Masterarbeit

DSGVO-Compliance von alternativen Webtracking Methoden

von:

Moritz Philipp Haaf, BSc.

mm191802

Begutachter:
FH-Prof. Mag. Dr. Tassilo Pellegrini

Zweitbegutachterin:
Mag. (FH) Mag. Dr. Astrid Ebner-Zarl

St. Pölten, am .....30.08.2021.....

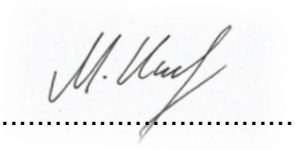
Ehrenwörtliche Erklärung

Ich versichere, dass

- ich diese Masterarbeit selbstständig verfasst, andere als die angegebenen Quellen und Hilfsmittel nicht benutzt und mich auch sonst keiner unerlaubten Hilfe bedient habe.

- ich dieses Masterarbeitsthema bisher weder im Inland noch im Ausland einem Begutachter/einer Begutachterin zur Beurteilung oder in irgendeiner Form als Prüfungsarbeit vorgelegt habe.

Diese Arbeit stimmt mit der vom Begutachter/von der Begutachterin beurteilten Arbeit überein.

Wien, 30.08.2021 

....

Ort, Datum Unterschrift

Danksagung

An dieser Stelle möchte ich mich bei FH-Prof. Mag. Dr. Tassilo Pellegrini für die Betreuung meiner Masterarbeit und die hilfreichen Anregungen und Rückmeldung bedanken, welche eine große Hilfestellung während des Schreibprozesses waren und maßgeblich zum Entstehen dieser Arbeit beigetragen hat.

Außerdem danke ich meinen Studienkolleg*innen, mit denen ich zusammen durch alle Höhen und Tiefen des Studienalltags gegangen bin. Gemeinsam haben wir die nicht immer einfache Zeit, vor allem während der COVID-19-Pandemie, gemeistert und uns gegenseitig unterstützt.

Außerdem möchte ich speziell meiner gesamten Familie für die Unterstützung danken. Hervorzuheben sind hier vor allem mein Vater Hartmut, meine Schwester Leonie und meine Oma Edeltraud, welche alle drei für mich persönlich, vor allem menschlich, große Vorbilder sind und mich in meiner persönlichen Entwicklung stark geprägt haben.

Diese Arbeit widme ich meiner Mutter Gunilla. Ruhe in Frieden!

Kurzfassung

Die Entwicklungen der letzten Jahre rund um das Thema Webtracking sowie die Datenverarbeitung im Internet beschäftigen derzeit zahlreiche Unternehmen. Werbetreibende sind auf Webtracking Technologien angewiesen, um ihr Geschäftsmodell betreiben zu können. Nutzungsdaten spielen dabei eine zentrale Rolle und der Markt rund um personenbezogene Nutzungsdaten boomt. Dabei gilt es eine Vielzahl von Aspekten und Interessensgruppen zu berücksichtigen. Vor allem der Schutz der Privatsphäre der Endnutzer*innen ist ein Kernthema, welches in der Forschung kontrovers diskutiert wird. Darüber hinaus haben sich die rechtlichen Rahmenbedingungen in den vergangen Jahren, unter anderem durch die Einführung der DSGVO, maßgeblich verändert und der Schutz der Privatsphäre wurde verschärft. In dieser Arbeit wurden verschiedene Alternativen zum klassischen Cookie-Tracking mithilfe eines Benchmarkings analysiert. Der Fokus hierbei lag auf der Vereinbarkeit der diversen Technologien mit den gegebenen rechtlichen Rahmenbedingungen. Darüber hinaus wurde auch das Verhalten ausgewählter Datenaggregator*innen untersucht, um gezielte Compliance-Maßnahmen für die Zukunft zu formulieren. Die Ergebnisse der Untersuchung zeigten, dass die Webtracking Methode auf Basis von IDs die beste Lösung, in Bezug auf die Funktionalität für Unternehmen, sowie aus der Datenschutzperspektive auf Nutzer*innenseite, ist. Die Analyse zeigte, dass diese Methode unter Berücksichtigung aller Dimensionen des Benchmarking die beste Kompromisslösung darstellt.

Schlüsselwörter: Alternative Webtracking Methoden, Compliance Management, DSGVO, Privatsphärenschutz, Personenbezogene Daten

Abstract

The developments in recent years around the topic of around the topic of web tracking as well as data processing on the Internet are currently occupying numerous companies. Advertisers are dependent on web tracking technologies to be able to operate their business model. User data plays a central role in this case and the business around data trading is booming. A wide variety of aspects and stakeholders must be considered. Above all, the protection of the privacy of end users is a core issue that is controversially discussed in research. Furthermore, the legal framework has changed significantly with the DSGVO, among other things, and privacy protection has been tightened. This paper analyzed different alternatives to the classic cookie tracking and classified them by means of benchmarking regarding their compatibility with the given legal framework. In addition, the behavior of selected data aggregators was examined to formulate targeted compliance measures for the future. The result of the analysis was that the webtracking solution based on IDs might be the best in terms of functionality for companies and privacy protection for users. Further, it could be shown that this method is the most balanced one considering all dimensions of the benchmarking.

Keywords: alternative webtracking methods, compliance management, GDPR, privacy, personal data

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

A/S	Aktieselskab (Rechtform f. Aktiengesellschaft in Dänemark)
Anm.	Anmerkung
API	Application Programming Interface (Programmierschnittstelle)
App	Applikation/Anwendung
BVDW	Bundesverband Digitale Wirtschaft
CCPA	California Consumer Privacy Act
CMP	Consent Management Platform
div	Container-Element HTML
DNS	Domain Name System
DOM	Document Object Model
DPV	Data Privacy Vocabularies
DSGVO	Datenschutz-Grundverordnung
EDPS	European Data Protection Supervisor
ePVO	ePrivacy Verordnung
FLOC	Federated Learning of Cohorts
EUGH	Europäischer Gerichtshof
GDPR	General Data Protection Regulation = DSGVO
HTML	Hypertext Markup Language
HSTS	HTTP Strict Transport Security
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IAB	Interactive Advertising Bureau
ID	Identifikation (-snummer)
Inc.	Incorporated (Unternehmens-Rechtsform)
IT	Informationstechnologie
LLC	Limited Liability Company (Unternehmens-Rechtsform)
ODRL	Open Digital Rights Language

SKOS	Simple Knowledge Organisation System
TCP	Transmission Control Protocol
URL	Uniform Resource Locator

1 Einleitung

Aufgrund der jüngsten Urteile des EuGHs und der Einführung der DSGVO sowie der geplanten Einführung der ePrivacy Verordnung und dem Markteinfluss von großen Internetkonzernen wie Google, steht das klassische Webtracking mit Cookies vor dem Aus. Beim Webtracking handelt es sich um eine Technologie, die bei öffentlichen Dienstleister*innen im Internet zum Einsatz kommt, um die Interaktionen der User*innen zu erfassen. Durch die verschärften Datenschutzbestimmungen stehen Publisher*innen (Websitebetreiber*innen, Anm. d. Autors) und Werbetreibende vor enormen Herausforderungen, um ihr Geschäftsmodell weiterhin bedienen zu können (vgl. Jakobi et al., 2019, S. 311; Geradin & Katsifis, 2020, S. 1-16).

1.1 Problemstellung und Relevanz des Themas

Die jüngsten Entwicklungen im Zusammenhang mit Cookie Tracking und deren korrekte Verwendung beschäftigt viele Unternehmen bereits vor und insbesondere seit der Einführung der DSGVO im Jahr 2018 (vgl. Aydin & Lehrmann, 2019, S. 3). Die ersten Konsequenzen sind bereits eingetreten. So gab es in jüngster Vergangenheit bereits vereinzelt Fälle, bei denen Unternehmen hohe Strafzahlungen aufgrund von Datenschutzverstößen leisten oder Umsatzeinbußen einstecken mussten (vgl. Possekel & Schiemann, 2020, S. 52-53). Durch die Reformen in der Rechtsprechung bezüglich des Datenschutzes ist auch in der Forschung ein Trend erkennbar, bei dem vermehrt nach Alternativen zum klassischen Cookie Tracking gesucht wird. Hierbei werden verschiedenste Technologien und Methoden untersucht, die es zum einen Websitenbetreiber*innen ermöglichen sollen, ein Nutzerprofil anhand der erhobenen Nutzungsdaten zu erstellen, aber gleichzeitig auch den neuesten Datenschutzbestimmungen entsprechen. Der Fokus der Forschung liegt aktuell darauf, welche Trackingmethoden momentan eingesetzt werden und ob diese rechtskonform im Zusammenhang mit der Datenschutzreform sind (vgl. Solomos et al. 2019, S. 2 ff). Genau an diesem Punkt soll diese Arbeit anknüpfen und die unterschiedlichen Technologien miteinander in Vergleich gesetzt werden, um geeignete Möglichkeiten für die Praxis herauszuarbeiten.

Der Verfasser dieser Arbeit ist der Ansicht, dass gerade aufgrund der Aktualität der Problematik die verschiedenen Methoden des Cookieless Trackings bislang in der Praxis erst wenig erprobt sind, da sich der Großteil der Publisher*innen und Werbetreibenden im Online-Marketing noch inmitten des Transformationsprozesses weg vom klassischen Cookie Tracking befindet. Diese Arbeit hat daher zum Ziel, diverse alternative Trackingmethoden zu untersuchen und diese unter Berücksichtigung der gegebenen Rahmenbedingungen im Rechtsraum der Europäischen Union zu evaluieren. Durch ein geeignetes Compliance Management Konzept soll Websitebetreiber*innen dabei geholfen werden, beim Einsatz von Tracking Tools die Datenschutzbestimmungen einzuhalten.

1.2 Zielsetzung und Aufbau der Arbeit

Diese Arbeit hat grundlegend zum Ziel, die unterschiedlichen Möglichkeiten des Cookieless Trackings zu analysieren und deren Vereinbarkeit mit der DSGVO zu untersuchen. Dadurch sollen geeignete Alternativen herausgearbeitet werden, die das klassische Cookie Tracking in der Zukunft ablösen könnten.
Die **zentrale Forschungsfrage** dieser Arbeit lautet daher:

„Inwieweit sind alternative Methoden des Webtrackings mit der DSGVO zu vereinbaren?“

Zudem wird auch auf das Compliance Management von Websitebetreiber*innen eingegangen und die Frage aufgeworfen, wie Compliance Regeln auf technischem Wege eingehalten werden können. Darüber hinaus soll das Verhalten von großen Datenaggregator*innen bzw. Vendor*innen im Hinblick auf dessen Umgang mit der Verarbeitung und dem Sammeln von personenbezogenen Daten untersucht werden.

In dieser Arbeit wird nicht auf alle möglichen Methoden des Webtrackings eingegangen, sondern nur auf die im Vorhinein festgelegten, aus der Sicht des Autors für die Praxis gängigsten Methoden:

- Semantisches Targeting
- Fingerprinting
- Cache-basierte Tracking Methoden
- Sonstige alternative Webtracking Methoden

Die vorliegende Masterarbeit ist wie folgt aufgebaut. Im ersten Schritt erfolgt eine kurze Einführung in die Thematik und die Vorstellung der Problemstellung sowie der Relevanz des Themas. Anschließend wird die Methodik kurz beschrieben. Im Anschluss an die Kurzbeschreibung der empirischen Untersuchung wird auf den aktuellen Forschungsstand des Themas eingegangen und mögliche Forschungslücken aufgezeigt.

Das zweite Kapitel dient zur Begriffsdefinition von Vendor*innen bzw. Datenaggregator*innen. Außerdem wird der Bezug dieser Unternehmen zum Thema Datenschutz von Endnutzer*innen sowie Umgang mit personenbezogenen Daten hergestellt.

Im dritten Kapitel geht es um das Compliance Management von Websitebetreiber*innen. Darauffolgend wird in Kapitel Vier auf die Thematik des Webtrackings näher eingegangen, insbesondere auf das Recht auf Privatsphäre auf Nutzer*innenseite und der Notwendigkeit der Interaktion zwischen Publisher*innen und User*innen.

In Kapitel Fünf wird das Forschungsdesign beschrieben und die Dimensionen für die Benchmarking-Analyse vorgestellt. Im Anschluss werden die Ergebnisse der Untersuchung präsentiert und Handlungsempfehlungen für die Praxis formuliert.

Im sechsten Kapitel folgt eine Diskussion, welche sich mit den Compliance Maßnahmen für Publisher*innen, alternativen Webtracking Methoden sowie dem Schutz der Privatsphäre von User*innen auseinandersetzt sowie auf die anfangs formulierte Forschungsfrage und Unterfragestellungen eingegangen.

In Kapitel Sieben wird dann ein abschließendes Fazit gezogen und Limitationen der Arbeit aufgezeigt sowie ein Forschungsausblick gegeben.

1.3 Kurzbeschreibung der Methodik

Im Rahmen dieser Arbeit wird ein heuristischer Ansatz gewählt. Bei der Heuristik handelt es sich grundsätzlich um ein Problemlösungsverfahren, welches auf wenig Erfahrungswerten beruht und eine Anweisung zur Gewinnung neuer Erkenntnisse bieten soll (vgl. Duden, 2021, o. S.). Die methodische Vorgehensweise lässt sich in zwei Schritte unterteilen. Mittels Desk Research sollen zunächst qualitative Kategorien herausgearbeitet werden, um die verschiedenen Methoden des Webtrackings und die DSGVO zueinander in Beziehung zu stellen. Anschließend werden die unterschiedlichen Tracking Methoden anhand der ausgearbeiteten Kategorien analysiert und mittels einer Likert-Skala gewichtet (Niedrigster Wert „1“ bis Höchster Wert „5“). Diese Gewichtung der Kategorien ermöglicht es, eine Benchmark Analyse durchzuführen und die unterschiedlichen Technologien miteinander sowie mit den relevanten Datenschutzbestimmungen in Relation zu setzen (vgl. Mertins et al., 1995, S. 223-229). Das Forschungsdesign und die Vorgehensweise beim Benchmarking werden in Abschnitt 5.1 ausführlicher vorgestellt.

1.4 Forschungsstand

1.4.1 Auswahl der relevanten Quellen

Mit zunehmender Prävalenz von Webtrackingpraktiken sowie dem Erfassen und Sammeln von User*innendaten rückte auch die Thematik des Privatsphärenschutzes und Datenschutzbestimmungen in den Vordergrund. Grundsätzlich tangiert das Sammeln von Benutzer*innendaten verschiedenste Bereiche und wirft dabei diverse rechtliche Fragestellungen auf. Beispielsweise gilt es meist auch wirtschaftliche und wettbewerbsrelevante Aspekte im Zusammenhang mit dem Datenschutzrecht zu beachten. Dementsprechend gibt es aktuell unterschiedlichste und breitgefächerte Studien zur Thematik des Webtrackings. Die Entwicklung rund um das Gebiet des Cookieless Trackings steht noch in ihren Startlöchern und es herrscht große Unsicherheit in der Praxis, wie sich der Markt entwickeln in den kommenden Jahren entwickeln wird, und welche Transformationsprozesse stattfinden könnten.

Im nachfolgenden Kapitel wird daher versucht, den aktuellen Forschungsstand in Bezug auf alternative Methoden des Webtrackings und den dazugehörigen relevanten Datenschutzbestimmungen sowie geeigneten Compliance-Maßnahmen darzustellen, auf welchem die empirische Untersuchung aufbaut. Begonnen wurde mit der Literaturrecherche im Oktober 2020 und diese wurde bis Juli 2021 ergänzt. Aufgrund der Aktualität des Themas gab es laufend kleinere Änderungen, die zu berücksichtigen waren. Dies spiegelte sich auch in den aktuellen Forschungsbeiträgen wider. Die ausgewählten Publikationen im Forschungsstand basieren auf folgenden Kriterien:

- Publikationen in akademischen Journalen mit Peer-Review sowie Whitepaper von Fachexpert*innen und verlässlichen Online-Quellen aus der Branche
- Sprache: Englisch und Deutsch

- Literaturdatenbanken, hauptsächlich:
    - IEEE
    - ACM
    - Springer Link
    - Sagepub
    - Science Direct
    - Nomos eBooks complete
    - Google Scholar
- Aufgrund der speziellen Thematik und der Aktualität wurden zudem folgende Publikationsformate ohne Peer-Review ebenfalls als forschungsrelevant angesehen:
    - Facheinschlägige und branchenspezifische Onlinequellen wie z. B. https://iabeurope.eu/ oder https://github.com
    - Whitepaper von ausgewählten Fachverbänden bzw. Fachexpert*innen

Die Literaturrecherche wurde hauptsächlich mit sorgfältig ausgewählten Keywords oder Phrasen, welche folgende Wörter enthalten, sowohl in englischer als auch in deutscher Sprache, durchgeführt.

Verwendete Keywords - Literaturrecherche	
Webtracking	DSGVO/GDPR
Alternative Webtracking Methoden	Compliance Management
Tracking Technologien	Consent Management
Cookieless Tracking	Cookie Tracking

Tabelle 1: Eigene Darstellung - Keywords für die Literaturrecherche

Bei der Suche nach geeigneter Literatur wurde speziell darauf Acht gegeben, dass Synonyme der ausgewählten Keywords einbezogen werden, um möglichst gute Ergebnisse zu erhalten. Außerdem ist darauf Wert gelegt worden, dass die

verwendeten Artikel in akademischen Fachzeitschriften veröffentlicht sowie überwiegend einem Peer-Review unterzogen wurden.

Die Recherche hat gezeigt, dass ein Großteil der relevanten Fachbeiträgen für diese Arbeit erst kürzlich veröffentlicht wurden. Dies könnte auf die Aktualität und Relevanz des Themas zurückzuführen sein.

1.4.2 Abbildung aktueller Forschungsstand und Forschungslücke

Da das Themengebiet breit gefächert ist, werden in diesem Abschnitt, die aus der Sicht des Autors relevantesten Werke aufgelistet, welche den Forschungsstand nach der vorangegangenen Literaturrecherche bestmöglich abbilden. Die Vorgehensweisen der einzelnen Studien werden kurz beschrieben, sowie deren Kernaussagen zusammengefasst und miteinander verglichen.

Jakobi et al. (2019) widmen sich in ihrer Untersuchung den Datensammelpraktiken der 100 beliebtesten Websiten in den Staaten der Europäischen Union laut dem Alexa Top Sites Ranking (vgl. Alexa Ranking, 2021, o. S.). In ihrer Studie weisen sie zum einen auf den bestehenden Interessenskonflikt zwischen Endnutzer*in und Websitebetreiber*in hin. Demnach gibt es vor allem drei große Streitpunkte im Zusammenhang mit der Regulierung beim Umgang mit personenbezogenen Daten im Internet. Erstens spielt die Frage nach Art und Umfang der zulässigen Verarbeitung von Metadaten ohne Einwilligung des bzw. der betroffenen Endnutzer*in zu wirtschaftlichen Zwecken der jeweiligen Anbieter*innen eine große Rolle (vgl. Jakobi et al., 2019, S. 312). Unter Metadaten werden im Allgemeinen strukturierte Daten verstanden, welche übergreifende Informationen über eine Ressource beinhalten und beispielsweise bei Suchmaschinen zur Anwendung kommen (vgl. Ryte, 2021, o. S.). Zweitens gibt es Unklarheiten über die Ausgestaltung der Vorgaben zum Einsatz von Cookies und Trackern auf Endgeräten oder dem Zugriff auf im Endgerät vorhandene Informationen. Drittens ist der Anwendungsbereich der ePrivacy Verordnung als Spezialgesetzgebung und dessen Abgrenzung zur DSGVO noch nicht eindeutig geklärt (vgl. Jakobi et al., 2019, S. 312). Außerdem zeigen Jakobi et al. (2019) in ihrer Fallstudie auf, dass auch nach der Einführung der DSGVO, Methoden des Webtrackings immer noch allgegenwertig sind und

häufig personenbezogene Daten weiterverarbeitet werden, auch ohne den oder die Nutzer*in darauf ausreichend aufmerksam zu machen (vgl. Jakobi et al., 2019, S. 312-318). Zum selben Ergebnis wie Jakobi et al. (2019) kommt auch Agogo (2020) in seiner Studie. Agogo (2020) macht deutlich, dass der Markt mit personenbezogenen Daten trotz der sich stetig ändernden rechtlichen Rahmenbedingungen robust scheint und es vielmehr darum geht, hinter den Schleier der Geheimhaltung zu blicken, der diesen Markt umgibt. In zukünftiger Forschung gelte es vor allem ein besseres Verständnis im Zusammenhang mit dieser Art von Daten zu schaffen (vgl. Agogo, 2020, S. 15-16).

Hils et al. (2020) kommen in ihrer Studie zu dem Schluss, dass durch die Verschärfungen der rechtlichen Rahmenbedingungen für Datenschutz ein Trend bei Unternehmen erkennbar ist, bei dem vermehrt auf sogenannte Consent-Management-Plattformen (CMPs) zur Verwaltung von personenbezogenen Daten zurückgegriffen wird. Mit der Verwendung von CMPs versuchen Unternehmen ein Consent-Ökosystem zu etablieren, welches dabei unterstützen soll, eine Rechtsgrundlage für Geschäftsmodelle zu schaffen, welche auf der Vermarktung von persönlichen Daten basieren (vgl. Hils et al., 2020, S. 326-328). Die Einführung neuer Datenschutzgesetze wie die DSGVO oder der CCPA (California Consumer Privacy Act) waren wichtige Treiber für die Akzeptanz von CMP-Lösungen, woraus man schließen kann, dass es bei diesen Compliance Maßnahmen mehr um die Einhaltung von Gesetzen als um eine Verbesserung der User*innen Experience für den oder die Endnutzer*in geht (vgl. Hils et al., 2020, S. 323).

Esteves und Rodríguez-Doncel (2021) haben sich in ihrer Forschung der Frage gewidmet, wie Compliance Regeln auf technischem Wege eingehalten werden können. Hierzu geben sie einen Überblick über bestehendes Vokabular, Ontologien und Policy-Sprachen, die zur Darstellung von Informationen verwendet werden können, welche auf Rechte und Pflichten der DSGVO verweisen (Esteves & Rodríguez-Doncel, 2021, S. 1-20). Insgesamt wurden 57 verschiedene Informationselemente beschrieben, welche in der DSGVO vorkommen. Zwölf datenschutzbezogene Policysprachen und Neun Datenschutzvokabulare sowie -ontologien wurden in Bezug auf die erstellte Überblicksliste von Informationspunkten untersucht. Dabei konnte gezeigt werden, dass sich die ODRL

(Open Digital Rights Language) als jene Sprache hervorhebt, welche die meisten Rechte und Pflichten in der DSGVO darstellen kann, sofern sie mit DPV (Data Privacy Vocabularies) und GDPRtEXT ergänzt wird (vgl. ebd., 2021, S. 1). GDPRtEXT dient zur Offenlegung des GDPR-Textes als verlinkte Datenressource sowie zur Erstellung eines SKOS-Vokabulars relevanter GDPR-Begriffe und -Konzepte (vgl. w3c, 2021, o. S.). In der Analyse geht hervor, dass bei GDPRtEXT 39 der 57 betrachteten Informationspunkte modelliert werden konnten. Außerdem sticht GDPRtEXT durch das Angebot von zusätzlichen Features (Merkmalen) heraus, wie beispielsweise durch eine einfache Suchanwendung sowie durch eine Taxonomie der identifizierten Einheiten (vgl. ebd., 2021, S. 1). Esteves und Rodríguez-Doncel (2021) kommen in Ihrer Analyse zum Entschluss, dass aktuell nach wie vor noch ein großer Bedarf an Entwicklung von neuen Technologien bestehe, welche Individuen dabei unterstützen sollen, ihre persönlichen Daten zu verwalten. Außerdem müssen diese Technologien in der Lage sein, Unternehmen dabei zu unterstützen, die bestehenden Rechtsvorschriften einzuhalten und ein geeignetes Compliance Management zu betreiben. Ein einheitliches Vokabular sowie gemeinsame Datenmodelle, um auf Datenschutzrechte hinzuweisen, würde die Interoperabilität zwischen verschiedenen Technologien und Tools sowohl aus der Seite des oder der Einzelne*n als auch auf Seite der Unternehmen erleichtern. ODRL, DPV und GDPRtEXT stellten sich als ausgereifte Ressourcen heraus, welche für die Darstellung datenschutzbezogener Rechte und Pflichten im Zusammenhang mit der DSGVO in der Praxis verwendet werden können (Esteves & Rodríguez-Doncel, 2021, S. 19-20).

Ähnlich wie Jakobi et al. (2019) haben Dabrowski et al. (2019) in ihrer Forschung die beliebtesten Websites nach dem Alexa Top Sites Ranking analysiert und das Verhalten der Cookies beobachtet. Sie konnten zeigen, dass es auch geografische Unterschiede im Zusammenhang mit dem Einsatz von dauerhaft gesetzten Cookies gibt. So entsteht der Eindruck, dass ein Zwei-Klassen-System im Internet geschaffen wird. Immerhin wurde in der Untersuchung bei 49,3 Prozent der analysierten Websites auf das Setzen von Cookies ohne Zustimmung der User*in verzichtet, wenn es sich um einen bzw. eine EU-Nutzer*in handelte. Insgesamt geht aber aus der Untersuchung hervor, dass die Verwendung von Cookies sinkt, welches

prinzipiell ein gutes Zeichen für die Privatsphäre der Nutzer*innen darstellt (vgl. Dabrowski et al., 2019, S. 258–270).

Bislang lag der Fokus der Forschung in diesem Bereich vor allem auf Vergleichen, wie sich der Umgang mit Cookies vor und nach der Einführung der jüngsten Datenschutzbestimmungen geändert hat. Die Erkenntnisse von Dabrowski et al. (2019) stehen in Einklang mit den Ergebnissen von Jakobi et al. (2019). Beide zeigen auf, dass es nach wie vor große Unterschiede und Unregelmäßigkeiten in Bezug auf das Tracking von personenbezogenen Daten gibt. An diesem Punkt soll diese Arbeit ansetzen, indem ausgewählte diverse Methoden des Cookieless Trackings beschrieben und analysiert werden und deren Übereinstimmung mit der DSGVO bewertet wird. Zudem werden spezifische Compliance Maßnahmen erarbeitet, welche es Unternehmen erleichtern sollen, sich rechtskonform zu verhalten, um User*innen den größtmöglichen Schutz an Privatsphäre zu gewährleisten.

2 Datenaggregator*innen sowie Vendor*innen und deren Rolle beim Verarbeiten von personenbezogenen Daten

Dieses Kapitel dient zur Definition und Abgrenzung von zentralen Begrifflichkeiten, welche für diese Arbeit eine wichtige Rolle spielen: Datenaggregator*innen und Vendor*innen. Ein bedeutendes Unterscheidungsmerkmal ist, ob ein Unternehmen als „Datenverantwortliche*r“ oder als „Datenauftragsverabeiter*in“ im Hinblick auf die DSGVO auftritt. Diese Begriffe werden im Folgenden näher erläutert und ausgewählte Unternehmen im Bereich des Markts mit personenbezogenen Daten kurz beschrieben.

2.1 Datenaggregator*in

Das Wirtschaftslexikon (2021) verwendet für den Begriff Aggregation verschiedene Definitionen. Der Autor dieser Arbeit hat sich dazu entschlossen zwei Begriffserklärungen anzuführen, welche als relevant angesehen werden können.

Definition aus der Wirtschaftstheorie:

„… Zusammenfassung mehrerer Einzelgrößen hinsichtlich eines gleichartigen Merkmals, um Zusammenhänge zu gewinnen … “

Definition aus dem Bereich der Informatik:

„…Verdichtung von Daten. In der Datenmodellierung bedeutet Aggregation, verschiedene miteinander in Beziehung stehende Objekttypen zu einem höheren Objekttyp zusammenzufassen, damit im Folgenden auf den höheren Objekttyp im Ganzen verwiesen werden kann. …“

(Wirtschaftslexikon, 2021, o. S.).

Müller (2019) beschreibt den Ausdruck Datenaggregator*in, als eine Organisation, welche Informationen zum Verhalten der Zielgruppen und zu Interaktionen im Web sammelt (vgl. Müller, 2019, S. 162-163).

Siegert und Brecheis (2017) gehen in ihrem Werk zum Thema Werbung in der Medien- und Informationsgesellschaft auf die Rolle von Datenaggregator*innen ein.

Sie führen an, dass sich diese zu neuen Akteuren im Werbeprozess entwickelt haben. Bedingt durch die Digitalisierung und Algorithmisierung in den vergangenen Jahren seien viele Marktkonstellationen dadurch verändert worden. Daten sammelnde Plattformen, Datenaggregator*innen und Aktionshäuser für Real Time Advertising sind als neue Player ins Spiel gekommen und haben vor allem die Struktur der Werbekommunikation verändert (vgl. Siegert & Brecheis, 2017, S. 133). Siegert und Brecheis (2017) erläutern, dass das Datensammeln und die Jagd nach Big Data (Große Datenmengen in Form von strukturierten und unstrukturierten Daten – Anmerkung des Verfassers) die Diskussionen und das Handeln nahezu aller Akteure im Werbeprozess, als auch außerhalb, beeinflussen würde (vgl. ebd., 2017, S. 194).

2.2 Vendor*in

Das IAB (2021) führt auf ihrer Seite den Begriff „Vendor“ an. Dabei handle es sich um ein Unternehmen, welches an der Bereitstellung digitaler Werbung auf der Website, in der App oder in anderen digitalen Inhalten eines Publishers bzw. einer Publisherin beteiligt sei, sofern dieses Unternehmen nicht selbst als Websitebetreiber*in agiert, und das entweder auf das Gerät eines oder einer Endnutzer*in zugreift oder personenbezogene Daten der User*innen verarbeitet, welche die Inhalte des Publishers bzw. der Publisherin aufrufen und sich an die Richtlinien des IABs gebunden hat. Ein oder eine Vendor*in kann demnach im Rahmen der DSGVO zum einen als Datenverarbeiter*in oder zum anderen auch als Datenverantwortlicher oder -verantwortliche auftreten bzw. sogar beide Funktionen gleichzeitig innehaben (vgl. IAB, 2021, o. S.).

