMG (RDV Online 2018) dürfen personenbezogene Daten nach Art. 6 Abs. 1 lit. a EU-DSGVO nur dann verarbeitet werden, wenn „die betroffene Person [...] ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten [...] gegeben“ (Europäisches Parlament 2016; sog. Opt-in) hat. Diese Regelung ist bis heute die wesentliche Rechtsnorm bezüglich des Speicherns und des Auslesens von Informationen – darunter Cookie-Daten – auf Endgeräten (LDI NRW 2022).

Die rechtlichen Bestimmungen für die elektronische Kommunikation im europäischen Raum wurden mit der Richtlinie (EU) 2018/1972 vom 11. Dezember 2018, auch bekannt als Europäischer Kodex für die elektronische Kommunikation (EKEK; Europäisches Parlament 2018), modernisiert. Diese Richtlinie wurde vom deutschen Gesetzgeber bei der Umsetzung ins nationale Recht als Gelegenheit genutzt, die Vorschriften des Telekommunikationsgesetzes (TKG) sowie des TMG zu überarbeiten und in ein neues Gesetz, das Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG) vom 23. Juni 2021 (Bundesministerium der Justiz 2021b), zu bündeln. Das TKG sowie das TMG bestehen zwar weiterhin, die Regelung der Datenschutzvorschriften erfolgt jedoch im neueren TTDSG, das am 1. Dezember 2021 in Kraft getreten ist (LfD Niedersachsen 2021; LDI NRW 2022).

Eine weitere Ergänzung zur EU-DSGVO in Deutschland ist das seit dem 25. Mai 2018 geltende Bundesdatenschutzgesetz-neu (BDSG-neu; LfD Niedersachsen 2024).

2.2 Cookies

Mit dem Begriff ‚Cookies‘ werden kleine Textdateien bezeichnet, die im Browser entweder temporär oder permanent gespeichert werden. Diese ermöglichen die Nutzung eines Telemediendienstes (TMD) bzw. einer Webseite oder beeinflussen sie funktionell (Calzavara et al. 2019; Verbraucherportal-BW 2023). Ferner ermöglichen sie in der alltäglichen Internetnutzung essenzielle Schlüsselfunktionen wie das Zwischenspeichern eines Onlinewarenkorbs oder die Geräteauthentifizierung für einen Onlinedienst (Oppenheimer 2006). Neben essenziellen Funktionen gewährleisten Cookies auch Funktionen, die für den Betrieb einer Webseite nicht zwingend notwendig sind, sondern z. B. für Analyse- und Marketingzwecke genutzt werden können (IONOS SE 2022).

Im Allgemeinen kann zwischen den folgenden beiden Cookie-Typen (CT) unterschieden werden:

- CT1: essenzielle bzw. funktionelle Cookies, die für den Betrieb einer Webseite technisch notwendig sind und grundlegende Funktionen wie einen Onlinewarenkorb, Log-in-Status oder eine Sprachauswahl ermöglichen oder lediglich für elektronische Kommunikationszwecke wie Live-Chat- und Messenger-Systeme genutzt werden (Salewski 2019). Für die Verarbeitung derartiger Cookies wird nach § 25 Abs. 2 TTDSG keine Einwilligung vonseiten des Anwenders benötigt (BMJ 2021).
- CT2: nicht essenzielle Cookies, die für den Betrieb einer Webseite technisch nicht notwendig sind und z. B. für die Erfassung und die Auswertung sonstiger Anwenderdaten erstellt werden (Bohlender et al. 2023). Diese Cookies können in die neun Unterkategorien Tracking-, Analyse-, Affiliate-, Remarketing-, Retargeting-, Skalierbare-zentrale-Messverfahren (SZM)-, Social-Media-, Multimedia- und Kartendienst-Cookies eingeteilt werden (IONOS SE 2022; Salewski 2019; INFOnline GmbH 2023). Nach Art. 6 Abs. 1 lit. a EU-DSGVO sowie § 25 Abs. 1 TTDSG dürfen derartige Cookies nur dann verarbeitet werden, wenn eine Einwilligung vonseiten des Anwenders erfolgt ist (Europäisches Parlament 2016; BMJ 2021).

3 Forschungsmethodik

Im Rahmen dieser Arbeit wurde eine quantitative Befragung durchgeführt, mittels derer die aktuelle Beeinträchtigung, die Cookie-Banner auf das Onlinenutzungserlebnis von Anwendern haben, mithilfe von 19 Fragen (Abb. 1) ermittelt wird sowie diverse weitere cookierelevante Erfahrungswerte eingeholt werden, um die FF dieser Arbeit zu beantworten. Einige der Fragen konnten mit einer fünfstufigen Likertskala bewertet werden, während andere Fragen mit diversen Auswahloptionen beantwortet werden konnten. Das Interview wurde mit einem Onlinewerkzeug erstellt und am 10. Juli 2023 über soziale Netzwerke, in Umfrageportalen sowie im eigenen akademischen, beruflichen und privaten Umfeld veröffentlicht. Die Umfrage endete am 6. Oktober 2023. Insgesamt begannen 362 Personen die Umfrage. Nach Ausschluss aller unvollständigen Antworten beträgt die Stichprobengröße der Onlinebefragung $n = 306$. Davon gehören 118 Teilnehmende der Altersgruppe 18 bis 24 Jahre, 84 Teilnehmende der Altersgruppe 25 bis 29 Jahre, 66 Teilnehmende der Altersgruppe 30 bis 39 Jahre, 24 Teilnehmende der Altersgruppe 40 bis 49 Jahre, fünf Teilnehmende der Altersgruppe 50 bis 59 Jahre und zwei Teilnehmende der Altersgruppe 60 Jahre und älter an. Sieben Teilnehmende machten keine Angaben zum Alter. 169 Befragte sind weiblich, 126 männlich, zwei divers und neun Befragte gaben keine Informationen zum Geschlecht an. Mit 297 Personen stammen annähernd alle Befragten aus Deutschland. Die Ergebnisse der Studie fließen in die jeweils relevanten Stellen der vorliegenden Arbeit ein.

4 Ergebnisse der Studie

Obwohl mittels Cookie-Banner versucht wird, den Anwender auf bedeutende datenschutzrelevante Informationen aufmerksam zu machen und das Selbstbestimmungsrecht über die Verarbeitung personenbezogener Informationen des Anwenders zu gewährleisten, werden die Banner während Webseitenbesuchen als Störfaktor wahrgenommen. Verifiziert wird diese These durch die im Rahmen der vorliegenden Arbeit durchgeführte quantitative Befragung. Auf die damit korrespondierende Umfragefrage UF1 antworteten 32 % mit ‚negativ‘ und 39 % mit ‚negativ bis neutral‘ (Abb. 1).

Somit werden insgesamt 71 % der befragten Personen von Cookie-Bannern während der alltäglichen Internetnutzung negativ beeinflusst. Dieses Ergebnis spiegelt das Resultat der Umfrage des Bitkom e. V. aus dem Jahr 2020 wider, in der 43 % der Befragten die Aussage ‚Cookie-Hinweise nerven mich‘ bestätigten (Bitkom 2020). Ferner blockieren 24 % der befragten Personen Cookie-Banner z. B. mithilfe von Browser-Plug-ins gänzlich (UF5). In Anbetracht der Tatsache, dass mittels der

Identifizierung von Herausforderungen beim Einsatz von Cookie-Bannern und Datenschutzerklärungen auf Webseiten und in Anwendungen