2.3 Begriffserklärung: Datenverantwortliche*r und Datenauftragsverarbeiter*in

Die europäische Kommission (2021) führt auf ihrer Website beide Begriffe an und definiert die Termini wie folgt:

Der oder die Datenverantwortliche*r sei in der Lage über die Zwecke und die Mittel der Verarbeitung personenbezogener Daten selbst zu entscheiden. Wenn ein

Unternehmen oder eine Organisation entscheiden kann, wofür und wie die personenbezogenen Daten verarbeitet werden sollen, wird die Institution als datenverantwortlich eingestuft. Mitarbeiter*innen, welche innerhalb einer Organisation personenbezogene Daten verarbeiten, tun dies, um ihre Aufgabe als Verantwortlicher oder Verantwortliche wahrzunehmen (vgl. Europäische Kommission, 2021, o. S.). Zusätzlich führt die Europäische Kommission (2021) und die Art-29-Datenschutzgruppe (2010) an, dass Unternehmen oder Organisationen auch als ein gemeinsam Datenverantwortliche*r bzw. -verantwortliche auftreten können, wenn gemeinsam mit einer oder mehreren Institutionen festlegt werde, wofür und wie die personenbezogenen Daten verarbeitet werden sollen. Dabei gehen diese Einrichtungen eine Vereinbarung ein, in der festgelegt wird, wer von ihnen welche Verpflichtungen gemäß den Vorschriften der DSGVO erfüllt. Wichtig hierbei sei, dass den beteiligten Personen, deren Daten verarbeitet werden, die wesentlichen Punkte der Vereinbarung mitgeteilt werden müssen (vgl. ebd., 2020, o. S.; Art-29-Datenschutzgruppe, 2010, S. 4).

Ein bzw. eine Auftragsverarbeiter*in oder -verarbeiterin hingegen verarbeitet ausschließlich im Auftrag des oder der Verantwortlichen personenbezogene Daten. Zudem erläutert die Europäische Komission (2021) sowie die Art-29-Datenschutzgruppe (2010), dass der oder die Auftragsverarbeiter*in in der Regel ein*e Dritte*r außerhalb des Unternehmens sei. Bei Unternehmensgruppen könne jedoch ein Unternehmen als Auftragsverarbeiter für ein anderes fungieren. Die Pflichten des oder der Auftragsverarbeiter*in gegenüber dem Verantwortlichen werden in einem Vertrag oder sonstigen Rechtsakt festgehalten. Der Vertrag müsse unter anderem Aussage darüber geben, was mit den personenbezogenen Daten geschieht, sobald er ausgelaufen ist. Die Haupttätigkeit von Auftragsverarbeiter*innen stellt das Bereitstellen von IT-Lösungen einschließlich der Speicherung von Daten und Informationen in einer Cloud dar (vgl. ebd., 2021, o. S.; Art-29-Datenschutzgruppe, 2010, S. 4).

2.4 Führende Unternehmen im Bereich der Datenaggregation

Nachfolgend werden die vom Autor für diese Arbeit ausgewählten und als wichtig erachteten Unternehmen, welche im Feld der Datenaggregation tätig sind, kurz beschrieben sowie auf deren Umgang in Bezug auf die Verarbeitung von personenbezogenen Daten eingegangen.

2.4.1 Google

2.4.1.1 Unternehmenskurzbeschreibung – Google LLC

Das Unternehmen Google LLC wurde 1998 gegründet und hat seinen Hauptsitz in Kalifornien (USA). Bekannt ist das Unternehmen hauptsächlich aufgrund der hauseigenen Suchmaschine. Neben diesem Service hat sich der Konzern auf das Anbieten von diversen Webanwendungen sowie auf den Vertrieb von Soft- und Hardware spezialisiert. Gerade diese Service-Vielfalt macht Google letztlich zu einem der wertvollsten Unternehmen weltweit, mit einem Markenwert von rund 324 Milliarden US-Dollar (Stand 2020). Seit der Gründung einer neuen Muttergesellschaft (Alphabet Inc.) gehört Google mit Calico, Waymo und einigen weiteren Unternehmen zu diesem Konzern. Den Hauptumsatz erzielt Google durch Werbung. 2020 sind etwa 94 Prozent des Gesamtumsatzes von Alphabet auf Google LLC zurückzuführen. Die größten Anteile wurden hierbei durch Google Sites und Google Network Member's Websites generiert. Insgesamt setzte das Unternehmen rund 123,8 Milliarden US-Dollar über Google Sites geschaltene Werbung um (vgl. Statista, 2021, o. S.).

2.4.1.2 Umgang mit personenbezogenen Daten – Google

Google (2021) führt in ihren Programmrichtlinien für den Ad Manager und Ad Exchange an, dass man für die hauseigenen Publisher-Produkte als Datenauftragsverantwortliche*r agiere, da regelmäßig Entscheidungen über die Daten getroffen werden, um die Produkte zur Verfügung stellen zu können und laufend zu verbessern. Informationen über User*innen-Interessen werden zur

gezielten Ansprache von Nutzer*innen verwendet (vgl. Google, 2021, o. S.). Google (2021) argumentiert, dass diese Daten zum Vorteil verschiedener Beteiligten verwendet werden und man sich somit als Datenverantwortlicher/e und nicht als Datenauftragsverarbeiter*in positioniere. Außerdem wird angeführt, dass Publisher, welche die Dienste von Google in Anspruch nehmen, sich an die Richtlinie zur EU-Nutzereinwilligung zu halten haben. Diese besagt, dass Endnutzer*innen im Europäischen Wirtschaftsraum sowie im Vereinigten Königreich bestimmte Informationen mitgeteilt und auch die Einwilligungen der End-User*innen zur Verwendung ihrer Daten eingeholt werden müssen. Beispielsweise müssen Publisher*innen gewährleisten, dass eine rechtswirksame Einwilligung der Endnutzer*innen für folgende Aktivitäten eingeholt wird:

- Einsatz von Cookies oder anderer Formen der lokalen Speicherung von Informationen, soweit die Einholung einer Einwilligung hierfür gesetzliche vorgeschrieben ist,
- Erhebung, Weitergabe und Nutzung von personenbezogenen Daten zur Personalisierung von Werbeanzeigen

(vgl. Google, 2021, o. S.).

Darüber hinaus merkt Google (2021) an, dass man sich als Publisher dazu verpflichtet, wenn die Einwilligung eingeholt wird, Aufzeichnungen über die von den End-User*innen abgegebenen Einwilligungen aufzubewahren und eine klare Anleitung zur Verfügung zu stellen, wie die abgegebene Einwilligung wieder widerrufen werden kann (vgl. ebd., 2021, o. S.).

Das Unternehmen Google erhebt, wie bereits erwähnt, auch selbst Daten, welche von den Nutzer*innen erfasst werden, die die Services von Google nutzen. In ihren Datenschutzerklärungen verkauft Google dieses Datensammeln mit dem Zweck zur Verbesserung ihrer Produkte und zur Steigerung der Nutzungsfreundlichkeit. Folgende Aufzählungsliste gibt einen Überblick, welche Art von Informationen hierbei von den User*innen abgegriffen werden:

- Daten über Geräteart, Apps und Browser
- Aktivitäten (bspw. Suchbegriffe, Kaufaktivitäten und Seitenaufrufe, etc.)

- Standortdaten (GPS, IP-Adresse, Sensordaten vom Endgerät, WLAN-Zugriffspunkte, Bluetoothfähige Geräte in der Nähe, Funkmasten, etc.)

Außerdem schreibt Google in seinen Datenschutzerklärungen, dass in manchen Fällen auch Daten über Endnutzer*innen aus öffentlich zugänglichen Quellen erhoben werden würden. Als Beispiel wird erwähnt, wenn ein Name eines bzw. einer User*in einer lokalen Zeitung erscheint (vgl. Google, 2021a, o. S.; Google, 2021b).

2.4.2 Facebook

2.4.2.1 Unternehmenskurzbeschreibung – Facebook Inc.

Bei Facebook Inc. ist handelt es sich um ein US-amerikanisches Unternehmen mit Hauptsitz in Kalifornien. Weltweit betrachtet besitzt Facebook 17 Datenzentren und Standorte in mehr als 80 Städten, welche rund um den Globus in unterschiedlichen Städten angesiedelt sind (vgl. Facebook, 2021, o. S.). Im Jahr 2020 konnte das Unternehmen einen Gesamtumsatz von rund 86 Milliarden US-Dollar erzielen. Ähnlich wie bei Google stammt auch hier der Großteil aus Werbeeinnahmen (ca. 84,2 Milliarden US-Dollar). Die Wachstumsrate von Facebook ist beachtlich. Während im Jahr 2010 nur rund 2100 Mitarbeiter*innen beim Unternehmen beschäftigt waren und der Jahresüberschuss bei 606 Millionen US-Dollar lag, wuchs die Beschäftigung bis zum Jahr 2020 kontinuierlich auf 58.604 Mitarbeiter*innen an. Zudem konnte 2020 ein Jahresüberschuss von 29,15 Milliarden US-Dollar erzielt werden (vgl. Facebook, 2021a, S. 1-12).

2.4.2.2 Umgang mit personenbezogenen Daten – Facebook

In den Datenschutzbestimmungen von Facebook wird angeführt, dass je nach Situation das Unternehmen die Rolle des oder der Datenverantwortlichen, Auftragsverarbeiters bzw. -verarbeiterin oder beide gleichzeitig einnehmen kann. Abhängig von der Rolle ergeben sich bestimmte Pflichten:

Als Datenverantwortliche*r wird man klassifiziert, wenn man selbst bestimmt, warum und wie personenbezogene Informationen verarbeitet werden. Die DSGVO besagt, dass Datenverantwortliche Compliance-Maßnahmen einrichten müssen, die sicherstellen, dass Art und Zweck der Datenerfassung sowie die Aufbewahrungsdauer der Daten rechtmäßig sind. Zusätzlich muss den betroffenen Personen Zugriff auf die Daten gewährleistet werden.

Facebook (2021) erläutert in seinen Datenschutzbestimmungen, dass ein Unternehmen hingegen unter den Begriff Auftragsverarbeiter*in falle, wenn es personenbezogene Daten im Auftrag eines oder einer Datenverantwortlichen verarbeitet. Die DSGVO schreibt vor, dass Auftragsverarbeiter die Daten auf sichere und rechtmäßige Weise verarbeiten müssen. In den meisten Fällen würde Facebook die Rolle des oder der Datenverantwortlichen einnehmen. Bei bestimmten Anwendungsfällen, wenn Facebook beispielsweise mit Dritten zusammenarbeitet, würde man jedoch als Auftragsverarbeiter*in auftreten (vgl. Facebook, 2021b, o. S.). Facebook (2021) schildert, wenn das Unternehmen Daten im Auftrag eines Werbekunden oder einer Werbekundin verarbeitet, sei Letztere*r dazu verpflichtet, eine angemessene Rechtsgrundlage für die Verarbeitung der Daten zu schaffen (vgl. ebd., 2021b, o. S.).

Folgende Aufzählung gibt wieder einen Überblick über die Arten von Informationen, welche von Facebook erfasst werden:

- Von Benutzer*innen bereitgestellte Informationen wie Inhalte, Kommunikationen und sonstige Informationen
- Netzwerke und Verbindungen (bspw. Personen, Seiten, Konten, Hashtags, Gruppen, Produktinteraktion, Kontaktinformationen vom Endgerät nach Synchronisation oder Import)
- Nutzungsinformationen (Art von Inhalten, Nutzungsdauer, Interaktionen, etc.)
- Durchgeführte Transaktionen
- Aktivitäten anderer und von ihnen über den oder die User*in bereitgestellte Informationen
- Geräteinformationen

- Geräteattribute (Betriebssystem, Browsertyp, App, etc.
- Vorgänge auf dem Gerät (z. B. Mausbewegungen)
- Identifikatoren (z. B. Geräte IDs)
- Gerätesignale (z. B. Bluetooth und WLAN
- Geräteeinstellungen wie GSP-Standort, Kamerazugriff oder Fotos
- Netzwerk- und Verbindungen
- Cookie-Daten von auf dem Endgerät gespeicherten Cookies, einschließlich Cookie-IDs und-Einstellungen
- Informationen von Partner*innen (Werbetreibende, App-Entwickler*innen und -Publisher*innen können die sozialen Plugins, Facebook Login, APIs und SDKs oder auch über das Facebook-Pixel Informationen austauschen) (vgl. Facebook, 2021c, o. S.).

2.4.3 Adform

2.4.3.1 Unternehmenskurzbeschreibung – Adform A/S

Das Unternehmen Adform A/S betreibt eine Plattform für digitale Werbetechnologie, welche speziell auf modernes Marketing ausgelegt ist. Mit der Unternehmenstechnologie „Adform Flow“ bietet das Unternehmen ihren Kunden eine modulare und offene Architektur zum Kampagnenmanagement. Adform (2020) führen auf ihrer Unternehmensseite an, dass Kontrolle und Transparenz über Werbeaktivitäten eine hohe Priorität haben, einschließlich des Eigentums an allen Daten der über die Plattform laufenden Kampagnen der Kunden. Bereits seit 2002 entwickelt Adform Technologien, um die Zusammenarbeit von Menschen und Maschinen zu verbessern und ist seitdem in über 25 Ländern auf der ganzen Welt vertreten. Aktuell sind über 600 Mitarbeiter*innen bei Adform beschäftigt. Das Headquarter ist in Kopenhagen, Dänemark, angesiedelt und weltweit gibt es aktuell 8 Datenzentren (vgl. Adform, 2021, o. S.). Für diese Arbeit konnten keine validen Daten über den Jahresabschluss 2020 ermittelt werden (Anm. d. Autors).

2.4.3.2 Umgang mit personenbezogenen Daten – Adform

Adform (2021) gibt in seiner Datenschutzerklärung Auskunft darüber, welche Informationen durch die Nutzung der Services erzeugt werden und welche Daten von Kund*innen sowie Partner*innen erhoben werden. Für einen Teil dieser Information agiert Adform als Datenverantwortliche*r, für andere Teile verarbeitet Adform im Auftrag der Kund*innen und fällt somit unter den Anwendungsfall der Datenverarbeitung im Sinne der DSGVO. Bei der Datenverarbeitung ist das Unternehmen somit an die Weisungen der Kund*innen gebunden (vgl. Adform, 2021a, o. S.).

Zur Erbringung ihrer Services erhebt und nutzt Adform folgende Informationen:

- Cookie-ID (Lebensdauer 60 Tage nach der letzten Interaktion),
- Mobile-Advertising-ID,
- Partner-ID.

Adform kooperiert zudem mit einer Vielzahl an PartnerInnen wie beispielsweise den Unternehmen Google, Adobe, Oracle, Amazon. Dabei werden pseudonyme Kennungen übertragen. Außerdem werden hierbei Daten über die Interaktion der NutzerInnen mit Werbeanzeigen und digitalen Medien wie Websites oder mobilen Anwendungen ausgetauscht. Beispiele hierfür sind:

- Browsertyp und -einstellungen
- Betriebssystem des Endgeräts
- Informationen über Cookie-IDs sowie anderen Kennungen, welche einem Endgerät zugeordnet werden können
- IP-Adressen
- Informationen über die Interaktion und Aktivität eines oder einer NutzerIn auf Websiten und mobilen Anwendungen
- Standort (Stadt, Region, Postleitzahl) des Endgeräts beim Zugriff auf eine Website

Zudem erhält Adform auch Daten von Dritten, um gezielt und individualisiert Werbung aussteuern zu können. Diese Informationen von Dritten stellt das Unternehmen zur Nutzung im Rahmen der Dienste zur Verfügung. Dabei halte man

sich jedoch strikt an die durch den Dritten auferlegten Berechtigungen und Einschränkungen (vgl. Adform, 2021a, o. S.). Adform (2021) distanziert sich in seiner Datenschutzerklärung klar von der Erhebung von solchen Daten, welche eine Person direkt identifizieren können, wie beispielsweise Namen, Adresse, Telefonnummern, E-Mail-Adressen oder behördliche Kennungen. Außerdem untersuche das Unternehmen stetig die über die Plattform erhobenen Daten aktiv auf Verstöße hin (vgl. ebd., 2021a, o. S.).

2.4.4 Cxense

2.4.4.1 Unternehmenskurzbeschreibung – Cxense ASA

Das Unternehmen Cxense ASA wurde 2010 in Oslo, Norwegen, gegründet und im Jahr 2019 von der Piano Media übernommen. Die Dachorganisation ist das Unternehmen Piano Software. Cxense arbeitet mit anderen bekannten Marken und Unternehmen wie beispielsweise The Wall Street Journal, Penske Media Corporation, Euronews und NBC Universal zusammen. Seit 2014 ist CXense an der Oslo Stock Exchange gelistet. Das Unternehmen hat sich auf die Analyse von Zielgruppendaten und KI-gestützter Echtzeitanalyse spezialisiert. Mithilfe dieser Informationen können Inhaltsempfehlungen sowie ein personalisiertes Nutzungserlebnis geboten werden, welches den Kund*innen von Cxense dabei helfen soll, den digitalen Umsatz zu steigern und ein nachhaltiges digitales Geschäftsmodell aufzubauen (vgl. Cxense, 2021, o. S.). Gleich wie beim Unternehmen Adform konnten keine validen Daten über den Jahresabschluss 2020 ermittelt werden (Anm. d. Autors).

2.4.4.2 Umgang mit personenbezogenen Daten – Cxense

Cxense (2021) schildert in seiner Datenschutzerklärung, dass eine Nutzung der Seite grundsätzlich ohne jegliche Angabe personenbezogener Daten möglich sei. Bei bestimmten Services sei die Verarbeitung von personenbezogenen Daten notwendig. Sensible Daten wie Name, Anschrift, E-Mail-Adressen oder Telefonnummern einer betroffenen Person werden nicht erhoben, es sei denn sie

werden freiwillig zur Verfügung gestellt, beispielsweise im Rahmen einer Newsletter-Anmeldung oder einer Online-Bewerbung. Als Datenverantwortliche*r habe man zahlreiche technische und organisatorische Maßnahmen umgesetzt, um einen möglichst lückenlosen Schutz über der von Cxense verarbeiteten personenbezogenen Daten sicherstellen zu können (vgl. Cxense, 2021a, o. S.). Cxense verwendet zur Datenerfassung Cookies. Mittels Cookie-ID stellt man den Nutzer*innen möglichst benutzerfreundliche Services zur Verfügung, welche ohne die Cookie-Setzung nicht möglich seien (vgl. ebd., 2021a, o. S.). Das Unternehmen weist in der Datenschutzerklärung ausdrücklich auf die Möglichkeit hin, dass man die Setzung dieser Cookies als User*in unterbinden kann und dieser auch dauerhaft widersprechen könne. Ferner wird nochmals genau aufgezeigt, dass User*innen über einen Internetbrowser oder andere Softwareprogramm bereits gesetzte Cookies wieder löschen können. Würden User*innen dies tun, seien hingegen bestimmte Funktionen der Seite nicht mehr vollumfänglich nutzbar (vgl. Cxense, 2021a, o. S.).

Cxense (2021) erfasst mit jedem Seitenaufruf durch eine betroffene Person oder ein automatisiertes System eine Vielzahl von allgemeinen Daten und Informationen, welche in den Logfiles der Server gespeichert werden. Dies sei notwendig, um die Inhalte der Internetseite korrekt auszuliefern, Inhalte und Werbung zu optimieren, die dauerhafte Funktionsfähigkeit der IT-Systeme sowie der Technik gewährleisten zu können und Strafverfolgungsbehörden im Falle eines Cyberangriffes die zur Verfolgung notwendigen Informationen bereitstellen zu können. Bei der Nutzung dieser allgemeinen Daten würden keine Rückschlüsse auf die betroffene Person gezogen werden. Außerdem weist Cxense ausdrücklich darauf hin, dass die anonym erhobenen Informationen einerseits statistisch ausgewertet werden, mit dem Ziel den Datenschutz sowie die Datensicherheit im Unternehmen zu erhöhen, um ein optimales Schutzniveau für die erhobenen personenbezogenen Daten sicherstellen zu können. Die anonymen Daten der Server-Logfiles würden zudem, getrennt von allen personenbezogenen Daten, gespeichert (vgl. ebd., 2021a, o. S.).

3 Compliance Management für Publisher*innen

Im folgenden Kapitel wird auf das Thema Compliance Management für Publisher*innen näher eingegangen. Unter Compliance Management versteht man im Allgemeinen die Ausgestaltung der rechtlichen Verantwortung von Unternehmen (vgl. Kreipl, 2020, S. 130). Compliance umschreibt die Summe aller organisatorischen Maßnahmen eines Unternehmens zur Gewährleistung des rechtmäßigen Verhaltens von der Geschäftsführung hin zu allen Mitarbeiter*innen (vgl. Behringer 2013, S. 35; Vetter 2008, S. 29; Ulrich 2012, S. 216 zitiert nach Kreipl, 2020, S.130-131). Dabei umfasst das Compliance Management vor allem drei Funktionen: Aufklärung, Krisenreaktion und Prävention. Bei der Funktion der Aufklärung geht es vor allem um die Aufdeckung von rechtswidrigen Aktivitäten. Dabei kann die Aufklärungsfunktion eine Signalwirkung für interne sowie externe Täter*innen einnehmen und eine abschreckende Wirkung entfalten (ebd. 2020, S. 133). Die Krisenreaktion kann Unternehmen dabei unterstützen, das Ausmaß von Krisen vor allem einzudämmen und diese möglichst schnell zu überwinden. Eine Krise kann in Form von Skandalen, aber auch als Unfall stattfinden (ebd. 2020, S. 135). Die Aufklärungsfunktion hat zur Aufgabe, Rechtsverstöße möglichst im Vorhinein zu vermeiden. Auch hierbei wird die Signalwirkung ausgesendet, dass ein Fehlverhalten mit großer Wahrscheinlichkeit aufgedeckt wird und der oder die Täter*in Konsequenzen zu tragen haben (ebd. 2020, S. 135-136). Datenschutz-Managementsysteme können Unternehmen dabei unterstützen, sich rechtskonform zu verhalten. Es handelt sich dabei um interne Compliance-Systeme, welche die Erfüllung datenschutz- und sicherheitsbezogener Pflichten überprüfen (vgl. Voigt & von dem Bussche, 2018, S. 6). Ein solches System besteht aus einem IT-Sicherheitskonzept, welches die Umsetzung und Überwachung von Datenverarbeitungstätigkeit umfasst, sowie die Vorgänge auch entsprechend dokumentiert, um die Vorgaben der DSGVO zu erfüllen (vgl. ebd., 2018, S. 42).

3.1 Anwendungsbereich Webtracking und Problematik

Unter Webtracking versteht man im Allgemeinen die Analyse der Nutzung von Internetangeboten (vgl. Fox, 2010, S. 787). Diese Form der Datensammlung dient der Weiterentwicklung und der Gestaltung von Websiten. Fox (2010) führt an, dass Publisher*innen mithilfe von entsprechenden Nutzungsanalysen Einblick über stark bzw. selten frequentierte Seiten erlangen sowie Auskunft erhalten können, wie der oder die User*in auf die jeweilige Websiten gekommen ist (z.B. über eine Suchmaschine, durch direkte Eingabe einer URL oder durch Klick auf ein Werbemittel). Außerdem können diverse Interaktionen erfasst werden, wie lange User*innen auf einer Seite verweilen, wie viele unterschiedliche Seiten aufgerufen werden oder auch an welcher Stelle der Kaufprozess beispielsweise abgebrochen wurde, auch Bounce Rate genannt. Sogar die Herkunft der Besucher*innen lässt sich durch Geolokalisierung der IP-Adresse nachverfolgen. Diese neuen Analyseverfahren ermöglichen außerdem eine Erfolgs- und Reichweitenmessung von Marketingmaßnahmen für Internet-Angebote (vgl. ebd. 2010, S. 787). Schärer (2021) erläutert, dass aufgrund der Verschärfung der rechtlichen Rahmenbedingungen, wie beispielsweise dem Inkrafttreten der DSGVO, das Messen des Nutzungsverhalten auf Websiten zunehmend anspruchsvoller wird. Mit der Einführung der DSGVO sollten die Privacy-Ansprüche der Nutzer*innen gestärkt werden und das Tracking personenbezogener Daten ohne explizite vorhergegangene Einwilligung verboten werden. Außerdem haben bereits diverse Technologieanbieter*innen, wie zum Beispiel Apple, auf das zunehmende Privacy-Bedürfnis reagiert und ihre Software dahingehend angepasst, dass die Analyse des Surfverhaltens von Nutzer*innen für Werbezwecke reduziert wird. Es wird somit immer schwieriger, unterschiedliche Werbemaßnahmen an den effektiven Nutzerbedürfnissen auszurichten (vgl. Schärer, 2021, o. S.). Auch das Unternehmen Google hat Anfang des Jahres 2020 offiziell verkündet, dass man in der Zukunft auf Third Party Cookies verzichten wird (vgl. Geradin & Katsifis, 2020, S. 1). Geradin und Katsifis (2020) erläutern, dass gerade diese Entscheidung einen enormen Einfluss auf das zukünftige Marktgeschehen hat, da Google mit dem hauseigenen Browser Chrome einen Marktanteil von über 64 Prozent erreicht (vgl. ebd., 2020, S. 8; Statcounter, 2021, o. S.). Die Konkurrenz hat bereits Bedenken

aufgeworfen, dass diese Entscheidung die Marktmacht von Google sowie auch Facebook weiter stärken könnte und außerdem ein Verstoß gegen das Wettbewerbsrecht vorliegen könnte. Aktuell herrsche zudem eine große Verunsicherung in der Branche (vgl. ebd. 2020, S. 1-12).

3.2 Rechenschaftspflicht beim Einsatz von Tracking-Tools

Mit der Einführung der DSGVO wurde ein neues Grundprinzip in Art. 5 Abs. 2 DSGVO geschaffen, welches dem oder der Verantwortlichen, im Falle von Websites des Publishers oder der Publisherin, die Verantwortung für die Einhaltung der Vorgaben der DSGVO in Bezug auf die Verarbeitungstätigkeiten auferlegt sowie ihn bzw. sie dazu verpflichtet, die Einhaltung nachzuweisen (vgl. Voigt & von dem Bussche, 2018, S. 40; Art. 5 Abs. 2 DSGVO 119/36). Die Datenschutzgrundverordnung hat somit die rechtlichen Rahmenbedingungen für den Umgang mit personenbezogenen Daten in Unternehmen neu definiert. Demnach müssen Unternehmen nun jederzeit darlegen können, welche personenbezogenen Daten in welchen Systemen für welchen Zweck auf welcher rechtlichen Basis von wem gespeichert und verarbeitet werden. Darüber hinaus muss auch ersichtlich sein, wer diese Daten wie und wofür nutzt. Zudem können Nutzer*innen nun zu jeder Zeit Änderungs-, Widerrufs-, oder Löschungswünsche der erfassten Personendaten äußern, welche das jeweilige Unternehmen umgehend umsetzen muss (vgl. Brockmann, 2018, S. 634). Bei Verstößen gegen die DSGVO können Bußgelder in Höhe von bis zu EUR 20.000.000,- bzw. bis zu 4 Prozent des weltweiten Jahresumsatzes verhängt werden. Die hoch angesetzten Strafen sollen den Druck auf Verantwortliche erhöhen, auch geeignete Datenschutzmaßnahmen zu ergreifen. Um die Einhaltung der rechtlichen Bestimmungen einzuhalten, müssen infolge bestimmte Maßnahmen in Organisationen getroffen werden, wie beispielsweise die Etablierung einer internen Policy sowie die Nutzung skalierbarer Programme zur Umsetzung von Datenschutzprinzipien. Aufgrund ihrer Rechenschaftspflicht müssen Publisher*innen, wie bereits eingangs dieses Abschnittes erwähnt, bei entsprechenden Nachfragen dazu in der Lage sein, gegenüber Aufsichtsbehörden die Einhaltung der Vorgaben der DSGVO nachzuweisen (vgl. Voigt & von dem Bussche, 2018, S. 39-41). Hierzu sind

Verzeichnisse über Verarbeitungstätigkeiten zu führen, welche einerseits eine oberflächliche Einschätzung der Rechtmäßigkeit erlauben, andererseits müssen die jeweiligen Zwecke auf eine Art und Weise dokumentiert werden, die eine derartige Bewertung zulassen (vgl. ebd. 2018, S. 55-56). Nach Voigt und von dem Bussche (2019) der Zweck in den Verzeichnissen nicht zu eng umrissen werden, da dies zu einer Einschränkung des Umfangs der rechtmäßigen Datenverarbeitung führen würde (vgl. Voigt & von dem Bussche, 2019, 154).

Kapitel 3 der DSGVO regelt die Rechte der betroffenen Personen. In den Art. 12 ff geht es um Transparenz und um die Pflicht zur Bereitstellung von Informationen, wenn personenbezogene Daten erhoben werden (vgl. Art. 12 ff. DSGVO 2016/119).