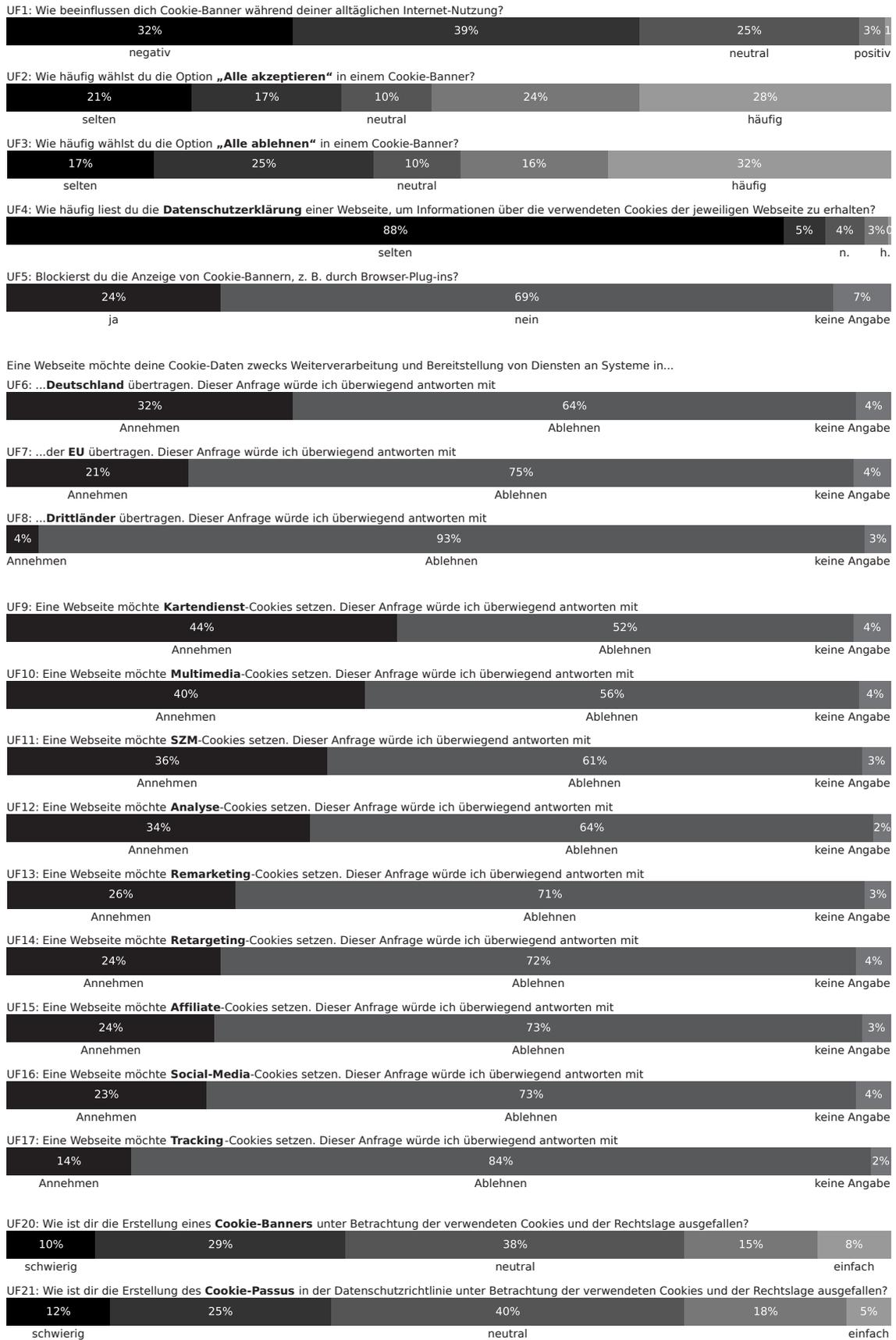


Abbildung 1: Ergebnisse der quantitativen Befragung dieser Arbeit

Cookie-Banner ein für die Anwender bedeutendes datenschutzrelevantes Ziel verfolgt wird, ist dies ein negatives Gesamtergebnis. Die zugrunde liegende Herausforderung ist demnach, die Einwilligung der Datenverarbeitung u. a. von Cookies vom Anwender so einzuholen, dass das Onlinenutzererlebnis nicht negativ beeinflusst wird. Weiterhin wird mittels der Befragung die These verifiziert, dass Anwender die Datenschutzerklärung einer Webseite nicht lesen, um Informationen über die verwendeten Cookies der jeweiligen Webseite zu erhalten. 88 % der befragten Personen beantworteten die mit dieser These korrespondierende Frage mit ‚selten‘ (UF4).

Mit zwei Fragen wurde ermittelt, welche der beiden Auswahloptionen ‚Alle akzeptieren‘ (UF2) und ‚Alle ablehnen‘ (UF3) in einem Cookie-Banner die Befragten präferieren. Mithilfe der Antworten wurde die Auswahlhäufigkeit beider Auswahloptionen miteinander verglichen. Nach einer Gewichtung der Antwortmöglichkeiten ‚selten‘ bis ‚häufig‘ mit den Werten 1 bis 5 konnten die arithmetischen Mittel der Resultate beider Fragen ermittelt und absteigend sortiert werden. Die Befragten neigen geringfügig eher dazu, die Option ‚Alle ablehnen‘ ($x_1 \approx 3,225$) auszuwählen, als die Option ‚Alle akzeptieren‘ ($x_2 \approx 3,216$) zu nutzen.

Neben den in Abb. 1 dargestellten Resultaten dient die quantitative Befragung u. a. dazu, weiterführende empirische Antworten zu cookierelevanten Fragen einzuholen. Dazu wurde die allgemeine Einstellung der Befragten gegenüber der in Abschnitt 2.2 aufgelisteten als CT2 kategorisierten neun Cookie-Typen eingeholt (UF9–17). Zunächst wurden die Datentypen ‚Annehmen‘, ‚Ablehnen‘ und ‚Keine Angabe‘ in die Werte 1, 2 und 0 konvertiert. Im Anschluss wurden die arithmetischen Mittel aller neun Antworten auf die Frage, ob der Anwender eher annehmen oder eher ablehnen würden, wenn Cookie-Daten von Typ x gesetzt werden dürfen, ermittelt und absteigend sortiert. Anhand der Werte kann geschlussfolgert werden, dass Anwender Cookie-Daten vom Typ ‚Kartendienst‘ mit $y_1 \approx 1,474$ am häufigsten annehmen würden, gefolgt von Multimedia- ($y_2 \approx 1,523$) sowie SZM-Cookies ($y_3 \approx 1,572$). Cookie-Daten vom Typ ‚Tracking‘ werden von der Mehrheit der Befragten mit $y_9 \approx 1,814$ am häufigsten abgelehnt, gefolgt von Affiliate- ($y_8 \approx 1,699$) sowie Social-Media-Cookies ($y_7 \approx 1,696$). Mithilfe dreier Fragen (UF6–8) wurde die allgemeine Einstellung von Anwendern gegenüber Übertragungen von Cookie-Daten in die Regionen Deutschland, die EU und unsichere Drittländer nach EU-DSGVO mit der Befragung eingeholt. Mit diesen Fragen sollten die Thesen geprüft werden, dass *a*) Anwender die Übertragung von Cookie-Daten eher in bundesweite Systeme präferieren als in Systeme mit Niederlassung in einem anderen EU-Land und *b*) Anwender grundsätzlich die Übertragung von Cookie-Daten in unsichere Drittländer gemäß EU-DSGVO ablehnen. Anhand der Antworten, dass 64 % bzw. 75 % der Befragten eher dazu neigen, die Übertragung von Cookie-Daten zwecks Weiterverarbeitung und Bereitstellung von Diensten an Systeme in Deutschland bzw. in der EU abzulehnen, lässt sich die obige These *a* nicht eindeutig verifizieren. Allerdings kann die obige These *b* eindeutig verifiziert werden, da 93 % der Befragten die Übertragung von Cookie-Daten zwecks Weiterverarbeitung und Bereitstellung von Diensten an Systeme in Drittländer eher ablehnen würden.