Laut Esteves & Rodríguez-Doncel (2021) müsse eine Reihe an Informationen bereitgestellt werden, damit die Verarbeitung personenbezogener Daten rechtmäßig und fair sowie nach Treu und Glauben und in transparenter Weise erfolge (Esteves & Rodríguez-Doncel, 2021, S. 2-3). Folgende Auflistung gibt einen Überblick, welche Informationen zur Verfügung gestellt werden müssen sowie die passenden gesetzlichen Grundbestimmungen dazu:

- Identität der für die Verarbeitung verantwortlichen Person (Art. 13 Z. 1 a, Art. 14 Z. 1 a, Art. 30 Z. 1 a, Art. 30 Z. 2 a DSGVO)
- Kontaktdaten des für die Verarbeitung verantwortlichen Person bzw. Personen (Art. 13 Z. 1 a, Art. 14 Z. 1 a, Art. 30 Z. 1 a, Art. 30 Z. 2 a DSGVO)
- Identität des Vertreters oder der Vertreterin der für die Verarbeitung verantwortlichen Person (Art. 13 Z. 1 a, Art. 14 Z. 1 a, Art. 30 Z. 1 a, Art. 30 Z. 2 a DSGVO)
- Kontaktdaten des Vertreters oder der Vertreterin der für die Verarbeitung verantwortlichen Person (Art. 13 Z. 1 a, Art. 14 Z. 1 a, Art. 30 Z. 1 a, Art. 30 Z. 2 a DSGVO)
- Kontaktdaten des DSB (Datenschutzbeauftragte*r) (Art. 13 Z. 1 b, Art. 14 Z. 1 b, Art. 30 Z. 1 a, Art. 30 Z. 2 a, Art. 33 Z. 3 b, Art. 34 Z. 2, Art. 36 Z. 3 d DSGVO)
- Zwecke der Verarbeitung (Art. 13 Z. 1 c, Art. 14 Z. 1 c, Art. 15 Z. 1 a, Art. 28 Z. 3, Art. 30 Z. b, Art. 35 Z. 7 a, Art. 36 Z. 3 b DSGVO)

- Rechtsgrundlage der Verarbeitung (Art. 6 Z. 1, Art. 9 Z. 2, Art. 13 Z. 1 c, Art. 14 Z. 1 c DSGVO)
- Berechtigte Interessen (Art. 6 Z. 1, Art. 13 Z. 1 d, Art. 14 Z. 2 b, Art. 35 Z. 7 DSGVO)
- Empfänger*in bzw. Kategorien von Empfänger*innen (Art. 13 Z. 1 e, Art. 14 Z. 1 e, Art. 15 Z. 1 c, Art. 17 Z. 2, Art. 19, Art. 30 Z. 1 d DSGVO)
- Übermittlungen in Drittländer (Art. 13 Z. 1 f, Art. Z. 1 e, Art. 30 Z. 2 c, Art. 46, Art. 47, Art 49 Z 1 DSGVO)
- Aufbewahrungsfrist (Art. 13 Z. 2 a, Art 14 Z. 2 a, Art. Z. 1 d, Art. 30 Z. 1 f DSGVO)
- Rechte der betroffenen Person (Art. 13 Z. 2 b, Art. 14 Z. 2 c, Art. 15 Z. 1 e, Art. 28 DSGVO)
- Recht auf Widerruf der Einwilligung (Art. 6 Z. 1 a, Art. 9 Z. 2 a, Art. 13 Z. 2 c, Art. 14 Z. 2 d DSGVO)
- Recht auf Einreichung einer Beschwerde (Art. 13 Z. 2 d, Art. 14 Z. 2 e, Art. 15 Z. 1 f DSGVO)
- Angaben zu gesetzlichen oder vertraglichen Verpflichtungen (Art. 13 Z. 2 e DSGVO)
- Vorliegen einer automatisierten Entscheidungsfindung (Art. 13 Z. 2 f, Art. 14 Z. 2 g, Art. 15 Z. 1 h, Art. 22 Z. 1, Art. 22 Z. 4 DSGVO)
- Kategorien von personenbezogenen Daten (Art 9 Z. 1, Art. 14 Z. 1 d, Art. 15 Z. 1 b, Art. 28 Z. 3, Art. 30 Z. 1 c, Art. 33 Z. 3 a DSGVO)
- Quelle der personenbezogenen Daten (Art. 14 Z. 2 f, Art. 15 Z. 1 g DSGVO)
- Gründe/Rechtfertigung für die Nichteinhaltung des Auskunftsrechts (Art. 13 Z. 4, Art. 15 Z. 1 g DSGVO)

(vgl. Esteves & Rodríguez-Doncel, 2021, S. 4; DSGVO, 2016/119)

Esteves & Rodríguez-Doncel (2021) haben mit ihrem Forschungsbeitrag versucht, die Rechte und Pflichten der DSGVO als Informationsfluss abzubilden. Die nachfolgende Abbildung 1 stellt den Informationsaustausch zwischen den beteiligten Stakeholdern dar. Während die bidirektionalen Pfeile für ein bestimmtes Recht oder eine Pflicht stehen, bei der eine Anfrage nach Informationen und eine entsprechende Antwort erwartet wird, stellen die unidirektionalen Pfeile nur eine Anfrage oder Meldung dar, bei der keine Antwort erwartet wird (vgl. Esteves & Rodríguez-Doncel, 2021, S. 3).

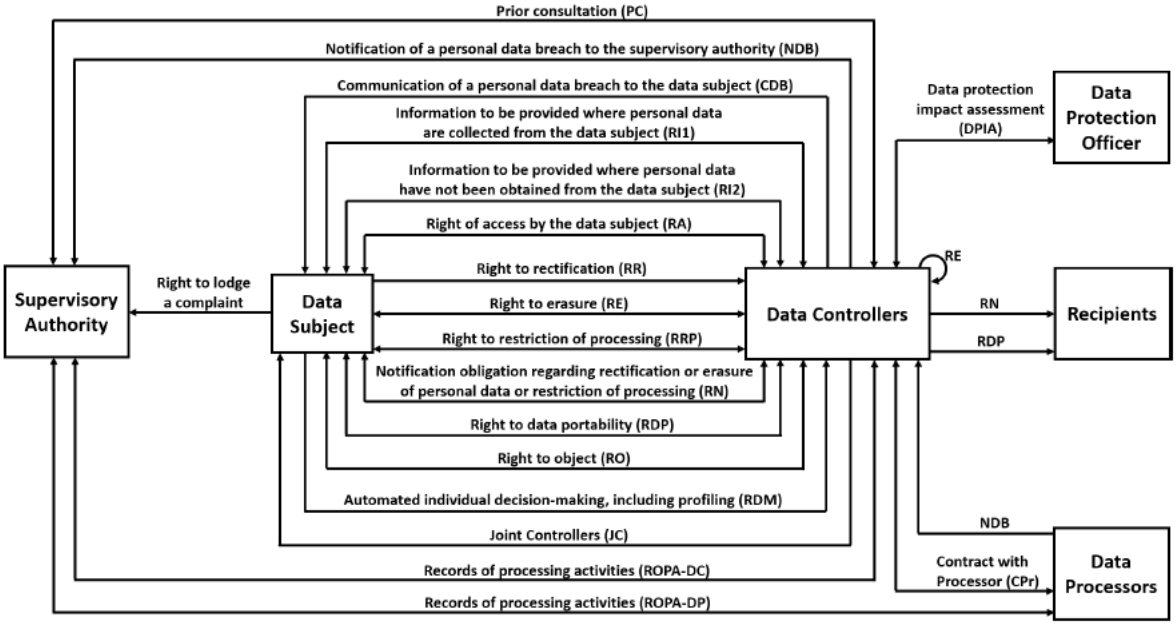


Abbildung 1: Informationsfluss der Rechte und Verpflichtungen der DSGVO (Esteves & Rodríguez-Doncel, 2021, S. 3)

Laut Esteves und Rodríguez-Doncel (2021) bestehe ein großer Bedarf an der Entwicklung von Technologien, welche Unternehmen bzw. Organisationen bei der Verwaltung von personenbezogenen Daten unterstützen, um die Einhaltung der gegebenen Rechtsvorschriften besser einhalten zu können. Außerdem weisen sie daraufhin, dass ein einheitliches Vokabular sowie standardisierte Datenmodelle dabei helfen würden, die Informationsasymmetrie zwischen den Datenverarbeiter*innen und den betroffenen Personen zu verringern. Einwilligungserklärungen können beispielsweise durch diese Technologien wesentlich einfacher eingeholt und verwaltet werden und betroffene Personen hätten die Möglichkeit, den Zugang zu ihren personenbezogenen Daten in verteilten

Speichern zu kontrollieren (vgl. Esteves & Rodríguez-Doncel, 2021, S. 19-20). Die EDPS. (2016) haben diesen letzten Punkt ebenfalls in ihrem Empfehlungsschreiben zum Thema „Personal Information Management Systems (PIMS)“ Unternehmen, welche personenbezogene Nutzungsdaten sammeln und verwalten, nahegelegt (vgl. EDPS, 2016, S. 1-17).

Esteves und Rodríguez-Doncel (2021) kommen in ihrem Forschungsbeitrag zu dem Schluss, dass ODRL, DPV und GDPRtEXT sich als geeignete REL (Rights Expression Language) herausgestellt haben (vgl. Esteves & Rodríguez-Doncel, 2021, S. 19-20). REL steht im Allgemeinen für eine von Maschinen lesbare Sprache, mit der Einzelheiten zu den Bestimmungen für geistiges Eigentum beschrieben werden können. Mithilfe dieser Sprache lassen sich Richtlinien für urheberechtlich geschützte digitale Inhalte erstellen und darstellen (vgl. Schmidt, 2019, o. S.). Die wesentlichen Punkte, welche für ODRL, DPV und GDPRtEXT sprechen, seien zum einen, dass sie frei zugänglich sind, gut dokumentiert und im Falle von ODRL sogar vom W3C für die Verwaltung digitaler Rechte empfohlen wurden (vgl. Esteves & Rodríguez-Doncel, 2021, S. 20).

3.3 Compliance Ziele

Compliance Ziele beschreiben, welche wesentlichen Ziele mit einem Compliance Managementsystem erreicht werden sollen (vgl. Kreipl, 2020, S. 171).

Schneider (2018) erklärt, dass Soll-Ist-Vergleiche im Compliance Management eine wichtige Rolle in der Unternehmensleitung spielen. Diese werden in der Regel auch mit dem Controlling und der Unternehmensleitung diskutiert. Um die Ergebnisse quantifizieren zu können, werden sogenannte Key Performance Indicators (KPIs) herangezogen. Compliance Ziele können sich deutlich von denen der operativen Unternehmensfunktionen wie beispielsweise dem Vertrieb oder Einkauf unterscheiden. Beim Compliance Management werden häufig eine Vielzahl unterschiedlicher Ziele definiert. Die Schaffung einer Compliance Kultur kann im Gegensatz zu anderen Unternehmenszielen nicht eindeutig quantifiziert werden und wird auch keiner unmittelbaren Bewertung und Erfolgskontrolle unterzogen (vgl. Schneider, 2018, S. 46-47). Kreipl (2020) schildert den Nutzen des Compliance Managements, und führt an, dass rechtliche und ökonomische Schäden vermieden werden, wie zum Beispiel Haft- und Geldstrafen oder auch Umsatzeinbußen. Zudem gilt es auch sogenannte vor-ökonomische Schäden, wie einen möglichen Imageverlust, zu vermeiden. Vor allem das Bekanntwerden eines Compliance-Verstoßes kann für ein Unternehmen einen enormen negativen Einfluss auf das Ansehen in der Öffentlichkeit haben, sowie auf die Motivation von Mitarbeiter*innen, Akzeptanz der Produkte im Markt und letztendlich somit auch auf den gesamten Unternehmenserfolg (vgl. Kreipl, 2020, S. 139). Ein effektives Compliance Management sollte nicht nur das Ziel der Schadensminderung verfolgen, sondern vielmehr die Steigerung der Unternehmenseffizienz anstreben, um dadurch den Unternehmenserfolg zu fördern. Die Risikominimierung sollte lediglich als ein Aspekt von guter Corporate Compliance gesehen werden (vgl. ebd. 2020, S. 140).

Erfolgreiche Compliance Systeme zeichnen sich zum einen durch eine Erhöhung der Transparenz aus. Andererseits ist eine frühzeitige Problemerkennung wichtig, da diese ein schnelles Reagieren ermöglicht und somit das Schadensausmaß geringgehalten werden kann. Die Förderung des Vertrauens in die Mitarbeiter*innen spielt auch eine zentrale Rolle. Mit entsprechenden Informationen und Schulungen

kann Vertrauen in das richtige Verhalten von Arbeitgeber*innen sowie Arbeitnehmer*innen aufgebaut werden. Zudem sollte auch die Unternehmensführung vertrauensbasiert erfolgen. Ergänzend zum Vertrauen können aber auch regelmäßige Kontrollen notwendig sein, um beispielsweise die Einhaltung von Trainings zu überprüfen (vgl. Kreipl. 2020, S. 140-141).

3.4 Monitoring und Verbesserung

Bay und Hastenrath (2016) legen dar, dass es verschiedener Maßnahmen bedarf, um ein Compliance System in Unternehmen erfolgreich umsetzen zu können. Mithilfe eines festgelegten Verhaltenskodex kann die Geschäftsführung sicherstellen, dass Integrität, Wertschätzung und Nachhaltigkeit in täglichen Geschäftsprozessen des Unternehmens gelebt werden. Außerdem sei es wichtig, ein gutes Compliance-Risk-Assessment zu etablieren. Das Ausmaß sowie die Eintrittswahrscheinlichkeit eines potenziellen Schadens spielen bei der Bewertung ebenfalls eine wichtige Rolle. Auch sogenannte indirekte Schäden sollten in die Bewertung miteinfließen, wie ein möglicher Reputations- und Vertrauensverlust bei Compliance-Verstößen. Darüber hinaus sind weitere Faktoren, wie die persönliche Haftung oder die Miteinbeziehungspflicht der Ermittlungsbehörden, zu beachten (vgl. Bay & Hastenrath, 2016, S. 139–141). Kreipl (2020) beschreibt, dass Monitoring und Verbesserung im Compliance die Angemessenheit und Wirksamkeit des gesamten Compliance-Systems überwachen. Wichtig sei zudem auch, durch permanente Messung der , eine gewisse Nachhaltigkeit zu gewährleisten (vgl. Kreipl, 2020, S. 172). Heutzutage gilt es für Unternehmen eine Fülle von Compliance-Anforderungen zu erfüllen (vgl. Erwin et al., 2013, S. 60). Erwin et al. (2013) erklärt, dass viele Compliance-Analysen häufig noch manuell durchgeführt werden und aufgrund der hohen Volumina nur stichprobenartig durchgeführt werden können. Mithilfe von automatisierten Compliance-Monitoring-Systemen könne eine umfassendere und verlässlichere Überwachung erfolgen. Zudem fördern diese Systeme effektive und standardisierte Prozesse, sodass sich diese auch positiv auf die Leistungsfähigkeit auswirken (vgl. ebd. 2013, S. 60). Der Monitoring-Prozess kann verschiedene Ausprägungen annehmen – die Formen der Analyse, Nachverfolgung und Vorhersage. Bei der Analyse ist es wichtig,

vordefinierte Kontrollen regelmäßig durchzuführen. Dies hilft auch dabei, zeitnah auf verdächtige Vorfälle reagieren zu können. Die Nachverfolgung erfolgt hierbei nach wie vor manuell. Bei der fortgeschrittenen Methode der Nachverfolgung wird diese auch mittels Workflow-Systems in das automatisierte Verfahren integriert. Dabei werden die identifizierten Compliance Vorfälle automatisch an die relevanten Stellen innerhalb des Unternehmens geleitet, wo die Sachverhalte bewertet werden und gegebenenfalls Maßnahmen zu Schadensbegrenzung eingeleitet werden können (vgl. Erwin et al., 2013, S. 61). Mithilfe von modernen Datenanalysemethoden können heutzutage neben strukturierten Daten auch unstrukturierte Date, wie beispielsweise E-Mails, in die Analyse einbezogen werden, um aussagekräftige Vorhersagen treffen zu können, sowie auch neue Muster mit Risikopotenzial zu identifizieren. Die Nutzung von digitalen Formen der Compliance Richtlinienvermittlung bietet eine effiziente Möglichkeit, lösungsorientierte Handlungsempfehlungen intuitiv darzulegen. Wichtig hierbei ist darauf zu achten, dass eine inhaltliche Vollständigkeit im fachlichen Sinne gewährleistet wird und die Inhalte auch so geliefert werden, dass sie der menschlichen Denkweise entsprechen (vgl. ebd. 2013, S. 61).

4 Webtracking und Legal Compliance

Dieses Kapitel widmet sich dem Thema Webtracking. Außerdem soll die Verbindung von Webtracking und Legal Compliance für Unternehmen verdeutlicht werden. Zu Beginn dieses Abschnittes wird zunächst auf das Webtracking Ökosystem näher eingegangen. Wie bereits in vorhergehenden Abschnitten erwähnt, beherrschen große Unternehmen wie Google, Facebook oder Apple den Markt. Aus Sicht des Autors dieser Arbeit prägen die strategischen Entscheidungen den Markt immens. Auch die Verteilung der weltweiten meistgenutzten Browser spielt eine wichtige Rolle. Anschließend zum Abschnitt über den Browsershare wird auf die rechtlichen Rahmenbedingungen eingegangen. Darüber hinaus wird auf das Recht der Nutzer*innen auf Privatsphäre auf der einen Seite eingegangen und andererseits die Notwendigkeit der Erfassung von Nutzungsdaten für Publisher*innen erläutert. Abschließend werden diverse Anwendungsfelder in Bezug auf Cookietracking erklärt sowie die alternativen Arten des Webtrackings beschrieben.

Täglich surfen Milliarden an Nutzer*innen im Internet und hinterlassen dabei ihre digitalen Spuren auf Millionen von Websites. Praktisch jeder Seitenaufruf, jede Bewegung mit der Computer-Maus und jeder Mausklick löst eine Kette an verstecktem Datenaustausch zwischen diversen Tracking-Unternehmen aus. Davon bekommen die User*innen nur bedingt etwas mit. Zumindest ist das Ausmaß dieses Datenabgriffs wahrscheinlich nur den Wenigsten bewusst. Gerade für Werbetreibende können die Userdaten, speziell Vorlieben und Gewohnheiten der Nutzer*innen äußerst nützlich sein. Diese helfen schließlich dabei, Werbung zielgerichtet auszuliefern. Dies führt in den meisten Fällen auch zu einer höheren Conversion Rate, also beispielsweise zu einer größeren Kaufwahrscheinlichkeit von Kund*innen (vgl. Bielova, 2017, S. 2607). Bielova (2017) führt an, dass gerade dieser Aspekt jedoch sehr besorgniserregend für die Privatsphäre der Nutzer*innen sei. Der einfachste Weg für User*innen sich zumindest vor den meisten Cookie Tracking Methoden zu schützen, bestehe einfach darin, mittels Browser-Konfiguration Third Party Cookies ausdrücklich zu blockieren. Dieses Feature gehört mittlerweile bei vielen Anbieter*innen fast schon zum Standard (vgl. ebd., 2017, S. 2608).

Das Surfen im Privatmodus helfe laut Bielova (2017) nur bedingt im Hinblick auf den Schutz der Privatsphäre. Moderne Browser würden zwar einen gewissen Schutz bieten, aber die Cookies von Drittanbieter*innen werden dadurch nicht deaktiviert (Bielova, 2017, 2608). Weitere Möglichkeiten zum Schutz vor unerwünschten Datenabgriffen stellen Browsererweiterungen, auch Add-ons genannt, dar. Beispiele dafür sind AdBlock Plus, Ghostery, uBlock, Disconnect und Privacy Badger (vgl. ebd., 2017., S. 2609). Laut Bielova (2017) zählten diese aufgezählten Add-ons zu den gängigsten Datenschutzerweiterungen im Jahr 2016. Diese Add-ons würden jedoch keinen vollständigen Schutz bieten, denn wenn ein Tracker sich an eine neue Domain richtet, welche noch nicht vom Algorithmus des Adblocker-Add-ons enthalten ist, wird das Tracking über die bestimmte Domain auch nicht blockiert (vgl. ebd., 2017, S. 2609).

4.1 Webtracking Ökosystem

Wie zu Beginn des Kapitels 4 bereits angeführt, surfen tagtäglich Milliarden an Menschen im World Wide Web. Hierfür können verschiedenste Browser verwendet werden. Im folgenden Abschnitt wird daher auf die Marktverteilung der diversen Browser-Anbieter*innen eingegangen. Jeder Browser hat seine technischen Eigenheiten und Features, somit gibt es durchaus, auch aus Sicht des Autors dieser Arbeit, Unterschiede im Sinne des Privatsphäre-Schutzes. Wie auch Bielova (2017) erläutert, hinterlässt jede*r User*in digitale Spuren beim Surfen, welche in der Browserumgebung erfasst werden (vgl. Bielova, 2017, 2607). Aufgrund dieser Tatsache spielen die verschiedenen Browser und deren Eigenschaften keine unwesentliche Rolle im Hinblick auf den Privatsphärenschutz von Individuen sowie im Zusammenhang mit Legal Compliance für Unternehmen bzw. Publisher*innen.

4.1.1 Browsershare Weltweit

Betrachtet man die Browser-Verteilung weltweit, ist deutlich zu erkennen, dass sich hier einzelne wenige Unternehmen den Markt untereinander aufteilen. Aus Sicht des Autors dieser Arbeit spielt diese Marktkonzentration keine unwesentliche Rolle in Bezug auf die Entwicklung des Webtracking Ökosystems. Die nachfolgende Abbildung 2 zeigt die Verteilung des Browser Shares für den Desktop Bereich weltweit gemessen an den generierten Page Views (Seiten-Aufrufe) im Zeitraum 01. April 2021 bis 30. April 2021. Das Unternehmen Google mit dem hauseigenen Browser Chrome kann im Desktop Bereich einen Anteil von 67,53 Prozent verzeichnen, gemessen an den weltweit generierten Page Views im Zeitraum April 2021. Apple nimmt mit dem Browser Safari Platz Zwei mit einem Anteil von 9,86 Prozent ein, gefolgt von Microsoft Edge mit 7,69 Prozent und Mozilla Firefox mit 7,79 Prozent.

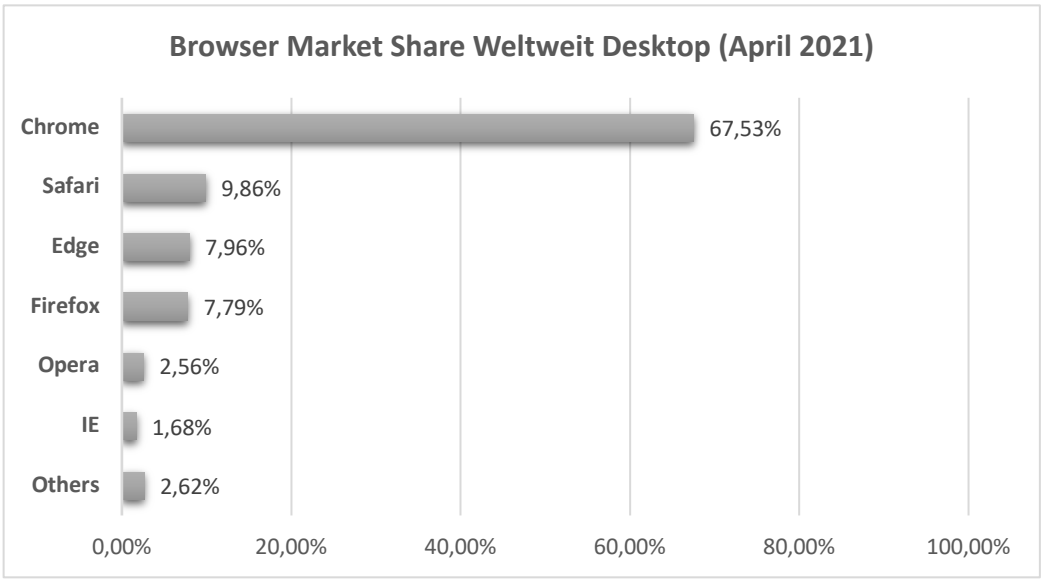


Abbildung 2: Browser Market Share Desktop April 2021 – Eigene Darstellung in Anlehnung an Statcounter. (2021, o. S.).

Auch im Mobile Bereich beherrscht Google mit Chrome den Markt. Abbildung 3 stellt die Browserverteilung für Mobile Devices im Zeitraum April 2021 dar. Hier dominiert Chrome, ähnlich wie bei Desktop, mit einem Anteil von 63,15 Prozent. Apples Safari verzeichnet im Mobile Sektor hingegen einen Anteil von 24,44 Prozent.

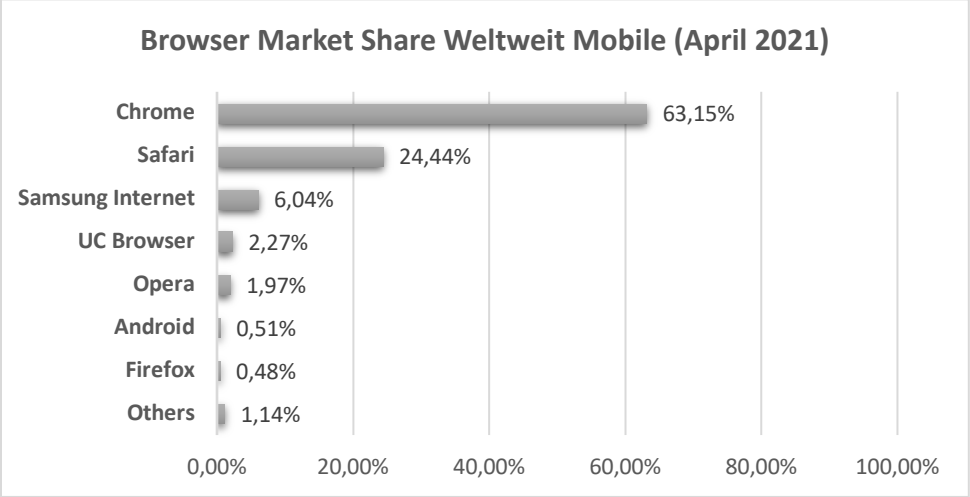


Abbildung 3: Browser Market Share Mobile April 2021 – Eigene Darstellung in Anlehnung an Statcounter. (2021, o. S.).

Diese Vormachtstellung von Google wird in der Praxis sowie auch in der Literatur kritisch betrachtet und diskutiert. Zinndorf (2020) beleuchtet in ihrer Arbeit, dass Google in den Medien bereits als Informationsmonopolist gesehen wird, der das Gleichgewicht der Märkte störe und es zunehmend zu einer Marktkonzentration komme (vgl. FAZ, 2013, o. S. zitiert nach Zinndorf, 2020, S. 27). Speziell Google verfolge eine Strategie, in der die Nachfrage der Nutzer*innen zunehmend durch eigene Dienste befriedigt wird. Die eigenen Dienste werden beispielsweise auf den Ergebnisseiten der Suchmaschine weit vorne und grafisch hervorgehoben angezeigt. Dieses Verhalten führe zu einem Marktmachttransfer, welcher den Leistungswettbewerb aushebeln und verzerren könne (vgl. ebd. 2020, S. 32-33).

4.1.2 Aktuelle Marktmacht von Internetkonzernen wie Google und Facebook

Krämer (2016) führt an, dass in der Digitalwirtschaft viele Geschäftsmodelle auf das Erheben von personenbezogenen Daten abzielen. Diese Daten ermöglichen es den Unternehmen, Werbung zielgerichteter zu platzieren und personalisierte Angebote auszuspielen. Durch den exklusiven Zugang zu einer gigantischen Datenbasis können durchaus Wettbewerbsvorteile und letztlich auch Marktmacht begründet werden. Problematisch in Hinblick auf das Wettbewerbsrecht wird es dann, wenn aufgrund des exklusiven Zugangs zu Nutzungsdaten, eine höhere Interaktion mit User*innen einhergeht und somit die Qualität der Datenbasis schneller verbessert werden kann, als dies für die Konkurrenz möglich ist (vgl. Krämer, 2016, S. 235). Große Internetkonzerne verfügen heutzutage über personelles Know-how, finanzielle Ressourcen und Daten, um gegenseitig im Sinne der Angebotssubstitution Wettbewerbsdruck ausüben zu können. Als Beispiel kann hier der Messenger-Dienst mit Ende-zu-Ende-Verschlüsselung „Threema“ genannt werden. Als im Februar 2014 bekannt wurde, dass WhatsApp von Facebook aufgekauft wird, erlebte der Messenger „Threema“ einen Aufschwung und führte die iTunes-Charts in Deutschland und Österreich kurzfristig an, aufgrund von aufkommenden Datenschutzbedenken bei WhatsApp. Dies veranlasste Facebook vermutlich, WhatsApp noch im selben Jahr ebenfalls mit einer Ende-zu-Ende Verschlüsselung auszustatten (vgl. ebd. 2016, S. 235). Am 14. Januar 2020 hat Google nach monatelangen Spekulationen veröffentlicht, dass das Unternehmen Cookies von Drittanbieter*innen in ihrem Browser Chrome innerhalb der nächsten zwei Jahre auslaufen lässt (vgl. Geradin & Katsifis, 2020, S. 1). Geradin und Katsifis (2020) erläutern, dass diese Nachricht eine Art Schockwelle in der Online-Werbebranche ausgelöst hat, da ein Großteil der digitalen Geschäftsmodelle auf den Einsatz von Web-Cookies aufgebaut ist (vgl. ebd., 2020, S. 1-12). Wie in Abschnitt 4.1.1 dargestellt, beherrscht Google den Markt sowohl im Desktop als auch im Mobile Bereich, aufgrund dessen könnte diese Entscheidung weitreichende Folgen mit sich bringen. Bereits seit dem Jahr 2010 ermittelt die Europäische Kommission gegen das Unternehmen Google mit dem Vorwurf, dass man die marktbeherrschende Stellung missbräuchlich ausnützen würde (vgl.