In Bezug auf die Erstellung von Webseiten wurden im Rahmen der vorliegenden Arbeit die folgenden Thesen aufgestellt: Personen, die bereits eine Webseite erstellt haben, fällt es schwer, ein Cookie-Banner sowie einen Cookie-Passus in der Datenschutzrichtlinie unter Berücksichtigung der auf der jeweiligen Webseite verwendeten Cookies und der aktuellen Rechtslage zu erstellen. Für die Überprüfung dieser These war es zunächst notwendig, diejenigen Personen unter den Befragten zu ermitteln, die bereits eine Webseite erstellt haben. Auf die entsprechende Frage antworteten 60 Personen mit ‚Ja‘. Anschließend konnte jedoch die obige Annahme anhand der weiterführenden Antworten weder eindeutig verifiziert noch falsifiziert werden, da die Mehrheit der Befragten – 38 % bzw. 40 % – diese Fragen (UF20–21) neutral beantworteten. 10 % bzw. 29 % der Befragten finden die Erstellung eines rechtskonformen Cookie-Banners ‚schwierig‘ bzw. ‚schwierig bis neutral‘. 12 % bzw. 25 % antworteten auf die Frage, wie schwierig die Cookie-Passus-Erstellung ausfällt, mit ‚schwierig‘ bzw. ‚schwierig bis neutral‘. Die Gesamtdarstellung aller in diesem Kapitel beschriebenen Antworten wird in Abb. 1 gezeigt.

5 Schlussbetrachtung

Mittels der Resultate der im Rahmen dieser Arbeit durchgeführten quantitativen Befragung wird belegt, dass Cookie-Banner von der Mehrheit der Befragten als Störfaktor wahrgenommen werden und die Mehrheit der Befragten die Datenschutzerklärung einer besuchten Webseite nicht liest. Dabei werden diese Komponenten dazu verwendet, den Anwender auf bedeutende datenschutzrelevante Themen aufmerksam zu machen sowie das Selbstbestimmungsrecht über die Verarbeitung eigener, personenbezogener Informationen zu gewährleisten. Daraus lässt sich schließen, dass bisherige Methoden wie Cookie-Banner und Datenschutzerklärungen auf Webseiten und in Anwendungen nachgebessert werden müssen. Für die Erstellung von TMD, z. B. einer Webseite, sind Anwendern und Unternehmen Hilfswerkzeuge wie Textgeneratoren anzubieten, die die rechtskonforme Erstellung von

cookierelevanten Informationen, z. B. einem in einer Datenschutzrichtlinie befindlichen Cookie-Passus, unterstützen.