Hiersche & Mayer, 2017, S. 53). Hiersche und Mayer (2017) untersuchen die verschiedenen Verfahren gegen das Unternehmen im Hinblick auf den Art. 102 AEUV, welcher die Wettbewerbsdiskriminierung regelt (vgl. Art. 102 AEUV 2012/326). Die Vorwürfe, welche gegen Google erhoben werden, sind zum einen die Selbstbevorzugung bei Preisvergleichsdiensten, wie Google Shopping, und die Beschränkung der Möglichkeiten anderer Konkurrenten, Suchmaschinenwerbung auf Websites Dritter zu platzieren. Außerdem wird das Unternehmen beschuldigt, Webinhalte konkurrierender Unternehmen unautorisiert zu kopieren, übermäßige vertragliche Beschränkungen gegenüber werbenden Unternehmen vorzunehmen und Produkte unzulässig exklusiv als Pakete zum Verkauf anzubieten, wie das beispielsweise bei dem Betriebssystem Android von Google der Fall ist. Die Autor*innen stellen dar, dass nicht jedes Verhalten eines Marktbeherrschers bzw. Marktbeherrscherin gleich missbräuchlich sei. Es komme dabei vor allem auf das Geschäftsfeld an, und gerade bei Märkten, welche auf der Verarbeitung von großen Datenmengen basieren und zu diesem Zweck in der Ausweitung der Tätigkeitsfelder in verschiedene Marktgebiete bestehen, könnten die gesetzten Maßnahmen auch als Form von Leistungswettbewerb angesehen werden, welche das Wettbewerbsrecht auch bewahren möchten (vgl. ebd., 2017, S. 53-58). Mit der jüngsten Entscheidung von Google, auf Third Party Cookies zu verzichten, hat das Unternehmen seine neue Technologie FLoC (Federated Learning of Cohorts) vorgestellt. Dabei handelt es sich um eine datenschutzfreundliche API (Programmierschnittstelle), welche innerhalb der Chrome Privacy Sandbox eingesetzt wird, um weiterhin interessenbasierte Werbung zu ermöglichen. Die Technologie basiert auf dem Konzept der Kohorten (Gruppen) von User*innen mit ähnlichen Interessen (vgl. Ravichandran & Vassilvitskii, 2021, S. 1-17). Aufgrund der marktbeherrschenden Rolle von Google wird diese Entscheidung kritisch gesehen, da das Unternehmen damit den Wettbewerb weiter verzerren würde (vgl. Morrison & Molla, 2020, o. S.). Am 27.06.2021 hat das itmagazine auf ihrer Website einen Artikel veröffentlicht, aus welchem hervorgeht, dass Google den geplanten Cookie-Bann, welcher mit der neuen Tracking Technologie FLOC einhergeht, auf das Jahr 2023 hinausschieben werde (vgl. itmagazine, 2021, o. S.).

4.2 Darstellung der rechtlichen Rahmenbedingungen

4.2.1 Grundsätze der Verarbeitung von personenbezogenen Daten

Die DSGVO kommt grundsätzlich zur Anwendung, wenn es sich um einen Personenbezug von Informationen handelt. Eckhardt und Kramer (2013) erläutern, dass die Grenzziehung, wann ein Personenbezug gegeben ist und wann nicht, für die Anwendung daher von entscheidender Bedeutung sei. Beim Aufrufen einer Website hinterlassen User*innen Spuren. Hierzu werden Online-Kennungen wie IP-Adressen oder Cookie-Kennungen zugeordnet, welche ein Gerät oder Software-Anwendungen und -Tools oder Protokolle liefern. Diese Angaben können mit anderen beim Server eingehenden Informationen verbunden werden, um so ein Profil der betroffenen Personen zu erstellen und sie zu identifizieren (vgl. Eckhardt & Kramer, S. 288). Heberlein (2017) merkt an, dass bei datenschutzrechtlichen Sachverhalten verschiedenste grundrechtlich verankerte Interessen immer miteinander abgewogen werden müssen. Diese Abwägung solle einzelfallbezogen erfolgen und sei oftmals zentrales Element bei der Beurteilung der Zulässigkeit der Verarbeitung personenbezogener Daten (vgl. Heberlein, 2017, S. 48).

4.2.2 Auswirkungen der DSGVO auf das Webtracking

Das Datenschutzrecht basiert auf dem Recht der informellen Selbstbestimmung sowie dem Schutz des allgemeinen Persönlichkeitsrechts. Der Hauptzweck dieses Rechtsgebiets dient dem Schutz der Privatsphäre von Individuen (vgl. Schelinski & Feuerhake, 2019, S. 613). Durch die DSGVO wurde das Datenschutzrecht mit dem 25. Mai 2018 europaweit einheitlich geregelt. Laut Schellinski und Feuerhake (2019) habe die Harmonisierung zum Ziel, einerseits dem technischen Wandel einer digitalisierten Welt Rechnung zu tragen und andererseits im Wesentlichen zu einer Angleichung des Datenschutzniveaus innerhalb des europäischen Binnenmarktes zu führen (ebd., 2019, S. 613).

Die DSGVO ist gem. Art. 99 Abs. 2 DSGVO zwei Jahre nach Inkrafttreten gültig anzuwendendes Recht, welches für das Territorium der europäischen Union gilt (vgl. Heberlein, 2017, S. 83; Art. 99 Abs. 2 DSGVO, 2016/119). Heberlein (2017)

erläutert, dass vor allem die jüngste Rechtsprechung des EuGHs eine Art Paradigmenwechsel in der Bestimmung des territorialen Rechts eingeläutet hat. Demnach ist man von einer zuvor überwiegend restriktiven und nicht im Wortlaut angelegten Auslegung des Niederlassungsbegriffs in Art. 4 Abs. 1 DSRL zu einer eher weiten Auslegung desselben übergegangen. Zuvor waren Unternehmen mit ausschließlicher Marketingfunktion wie auch das Unternehmen Facebook nicht als Niederlassung anerkannt und somit war die DSGVO nicht anzuwenden. Seit der DSGVO geht die Rechtsprechung vermehrt vom Marktortprinzip aus. Dieses besagt, dass es für den räumlichen Anwendungsbereich schon ausreiche, wenn im Unionsgebiet Waren oder Dienstleistungen angeboten oder sogar auch nur deren Verhalten beobachtet wird (vgl. ebd. 2017, S. 89-91). Degeling et al. (2020) merken an, dass die europäische Datenschutz-Grundverordnung ursprünglich als Parallele zur ePrivacy-Verordnung angedacht war und daher den Online-Bereich nur am Rand behandelt. Da bislang noch keine Einigung zwischen den Mitgliedsstaaten der europäischen Union erzielt werden konnte, hat sich die Einführung der ePrivacy Verordnung allerdings nach hinten verschoben. Für Nutzer*innen sind die Änderungen seit der Einführung der DSGVO vor allem durch die vermehrten Einverständniserklärungen auf Websiten und in der Online-Kommunikation sichtbar (vgl. Degeling et al., 2020, S. 77). Die Auswirkungen durch die geänderten rechtlichen Rahmenbedingungen auf Online-Werbung wurden mehrfach kritisch diskutiert. In unterschiedlichen Forschungsarbeiten konnte allerdings nachgewiesen werden, dass trotz der DSGVO nicht signifikant weniger Werbeplatzierung auf Websiten die Folge waren. Hingegen konnten eher Werbetreibende mit hohen Marktanteilen ihre Position am Markt festigen oder sogar weiter ausbauen und die Anteile kleinerer Unternehmen sind geringer geworden oder jene Anbieter*innen mussten sich ganz aus dem Wettbewerb zurückziehen (vgl. ebd. 2020, S. 79).

Die DSGVO hat somit zu einer Marktkonzentration geführt. Urban et al. (2020) haben in einer Studie das Ausmaß dieser Marktkonsolidierung und die Reichweite einzelner Trackingdienste anhand von „Cookie Syncing“ untersucht (vgl. Urban et al., 2020, S. 222-235).

Beim Cookie Syncing handelt es sich um eine Methode, bei der zwei oder mehr Werbetreibende Nutzerdaten untereinander austauschen. Mithilfe dieses Datenabgleichs zwischen Unternehmen ist es möglich, eine größere Datenbasis aufzubauen und Algorithmen für Werbeanzeigen zu optimieren (vgl. Papadopoulos et al., 2019, S. 1432-1442). Das Ergebnis der Studie von Urban et al. (2020) konnte zeigen, dass zwar die durchschnittliche Anzahl von Tracker*innen auf einer Website leicht nach Einführung der DSGVO abgenommen hat. Die Praxis des Cookies Syncing ist statistisch signifikant hingegen nicht zurückgegangen (vgl. Urban et al., 2020, S. 230-233).

Abbildung 4 zeigt die Veränderung im Werbenetzwerk nach Einführung der DSGVO. Die einzelnen Knoten stellen die Unternehmen dar und die Kanten die Verbindungen zwischen ihnen. Je größer ein Knoten ist, desto stärker ist er in dem Netzwerk eingebunden. Erkennbar ist, dass sich die grundlegende Struktur des gesamten Netzwerks nicht verändert hat. Das Unternehmen Google ist beispielsweise nach wie vor der wichtigste Datenumschlagsplatz.

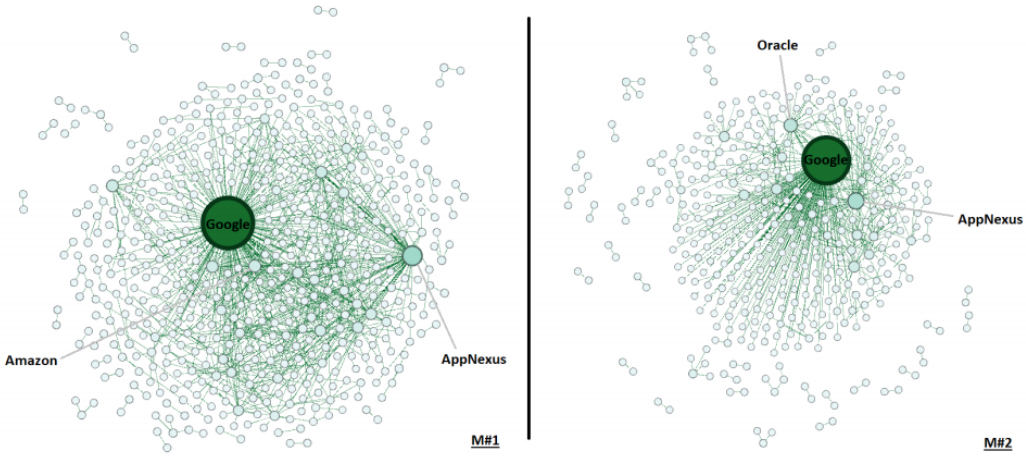


Abbildung 4: Veränderung im Werbenetzwerk nach Einführung der DSGVO (Urban et al., 2020, S. 229)

Ein weiterer Aspekt, der mit der Verschärfung des Datenschutzrechts durch die DSGVO angeführt werden kann, ist jener, dass Publisher*innen ihre Websiten umrüsten mussten. Einen großen Einfluss habe laut Degeling et al. (2019) die neue

Rechtsordnung auf die Datenschutzinformationen im Internet und Datenverarbeitungspraktiken gehabt (vgl. Degeling et al., 2019, S. 15). Degeling et al. (2019) haben in ihrer Studie die 500 beliebtesten Websiten in jedem EU-Mitgliedsstaat (insgesamt 6579 Websites) im Zeitraum von Dezember 2017 bis August 2018 analysiert. Die Ergebnisse zeigten, dass viele Publisher*innen trotz der 24-monatigen Übergangsfrist zur Umsetzung der DSGVO erst zu deren Ende aktiv geworden sind (vgl. Degeling et al., 2019, S. 1-20).

Abbildung 5 zeigt die Änderungen in Datenschutzerklärungen im zeitlichen Verlauf (dunkelblaue Linie) sowie in verschiedenen Zeitabschnitten (rote Balken). Die blauen Balken veranschaulichen, wie viel Prozent der Erklärungen auf den im Zuge der Forschungsarbeit von Degeling et al. (2019) untersuchten Websites im Zeitraum Dezember 2017 bis August 2018 eine Änderung erfahren haben. dass rund 75 Prozent der Websiten ihre Datenschutzerklärungen erst im Jahr 2018 überarbeitet haben. Zusätzlich wurde in der Studie deutlich, dass auch die Länge der untersuchten Datenschutzerklärungen um knapp 42 % angestiegen ist, gemessen an der durchschnittlichen Wortanzahl. Die Ursache hierfür könne laut Degeling et al. (2019) in den neuen Transparenzanforderungen der Art. 13 f. DSGVO liegen (vgl. Degeling et al., 2019, S. 6-15).

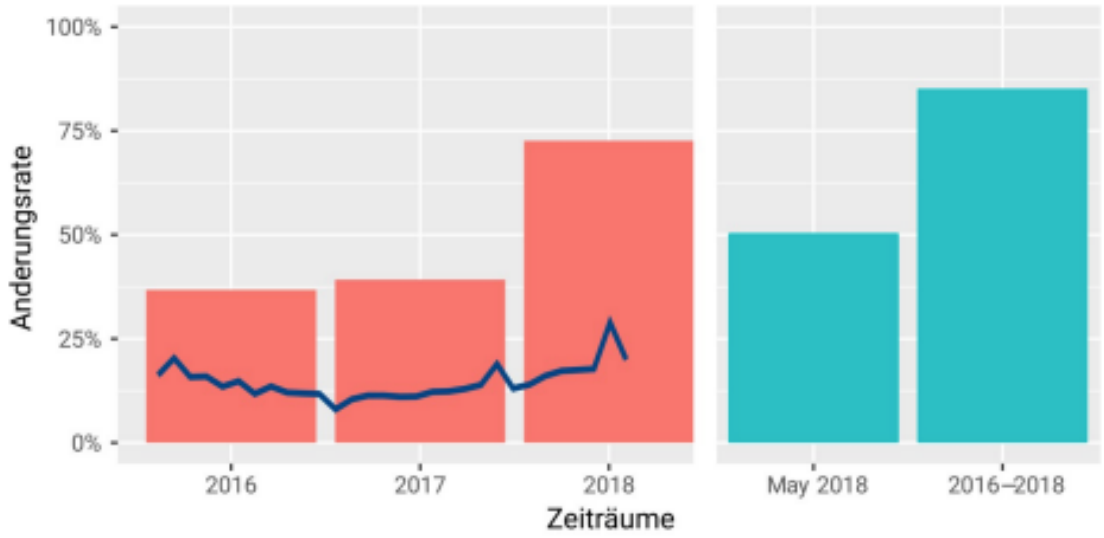


Abbildung 5: Zeitliche Veränderung der Datenschutzerklärungen im Zeitraum 2016 bis 2018 (Degeling et al., 2019, S. 7)

Mühlenhoff und Rudloff (2021) beleuchten die Auswirkungen von DSGVO und der geplanten ePrivacy-Verordnung auf das Dynamic Advertising. Der bzw. die Browseranbieter*in „Mozilla Firefox“ blockiert bereits seit September 2019 standardmäßig die Speicherung von Tracking-Cookies. Das Unternehmen Google habe ebenfalls angekündigt, wie schon in Abschnitt 4.1.2 angeführt, dass sie dieses Vorgehen für ihren Browser Chrome ebenfalls bis spätestens 2023 nachziehen wollen (vgl. Mühlenhoff & Rudloff, 2021, S. 512; itmagazine, 2021, o. S.). Mühlenhoff und Rudloff (2021) argumentieren weiter, dass Cookies die Grundlage für die Generierung und Ausspielung im Online-Marketing bilden (vgl. Mühlenhoff & Rudloff, 2021, S. 512). Anzumerken ist hier aber, dass dies, zumindest aus Sicht des Autors dieser Arbeit, auf die vergangenen Jahre zutrifft.

Mühlenhoff und Rudloff (2021) führen an, dass das Verlustpotenzial auf 50 % geschätzt werden könne, wenn keine First und Third Party Cookies in Zukunft mehr zum Einsatz kommen (vgl. Mühlenhoff & Rudloff, 2021, S. 512). Hinzu komme, dass im digitalen Bereich der sogenannte „Consens“ als Einwilligung zur werblichen Nutzung aktiv und rechtssicher eingeholt werden müsse, was wiederum einen beträchtlichen Verlust der Reichweite mit sich ziehen könne (vgl. ebd., 2021, S. 512).

Laut Bunte (2019) könne man allein in Deutschland von einem cookie-freien Traffic von rund 75 % ausgehen. Auch im UK und Frankreich werde bereits jegliche datenbasierte Aussteuerung seitens von Datenschutzbehörden infrage gestellt (vgl. Bunte, 2019, o. S.). Mühlenhoff und Rudloff (2021) erläutert in seiner Arbeit weiter, dass aufgrund dieses Wandels in der Webtracking-Landschaft ganze Geschäftsmodelle vor dramatischen Herausforderungen stehen. Nützliche Funktionen wie Retargeting, Demand Side Platforms (DSPs), Sell Side Platforms (SSPs), Data Management Platforms (DMPs) würden in ihrer bisher eingesetzten und genutzten Form vor dem Aus stehen. Außerdem würden ebenfalls taktische Maßnahmen wie das im Online-Marketing gängige Frequency Capping, mit dem festgelegt werden kann, wie oft ein oder eine User*in eine bestimmte digitale Kommunikation sieht, nicht mehr nutzbar sein (vgl. ebd., 2021, S. 512). Neumann et al. (2019) hingegen haben in ihrer Feld-Studie zum Thema „Frontiers: How Effective Is Third-Party Consumer Profiling? Evidence from Field Studies“

dargelegt, dass die drohenden Änderungen im Cookie Tracking Ökosystem wohl in der Praxis doch eher keine so großen Auswirkungen haben werden, da das Potential der Nutzer*innenprofilerstellung bis dato ohnehin nicht voll ausgenutzt werde. Untersucht wurde die Genauigkeit von mehr als 90 Third Party Audiences (Drittanbieter*innen-Zielgruppen) über 19 Datenbroker. Anzumerken sei, dass die Zielgruppensegmente allerdings stark in ihrer Qualität variieren, und oftmals ungenau bei führenden Datenbrokern waren. Im Gegensatz zur zufälligen Audience-Auswahl führte die Verwendung von sogenannten Blackbox-Datenprofilen im Durchschnitt zu einer Steigerungsrate von 0 Prozent auf 77 Prozent bei der Identifikation eines oder einer Nutzer*in mit einem gewünschten Einzel-Attribut. Zudem könne die Identifizierung der Zielgruppen in Kombination mit einer Optimierungssoftware um durchschnittlich 123 Prozent verbessert werden (vgl. Neumann et al., 2019, S. 918-926). Allerdings würde man in der Praxis aus wirtschaftlichen Gründen häufig auf den Einsatz dieser Targeting-Lösung ohnehin verzichten. Zum einen aufgrund der hohen Zusatzkosten, die mit dem Erwerb bzw. auch der Nutzung solcher Tools einhergehen. Zum anderen sei die relative Ungenauigkeit für viele Unternehmen ein ausschlaggebendes Argument gegen den Einsatz dieser Software-Programme. Zusammenfassend kann daher gesagt werden, dass Third Party Audiences in der Praxis generell unattraktiv seien (vgl. Neumann et al., 2019, S. 918-926). Eine Ausnahme würde laut Neumann et al. (2019) für höherpreisige Medienplatzierungen gelten (vgl. ebd., 2019, S. 918).

4.2.3 Mögliche Änderungen durch die geplante Einführung der ePrivacy-Verordnung

Die ePrivacy Verordnung (ePVO) sollte schon im Jahre 2018 als Ergänzung zur DSGVO eingeführt werden und die teilweise stark veralteten nationalen Datenschutzrichtlinien ersetzen. Viele Bestimmungen wurden schon vor etlichen Jahren verabschiedet, noch vor dem Zeitalter der Smartphones oder Tablets sowie Messenger-Dienste wie WhatsApp, Skype, Facebook, etc. Ziel der geplanten ePVO ist es, die Vertraulichkeit der Kommunikation zu schützen (vgl. Gradow & Greiner, 2021, S. 32). In diesem Zusammenhang wichtig zu erwähnen ist, dass die ePrivacy Verordnung nicht unmittelbar gilt, bzw. angewendet werden kann. Da es sich eben

um eine Verordnung handelt, muss diese zuvor in nationales Recht umgewandelt werden. Bisher konnte unter den Mitgliedsstaaten keine Einigung auf einen Gesetzesentwurf erzielt werden, weshalb eine Verabschiedung der Verordnung nach hinten verschoben wurde. Laut Gradow und Greiner (2021) sei aber jedenfalls mit einer Übergangsfrist von zwei Jahren danach zu rechnen, weshalb ein Inkrafttreten vor 2025 als unrealistisch scheint (vgl. ebd., 2021, S. 32-33).

4.2.4 Recht auf Privacy auf Nutzer*innenseite sowie Notwendigkeit der Interaktion zwischen Publisher*innen und Nutzer*innen

Das Datenschutzrecht steht vor der Herausforderung gegenüberstehende grundrechtlich verankerte Interessen miteinander abzuwägen. Auf der einen Seite stehen die privaten Nutzer*innen, welche ihr Recht auf Privatsphäre wahren wollen. Auf der anderen Seite hingegen sind aber aus Sicht des Autors dieser Arbeit Publisher*innen und Werbetreibende auf die Interaktion mit den User*innen und Erfassung der Nutzungsdaten angewiesen, um ihr Geschäftsmodell entsprechend betreiben zu können. Roßnagel (2007) und Wenhold (2018) erläutern in ihren Beiträgen zum Thema Nutzerprofilbildung durch Webtracking, dass schon zu Beginn der 1990er Jahre die Risiken einer allgegenwärtigen Datenverarbeitung intensiv diskutiert wurden (vgl. Roßnagel, 2007, S. 13 f.; Wenhold, 2018, S. 37). Roßnagel und Müller (2004) und Wenhold (2018) weisen darauf hin, dass die technischen Möglichkeiten in der Datenverarbeitung, speziell in Formen einer unbefugten Kenntnisnahme, Überwachung und Auswertung personenbezogener Daten, zu der damaligen Zeit stark beschränkt gewesen seien (vgl. Roßnagel & Müller, 2004, S. 628; Wenhold, 2018, S. 37).

Wenhold (2018) führt weiter aus, dass das menschliche Handeln durch die Quantität der gesammelten Informationen sowie der technischen Entwicklung der Datenanalysemethoden besser prognostizierbar und bis zu einem gewissen Grad auch vorhersehbar geworden sei. Die Grenzen vom privaten und öffentlichen Raum wurden ausgehebelt und aufgrund des rasanten Fortschritts der Informationstechnologien sind Öffentlichkeit und Privatsphäre nicht mehr wirklich voneinander zu trennen. Dies habe dazu geführt, dass sich auch die Risiken der Datenverarbeitung für den oder die Nutzer*in erheblich verschärft haben (vgl. ebd., 2018, S. 39). Wenhold (2018) führt in ihrer Arbeit an, dass auf der einen Seite

Nutzer*innen heutzutage in der Wirtschaft die Vorteile des technologischen Fortschritts anpreisen. Andererseits gäbe es jedoch eine Vielzahl an Datenschutzorganisationen, welche vor den Gefährdungspotentialen für eine substanzielle Verletzung der verfassungsrechtlich gewährleisteten allgemeinen Persönlichkeitsrechte eines jeden Einzelnen warnen (vgl. ebd., 2018, S. 39-40).

4.3 Nutzungspotenziale und Funktionsweise von Webtracking

Publisher*innen finanzieren ihre Angebote in der Regel nicht durch die Erhebung eines Nutzungsentgeltes, sondern die Haupteinnahmequelle stellt die Schaltung von Werbung dar. Aufgrund dessen besteht ein besonderes Interesse an personenbezogenen Daten der Nutzer*innen, um Werbung möglichst zielgerichtet anzeigen zu können. Hierzu werden verschiedene Tracking Tools verwendet, welche vielfältige Möglichkeiten bieten, Nutzer*innen bestimmbar zu machen und ihr Surfverhalten zu beobachten (vgl. Heberlein, 2017, S. 40-44). Der BVDW (2015) führt aus, dass ein verlässlich funktionierendes Tracking, welches eindeutige Ergebnisse über alle benötigten Metriken liefert und zugleich eine optimale Aussteuerung erlaubt, für Webangebote sowie auch für werbetreibende Unternehmen im heutzutage vorherrschenden wirtschaftlichen Wettbewerb unerlässlich sei. Den technologischen Schlüssel zu einem leistungsfähigen Tracking hat bis heute das klassische Browser Cookie geliefert (vgl. BVDW, 2015, S. 2).

4.3.1 Formen des klassischen Cookie Trackings

Das klassische Cookie Tracking wird häufig von Publisher*innen und Drittanbieter*innen verwendet, um User*innen und ihr Verhalten zu erfassen bzw. aufzuzeichnen (vgl. Cahn et al., 2016, S. 891). Die klassischen Web Cookies wurden bereits 1994 erfunden oder eingeführt und ermöglichten es, den Status zwischen Clients und Servern aufrecht zu erhalten, erläutern Cahn et al. (2016) in ihrer empirischen Studie über Web Cookies. Ein Cookie ist ein Textstring, also eine Verkettung von einzelnen Zeichen, der im Client-Browser gespeichert wird, sobald

dieser auf einen bestimmten Server zugegriffen wird. Das Cookie wird allgemein im Header im Quellcode einer Website verbaut und sendet nach erfolgtem Seitenaufruf Informationen an den Server zurück. Die erste Form von Web Cookies wurde wie anfangs schon erwähnt in den Vor-1.0-Versionen des Mosaic-Browsers unterstützt und im Jahre 1997 wurde der erste Standard für Web Cookies veröffentlicht. Im Laufe der Jahre haben sich Cookies zu einer zentralen Komponente im World Wide Web entwickelt und ihre Verwendung hat sich im zeitlichen Verlauf mit der Entwicklung der Anwendungsanforderungen erweitert (vgl. Cahn et al., 2016, S. 891).

Beim Webtracking kann zudem einerseits zwischen dem lokalen und globalen Tracking unterschieden werden. Beim lokalen Tracking wird das Verhalten eines Nutzers oder einer Nutzerin auf der Website eines einzelnen Publishers bzw. einer einzelnen Publisherin hinweg beschrieben. Das globale Tracking wiederum bezieht sich auf das webseitenübergreifende Erfassen von Nutzungsdaten. Aufgrund der unterschiedlichen Datenquellen ist es somit möglich, detaillierte Nutzer*innenprofile zu erstellen. Es geht hierbei darum, ein präzises und ein in möglichst vielen Interessensbereichen aussagekräftiges Profil der User*innen zu erstellen (vgl. Wenhold, 2018, S. 52). Um Nutzer*innen über diverse Websiten hinweg zu erkennen, ist eine eindeutige Identifikation (sogenannte Unique Identification, kurz UID) notwendig. In der Regel handelt es sich dabei um eine Zahl, eine Zeichenfolge oder um einen eindeutig zuordenbaren Nutzer*innennamen, welcher server-seitig gespeichert wird. Bei einem erneuten Websitenaufruf ist eine Zuordnung mithilfe dieser auf dem Server gespeicherten UID möglich, sofern ein übereinstimmender Wert übergeben oder ermittelt wird (vgl. ebd. 2018, S. 52-53).

4.3.2 Anwendungsfeld First Party Cookies

Während User*innen sich im Internet bewegen, werden sie sozusagen beobachtet und ihre „Schritte“ aufgezeichnet. Dieses Sammeln von User*innendaten nennt man wie bereits zu Beginn dieses Kapitels beschrieben „Tracking“. Diese Daten können von First Parties gesammelt, aber auch von Third Parties (Drittanbietern) abgegriffen werden (vgl. Traverso et al., 2017, S. 2). Die folgenden beiden Unterkapitel versuchen diese Unterscheidung deutlich zu machen, welche in der Praxis des Webtrackings eine bedeutende Rolle einnimmt. In der Regel werden First Party Cookies ausschließlich vom Publisher selbst verwendet. Dies bezeichnet man dann als sogenanntes Zwei-Parteien-Modell. Der technische Ablauf ist wie folgt: Die Cookies werden nach der technischen Abfrage des Dienstanbieters oder der Dienstanbieterin bei dem oder der User*in, ob dieser oder diese das Cookie akzeptiert, auf dem entsprechenden Computer des oder Nutzer*in gespeichert. Bei jedem neuerlichen Request der jeweiligen Seite kann das aufgerufene IT-System diverse Seitenaufrufe dem oder der einzelnen Nutzer*in eindeutig zuordnen (vgl. Schallaböck, 2014, S. 19 f.).

Laut Voigt und von dem Bussche (2018) lasse der Wortlaut des Art. 4 Nr. 1 DSGVO offen, wer zur Identifizierung der betroffenen Person in der Lage sein muss. Daraus könne man schließen, dass zusätzliche Informationen für die Identifizierung einer Person nicht zwingend im Datenbestand der oder des Verantwortlichen bzw. des Auftraggebers oder der Auftraggeberin vorhanden sein müssen. Zusammengefasst könne gesagt werden, je einfacher und schneller eine natürliche Person ermittelt werden kann, desto eher handele es sich um eine „identifizierbare natürliche Person“ (vgl. Voigt, P., & von dem Bussche, A., 2018, S. 14-16).

Cahn et al. (2016) haben in ihrer empirischen Studie 2016 über Web Cookies die Top 100.000 Websiten im Alexa Ranking nach deren Cookie-Beschaffenheit untersucht. Insgesamt wurden 1.895.023 Cookies im Beobachtungszeitraum aufgezeichnet. Davon waren ca. 31.9 % sogenannte First Party Cookies. Außerdem konnte ein Anstieg dieser Art von Cookies in Höhe von 43,4 % innerhalb der Untersuchungsperiode verzeichnet werden (vgl. Cahn et al., 2016, S. 894).

Die nachfolgende Abbildung 6 stellt die Verteilung von First Party Cookies nach dem Cookiepedia Kategoriensystem dar. Die grauen Balken zeigen auf der rechten Skala die Gesamtzahl der Fist Party Cookies. Die farbigen Balken zeigen die normalisierten Werte aller First Party Cookies mit verschiedenen Attributen (vgl. ebd., 2016, S. 894).

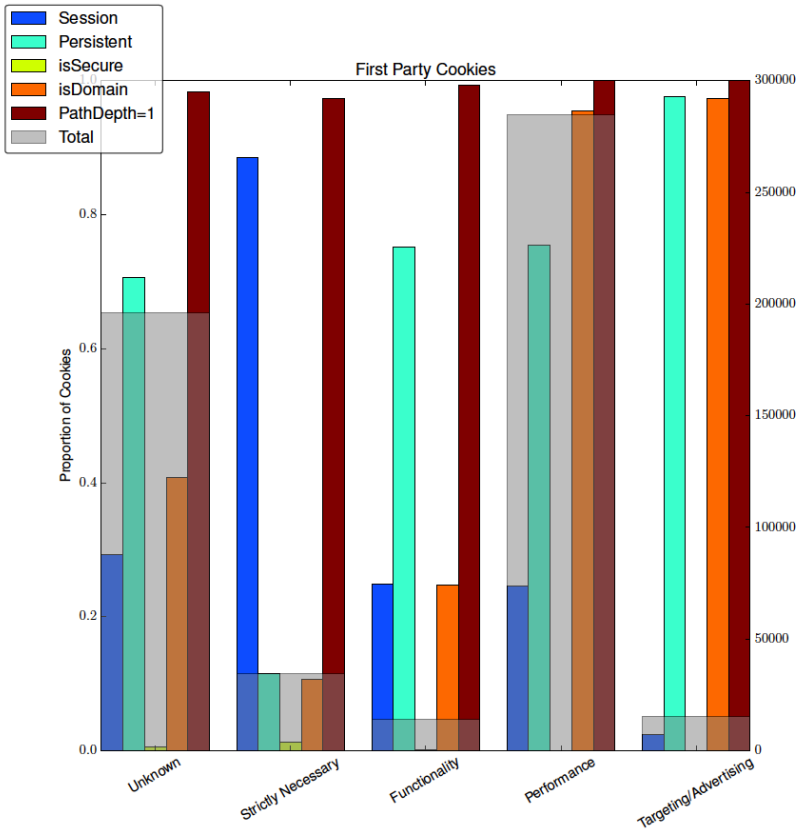


Abbildung 6: First Party Cookies Verteilung nach Cookiepedia Kategoriensystem (Cahn et al., 2016, S. 894)

4.3.3 Anwendungsfeld Third Party Cookies

Cahn et al. (2016) haben in ihrer empirischen Studie 2016 über Web Cookies die Top 100.000 Websiten im Alexa Ranking nach deren Cookie-Beschaffenheit untersucht. Insgesamt wurden 1.895.023 Cookies im Beobachtungszeitraum aufgezeichnet. Davon waren rund 68 % sogenannte Third Party Cookies. Außerdem konnte ein Anstieg dieser Art von Cookies in Höhe von 43,4 % innerhalb der Untersuchungsperiode verzeichnet werden (vgl. Cahn et al., 2016, S. 894). Laut Cahn et al. (2016) sei dieser Anstieg auf die vermehrte Implementierung sowie

deren Popularität von Third Party Services wie Targeted Advertising, Site Analytics und Social Media Widgets zurückzuführen. Bemerkenswert ist auch, dass über 60 % der gesamten beobachteten Third Party Cookies von nur insgesamt rund 50 Anbietern stammen. Dieser Trend verdeutlicht, dass die Masse an gesammelten Daten zwar signifikant zunimmt, aber die Anzahl der Datenaggregator*innen eher zurückgeht bzw. der Markt unter wenigen Teilnehmern aufgeteilt wird. Dieser Aspekt spiegelt sich auch in der vorliegenden Forschungsliteratur wider (vgl. ebd., 2016, S. 894; Dabrowski et al., 2019; Jakobi et al., 2019).

Abbildung 7 zeigt die Verteilung von Drittanbieter*innen Cookies nach dem Cookiepedia Kategoriensystem. Die grauen Balken zeigen die gesamte Anzahl an Drittanbieter*innen-Cookies. Die farbigen Balken hingegen stellen die normalisierten Werte von Third Party Cookies mit verschiedenen Attributen dar.

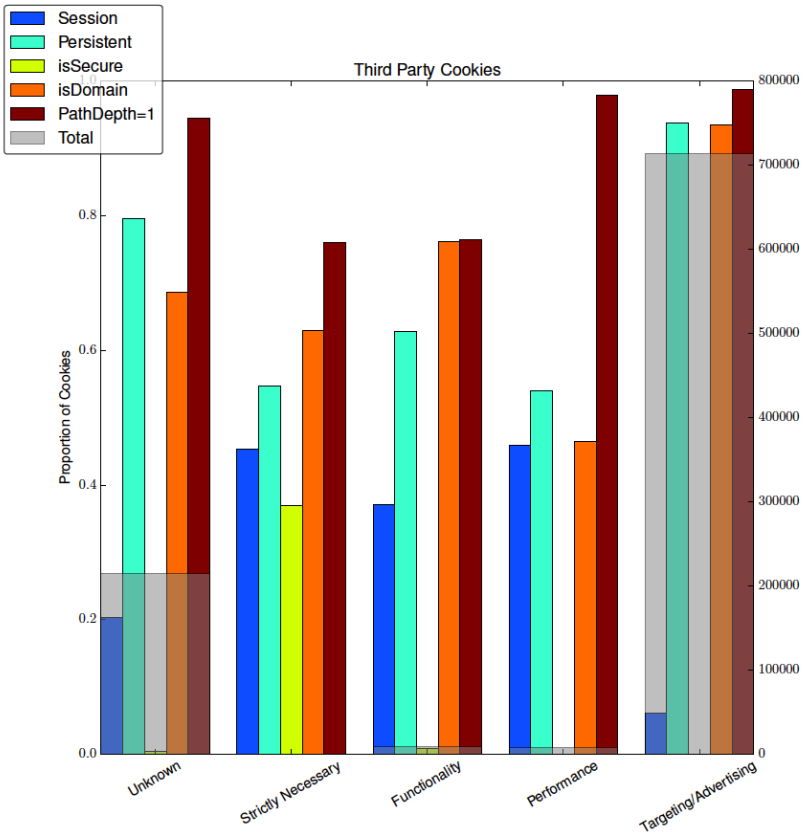


Abbildung 7: Third Party Cookies Verteilung nach Cookiepedia Kategoriensystem (Cahn et al., 2016, S. 894)

5 Methodik

5.1 Methodisches Vorgehen

Um die eingangs aufgestellten Forschungsfragen beantworten zu können, dient dem Forschungsdesign dieser Arbeit eine Benchmarking Analyse. Die Beweggründe hierzu werden nachfolgend erläutert. Aufgrund der Tatsache, wie bereits im theoretischen Teil dieser Arbeit erläutert, dass sich das Webtracking inmitten eines Transformationsprozesses befindet und in der Praxis noch große Unsicherheit besteht, wie es in Zukunft mit dem klassischen Cookie Tracking weitergeht, hat sich der Autor dieser Arbeit für diese Form der empirischen Methode entschieden (Dabrowski et al., 2019; Jakobi et al., 2019). Die Benchmarking Analyse soll dazu dienen, die alternativen Technologien zum Erfassen von persönlichen Daten im Internet in einem entwickelten Kategoriensystem miteinander zu vergleichen und diese in Relation mit den gegebenen rechtlichen Rahmenbedingungen zu setzen. Außerdem werden verschiedene Datenaggregator*innen für die Analyse herangezogen und deren Verhalten im Umgang mit personenbezogenen Daten untersucht.

Mertins et al. (1995) erläutern, dass mithilfe eines Benchmarkings unstrukturierte Prozesse einer andauernden Transformation bzw. Veränderung in einen objektiven Aktionsplan verwandelt werden können. Der Benchmarking Prozess beginnt grundlegend mit dem Erkennen einer Problemstellung und man konzentriert sich dabei auf die Kernprobleme, um die aktuelle Praxis zu verbessern (vgl. Mertins et al., 1995, S. 223).

Die im Literature-Review herausgestellten Bedarfe der Theorie-Bildung in Bezug zu diesem Thema, in Kombination mit der Neuartigkeit der diversen Technologien im Anwendungskontext des Webtrackings, machen es notwendig, mithilfe der Benchmarking Analyse eine Vergleichsbasis zu schaffen und Merkmale sowie rechtliche Konflikte zu identifizieren.

Zum besseren Verständnis wurde folgende Grafik (Abb. 8) angefertigt, welche den Prozess der Benchmarking Analyse abbilden soll. Beginnend mit der Literaturrecherche werden nachfolgend verschiedene Alternativen zum klassischen Cookie Tracking identifiziert und beschrieben. Anschließend wird ein eigenes Kategoriensystem für das Benchmarking entwickelt. Die Analyse beinhaltet diverse Aspekte wie die Vereinbarkeit mit datenschutzbezogenen Rechtsvorschriften, wobei der Fokus auf die im europäischen Rechtsraum gültigen DSGVO gelegt wurde. Zudem soll das Verhalten von ausgewählten und in der Praxis gängigen Datenaggregator*innen/Vendor*innen analysiert werden. Diese Vorgehensweise soll dazu dienen, Maßnahmen zu entwerfen, welche als eine Art Orientierungshilfe für Publisher*innen/Unternehmen dienen sollen, um das Compliance Management optimieren zu können und dabei unterstützen soll, sich aus Datenschutzsicht möglichst rechtskonform zu verhalten.

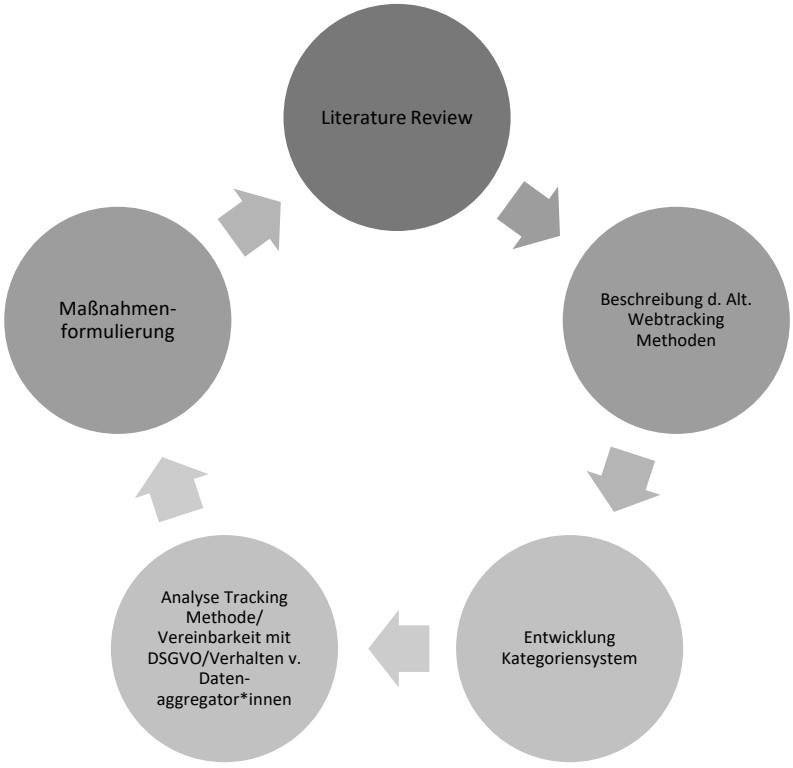


Abbildung 8: Eigene Darstellung - Benchmarking-Prozess

Wie bereits anfangs kurz beschrieben, wurden mittels Desk Research qualitative Kategorien und Merkmale ausgearbeitet, welche dazu dienen sollen, die alternativen Webtracking Methoden miteinander vergleichen zu können sowie mit den relevanten Datenschutzbestimmung, wie beispielsweise der DSGVO, in Relation setzen zu können. Hierzu wurde mithilfe von zuvor bestimmten relevanten Keywords in diversen Datenbanken nach einschlägiger Fachliteratur und Journals gesucht. Hauptsächlich wurde die Recherche auf folgenden Seiten durchgeführt: Springer Link, Sage, ACM, und IEEE. Nach Erstellung eines Kategorienkatalogs wird eine Benchmarking Analyse durchgeführt. Ziel des Benchmarkings ist es, Kriterien zu definieren, welche auf die rechtlichen Rahmenbedingungen, im Zusammenhang mit dem Sammeln von User-Daten, abgestimmt sind. Hierdurch soll ersichtlich werden, was der rechtliche Status-Quo ist, was erlaubt das Gesetz und was verbietet die Gesetzgebung im Hinblick auf das Sammeln von Informationen im Internet. In einem nächsten Schritt werden diese festgelegten Kategorien auf die diversen Cookieless Tracking Methoden angewandt und analysiert, ob diese mit den definierten Kriterien in Konflikt stehen.

Für die Auswertung hat sich der Autor dazu entschieden, eine Likert-Skala mit den Werten 1 bis 5, zu verwenden, um die unterschiedlichen Technologien pro Kategorie zu gewichten. Der Wert 1 stellt dabei den niedrigsten Wert dar und der Wert 5 den höchsten. Nachfolgende Aufzählung schlüsselt die einzelnen Codes zur besseren Nachvollziehbarkeit auf:

1 = Überhaupt nicht praktikabel (Schlechteste Bewertung),

2 = Nur bedingt praktikabel,

3 = Etwas praktikabel,

4 = Sehr praktikabel,

5 = Äußerst praktikabel (Beste Bewertung).

Die einzelnen Dimensionen sowie Einordnungswerte werden im Abschnitt 5.4 genauer beschrieben. Die Einordnungen für die alternativen Methoden des Webtrackings basieren auf Grundlage, der in Tabelle 2 gesichteten Literatur sowie den Ausführungen in Kapitel 5.3. Für die ausgewählten Unternehmen dient das

Kapitel 2.4 als Grundlage sowie die zugrunde liegenden Datenschutzbestimmungen und Nutzungsbedingungen der einzelnen ausgewählten Unternehmen. Mithilfe dieser Informationen wurden die Bewertungskriterien (siehe Auflistung, S. 53) für das Benchmarking abgeleitet. Diese Gewichtung der einzelnen Kriterien ermöglicht es, die zuvor festgelegten alternativen Webtracking Methoden mit der DSGVO in Relation zu setzen und Vergleiche zwischen den einzelnen Technologien anzustellen. Die Ergebnisse werden anschließend grafisch in Form von Diagrammen und Tabellen dargestellt. Ziel dieser methodischen Herangehensweise soll es sein, einen Überblick über mögliche alternative Webtracking Methoden zu geben sowie Denkansätze für zukünftige Forschung zu schaffen.

5.2 Desk Research – Alternative Webtracking Methoden

Der Ausgangspunkt für die empirische Untersuchung stellt eine ausführliche Literaturrecherche über alternative Webtracking Methoden dar. Der Ablauf und die Vorgehensweise werden nachfolgend genauer skizziert. In einem ersten Schritt wurde nach Sekundärliteratur gesucht, welche sich mit der Thematik rund um alternative Webtracking Methoden beschäftigen. Hierzu wurden im Vorhinein festgelegte Keywords verwendet.

Hauptsächlich wurde die Suche in der ersten Phase mit folgenden Schlüsselwörtern/-phrasen in deutscher sowie englischer Sprache durchgeführt:

- Cookieless Tracking
- Alternative Webtracking Methoden
- Webtracking ohne Cookies

Recherchiert wurde überwiegend auf folgenden Literatur-Datenbanken:

- IEEE
- ACM
- Springer Link
- Science Direct

- Nomos eBooks complete
- Google Scholar

Aufgrund der speziellen Thematik und der Aktualität wurden, ähnlich wie beim Forschungsstand, auch Publikationsformate ohne Peer-Review als forschungsrelevant angesehen:

- Facheinschlägige und branchenspezifische Onlinequellen: *W3C*
- Whitepaper von ausgewählten Fachverbänden sowie Fachexpert*innen: z.B.: Bundesverband für Digitale Wirtschaft (BVDW) e.V.

Außerdem wurden andere Masterarbeiten und Dissertationen herangezogen, welche ein ähnliches Themengebiet untersucht haben und die zu Grunde liegende Literatur wurde demnach recherchiert und relevante Quellen herangezogen.

Die erste Phase der Recherche wurde im Zeitraum vom 01. Oktober 2020 bis 31. Dezember 2020 durchgeführt. Nach diesem Durchgang hat sich vor allem die Studie von Bujlow et al. (2017) zum Thema Webtracking sowie das Whitepaper des Bundesverbands für Digitale Wirtschaft (2015) als Kernliteratur herauskristallisiert, welches verschiedene alternative Tracking Technologien sowie deren Funktionsweise beschreibt (vgl. BVDW, 2015, S. 1-27). Die zweite Phase der Literatursichtung erfolgte dann im Zeitraum von 01. April 2021 bis 31. Juli 2021. Dieser Durchgang diente vor allem dazu, die ausgewählten Quellen über alternative Webtracking Methoden (Whitepaper und Onlinequellen) mit geeigneter Fachliteratur zu stützen, bzw. deren Aussagekraft zu belegen. Hierbei wurde darauf Wert gelegt, Journals zu finden, welche einem Peer-Review standgehalten haben. Aufgrund der Aktualität und der bereits erwähnten Unsicherheit in der Praxis über die zukünftigen technischen und rechtlichen Entwicklungen muss an dieser Stelle gesagt werden, dass nicht über jede einzelne Technologie spezifisch eine wissenschaftliche Studie gefunden werden konnte.

Die folgende Tabelle 2 gibt Aufschluss darüber, welche Literaturbanken und Quellen für die Beschreibung der verschiedenen Technologien verwendet wurden. Außerdem ist ersichtlich, welche Schlüsselwörter für die Recherche verwendet wurden. Der Übersicht halber hat sich der Autor dazu entschieden, an dieser Stelle die Kurzform des Zitats zu verwenden. Der Titel des entsprechenden Beitrags bzw.

Werk kann dem Literaturverzeichnis entnommen werden. Nachfolgend werden die einzelnen alternativen Webtracking Methoden beschrieben und ein Überblick über die Art und den Umfang der Nutzungsdatenaufzeichnung gegeben. Daran anknüpfend werden die, aus der Forschungsliteratur sowie den Datenschutzbestimmungen und Nutzungsbedingungen, ausgearbeiteten Dimensionen für die Analyse vorgestellt. Außerdem werden die für die Analyse notwendigen Codes zur Einordnung in die Kategorien erläutert.

Alternative Webtracking Methoden / Keywords Recherche	Verwendete Literaturquellen/ Datenbanken	Grundlagenliteratur Quellen
Semantisches Targeting ***Verwendete Keywords:*** *Semantic Targeting;* *Semantisches Targeting*	Springer Link	Bauer, et al. (2011); Hillebrand (2018)
Fingerprinting ***Verwendete Keywords:*** *Fingerprinting;* *Fingerprinting Methode* *Webtracking*	IEEE; Springer Link; Nomos eBooks complete	Bujlow et al. (2017) Eckersley (2010); Schott (2014); Wenhold (2018); Woitke (2003)
Cache-basierte Tracking Methoden ***Verwendete Keywords:*** *Cache Tracking;* *Authentication Cache;* *entity Tag;* *eTag*	IEEE; Online-Quelle: *BVDW (Whitepaper, PDF;* *F5 (Website);*	Bujlow et al. (2017); BVDW (2015); F5 (2014)

Common IDs / ***Universal IDs*** ***<u>Verwendete Keywords:</u>*** *Common ID* *Universal ID Webtracking*	<u>Online-Quellen:</u> Trusted Targeting (Website + PDF); BVDW (Whitepaper, PDF)	TrustedTargeting (2021); BVDW (2015)
Local-/Web-/DOM-Storage ***<u>Verwendete Keywords:</u>*** *Local Storage* *Web Storage Tracking* *DOM Storage*	<u>Online-Quellen:</u> W3C (Website); BVDW (Whitepaper, PDF)	W3C (2021); BVDW (2015)

Tabelle 2: Eigene Darstellung - Überblick Forschungsliteratur Cookieless Tracking Methoden

5.3 Beschreibung und Funktionsweise der ausgewählten alternativen Webtracking Methoden

Im folgenden Abschnitt werden die ausgewählten alternativen Webtracking Methoden nun genauer in Hinblick auf deren Funktionsweise sowie Art und Umfang der Datenaufzeichnung beschrieben. Diese Ausführungen bilden die Grundlage für die anschließende Benchmarking-Analyse.

5.3.1 Semantisches Targeting

Beim Semantischen Targeting erfolgt die Werbemittelauslieferung auf Basis einer Kombination von mehreren Wörtern und der semantischen Auswertung der möglichen Bedeutung dieser Kombination. Im Gegensatz zum reinen Keywordtargeting ist es beim semantischen Targeting möglich, den gesamten Text einer Website zu analysieren, anstatt nach einzelnen Keywords zu suchen. Die enthaltenen Schwerpunktthemen können bestimmt und dementsprechend ein themenspezifisches Werbemittel platziert werden. Der Vorteil bei dieser Methode

ist, dass auch der komplette Sinnzusammenhang des Textinhaltes erfasst werden kann und auch die Bedeutung von mehrdeutigen Worten erkannt wird. Mithilfe dieser Methode können Werbetreibende sehr präzise Themenumfelder festlegen, in denen die Werbeschaltungen durchgeführt werden (vgl. Bauer, et al., 2011, S. 12-13, XIV). Das Unternehmen Google verwendet diese Technologie bereits bei ihrem Google Display-Netzwerk. Publisher, welche diesem Netzwerk angehören, binden keine Werbemittel eines einzelnen Werbetreibenden ein, sondern JavaScript- und HTML-Codes von Google. Welche Anzeige schlussendlich angezeigt wird, ist im Vorhinein, anders als bei einem Affiliate Netzwerk, noch nicht definiert. Google untersucht mittels einer semantischen Suchmaschinentechnologie die entsprechende Website und ordnet jedes einzelne Dokument genau bestimmten Themen oder Begrifflichkeiten zu (vgl. Hillebrand, 2018, S. 228-229).

Hillebrand (2018) erläutert, dass Google Advertiser*innen diverse Formen des Semantischen Targetings bieten würde (vgl. Hillebrand, 2018, S. 229):

- *Kontext-Targeting*: Hierbei gibt der oder die Advertiser*in Keywords an. Die Werbung werde dann innerhalb von Dokumenten geschalten, welche Google als relevant erachtet (vgl. ebd., 2018, S.229). Laut Hillebrand (2018) dürften das hauptsächlich Dokumente sein, welche bei ihrer Suchmaschinenoptimierung die gleichen Keywords verwenden. Dabei spiele auch die Größe der Websites keine entscheidende Rolle. Vielmehr würden jene Seiten als Suchtreffer angezeigt werden, welche sich intensiv bzw. genau mit dem eingegebenen Keyword und dessen zugehörigen Themenbereich beschäftigen (vgl. ebd., 2018, S. 229).
- *Themenbezogenes Targeting*: Hierbei kann der oder die Advertiser*in aus einem durch Google bereitgestellten systematischen Katalog Themen auswählen. Laut Hillebrand (2018) sei hierbei das Targeting naturgemäß weniger dezidiert. Unter anderem können hier statt Themen der jeweiligen Medien der Publisher*innen auch Interessen der Zielgruppe angegeben werden (vgl. ebd., 2018, S. 229).
- *Placement Targeting*: Der oder die Advertiser*in kann hierbei Publisher*innen vorgeben, auf denen er oder sie werben möchte. Google ermittelt hierzu individuell für den oder die Advertiser*in passende

Publisher*innen und bietet sie zur Auswahl an (Bsp.: Fachmedien oder Blogs zu einem spezifischen Themenbereich). Der oder die Advertiser*in kann auch Websites von Publisher*innen selbst angeben, sofern diese Mitglied bei Google AdSense seien (vgl. ebd., 2018, S. 229).

Advertiser*innen haben beim Semantischen Targeting zudem die Möglichkeit, auch demografische und geografische Eigenschaften einer Zielgruppe vorzugeben. Die Werbeschaltungen werden dann beispielsweise nur in einem bestimmten Land, nur einer Altersgruppe und nur einem Geschlecht angezeigt. Außerdem stehen in Bezug auf das Google Display-Netzwerk alle Möglichkeiten der Auswertung und Optimierung zur Verfügung, welche „Google AdWords“ und „Google Analytics“ bieten (vgl. ebd., 2018, S. 229).

Rodrìguez-Garcia et al. (2021) gehen in ihrem Forschungsbeitrag ebenfalls darauf ein, dass während User*innen eine Abfrage bei einer Suchmaschine im Internet abgeben, stetig Daten und Informationen über Server gesammelt und aggregiert werden. Dies diene zum einen zur Erstellung von Nutzungsprofilen, welche zur Bereitstellung personalisierter Services verwendet werden (vgl. Rodriguez-Garcia et al., 2021, S. 1). Andererseits könne laut Garcia et al. (2021) mit diesen Informationen sogenanntes Behavioral Targeting betrieben werden, bei dem das Verhalten von Nutzer*innen beobachtet wird. Noch bedenklicher aus Datenschutzperspektive ist, dass diese Daten dann auch an Dritte weitergegeben werden können (vgl. ebd., 2021, S. 1). Rodriguez-Garcia et al. (2021) schlagen als Lösung in ihrer Studie eine automatisierte Methode zur Vortäuschung von falschen Suchanfragen vor, um die Privatsphäre von User*innen zu schützen und die Vorhersagekraft ihres Verhaltens zu minimieren. Dabei würde ein vollständiger Schutz geboten werden, bei dem das Profil vollständig generisch sei und keine dominanten Interessen aufweise. Außerdem würden die vorgetäuschten Suchanfragen keinem bestimmbaren Muster folgen, mithilfe des Einsatzes einer semantisch konsistenten Randomisierung (vgl. ebd., 2021, S. 1-23). Damit die Methode in der Praxis anwendbar ist, müssen die verwendete Ontologie den Großteil der Anfragenkonzepte der User*innen abdecken. WordNet und andere größere Ontologien wie YAGO haben sich als geeignet erwiesen und könnten den Abgleich von Abfragen mit den entsprechenden Kategorien erleichtern. Außerdem

sei eine Vielzahl an Tools sowie ein Mechanismus zur automatisierten Erkennung der Abfragesprache erforderlich und die gefälschten Suchanfragen dürften, wie bereits erwähnt, keinem deterministischen Muster folgen (vgl. ebd., 2021, S. 20). Diese Vorgehensweise könnte zukünftig eine vielversprechende Lösung zur Verbesserung des Privatsphären-Schutzes für Nutzer*innen darstellen.

5.3.2 Fingerprinting

Unter Fingerprinting versteht man eine Gruppe von Tracking Methoden, die ein breites Spektrum an diversen Technologien abdeckt. Unterschieden werden kann zwischen verschiedenen Formen, welche unterschiedliche Daten von User*innen erfassen können:

- *Network und Location Fingerprinting*:

  Trackingmöglichkeit von IP-Adresse, Herkunftsland, -Stadt sowie -Nachbarschaft des oder der User*in

- *Device Fingerprinting (Endgerät Fingerprinting)*:

  Trackingmöglichkeit von Endgeräte ID, IP-Adresse (gesamte oder abgeschnittene), Betriebssystem, Bildschirmauflösung, Zeitzone, System-Schriftarten, Webbrowser, Informationen über Hardware-Komponenten (Maus, Tastatur, Mikrofon, Kamera, etc.), TCP Timestamps (= Kommunikationsstandard, welcher den Austausch von Informationen zwischen versch. Programmen und Computern ermöglicht, Anm. d. Autors)

- *Betriebssysteminstanz Fingerprinting*:

  Trackingmöglichkeit von Betriebssysteminstanz, -version sowie -architektur, Systemsprache, User*innen-spezifische Sprache, Lokale Zeitzone, Lokale Zeit und Datum, System-Schriftarten, Farbtiefe, Bildschirmgröße, Audio-Eigenschaften, Kamera, Mikrofon, Festplatte, TCP/IP Parameter, Computer-Name, Internet Explorer Produkt ID, Windows Digital Product ID, Installierte Treiber

- *Browser Version Fingerprinting*:

  Trackingmöglichkeit von einer detaillierten Browserversion des oder der User*in

- *Diverse Browserinstanz Fingerprinting Methoden*:

  Canvas-Tracking: Browserinstanz ID

  Browserverlauf-Tracking: Browserinstanz ID, Browserverlauf des oder der User*in

  Trackingmöglichkeiten weiterer Browserinstanz Fingerprinting Methoden: Browserinstanz ID, detaillierte Browserversion, Unterstützte Bildformate und anderen Mediendateien, Bevorzugte und Standard-Sprache, Browser-Plugins, Standardsprache vom Browser des oder der User*in, Browser-Dimensionen, Flash Version, Bildschirmauflösung, Farbtiefe, Zeitzone, System-Schriftarten, IP-Adresse, Akzeptierte HTTP Header, Genehmigte Cookies, Supercookies, Einschränkungen

(vgl. Bujlow et al., 2017, S. 1482-1483)

Bujlow et al. (2017) erklären, dass ein Fingerprint (eindeutig zuweisbare ID eines Geräts, Betriebssystems, Browser oder einer anderen Instanz) aus einem oder mehreren Werten bestehen kann, welche vom Web-Service ausgelesen werden kann, wenn ein oder eine User*in verschiedene Websites aufruft und sich dort aufhält. Auf diese Weise kann der oder die Nutzer*in verfolgt werden. Vorteil des Fingerprinting-Trackings ist daher, dass eine Nachverfolgung, über verschiedene Websites hinweg, möglich ist. Außerdem ist keine Anmeldung des Users oder der Userin. Aus der Sicht der Privatsphäre bedeutet dies allerdings, dass Nutzer*innen oftmals gar nicht bemerken können, dass ihre Daten in dem Moment erfasst und aufgezeichnet werden (vgl. Bujlow et al., 2017, S. 1486). Zusätzlich sei es laut Bujlow et al. (2017) auch kaum möglich, das Fingerprinting gänzlich zu verhindern. Zwar könne man durch Unterbinden der Unterstützung von JavaScript, Java und Flash dagegenwirken, aber das passive Fingerprinting könne nicht verhindert werden. (vgl. ebd. et al., 2017, S. 1486).