Literatur

- [1] Amt für Veröffentlichungen der Europäischen Union (2018) Die Datenschutz-Grundverordnung gilt ab dem 25. Mai 2018 in allen Mitgliedstaaten. <https://eur-lex.europa.eu/content/news/general-data-protection-regulation-GDPR-applies-from-25-May-2018.html>. Zugegriffen: 02. Juni 2023
- [2] Bitkom (2020) Cookie-Banner – Meinung in Deutschland 2020. <https://de.statista.com/statistik/daten/studie/884689/umfrage/meinung-zu-cookies-und-cookie-bannern-auf-webseiten-in-deutschland>. Zugegriffen: 17. Juli 2023
- [3] BMJ (2021) TTDSG – Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei Telemedien
- [4] Bohlender M, Dietmann H, Volkamer M (2023) Cookie-Nutzung nach Inkrafttreten des TTDSG: Zur Datenschutzkonformität des Cookie-Einsatzes auf den meistgenutzten deutschen Websites. *Datenschutz und Datensicherheit* 47:283–288. <https://doi.org/10.1007/s11623-023-1762-4>
- [5] Bundesministerium der Justiz (2021a) Fassung § 15 TMG a.F. bis 01.12.2021 (geändert durch Artikel 3 G. v. 23.06.2021 BGBl. I S. 1982). <https://www.buzer.de/gesetz/7616/al162177-0.htm>. Zugegriffen: 02. Juni 2023
- [6] Bundesministerium der Justiz (2021b) TTDSG – Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei Telemedien
- [7] Calzavara S, Rabitti A, Bugliesi M (2019) Sub-session hijacking on the web: Root causes and prevention. *JCS* 27:233–257. <https://doi.org/10.3233/JCS-181149>
- [8] EDPS (2018) Entwicklungsgeschichte der Datenschutz-Grundverordnung. https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_de. Zugegriffen: 01. Juni 2023
- [9] Europäisches Parlament (1995) Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr
- [10] Europäisches Parlament (2002) 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 (Datenschutzrichtlinie für elektronische Kommunikation)
- [11] Europäisches Parlament (2009) Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz
- [12] Europäisches Parlament (2016) Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)
- [13] Europäisches Parlament (2018) Richtlinie (EU) 2018/1808 des Europäischen Parlaments und des Rates vom 11. Dezember 2018 über den europäischen Kodex für die elektronische Kommunikation (Neufassung)
- [14] Heine M, Wessel D (2021) E-Government und Datensouveränität – Einblicke und Lösungsansätze. *HMD* 58:1081–1091. <https://doi.org/10.1365/s40702-021-00766-4>
- [15] INFOnline GmbH (2023) INFOnline Measurement. <https://www.infonline.de/measurement>. Zugegriffen: 04. Juli 2023
- [16] IONOS SE (2022) Die Umsetzung der EU-Cookie-Richtlinie in Deutschland. <https://www.ionos.de/digitalguide/websites/online-recht/cookie-richtlinie>. Zugegriffen: 01. Juni 2023
- [17] Jakobi T, Balthasar M, Borkowsky M, Schmitt H (2020) Transparenz & Datenschutz: Privacy Icons aus Sicht von UX Professionals. <https://doi.org/10.18420/MUC2020-UP-0384>
- [18] LDI NRW (2022) PIMS, Apps, Cookies & Co – Neues Datenschutzrecht für Telekommunikation und Telemedien. <https://www.lds.nrw.de/pims-apps-cookies-co-neues-datenschutzrecht-fuer-telekommunikation-und-telemedien>. Zugegriffen: 05. Juni 2023

- [19] LfD Niedersachsen (2021) Telekommunikations-Telemediendatenschutz-Gesetz (TTDSG) – Fragen und Antworten. https://lfd.niedersachsen.de/startseite/infothek/faqs_zur_ds_gvo/faq-telekommunikations-telemediendatenschutz-gesetz-ttdsg-206449.html. Zugegriffen: 02. Juni 2023
- [20] LfD Niedersachsen (2024) Bundesrecht. <https://lfd.niedersachsen.de/startseite/datenschutzrecht/bundesdatenschutzgesetz/bundesrecht-56250.html>. Zugegriffen: 18. Juni 2024
- [21] Oppenheimer MS (2006) Internet Cookies: When Is Permission Consent?. Nebraska Law Review 85:383–416
- [22] RDV Online (2018) Verhältnis von DS-GVO und TMG klärungsbedürftig. <https://www.rdv-online.com/news/verhaeltnis-von-ds-gvo-und-tmg-klauerungsbeduerftig>. Zugegriffen: 03. Juni 2023
- [23] Salewski P (2019) Einwilligungspflicht oder nicht? Technisch notwendige und technisch nicht notwendige Cookies im Online-Shop. <https://www.it-recht-kanzlei.de/notwendige-nicht-notwendige-cookies.html>. Zugegriffen: 04. Juli 2023
- [24] Verbraucherportal-BW (2023) Cookies – hilfreich oder gefährlich? https://www.verbraucherportal-bw.de/,Lde/Startseite/Verbraucherschutz/Cookies+_+hilfreich+oder+gefaehrlich_. Zugegriffen: 01. Juni 2023