Woitke (2003) führt weiter aus, dass beim Fingerprinting-Tracking sogenannte Web-Bugs zum Einsatz kommen, welche vom Einsatzzweck mit gewöhnlichen Cookies vergleichbar sind. Die Funktionsweise ist aber grundlegend anders gestaltet (vgl. Woitke, 2003, S. 310). Anders als bei der herkömmlichen Cookie Tracking Methode, kommen beim Fingerprinting 1x1 Pixel große, transparente, oder an den Hintergrund einer Website angepasste und insofern unsichtbare Grafiken zum Einsatz. Diese Pixel fragen Informationen, wie beispielsweise die IP-Adresse, die URL der besuchten Seite, den Zeitpunkt und die Länge des Besuchs sowie den Browsertyp ab und speichern diese erhobenen Daten (vgl. Woitke, 2003, S. 310-314; Wenhold, 2018, S. 61). Beim Fingerprinting wird das benutzte Gerät der User*innen auf dessen Beschaffenheit und Setting ausgelesen. Damit können auch die Bildschirmauflösung und Art des Betriebssystems ausgelesen werden (vgl. Heberlein, 2017, S. 83).

Schott (2014) erklärt, dass das Auslesen durch den Browser notwendig sei, um Inhalte ideal darstellen zu können. Diese Methode sei aber insbesondere unter Datenschutzaspekten sehr umstritten, da sie ohne Kenntnis der User*innen verwendet werden kann und damit auch keine Wahlfreiheit lasse, ob Informationen gespeichert werden oder nicht (vgl. Schott, 2014, S. 581). Dies verstößt klar gegen die DSGVO, welche in Art. 6 ff regelt, dass bei einer Datenverarbeitung der oder die Endnutzer*in ihre Einwilligung zur Verwendung der personenbezogenen Daten gegeben haben muss (vgl. Art. 6 ff, DSGVO, 2016/119).

Eckersley (2010) führt an, dass das Canvas Fingerprinting zudem für den oder die Nutzer*in praktisch kaum bemerkbar sei. Außerdem würde das Hinterlassen eines solchen „Fingerabdrucks“ fast nicht umkehrbar sein, obwohl sich die Fingerprints rasch ändern können. Dies könnte aus datenschutzrechtlicher Sicht äußerst bedenklich sein (Anm. d. Autors). Mittels Algorithmen könne man nämlich die neuen Fingerprints mit den alten in Verbindung setzen. Zudem sei es mit dieser Methode auch möglich, in Verbindung mit der IP-Adresse der Nutzer*innen, gelöschte HTTP-Cookies wiederherzustellen (vgl. Eckersley, 2010, S. 2-3).

5.3.3 Cache-basierte Tracking Methoden

Cache-basierte Tracking Methoden nutzen, ähnlich wie die klassische Cookie Technologie, die clientbasierte Speicherung. Im Gegensatz zur herkömmlichen Trackingart mit Cookies wird hierbei der Storage (Speicher) nicht explizit für die Aufbewahrung von Daten ausgelegt, sondern es werden verschiedene Caches zur Identifizierung von Browserinstanzen sowie zur Ermittlung von zuvor besuchten Websites verwendet (vgl. Bujlow et al., 2017, S. 1485). Bei dieser Technologie können folgende Informationen, zur Wiedererkennung von User*innen, abgegriffen werden:

- Browser Instance ID (Browserinstanz-ID)
- Browser-Verlauf
- Operating System Instance ID (Betriebssysteminstanz-ID) (vgl. ebd., 2017, S. 1483).

5.3.3.1 Web-Cache

Eine Form der cache-basierten Trackingtechnologie ist das Web Cache Tracking. Bujlow et al. (2017) merken an, dass bis zum Jahre 2010 der Browserverlauf prinzipiell mit Hilfe der DOM-API automatisch ermittelt werden konnte. Es konnte eingestellt werden, dass die vom Browser verwendete Farbe für die Anzeige besuchter und nicht besuchter Links nach eigenen Wünschen eingestellt wird. Mithilfe von JavaScript war es dann möglich, Links zu erzeugen, welche auf ein bestimmtes Ziel zeigen (z. B.: http://www.cnn.com), welche der oder die Datenangreifer*in im Browserverlauf überprüfen konnte. Die Farbe der generierten Links kann von JavaScript ausgelesen werden und mit anderen verglichen werden. Mit dieser Methode war es möglich zwischen 10.000 und 30.000 Links auf ihr Vorhandensein im Browserverlauf zu testen. Mittlerweile wurde diese Bedrohung der Privatsphäre und des Datenschutzes von allen gängigen Browsern behoben. Aus technischer Perspektive wurde die Rückgabe des Stils aller Hyperlinks durch API-Aufrufe auf „nicht besucht“ zurückgesetzt. Unabhängig davon, ob die Links tatsächlich vom User oder von der Userin aufgerufen wurden. Trotz alldem kann der

Browserverlauf heutzutage immer noch über eine Reihe von Wegen erlangt werden (vgl. Bujlow et al., 2017, 1485). Wenn ein Browser beispielsweise ein Objekt (Beispiel: Bilddatei) herunterlädt, wird dies im Normalfall im Browser-Cache gespeichert, damit es bei einem erneuten Aufruf der Website schneller angezeigt werden kann. Damit kann über die Seite aber auch festgestellt werden, ob der oder die User*in schon einmal die Website besucht. Hat ein Werbetreibender bzw. eine Werbetreibende seine oder ihre Objekte auf vielen Seiten platziert, kann man diese Informationen leicht mit „gecachten“ Kopien vergleichen und feststellen, welche Seiten am häufigsten von User*innen aufgerufen werden (vgl. Bujlow et al., 2017, 1485). Bujlow et al. (2017) beschreiben die unterschiedlichen Funktionen der Web-Cache Technologie:

- Einbettung von IDs in zwischengespeichterte Dokumente:
  Nutzer*innen fordern eine HTML-Daten an, welche eine eingebettete ID enthält, die in einem unsichtbaren div-Element gespeichert und anschließend mithilfe der div-ID aus dem Browser-Cache ausgelesen werden kann. Da die im Cache gespeicherten Dateien von praktisch jeder Website eingebunden werden können, ist es möglich, dass die darin gespeicherten Informationen auch von unterschiedlichen Diensten verwendet werden.

- Ladeleistungstests
  Mittels JavaScript kann die Ladezeit eine beliebigen Objekts (z. B.: Bilddatei) von einer beliebigen URL gemessen werden und an den Host-Dienst gemeldet werden, um zu ermitteln, ob das Objekt im Cache vorhanden ist oder nicht. Somit kann auch festgestellt werden, ob die Seite schon einmal aufgerufen wurde oder nicht.

- eTags und Last-Modified-HTTP-Header

  Um Nuter*innen über den Web-Cache identifizieren zu können, kommen eTags (Entity Tags) oder Last-Modified-HTTP-Header zur Anwendung. Der HTTP-Header, welcher mit dem ersten Download einer Datei erstellt wird, enthält verschieden Felder wie: Last-Modified ETag, Cache-Control und Expires. Vor allem das ETag-Feld kann genügend Informationen für die

Benutzer*innenkennung speichern, welche von Tracking-Unternehmen verwendet wird. Der Last-Modified-Header ist in der Lage jede zufällige Zeichenfolge zu akzeptieren, nicht nur ein gültiges Datum, welches aber auch für Tracking-Zwecke genutzt werden kann. Bei einer HTTP-Anfrage überprüft der Web-Server, ob die im Cache zwischengespeicherten Kopien veraltet sind oder nicht. Wenn eine Kopie noch gültig ist, gibt der Server eine Rückmeldung mit dem Status „HTTP 304 Not Modified“. Falls es ein veraltetes Dokument ist, wird ein neues zurückgegeben.

Bujlow et al. (2017) weisen zudem darauf hin, dass aus Datenschutzperspektive User*innen das Tracking durch eTags vermeiden können, indem der Browser-Cache vor jedem Besuch auf eine Website gelöscht wird. Die Tracking Methode mit eTags funktioniert zudem auch bei einer einzelnen privaten Browsersitzung, da der Cache bis zum Schließen des letzten Browserfenster in der Lage ist, Informationen abzuspeichern. Bei der Methode mittels Last-Modified-Headern sei es zudem auch möglich Web-Proxys zu umgehen (vgl. Bujlow et al., 2017, 1485). Dies ist vor allem aus Sicht des Privatsphärenschutzes von User*innen kritisch zu hinterfragen.

5.3.3.2 Authentication-Cache

Der Bundesverband Digitale Wirtschaft (2015), kurz BVDW, führt aus, dass mithilfe des Authentication Cache die erforderlichen Zutrittsdaten (Name und Passwort) für den Zugriff auf eine passwortgeschützte Website im Cache gespeichert werden. Diese Daten könne man auch für Webtrackingzwecke heranziehen. Das Tracking über den Authentication Cache basiert auf der sogenannten „HTTP basic authentication“. Hierbei wird server-seitig festgelegt, dass für den Zugriff auf eine Ressource bei diesem Webserver im Header des entsprechenden HTTP-Requests eine dem Server bekannte Kombination von Namen und Passwort übergeben werden muss. Werden diese Informationen übergeben, kommt es zum Fehlercode „HTTP 401 Not Authorized“ bzw. „HTTP-Fehler 401 Unauthorized“. Wenn dieser Fehler angezeigt wird, öffnet sich im Normalfall auch ein kleines Dialogfenster, in welchem der oder die Nutzer*in dazu aufgefordert werden, den

Namen und das Passwort einzugeben. Ruft man dieselbe Seite ein zweites Mal auf oder geht man auf einen Link auf einer anderen Seite desselben Servers, erfolgt standardmäßig bei allen Browsern eine Zwischenspeicherung der angeführten Informationen und gespeicherte Nutzernamen sowie Passwörter werden automatisiert übergeben (vgl. BVDW, 2015, S. 20).
Das Tracking mittels dieser Methode erfolgt folgendermaßen: Ein Aufruf, sogenannter Request einer bestimmten Ressource, beispielsweise in Form eines Pixels, wird auf dem Server durch einen JavaScript-Code eingebunden und vor Zugängen geschützt. Beim allerersten Aufruf dieser Ressource sind noch keine Informationen über den oder die User*in bekannt. Die eingegebenen Informationen über Namen und Passwort werden mittels einer neuen User-ID im Authentication Cache gespeichert. Bei einem erneuten Aufruf über denselben Server ist der Browser nun in der Lage, automatisch Name und Passwort mithilfe einer eindeutigen ID (Browserinstanz ID) zuzuordnen.
Bei dieser Tracking Methode hängt viel von der Speicherdauer im Cache ab. Laut BVDW (2015) könne der hauseigene Browser Safari von Apple die Informationen im Cache überdurchschnittlich lange speichern (vgl. ebd. 2015, S. 20-21).

5.3.3.3 eTag

Beim eTag (Kurzform für entity tag) handelt es sich um ein Code Snippet, welches im Header einer Website verbaut wird und welches auch für das Browsercaching genutzt werden kann. Jede vom Webserver angefragte Ressource bekommt eine eigene Prüfsumme, welche abgelegt und in Form eines eTags bei jedem Request mitgesendet wird. Bei einem erneuten Request werden diese Prüfsummen miteinander verglichen und bei einer Übereinstimmung wird aus dem Cache eine vorhandene Ressource geladen. Das Tracking über eTag-Parameter erfolgt auch über JavaScript. Jedoch kann hierbei nicht auf bereits gesendete Header-Informationen zugegriffen werden. Abhilfe schafft man aber mit dem sogenannten Ajax-Call, beispielsweise in Form eines 1x1 Pixels, welches auf jeder Website und Subsite integriert wird. Kommt es zu einem erfolgreichen Call, können somit auch die eTag-Parameter im Header vom Webserver mitübergeben werden und vom JavaScript ausgelesen werden. Der Wert des eTags kann, ähnlich wie das

klassische Cookie benutzt werden, um Nutzer*inneninformationen abzubilden. Der große Vorteil dieser Methode ist, dass diese Technologie unabhängig von Cookies, JavaScript und IP-Adresse funktioniert. Nutzer*innen müssten mit jedem Seitenaufruf ihren Browsercache erneut löschen, um dem Tracking aus dem Weg zu gehen (vgl. BVDW, 2015, S. 16-18). Wie schon eingangs im Abschnitt Web Storage erwähnt, ist ein großer Pluspunkt zudem, dass der Browser bei wiederholten Requests keine Inhalte mehr herunterladen muss, und somit die Leistung von Webanwendungen erheblich verbessert werden kann (vgl. F5, 2014, o. S.).

5.3.3.4 DNS-Cache

Das Webtracking, basierend auf dem DNS-Cache, nutzt ebenfalls die Möglichkeit von JavaScript, um indirekt einen DNS-Lookup auszulösen und dessen Zeit zu messen. Dieser Lookup dient dazu, einen Eintrag vom DNS-Server abzufragen. Mithilfe vom DNS können unterschiedliche Information abgefragt werden, unter anderem auch die IP-Adresse zu einer Domain gesucht werden und umgekehrt. Wenn eine bestimmte Website schon einmal aufgerufen wurde, ist der entsprechende Eintrag im DNS-Cache vorhanden und somit die Suchanfrage erheblich verkürzt (vgl. Bujlow et al., 2017, 1485; Domaintechnik, 2021, o. S.).

5.3.3.5 Operational-Cache

Unter Operational Cache versteht man Komponenten, welche zum Speichern von Informationen im Zusammenhang mit den von Browsern durchgeführten Operationen verwendet werden. Im Gegensatz zu anderen Trackingtechnologien erfolgt hier keine Speicherung der Kopien von heruntergeladenen Dateien. Die Informationen, welche im Operational-Cache erfasst werden, sind hauptsächlich folgende:

- Permanente Redirects (Weiterleitung auf eine andere Website)
- Authentifizierungsdaten
- Domains mit HTTP Strict Transport Security (HSTS)

(vgl. Bujlow et al., 2017, 1485).

Bujlow et al. (2017) beschreiben in ihrem Beitrag die verschiedenen Formen des Operation-Cache-Trackings. Diese werden folgend kurz beschrieben:

- HTTP 301 Redirect Cache: Dieser Mechanismus wurde grundsätzlich entwickelt, um dem Browser mitzuteilen, dass die angefragte Ressource unter einer anderen URL dauerhaft verfügbar ist. Der Redirect wird gespeichert und, anstelle der ursprünglichen Adresse, bei denselben Site-Requests dieser URL verwendet.
- HTTP-Authentifizierungs-Cache: In der Praxis gibt es zwei häufig verwendete HTTP-Authentifizierungsmechanismen. Erstens, die Basic Access Authentifizierung. Diese speichert die Anmeldedaten vorübergehend, damit sie beim nächsten Request des- oder derselben User*in automatisch im HTTP-Autorisierungsheader an den Server übermittelt werden kann.
- HTTP Strict Transport Security Cache: Dieser Mechanismus stellt eine weitere Methode dar, um eine Cookie-ähnliche Speicherung von User*inneninformationen vorzunehmen. Der aktuelle Standard von HSTS verlangt, dass Verbindungen zur Server-Domain über HTTPS anstelle von HTTP hergestellt werden (vgl. Bujlow et al., 2017, 1485).

5.3.4 Weitere alternative Webtracking Methoden

5.3.4.1 Common IDs/Universal IDs

Bei Common IDs handelt es sich um eine Technologie, welche die Nutzung von Web Angeboten mit Registrierung und Log-in voraussetzt. Registriert man sich bei einem bestimmten Webangebot, wird für jeden oder jede Nutzer*in eine eigene personenbezogene und eindeutige ID (Identifier) erstellt, mithilfe derer alle Informationen über die Besucher*innen gespeichert werden können. Nutzer*innen müssen hierzu aktiv ihr Einverständnis zur Speicherung und Verarbeitung der personenbezogenen Daten geben, beispielsweise durch Einwilligung der AGB bei der Registrierung. Wichtig in diesem Kontext zu erwähnen ist, dass die Zugangsdaten großer Portale nicht nur zur Anmeldung auf dem Portal selbst gültig sind, sondern eben auch auf anderen Websiten zur Authentifizierung benutzt

werden können, wie beispielsweise Facebook Connect oder auch die IDs anderer großer Identitätsverwalter wie Google, Microsoft und Yahoo, die sich auch an den OpenID-Standard halten (vgl. BVDW, 2015, S. 16). Viele dieser Log-in-Portale stellen zudem APIs (Programmierschnittstellen) bereit, mit denen dann Dritte, sogenannte Third Parties, auf die Identifier zugreifen können, sofern der oder die User*in mit demselben Browser bei der entsprechenden Seite angemeldet ist. Somit haben die Website-Betreiber*innen die Möglichkeit geschaffen, solche Features des Log-In-Portals in ihren Content zu integrieren, die über eine erleichterte Anmeldung hinausgeht. Als Beispiele hierfür können die Social-Plugins genannt werden, welche bei Twitter, XING, Facebook oder auch Pinterest zum Einsatz kommen. Auf Anfrage können diese Schnittstellen in der Regel eine eindeutige Kennung des oder der Portalnutzer*in zurücksenden. Drittanbieter*innen können dies dann dafür nutzen, um selbst einen Pool an Unique Identifiern aufzubauen und in Form eines gewöhnlichen Browser-Cookies diesen auf dem Endgerät der jeweiligen Nutzer*innen zu hinterlegen. Kehrt ein oder eine User*in auf dieselbe Website mit dem Log-in-Portal zurück, kann die ID dann neu abgefragt werden und das Nutzer*innenprofil des Tracking-Dienstes wiederhergestellt werden, falls in der Zwischenzeit die Cookies vom User oder von der Userin gelöscht wurden. Bei der ID handelt es sich um personenbezogene Informationen, mit denen man ein Nutzungsprofil erstellen kann, welches nicht nur über alle verfügbaren Browser auf einem Gerät, sondern eben auch über mehrere Endgeräte hinweg, eine Wiedererkennung des oder der User*in möglich macht. In Bezug auf die Privatsphäre der User*innen kann in diesem Zusammenhang gesagt werden, dass der oder die Nutzer*in den Gebrauch von Common IDs zur Profilbildung durch Dritte unterbinden kann, indem man sich nach Nutzung eines Log-in-Portals abmeldet und den Browser während des Log-in-Status nicht zum Besuch anderer Web-Angebote nutzt (vgl. ebd., 2015, S. 16). Bei der (Digitrust) Universal ID handelt es sich um einen standardisierten Token, welcher es Nutzer*innen ermöglicht, die über sie erhobenen Informationen selbstständig zu kontrollieren. Hiermit will man einen möglichst guten Kompromiss zwischen Datenschutz und Personalisierung finden und zum einen die Datenkontrolle auf Seite der User*innen ermöglichen und auf der anderen Seite wiederum den Datenzugriff seitens Unternehmen weiterhin gewährleisten (vgl. TrustedTargeting, 2021, o. S.).

5.3.4.2 Local Storage/Web Storage/DOM Storage

Der BVDW (2015) führt den Local Storage, auch Web-Storage bzw. DOM Storage genannt, als weitere alternative Webtracking Technologie an. Diese Methode bietet die Möglichkeit, lokal Daten über den Web-Browser zu speichern, welche auch nach Schließen der Sitzung oder dem Beenden des Browser-Programms weiterhin bestehen und jederzeit auch wieder ausgelesen werden können. Diese Methode war noch vor einigen Jahren nicht möglich, da es in JavaScript damals unmöglich war, Daten im lokalen Dateisystem eines Endgeräts, auf welchem der entsprechende Web-Browser installiert ist, zu lesen und/oder zu schreiben. Dies wurde zum einen aus Gründen des Datenschutzes untersagt, sowie zum anderen zur Vermeidung von Virusinfektionen unterbunden. Zu der Zeit war das klassische Cookie die einzig mögliche Methode, Daten abzulegen, auch wenn das Browserfenster geschlossen wurde, bzw. das Browser-Programm an sich beendet wurde. Das Problem dabei war aber, dass Cookies vor allem hinsichtlich ihrer Speicherkapazität stark beschränkt sind. Mithilfe von HTML5 wurde daher ein Verfahrensweg eingeführt, mittels dem sich Daten dauerhaft speichern lassen und ein Zugriff auf beliebige lokale Daten unmöglich ist. Die Web Storage Technologie wurde 2013 durch das World Wide Web Consortium, kurz W3C, standardisiert (vgl. W3C, 2021, o. S.). In diesem Kontext zu erwähnen ist, dass es für diese Art Daten zu speichern, grundsätzlich keine Größenbeschränkung gibt. Gegebenenfalls gibt es jedoch vereinzelt Browser-Typen, welche individuell ein bestimmtes Limit festlegen. Ein großer Vorteil bei dieser Methode ist, dass der HTML5 Local Storage sehr flexibel ist und ähnlich wie Cookies direkt dazu verwendet werden kann, um Daten über den oder die Nutzer*in zu speichern, sowie die User*innen wiedererkennbar zu machen, indem eine entsprechende ID im Local Storage abgelegt wird. Ein weiteres Merkmal ist, dass ähnlich wie bei der Common ID Methode, die Verwendung von Local Storage nur mit JavaScript möglich ist. Sobald User*innen JavaScript in ihren Browsern deaktivieren, wird damit auch die Möglichkeit des Trackings unterbunden. Dies beeinträchtigt allerdings auch die Nutzung vieler Websites. Bestimmte Browser-Anbieter, wie zum Beispiel Safari von Apple oder Mozilla Firefox, bieten für die Nutzer*innen Möglichkeiten zur Verwaltung von Local-Storage-Daten an, ähnlich wie bei Cookies. Diese Methode ermöglicht

es, alle Daten auflisten und auch löschen zu lassen. Laut BVDW (2015) können daher Werbetreibende und Publisher*innen nicht mehr generell davon ausgehen, dass die bestehenden Zugriffsbeschränkungen auf Third Party Cookies mithilfe der Local-Storage Technologie umgangen werden kann (vgl. BVDW, 2015, S. 18).

5.4 Benchmarking – Bewertender Vergleich zwischen Alternativen Webtracking Methoden, DSGVO und der Compliance von Datenaggregator*innen

Wie aus dem Literaturteil hervorgegangen ist, befindet sich der Markt rund um den Informations- und Datenaustausch aktuell in einer großen Umbruchphase. Während die einen Stakeholder sich nach besserem Schutz der Privatsphäre sehnen, wollen andere Parteien immer genauere und aussagekräftigere personenbezogene Daten sammeln und verwalten, um beispielsweise Zielgruppensegmente effizienter bilden zu können. Die folgende Benchmarking Analyse soll dazu dienen, die verschiedenen Dimensionen rund um das Thema Webtracking und DSGVO Compliance abzubilden. Außerdem werden die ausgewählten Unternehmen im Bereich der Datenaggregation untersucht und deren Übereinstimmung mit den vorformulierten Kategorien gewichtet.

Zur rechtlichen Einordnung wurden bestimmte Kriterien gebildet, welche dazu dienen sollen, Aussagen über die Art der erhobenen Daten zu treffen. Außerdem soll die Rechtssicherheit der alternativen Webtracking Methoden bewertet sowie das Verhalten der Datenaggregator*innen analysiert werden und Vergleiche zwischen den einzelnen Unternehmen möglich machen. Zudem soll auch Aufschluss über die Einfachheit der Implementierung der ausgewählten Technologien gegeben werden.

Aus der Theorie haben sich folgende Stakeholder im Zusammenhang mit dem Datenaustausch durch Webtracking ergeben:

- Aufsichtsbehörden (Datenschutzbehörden)
- Betroffene Personen/Endnutzer*innen
- Datenverantwortliche*r
- Datenverarbeiter*in
- Datenschutzbeauftragte*r
- Empfänger*in

Wichtig hierbei zu erwähnen ist, dass diese Stakeholder teilweise eigene Interessen vertreten, welche nicht selten in Konflikt miteinander stehen. Außerdem besteht oftmals ein bestimmter Grad an Informationsassymetrie zwischen den Unternehmen auf der einen Seite und den End-User*innen auf der anderen Seite.

Für das Benchmarking wurden eigene Dimensionen bzw. Kategorien entwickelt, welche im Hinblick auf das Compliance Management im Webtracking als wichtig erachtet werden. Der Fokus der Analyse liegt speziell auf dem Interessenskonflikt zwischen Unternehmen im Bereich des Daten- und Informationsaustausches und den betroffenen Personen bzw. den User*innen.

Als Überkategorien haben sich zum einen auf Seiten der User*innen bzw. betroffenen Personen der Schutz der Privatsphäre (siehe Tabelle 3) herauskristallisiert und zum anderen seitens der Datenaggregator*innen bzw. der Unternehmen die Notwendigkeit der Interaktion mit den Endnutzer*innen (siehe Tabelle 3 – Datenaggregator*innen und Tabelle 4 – Ausgewählte Unternehmen aus der Praxis). Die folgenden Auflistungen stellen die ausgearbeiteten Dimensionen übersichtlich dar:

Datenaggregator*innen-Perspektive	**User*innen-Perspektive**
Notwendigkeit d. Interaktion	**Schutz der Privatsphäre**
Allgemeine Funktionalität	User Identifikation
Cross-Device Tracking	Einwilligungsvorgehen
Cross-Browser Tracking	Widerrufsmöglichkeit
Implementierungsaufwand	Transparenz
Erstellung Zielgruppen-Segmente	Datensicherheit
Targetingeffizienz	
Datenumfang	
Lebensdauer	

Tabelle 3: Eigene Darstellung - Übersicht Benchmarking-Dimensionen – Interaktionsnotwendigkeit vs. Schutz der Privatsphäre

Ausgewählte Unternehmen
Google, Facebook, Adform, Cxense
Funktionalität Tracking Methode
Cross-Device Tracking
Cross-Browser Tracking
Implementierungsaufwand
Targetingeffizienz
Transparenz
Datenumfang
Lebensdauer
Einwilligungsverfahren
Widerrufsmöglichkeit

Tabelle 4: Eigene Darstellung - Übersicht Benchmarking-Dimensionen – Unternehmen im Bereich der Datenaggregation

5.4.1 Erläuterung der Codes / Bewertung

Nachfolgend werden die unterschiedlichen Dimensionen und die Einstufung der für das Benchmarking kurz beschrieben. Außerdem werden die Codes für die Bewertung zur besseren Nachvollziehbarkeit der Analyse erläutert. Der Wert 5 stellt hier immer den Höchst-/Bestwert dar. Aus Sicht der User*innen bedeutet dies dann beispielsweise bestmöglichen Schutz der Privatsphäre und aus Unternehmenssicht steht der höchste Wert beispielsweise für die größte Aussagekraft der Daten oder geringsten Implementierungsaufwand der Trackingtechnologie. Der Wert 1 hingegen stellt den schlechtesten Wert dar.

Datenaggregator*innen-Perspektive

Notwendigkeit der Interaktion mit User*innen:

(Allgemeine *Einordnung - Benchmarking: Wert 1 = geringe Wertschöpfung/geringster Nutzen bis Wert 5 = größte Wertschöpfung/größter Nutzen*)

- ***Allgemeine Funktionalität:***

  (*Einschätzung - Benchmarking: Wert 1 = geringster Grad an Funktionalität bis Wert 5 = höchster Grad an Funktionalität*)

  Vielfalt und Praktikabilität der technischen Eigenschaften und Möglichkeiten

- ***Cross-Device Tracking*:**

  (*Einschätzung - Benchmarking: Wert 1 = Cross-Device Tracking nicht umsetzbar Funktionalität bis Wert 5 = Aussagekräftiges Cross-Device Tracking möglich*)

  Einschätzung, ob eine geräteübergreifenden Analyse von Nutzer*innendaten mit der aktuellen Methode und den zur Verfügung stehenden Nutzungsdaten möglich ist

- ***Cross-Browser Tracking*:**

  (*Einschätzung - Benchmarking: Wert 1 = Cross-Browser Tracking nicht umsetzbar Funktionalität bis Wert 5 = Aussagekräftiges Cross-Browser Tracking möglich*)

  Einschätzung, ob eine browserübergreifende Analyse von Nutzer*innendaten mit der aktuellen Methode und den zur Verfügung stehenden Nutzungsdaten möglich ist

- ***Implementierungsaufwand*:**

  (*Einschätzung - Benchmarking: Wert 1 = hoher Implentierungsaufwand – Wert 5 = niedriger Implementierungsaufwand*)

  Zeit und Kosten des technischen Setups

- ***Erstellung Zielgruppen-Segmenten*:**

  (*Einschätzung - Benchmarking: Wert 1 = Einteilung in Zielgruppen-Segmente gar nicht bzw. nur bedingt möglich bis Wert 5 = Einteilung in Zielgruppen-Segmente leicht umsetzbar*)

  Möglichkeit zur Aufteilung in Zielgruppen nach bestimmten Kriterien

- ***Effizienz der* Targeting-Möglichkeiten:**

  (*Einschätzung - Benchmarking: Wert 1 = Targetingfunktionen stark eingeschränkt bis Wert 5 = umfangreiche Targetingfunktionen zur Verfügung)*

  Genauigkeit der Zielgruppen-Ansprache – Wie zuverlässig sind die Daten für eine Kategorisierung von potenziellen Käufergruppen?

- ***Datenumfang*:**

  (*Einschätzung - Benchmarking: Wert 1 = kleiner Datenpool und geringe Diversität der Daten bis Wert 5 = großer Datenpool und hoher Grad an Diversität der Daten*)

  Art und Umfang der Daten, welche mit der bestimmten Tracking Technologie gespeichert werden können

- ***Lebensdauer*:**

  (*Einschätzung - Benchmarking: Wert 1 = sehr kurze Speicherdauer der User*inneninformationen bis Wert 5 = sehr lange Speicherdauer der User*inneninformationen*)

  Lebens-/Speicherdauer der personenbezogenen Daten durch die eingesetzte Technologie

User*innen-Perspektive

Schutz der Privatsphäre:

(*Einordnung - Benchmarking: Wert 1 = geringster Schutz d. Privatsphäre bis Wert 5 = höchster Schutz*)

- ***User-Identifikation*:**

  (*Einschätzung - Benchmarking: Wert 1 = Aus Datenschutzperspektive (DSGVO) sehr fragwürdig bis Wert 5 = DSGVO konform und kompatibel*)

  Art der Benutzer*innenkennung zur Verknüpfung der Interaktionsdaten ein und desselben Nutzers bzw. derselben Nutzerin

- ***Einwilligungsvorgehen*:**

  (*Einschätzung - Benchmarking: Wert 1 = User*innen erlangen keine Kenntnis über Datenverarbeitung bis Wert 5 = User*innen geben ihr Einverständnis zur Datenverarbeitung und sind sich über Datenverarbeitung im vollen Umfang bewusst*)

  Art und Weise zur Einholung der Einwilligung zur Datenverarbeitung

- ***Widerrufsmöglichkeit*:**

  (*Einschätzung - Benchmarking: Wert 1 = Aus Datenschutzperspektive (DSGVO) sehr fragwürdig bis Wert 5 = DSGVO konform und kompatibel*)

  Möglichkeit für User*innen die Datenverarbeitung zu unterbinden

- ***Transparenz*:**

  (*Einschätzung - Benchmarking: Wert 1 = Nutzer*innen sind nicht in der Lage, nachzuvollziehen, was mit ihren Daten geschieht bis Wert 5 = Nutzer*innen erlangen umfangreiche Kenntnis über die Datenverarbeitung*)

  Barrierefreiheit und Zugang zu Datenschutzerklärungen & Nutzungsbedingungen

- ***Datensicherheit**:*

  (*Einschätzung - Benchmarking: Wert 1 = Stark personenbezogene Daten werden an Dritte weitergegeben ohne Kenntnis der User*innen bis Wert 5 = Daten werden nur unter Einverständnis und dem Bewusstsein der User*innen an Dritte weitergegeben)*

  Umfang sowie Art und Weise der Datenverarbeitung aus der Perspektive des Schutzes der Privatsphäre

Unternehmens-Perspektive

Funktionalität und Rechtssicherheit:

(*Einordnung Benchmarking: Wert 1 = geringste Funktionalität/geringe Rechtssicherheit – Wert 5 = größte Funktionalität/hohe Rechtssicherheit*)

- ***Funktionalität der aktuellen Tracking Methode*:**

  (*Einschätzung - Benchmarking: Wert 1 = geringster Grad an Funktionalität bis Wert 5 = höchster Grad an Funktionalität*)

  Wie praktikabel ist die aktuelle Tracking Methode im Hinblick auf das Geschäftsmodell?

- ***Cross-Device Tracking*:**

  (*Einschätzung - Benchmarking: Wert 1 = Cross-Device Tracking nicht umsetzbar Funktionalität bis Wert 5 = Aussagekräftiges Cross-Device Tracking möglich*)

  Einschätzung, ob eine geräteübergreifenden Analyse von Nutzer*innendaten mit der aktuellen Methode und den zur Verfügung stehenden Nutzungsdaten möglich ist.

- ***Cross-Browser Tracking*:**

  (*Einschätzung - Benchmarking: Wert 1 = Cross-Browser Tracking nicht umsetzbar Funktionalität bis Wert 5 = Aussagekräftiges Cross-Browser Tracking möglich*)

  Einschätzung, ob eine browserübergreifende Analyse von Nutzer*innendaten mit der aktuellen Methode und den zur Verfügung stehenden Nutzungsdaten möglich ist.

- ***Implementierungsaufwand:***

  (*Einschätzung - Benchmarking: Wert 1 = hoher Implentierungsaufwand – Wert 5 = niedriger Implementierungsaufwand*)

  Einschätzung betreffend Zeit und Kosten des technischen Setups

- ***Targetingeffizienz:***

  (*Einschätzung - Benchmarking: Wert 1 = Targetingfunktionen stark eingeschränkt bis Wert 5 = umfangreiche Targetingfunktionen zur Verfügung)*

  Genauigkeit *der Zielgruppen-Ansprache* – Wie zuverlässig sind die Daten für eine Kategorisierung von potenziellen Käufergruppen?

- ***Transparenz*:**

  (*Einschätzung - Benchmarking: Wert 1 = Nutzer*innen sind nicht in der Lage, nachzuvollziehen, was mit ihren Daten geschieht bis Wert 5 = Nutzer*innen erlangen umfangreiche Kenntnis über die Datenverarbeitung*)

  Barrierefreiheit und Zugang zu Datenschutzerklärungen & Nutzungsbedingungen für Stakeholder*innen

- ***Datenumfang*:**

  (*Einschätzung - Benchmarking: Wert 1 = kleiner Datenpool und geringe Diversität der Daten bis Wert 5 = großer Datenpool und hoher Grad an Diversität der Daten*)

  Art und Umfang der Daten, welche mit der aktuellen Tracking Technologie gespeichert werden können

- ***Lebensdauer*:**

  (*Einschätzung - Benchmarking: Wert 1 = sehr kurze Speicherdauer der User*inneninformationen bis Wert 5 = sehr lange Speicherdauer der User*inneninformationen*)

  Lebens-/Speicherdauer der personenbezogenen Daten durch die eingesetzte Technologie

- ***Einwilligungsverfahren:***

  (*Einschätzung - Benchmarking: Wert 1 = User*innen erlangen keine Kenntnis über Datenverarbeitung bis Wert 5 = User*innen geben ihr Einverständnis zur Datenverarbeitung und sind sich über Datenverarbeitung im vollen Umfang bewusst*)

  Art und Weise zur Einholung der Einwilligung zur Datenverarbeitung

- ***Widerrufsmöglichkeit*:**

  (*Einschätzung - Benchmarking: Wert 1 = Aus Datenschutzperspektive (DSGVO) sehr fragwürdig bis Wert 5 = DSGVO konform und kompatibel*)

  Möglichkeit für User*innen die Datenverarbeitung zu unterbinden

5.5 Auswertung – Alternative Methoden des Webtrackings

In diesem Abschnitt werden die Ergebnisse der Benchmarking-Analyse der alternativen Webtracking Methoden dargestellt und erläutert. Für jede einzelne ausgewählte Webtracking Methode wurden für eine übersichtliche Darstellung eigene Grafiken erstellt, welche nachfolgend genau beschrieben werden. Der Fokus hierbei liegt vor allem auf der Art und Weise, wie die entsprechende Einstufung im Kategoriensystem zustande gekommen ist. Als Grundlage für die Einordnung dient die identifizierte Forschungsliteratur zu den alternativen Methoden des Webtrackings (siehe Tabelle 2 sowie Abschnitt 5.3).

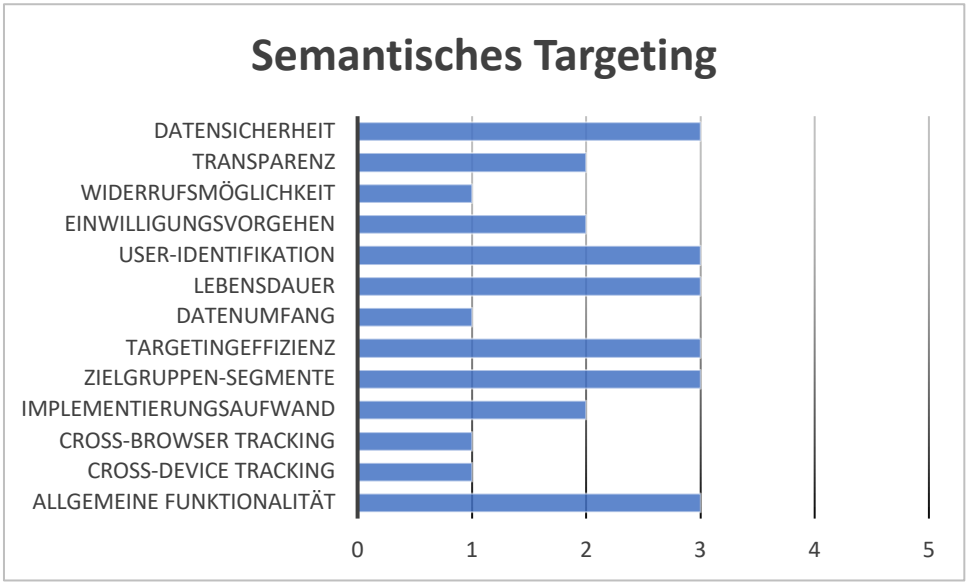


Abbildung 9: Eigene Darstellung - Benchmarking Semantisches Targeting

Abbildung 9 stellt das Ergebnis der Benchmarking-Analyse für die Methode des Semantischen Targetings dar. Der Umfang der erhobenen personenbezogenen Daten ist hier eher beschränkt und nicht so umfangreich wie bei anderen Tracking Lösungen. Dies führt in der Einstufung im Kategoriensicht aus Datenschutzsicht zu einer hohen Bewertung. Allerdings werden die Informationen meist ohne wirkliche Kenntnisnahme der User*innen erhoben und auf Grundlage dessen Zielgruppen-Segmente gebildet (vgl. Bauer et al., 2011, S. 12-13; Hillebrand, 2018, S. 229). Aus Sicht der Datenaggregator*in kann man folgern, dass der Datenumfang der personenbezogenen Informationen, relativ betrachtet, gering ist und auch die

Möglichkeit des Cross-Browser bzw. Cross-Device Tracking stark eingeschränkt ist. Andererseits stellt die Möglichkeit des Behavioral Targetings ein attraktives Feature für Unternehmen dar, weshalb die allgemeine Funktionalität auch mit dem Wert 3 angesetzt wurde.

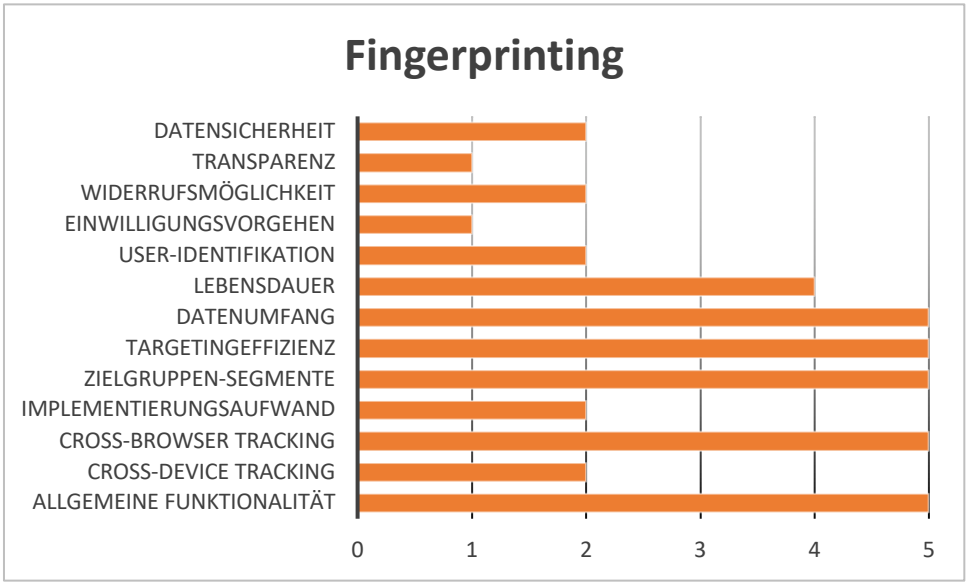


Abbildung 10: Eigene Darstellung - Benchmarking Fingerprinting

Die Fingerprinting Methode (Abb. 10) sticht vor allem durch ihre diversen Formen und der Datenvielfalt heraus. Neben diversen IDs (Endgerät, Browser, etc.), ist es zudem möglich, spezifische Settings auf den Endgeräten der User*innen zu identifizieren, welches eine hohe Aussagekraft der erhobenen personenbezogenen Daten mit sich zieht. Dadurch sind Unternehmen in der Lage, detaillierte Profile der Nutzer*innen zu erstellen und diese Daten weiter zu vermarkten. Die Kehrseite dieser Technologie ist aber, dass dieser Datenabgriff oftmals im Hintergrund geschieht. Dies führt zu der schlechten Bewertung in der Kategorie „Transparenz“. Vor allem das passive Fingerprinting ist für User*innen nur schwer nachzuverfolgen und kaum zu unterbinden (vgl. Bujlow et al., 2017, S. 1486). Für die Praxis scheint diese Tracking Methode eine der vielversprechendsten aus Sicht der Datenaggregator*innen und Publisher*innen zu sein. Die Analyse verdeutlicht dennoch, dass es hier einige offene Fragen in Bezug auf den Privatsphärenschutz von Endnutzer*innen gibt. Vor allem das Einwilligungsverfahren zur

Datenverarbeitung müsse aus Sicht des Verfassers eindeutig rechtlich geregelt werden, um somit mehr Transparenz zu schaffen.

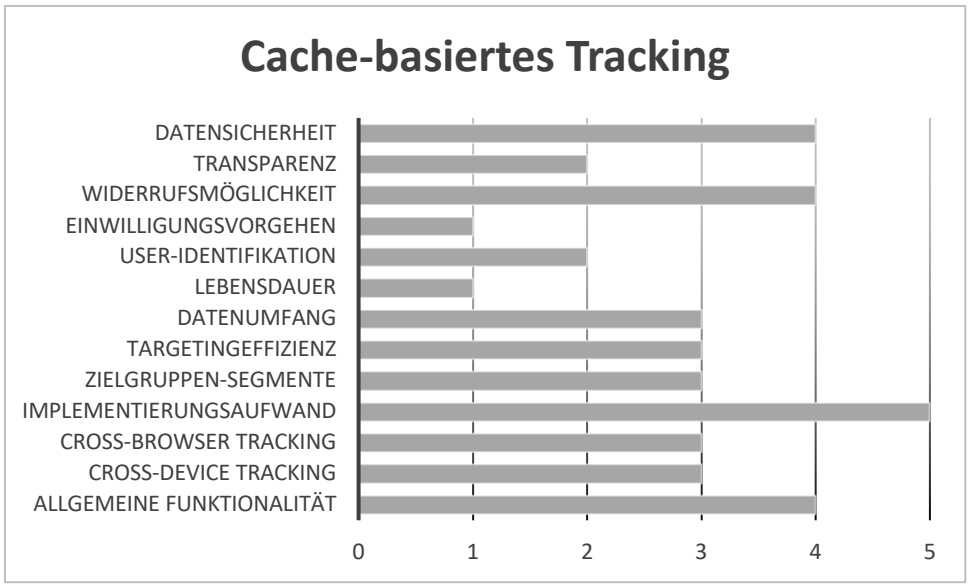


Abbildung 11: Eigene Darstellung - Benchmarking Cache-basiertes Tracking

Beim Cache-basierten Tracking (Abb. 11) werden ähnlich wie beim herkömmlichen Cookie Tracking clientbasierte Speicher zur Datengenerierung genutzt (vgl. Bujlow et al., 2017, S. 1485). Da User*innen die Möglichkeit haben, diese Speicher selbstständig zu löschen, wurde die Lebensdauer als gering eingestuft. Aufgrund dessen, dass die Speicherung der Daten allerdings browserseitig standardmäßig vorgenommen wird, ist die Bewertung des Einwilligungsvorgehens gleich gering anzusetzen. Diese Methode zeichnet sich vor allem durch die Datensicherheit aus, da User*innen, verhältnismäßig, autonom im Umgang mit ihren Daten sind. Vor allem der geringe Implementierungsaufwand und auch die Praktikabilität sprechen aus Unternehmens- bzw. Publisher-Sicht für diese Form des Webtrackings.

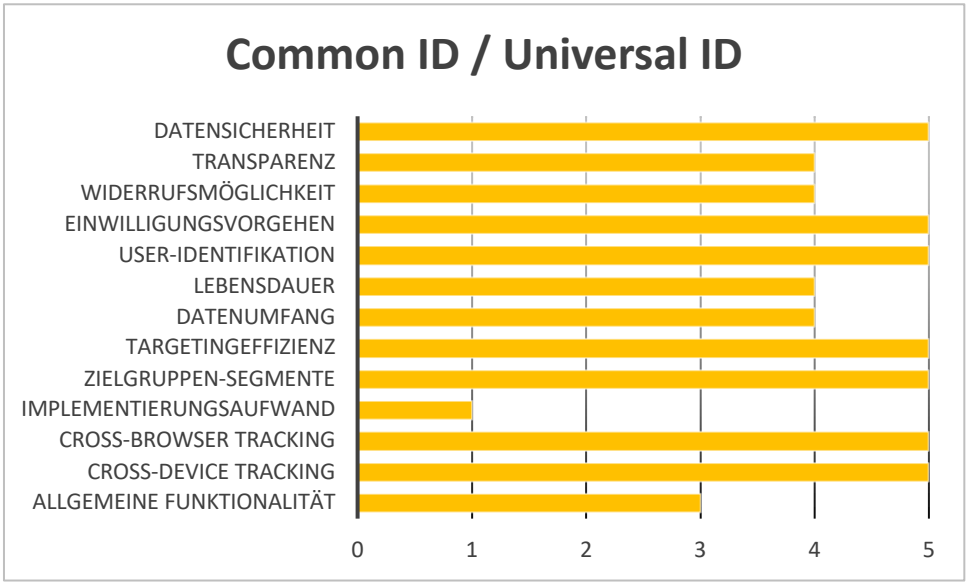


Abbildung 12: Eigene Darstellung - Benchmarking Common ID / Universal ID

Die Common ID bzw. Universal ID Lösungen konnten in der Benchmarking-Analyse das beste Ergebnis erzielen. Durch den Registrierungsprozess und LogIn kann zum einen aus Unternehmenssicht auf eine Vielzahl an Nutzungsdaten zurückgegriffen werden. Andererseits haben User*innen bei dieser Methode einen höheren Grad an Selbstbestimmtheit, weshalb diese Tracking Technologie auch aus Sicht des Datenschutzes, im Vergleich zu den anderen alternativen Methoden, auch gute Ergebnisse erzielt. Diese Methode stellt somit einen guten Kompromiss zwischen Privatsphärenschutz und zielgerichteter Datenverarbeitung dar (vgl. TrustedTargeting, 2021, o. S.).

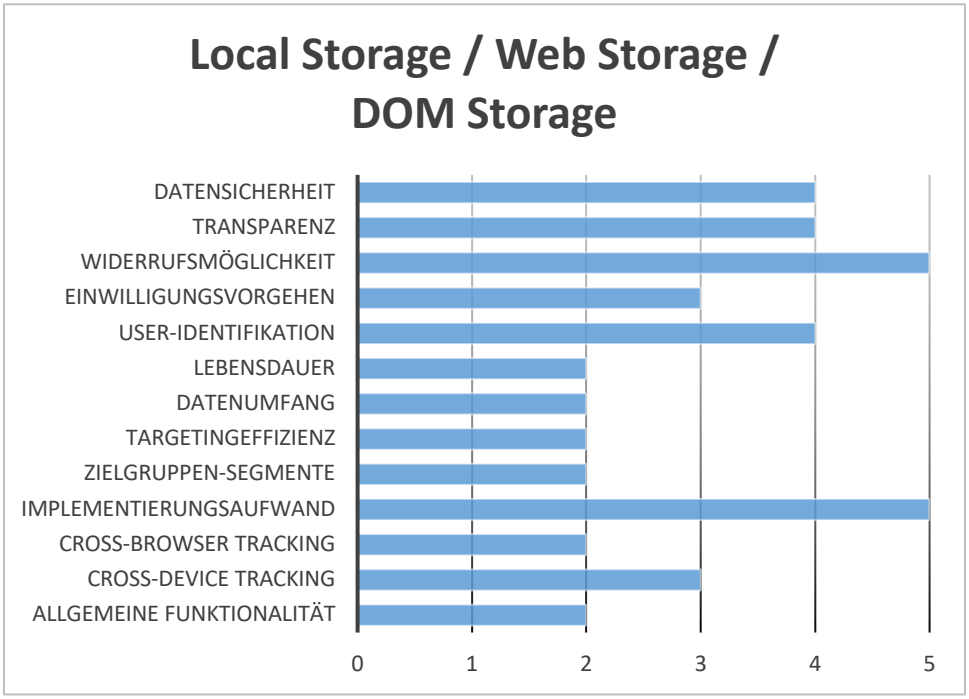


Abbildung 13: Eigene Darstellung - Benchmarking Local Storage/Web Storage/DOM Storage

Die Trackingmethoden basierend auf dem Storage des Web-Browsers stechen vor allem durch den geringen Implementierungsaufwand auf Unternehmensseite, und der einfachen Möglichkeit für User*innen, die Datenverarbeitung zu unterbinden, hervor. Die allgemeine Funktionalität ist allerdings gering zu bewerten, da diese Methode das Aktivieren von JavaScript voraussetzt. Sobald dies deaktiviert ist, wird das Tracking unterbunden. Dies führt aber auch zu einer Beeinträchtigung der Usability auf Nuter*innenseite (vgl. BVDW, 2015, S. 18).

Nachfolgendes Kreisdiagramm (Abb. 14) bildet das Endergebnis des Benchmarkings für die alternativen Methoden des Webtrackings ab. Zusammenfassend lässt sich sagen, dass sich vor allem zwei alternative Methoden des Webtrackings als vielversprechende Lösungen für den Ersatz des herkömmlichen Cookie Trackings hervorgetan haben: Common bzw. Universal ID und auch die Fingerprinting Methode. Während die Fingerprinting Technologien vor allem auf der Seite der Datenaggregator*innen die besten Werte erzielen konnten, stellt die ID-Lösung, die wohl am besten ausgeglichene Alternative dar. Hier bewahren User*innen ein hohes Maß an Selbstbestimmtheit, während Unternehmen und Publisher*innen eine Vielzahl an Möglichkeiten haben, Nutzungsdaten zu verarbeiten.

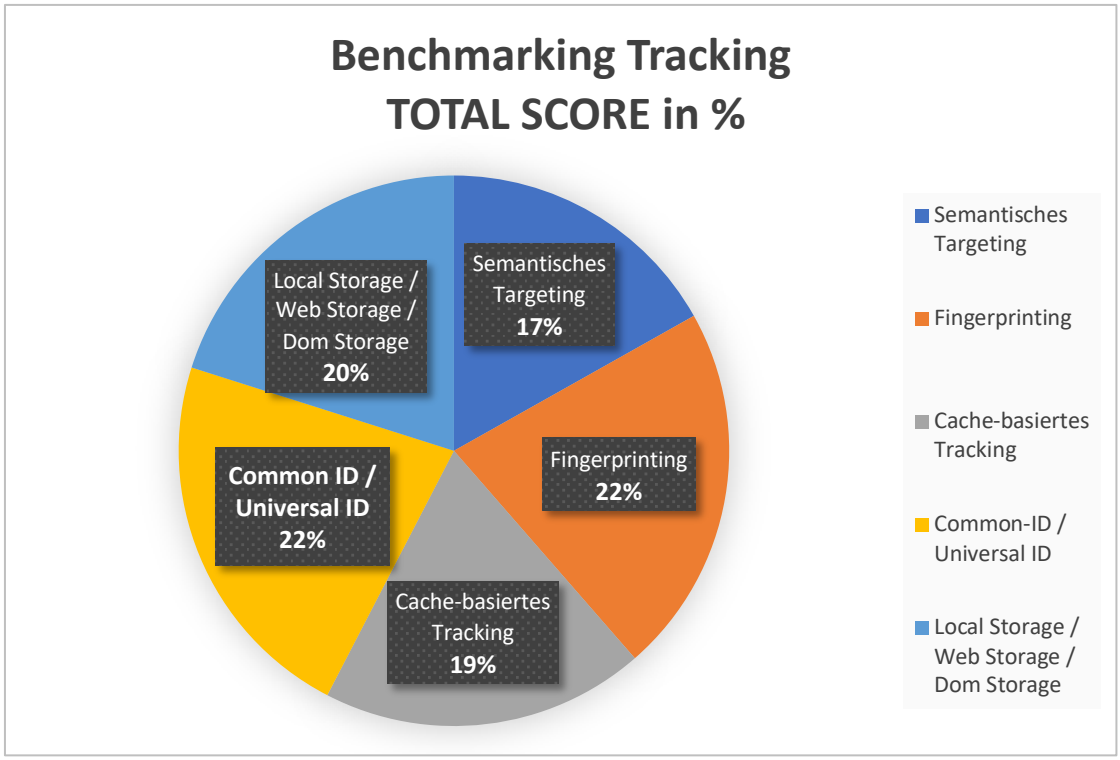


Abbildung 14: Eigene Darstellung – Total Score in %: Alternative Methoden d. Webtrackings

5.6 Auswertung – Unternehmen

In diesem Unterkapitel werden die Ergebnisse der Benchmarking Analyse der ausgewählten Unternehmen im Bereich der Datenaggregation vorgestellt. Besonderes Augenmerk lag hierbei auf der Art der Daten, die erhoben werden. Außerdem wurde untersucht, wie die Daten weiterverarbeitet werden, und ob dies auf Grundlage der Einwilligung von User*innen geschieht. Grundlage für die Bewertung waren zum einen die identifizierte Forschungsliteratur als auch die jeweiligen Datenschutzbestimmungen der Anbieter*innen.

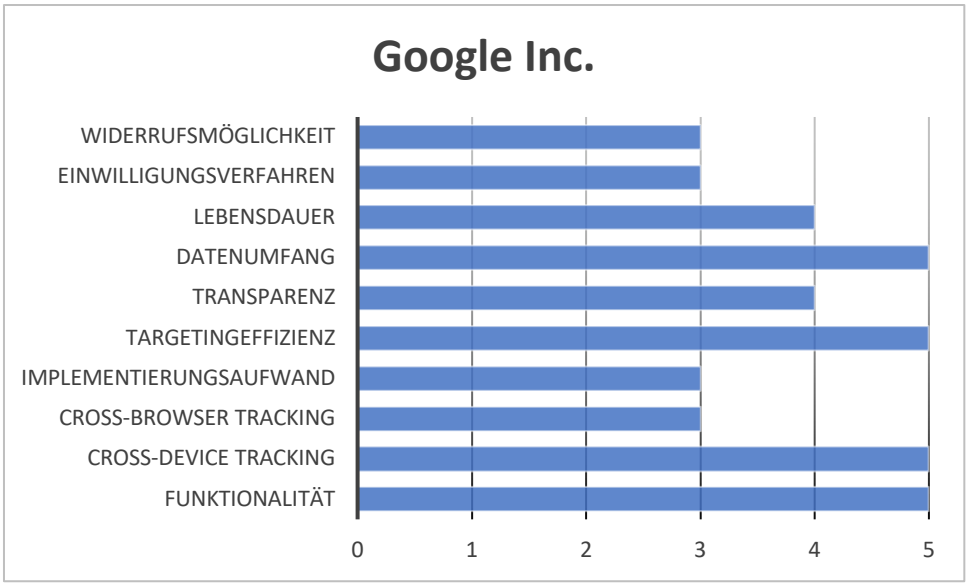


Abbildung 15: Eigene Darstellung - Benchmarking Google Inc.

Das Unternehmen Google konnte in der Benchmarking Analyse der Unternehmen die besten Ergebnisse erzielen (siehe Abb. 15). Dies hat sich bereits nach Sichtung der Forschungsliteratur abgezeichnet. Die riesige Marktmacht und die Verfügbarkeit eines riesigen Datenpools von User*inneninformationen führen dazu, dass dem Unternehmen beinahe eine Monopolmacht unterliegt, welche in den vergangenen Jahren erreicht wurde. Dies spiegelt sich auch in der Analyse wider. Der Datenumfang, den Google zur Verfügung hat, sucht weltweit seines gleichen. Diese Vielzahl als auch die Diversität der Informationen über User*innen, führt dazu, dass die Targetingmöglichkeiten besonders effizient sind. Zudem hat Google mit ihrem hauseigenen Browser Chrome eine effiziente Möglichkeit geschaffen, schnell und

unkompliziert, über den User-LogIn, an eine Vielzahl an personenbezogenen Daten zu kommen. Dieser, bereits bestehende, riesige Datenpool hat vermutlich auch zu der Entscheidung des Unternehmens geführt, in Zukunft auf die Verwendung von Cookies zu verzichten, um sich weiter von der Konkurrenz abzuheben. Außerdem ist Google in der Lage, durch ihre diversen Webserviceangebote, sowohl für Desktop als auch auf Mobile-Devices, ihre User*innen praktisch auf jedem End-Gerät nachzuverfolgen. Speziell in dieser Kategorie (Cross-Device Tracking) hebt sich das Unternehmen deutlich von der Konkurrenz ab.

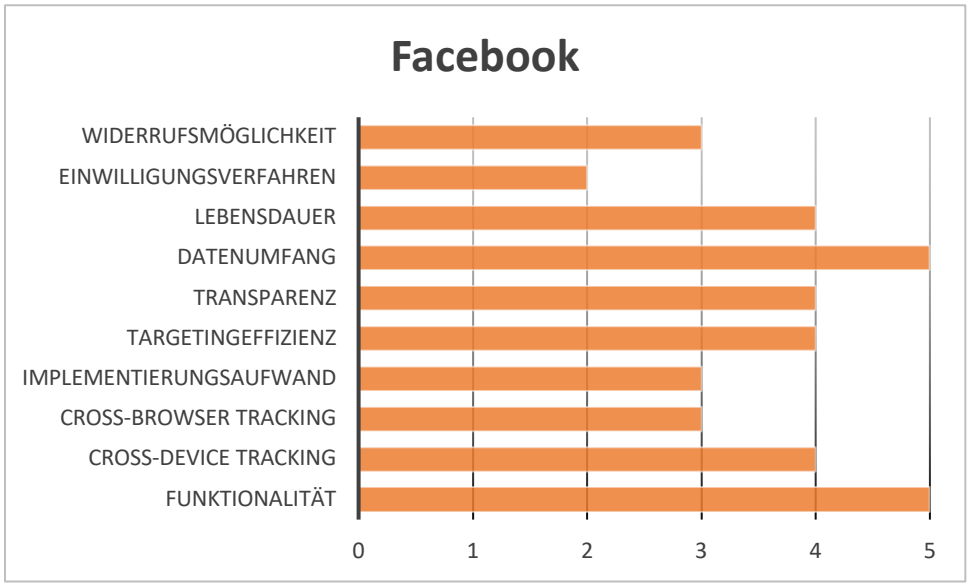


Abbildung 16: Eigene Darstellung - Benchmarking Facebook

In Abbildung 16 werden die Benchmarking-Ergebnisse des Unternehmens Facebook dargestellt. Facebook kann vor allem durch seine hohe Useranzahl (knapp 2,9 Mrd. Monthly Active Users, Stand: 1. Quartal 2021) auf dessen Social-Media Plattform, ähnlich wie Google, auf einen riesigen Datenpool zurückgreifen (vgl. Statista, 2021a, o. S.). Der Umfang der personenbezogenen Daten, welche vom Unternehmen Facebook erfasst werden, kann aus Abschnitt 2.4.2.2 entnommen werden. Auch die Funktionalität der Trackingmethoden ist hoch einzustufen, da durch den User*innen-LogIn eine Vielzahl an personenbezogenen Daten preisgegeben wird. Auffällig in der Analyse war, dass die Datenschutzbestimmungen, sowohl von Google als auch von Facebook, sehr

detailliert und auch leicht nachvollziehbar für den oder die Endnutzer*in sind. Deshalb wurde die Bewertung in der Kategorie „Transparenz“ gleich hoch festgelegt wie bei Google. Der Zugang zu den Datenschutzerklärungen wurde mit dem Wert Vier eingestuft, da die Datenschutzbestimmungen leicht auffindbar und zugänglich sind. Das Einwilligungsverfahren wurde mit einer durchschnittlichen Bewertung festgelegt, da User*innen beim Opt-In aus Erfahrungswerten aus der Praxis, zwar die Möglichkeit zur Einsicht der Datenschutzbestimmung haben, dies aber im Zuge des Registrierungsprozesses aus Zeitgründen wahrscheinlich nicht wahrnehmen (vgl. Europäische Kommission, 2019, o. S.).

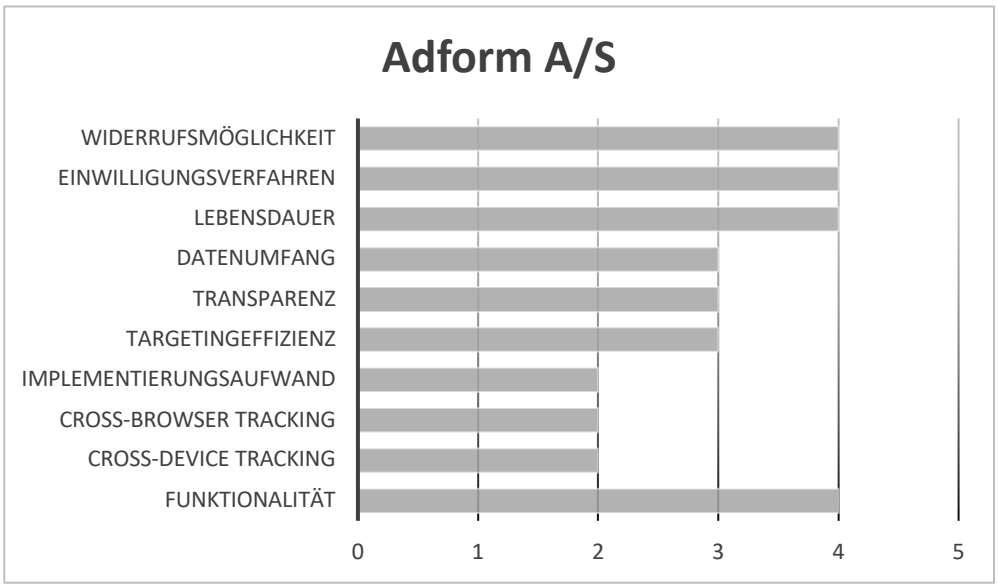


Abbildung 17: Eigene Darstellung - Benchmarking Adform A/S

Das Unternehmen Adform kann vor allem in den Kategorien Widerrufsmöglichkeit, Einwilligungsverfahren, Lebensdauer und Funktionalität punkten und bei diesen Dimensionen einen Wert von Vier des Benchmarkings erreichen (siehe Abb. 17). Vor allem ihre hauseigenen ID-Lösungen sprechen für eine hohe Funktionalität (vgl. Adform, 2021b, S. 1-8). Der Implementierungsaufwand kann als mittelmäßig eingestuft werden, da die Plattform für Publisher*innen, aus Erfahrungswerten des Verfassers aus der Praxis, ein hohes Maß an Usability aufweisen kann. Cross-Browser sowie Cross-Device Tracking sind aufgrund der Art der Trackingtechnologien und der geringeren Datenmenge, welche den Kund*innen von Adform zur Verfügung

stehen, nur eingeschränkt möglich. Hierzu müssen andere Technologie-Anbieter hinzugezogen werden.

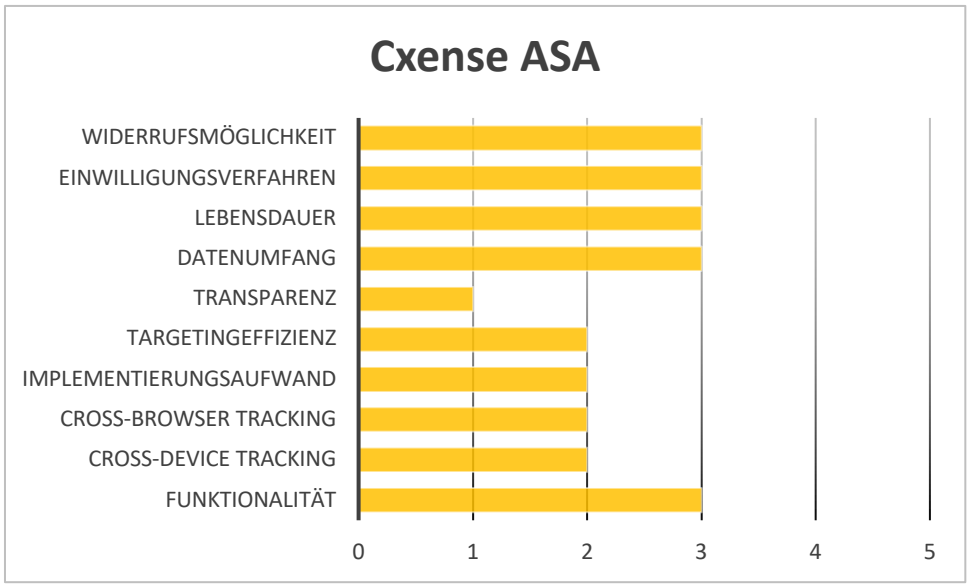


Abbildung 18: Eigene Darstellung - Benchmarking Cxense ASA

Abbildung 18 veranschaulicht die Resultate der Benchmarking-Analyse des Unternehmens Cxense ASA. Besonders auffällig in der Untersuchung war, dass die Darstellung und Aufbereitung der Datenschutzerklärung, in Hinblick auf die Benutzer*innenfreundlichkeit, im Vergleich zu den anderen Datenaggregator*innen stark abfällt. Hier bedarf es das Layout der Seite optisch übersichtlicher und ansprechender zu gestalten. Die großen Unternehmen, wie Google oder Facebook, können in diesem Aspekt als Vorreiter gesehen werden. Deshalb wurde die Transparenz als gering eingestuft. In den Dimensionen Widerrufsmöglichkeit, Einwilligungsverfahren, Lebensdauer, Datenumfang sowie Funktionalität konnten durchschnittliche Werte erzielt werden. Im Vergleich zu den anderen Unternehmen fällt das Unternehmen in der Analyse ein wenig ab. Als Webtrackingmethode kommt bei Cxense die klassische Cookie-Methode zum Einsatz. User*innen können das Setzen der Cookies zwar unterbinden, das Einwilligungsverfahren ist, aus Sicht der Nutzungsfreundlichkeit, aber verbesserungswürdig und sollte umfangreicher und informativer gestaltet werden.

Im Folgenden wird der Gesamtscore (in %) des Unternehmens-Benchmarking in einem Kreisdiagramm übersichtlich dargestellt (siehe Abb. 19). Das Unternehmen Google hat aufgrund des großen Datenumfangs sowie der praktikablen Möglichkeit des Cross-Device Trackings und der Funktionalität am besten abgeschnitten. Auf Platz Zwei mit 26 % steht Facebook, gefolgt von Adform und zuletzt das Unternehmen Cxense. Aus der Datenschutzperspektive und dem Umgang mit personenbezogenen Daten ist jedoch das Unternehmen Adform hervorzuheben, welches in den Datenschutz-Dimensionen am besten abgeschnitten hat.

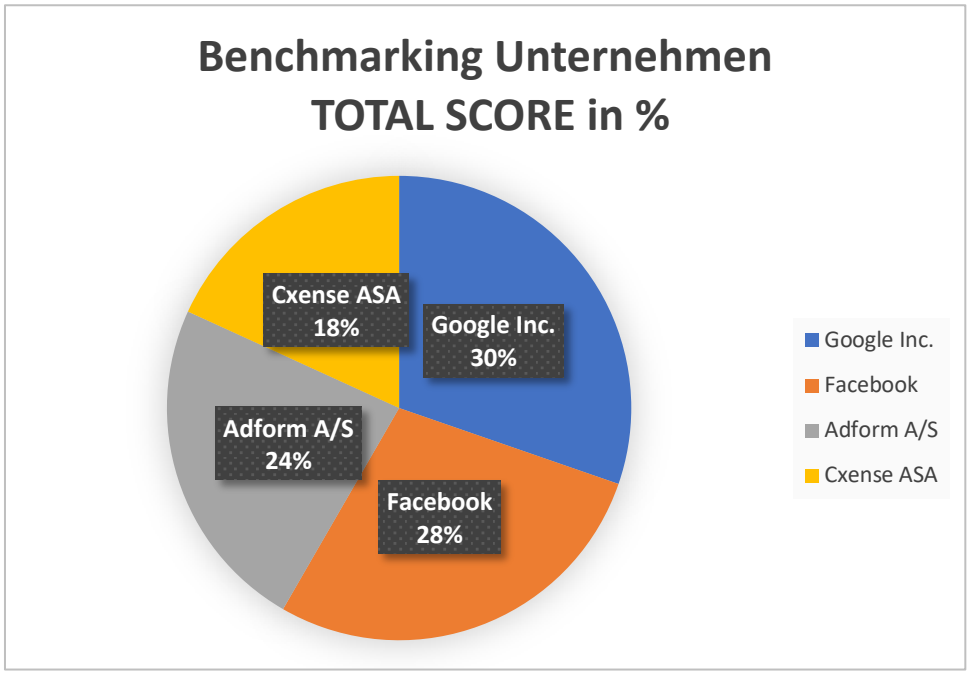


Abbildung 19: Eigene Darstellung - Total Score in %: Unternehmen im Bereich d. Datenaggregation

5.7 Handlungsempfehlungen

Die Benchmarking Analyse hat den großen Interessenskonflikt und vor allem die Informationsassymetrie zwischen Unternehmen bzw. Publisher*innen und Endnutzer*innen bestätigt. Zur Schließung dieser Lücke bedarf es gezielter Compliance Maßnahmen, um sich in Bezug auf den Datenschutz rechtskonform zu verhalten. Deshalb hat sich der Verfasser dieser Arbeit dazu entschlossen, bestimmte Maßnahmen zu formulieren, welche für die Praxis als relevant angesehen werden könnten und den Privatsphärenschutz von User*innen zu verbessern. Die Untersuchung verdeutlicht, dass je mehr Daten gesammelt werden, wie beispielsweise bei den großen Unternehmen, wie Facebook oder Google, umso weniger Einblick haben Nutzer*innen darauf, was letztendlich mit den personenbezogenen Daten geschieht. Zwar stechen diese Institutionen mit ihren ausführlichen Datenschutzbestimmungen im Vergleich zu kleineren Anbieter*innen heraus, dennoch haben Nutzer*innen bei den diversen Trackingtechnologien keinen Einblick darauf, wie groß der Datenumfang tatsächlich ist. Die Datenerhebung geschieht bei den meisten Verfahren im Hintergrund und automatisch schon bevor dem oder der User*in dies bewusst ist. Außerdem scheint es oftmals undurchsichtig, wie viele Daten tatsächlich ohne Kenntnis der User*innen an Dritte weitergegeben werden.

Tinnefeld et al. (2019) untermauern, dass gezielte Maßnahmen und Verhaltensregeln für Unternehmen, geeignet sind, den Gedanken der Datenschutz-Compliance voranzutreiben (vgl. Tinnefeld et al., 2019, S. 41). Unabhängig, welche Trackingtechnologie letztendlich zum Einsatz kommt. Folgend werden die sich aus dieser Arbeit herauskristallisierten wichtigsten Maßnahmen und Anforderungen an das Compliance-Management rund um die Verarbeitung von personenbezogenen Daten übersichtlich angeführt:

1. Einheitlicher Verhaltenskodex und unternehmensweite Datenschutzregelungen (vgl. Bay & Hasenrath, 2016, S. 139-141; Tinnefeld, 2019, S. 41)
2. Angemessener Umgang mit Betroffenenrechte – Informationspflicht
3. Privacy by Design (Konkrete Gestaltung der Datenverarbeitung): Minimierung der Verarbeitung von personenbezogenen Daten,

Pseudonymisierung personenbezogener Informationen und Schaffung von Transparenz bezüglich Funktion und Verarbeitung der Daten (vgl. Bauer, 2017, S. 9)

4. Privacy by Default (Datenschutzrechtliche Voreinstellung): Daten werden nur für den vorgesehen Zweck verwendet (vgl. Bauer, 2017, S. 9)
5. Monitoring und gezielte Verbesserungsmaßnahmen (vgl. Kreipl, 2020, S. 172)
6. Automatisierte Compliance-Analysen zur besseren Handhabung von großen Datenmengen (vgl. Erwin et al., 2013, S. 60)
7. Einheitliches Vokabular (ODRL, DPV oder GDPRtEXT) zur Erstellung von Datenschutz-Richtlinien (vgl. Esteves & Rodríguez-Doncel, 2021, S. 19-20)
8. Standardisierte Datenmodelle (vgl. EDPS, 2016, o. S.)
9. Ausführliche Dokumentation der Datenverarbeitung
10. Datenschutzsensibilisierung, insbesondere Schulungen zum Thema Datenschutz innerhalb von Unternehmen sowie Bestellung eines DSB
11. Angemessenes Datenschutzaudit
12. Datenschutzzertifikate (Bsp.: ISO Datenschutzstandards)

Diese Punkte sollen als eine Art Orientierungshilfe für Publisher*innen und Unternehmen dienen, um die aus dem Benchmarking hervorgegangene Lücke der Informationsassymetrie zu schließen. Die Vollständigkeit der Liste kann an dieser Stelle nicht gewährleistet werden und bedarf noch weiterer Überarbeitung und zusätzlicher Forschung (Anm. d. Autors).

6 Diskussion

In diesem Abschnitt der Arbeit werden nun die Erkenntnisse der Literaturrecherche mit den Ergebnissen der Benchmarking Analyse verglichen und diskutiert. Im Zuge dessen wird auch versucht, die eingangs formulierte Forschungsfrage sowie die weiteren Unterfragestellungen zu beantworten.

Um die Vereinbarkeit von alternativen Methoden des Webtrackings und der DSGVO zu untersuchen, wurde eine Benchmarking Analyse anhand von verschiedenen Dimensionen aus der Perspektive von Endnutzer*innen sowie Datenaggregator*innen durchgeführt. Insgesamt wurden fünf ausgewählte Technologien als Alternative zum klassischen Cookie Tracking untersucht. Hierzu wurden aus der zuvor revidierten Forschungsliteratur relevante Dimensionen abgeleitet, um die Bewertungen einordnen zu können. Aus Sicht der Unternehmen im Bereich der Datenverarbeitung scheint die Methode des Fingerprintings am vielversprechendsten. Diese sticht vor allem durch den Umfang der Datenerfassung und damit einhergehenden Targeting Möglichkeiten hervor. Aus Nutzer*innensicht und deren Schutz der Privatsphäre erscheint diese Methode allerdings als fragwürdig, da die Daten meist automatisch im Hintergrund erfasst und verarbeitet werden, was wiederum zu einer geringen Transparenz führt. Technologieanbieter*innen wie das Unternehmen Adform A/S haben hingegen bereits eigene ID-Lösungen zur User*innenverfolgung auf den Markt gebracht, welche der Technologie Universal ID/Common ID zuzuordnen sind (vgl. Adform, 2021b, o. S.). Diese Trackinglösung hat sich in der durchgeführten Analyse als beste Alternative bewährt. Vor allem der gute Kompromiss zwischen Funktionalität und Anwendungsfelder im Hinblick auf die Nachverfolgung von Nutzer*innen auf Unternehmensseite und dem Aufrechterhalten des Schutzes der Privatsphäre, sowie der Autonomie von User*innen, spricht für diese Art des Webtrackings. Das Unternehmen Google scheint dies in der Vergangenheit schon früh erkannt zu haben und hat mit ihrem hauseigenen Browser Chrome eine Benchmark geschaffen, die seinesgleichen sucht. Da ein Großteil der User*innen (über 70 % weltweit) diesen Browser tagtäglich verwenden und meist in Kombination eines Google-Kontos, welche einen Registrierungsprozess voraussetzt, ist es möglich, einfach und unkompliziert an personenbezogene und sensible Daten zu gelangen. Mithilfe

dieser ist man in der Lage ausführliche Nutzungsprofile erstellt werden, welche teuer an Dritte vermarktet werden können. Es bleibt spannend, wie sich der Online-Markt entwickeln wird, wenn das Unternehmen Google ihre geplanten Änderungen in Bezug auf das Webtracking umsetzt. Die neue Technologie FLoC (Federated Learning of Cohorts) von Google führt zu einem kritischem Diskurs in der Branche und ist auch aus wettbewerbsrechtlicher Sicht in Frage zu stellen. Bei dieser Methode soll schließlich gänzlich auf die Verwendung von Drittanbieter Cookies verzichtet werden, auf denen der Online-Markt und das digitale Marketing rundherum aktuell hauptsächlich aufbaut (vgl. Ravichandran & Vassilvitskii, 2021, S. 1-17; Geradin & Katsifis, S. 1-12).

Wie bereits in der Forschungsliteratur hervorgegangen ist, herrscht in der Praxis generell ein großes Maß an Informationsassymetrie im Bereich der Datenverarbeitung im Internet (vgl. Jabobi et al., 2019, S. 312). Jakobi et al. (2019) verdeutlichen in ihrer Studie, dass häufig im Hintergrund personenbezogene Daten erfasst und verarbeitet werden. Meist sogar ohne vorherige ausdrückliche Einwilligung der Nutzer*innen (vgl. ebd., 2019, S. 310-319). Geradin und Katsifis (2021) kommen in ihrem Forschungsbeitrag zum selben Ergebnis, speziell in Bezug auf das Unternehmen Google (vgl. Geradin & Katsifis, 2020, S. 1-12). Die Benchmarking Analyse der alternativen Methoden des Webtrackings ergab, dass die in der Literatur existierenden Annahmen (Jakobi et al. 2019; Geradin & Katsifis, 2020) bestätigt werden können. Es bleibt abzuwarten, wie sich der Markt rund um die Datenverarbeitung von personenbezogenen Informationen in den kommenden Jahren entwickeln wird.

Außerdem hatte diese Arbeit zum Ziel, das Datenverarbeitungsverhalten von Unternehmen im Hinblick auf deren Informationspflichten im Umgang mit personenbezogenen Daten zu analysieren. Jakobi et al. (2019) gehen in ihrer Forschungsarbeit auf diese Thematik ein und erläutern, dass nach wie vor ein großer Bedarf an einer Aufklärung, über die Ausgestaltung und den Einsatz von diversen Trackingtechnologien, besteht (vgl. Jakobi et al., 2019, S. 310-319). Die empirische Untersuchung konnte dies untermauern. Vor allem bei den Fingerprinting Technologien geschieht der Datenabgriff oftmals im Hintergrund, ohne Kenntnis der Endnutzer*innen. Hier scheint es notwendig, die geltenden Datenschutzvorschriften zu präzisieren und mit neuen Rechtsnormen zu erweitern,

wie beispielsweise der geplanten ePrivacy Verordnung (vgl. Gradow & Greiner, 2021, S. 32-33).

Esteves und Rodríguez-Doncel (2021) heben in ihrem Forschungsbeitrag den Bedarf eines einheitlichen Vokabulars im Zusammenhang mit Datenschutzrichtlinien, wie der DSGVO, hervor. Hierzu schlagen sie vor allem als REL die ODRL, DPV und GDPRtEXT als praktikable Lösungsansätze vor. Eine Standardisierung der verwendeten Sprache würde sich positiv auf die Transparenz, das Einwilligungsverfahren sowie generell auf das Verständnis von User*innen, über das Ausmaß der Datenverarbeitung und des Informationsflusses, auswirken. Dieser Handlungsbedarf wurde durch die durchgeführte Analyse ebenfalls aufgedeckt und bestätigt.

7 Fazit

Ziel dieser Arbeit war es, Methoden des Webtrackings zu identifizieren, welche in Zukunft die gängige Form des klassischen Cookie Trackings ersetzen könnten und zu evaluieren, wie diese Technologien in Einklang mit der DSGVO stehen. Außerdem wurden die ausgewählten Methoden auf deren Praktikabilität aus Sicht der Unternehmen untersucht sowie das Verhalten von Datenaggregator*innen und der Umgang mit personenbezogenen Daten überprüft. Aus User*innensicht wurde außerdem die Perspektive des Privatsphärenschutzes und die Kenntlichmachung der Technologien analysiert.

Die Ergebnisse der Analyse zeigen, dass das Fingerprinting die praktikabelste Technologie für Unternehmen zu sein scheint, da der Datenumfang, welche erfasst werden können, am größten ist. Dies lässt aussagekräftige Analysen zu und detaillierte Nutzungsprofile der User*innen erstellen. Dennoch konnte die ID-basierte Webtracking Methode (beispielsweise Universal ID/Common ID) die höchste Punktzahl im Benchmarking erzielen, da diese einen guten Kompromiss zwischen Praktikabilität auf der einen Seite und Privatsphärenschutz aus Endnutzer*innensicht auf der anderen Seite zulässt. Dies spiegelt sich auch in der Forschungsliteratur wider. Hinsichtlich der Vereinbarkeit mit der DSGVO konnte vereinzelt eine Diskrepanz zwischen Datenverarbeitungsvorgängen und der Einwilligung von Nutzer*innen festgestellt werden. Oftmals geschieht die Nutzungsdatenerfassung im Hintergrund und User*innen können nur erschwert erkennen, wann diese Datenaufzeichnung beginnt und wann sie endet. Zudem ist es aus User*innensicht oftmals impraktikabel den Widerruf zur Datenverarbeitung vorzunehmen. Es herrscht zudem in der Forschung Konsens darüber, dass trotz der geänderten rechtlichen Rahmenbedingungen im Bereich des Datenschutzes, nach wie vor eine große Informationsassymetrie zwischen Unternehmen und Nutzer*innen vorliegt. Dies konnte durch die durchgeführte Analyse in dieser Arbeit bestätigt werden. Für die Praxis wurde ein Maßnahmenkatalog vorformuliert, welcher aus der Sicht des Verfassers als Anhaltspunkt dienen kann, um das Compliance Management von Unternehmen auszubauen und zu verbessern. Außerdem besteht ein großer Bedarf an der Schaffung einer größeren Transparenz, wenn es um die Verarbeitung von personenbezogenen Daten geht. Hierzu gibt es bereits einige technische Lösungsansätze, welche in dieser Arbeit aufgegriffen

wurden. Außerdem wird es notwendig sein, das Vokabular für die Verfassung von zukünftigen Rechtsvorschriften zu vereinheitlichen, um somit auch für User*innen mehr Klarheit und Nachvollziehbarkeit schaffen zu können.

7.1 Limitationen

In dieser Arbeit konnten nicht alle möglichen Alternativen des Webtrackings für die Analyse herangezogen werden. Lediglich die eingangs ausgewählten Technologien wurden untersucht und mit der DSGVO in Verbindung gesetzt. Zudem konnten nur wenige ausgewählte Unternehmen im Bereich der Datenaggregation analysiert werden. Eine Analyse von weiteren Technologien als auch Unternehmen ist im Rahmen dieser Arbeit nicht möglich, da dies den Umfang dieser Arbeit überschreiten würde. Daher können keine allgemein validen Aussagen für die Praxis getroffen werden. Um die genannten Erkenntnisse zu untermauern, ist daher zusätzliche empirische Forschung erforderlich. Eine weitere Limitation der Arbeit ist zudem der Mangel an aktueller Forschungsliteratur über die spezifischen Technologien.

7.2 Ausblick

Die durchgeführte Analyse lässt erste Annahmen zu, welche Technologien in der Zukunft das klassische Cookie Tracking ersetzen könnten. Dennoch besteht der Bedarf für zukünftige Forschungen, die Untersuchung durch weitere Technologien zu erweitern. Außerdem müsste das Verhalten von weiteren Unternehmen im Bereich der Datenaggregation analysiert werden, um aussagekräftigere und valide Erkenntnisse zu erhalten. Vor allem aufgrund der sich stetig ändernden rechtlichen Rahmenbedingungen sowie der schnelllebigen Technologie und des rasanten digitalen Fortschritt bedarf es hier weiterer Forschungsarbeit. Zudem ist offen, wie sich der Markt verändern wird, wenn es zu der geplanten Einführung der ePrivacy-Verordnung kommt und Google seine Pläne, gänzlich auf Third Party Cookies zu verzichten, tatsächlich in die Realität umsetzt.

8 Literaturverzeichnis

Adform. (2021). About Adform. Online: https://site.adform.com/company/about-adform/, Zugriff: 16.08.2021.

Adform. (2021a). Datenschutzrichtlinie für Produkte und Services. Online: https://site.adform.com/de/privacy-center/platform/datenschutzrichtlinie-fuer-produkte-und-services/, Zugriff: 16.08.2021.

Adform. (2021b). Whitepaper – Driving A New Era of ID Management. Online: https://site.adform.com/knowledge-center/white-papers/the-1st-party-solution-a-new-era-of-id-management/, Zugriff: 25.08.2021.

AEUV. (2012). Vertrag über die Arbeitsweise der Europäischen Union. Online: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:12012E/TXT:de:PDF, Zugriff: 30.04.2021.

Agogo, D. (2020). Invisible market for online personal data: An examination. Electronic Markets. https://doi.org/10.1007/s12525-020-00437-0

Artikel-29-Datenschutzgruppe. (2010). Stellungnahme 1/2010 v. 16.02.2010 zu den Begriffen „für die Verarbeitung Verantwortlicher“ und „Auftragsverarbeiter“ Online: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_de.pdf. Zugriff: 13.08.2021.

Artikel-29-Datenschutzgruppe. (2013). *Stellungnahme 6/2013 v. 05.06.2013 zu den Offenen Daten („Open Data“) und der Weiterverwendung von Informationen des öffentlichen Sektors („PSI“)*. Justiz und Verbraucher. Europäische Kommission. ISSN 2363-1015

Aydin, V. & Lehrmann, M. (2019). Whitepaper – Das Ende des Online-Marketing durch EuGH Urteil?. Online: https://www.trustedtargeting.com/whitepaper-eughcookies, Zugriff: 10.04.2021.

Barth, G. (2020). *Der Kampf um die Werbung im Internet: Online-Werbung, ihre Blockade und Schutzmaßnahmen vor Werbeblockade auf dem Prüfstand des Lauterkeits- und Urheberrechts mit Bezügen zum Datenschutz- und Kartellrecht*. Nomos Verlagsgesellschaft mbH & Co. KG. https://doi.org/10.5771/9783748908227

Bauer, A. (2017). 10 Schritte zur Datenschutz-Compliance. Online: https://www.lansky.at/fileadmin/content/PDF/LGP_News_12/LGPNews12_D_S8ff_Bauer.pdf.pdf, Zugriff: 25.08.2021.

Bauer, C. Greve, G. & Hopf, G. (2011). Einführung in das Online Targeting. In C. Bauer, G. Greve, & G. Hopf (Hrsg.), *Online Targeting und Controlling: Grundlagen – Anwendungsfelder – Praxisbeispiele* (1. Aufl.). Gabler Verlag.

Bay, K.-C., & Hastenrath, K. (2016). Compliance-Management-Systeme. *Praxiserprobte Elemente, Prozesse und Tools, München*.

Bielova, N. (2017). Web Tracking Technologies and Protection Mechanisms. *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, 2607–2609. https://doi.org/10.1145/3133956.3136067

Brockmann, H.-C. (2018). Effizientes und verantwortungsvolles Datenmanagement im Zeitalter der DSGVO: Technisch-organisatorische Herausforderungen. *Datenschutz und Datensicherheit - DuD*, *42*(10), 634–639. https://doi.org/10.1007/s11623-018-1015-0

Bujlow, T., Carela-Espanol, V., Lee, B.-R., & Barlet-Ros, P. (2017). A Survey on Web Tracking: Mechanisms, Implications, and Defenses. *Proceedings of the IEEE*, *105*, 1510. https://doi.org/10.1109/JPROC.2016.2637878

Bunte, B. (2019). Cookiecalypse: Müssen künftig 85 Prozent des Traffics ohne Cookies vermarktet werden?. Online: https://omr.com/de/cookiecalypse-tod-des-cookies-ben-bunte-performance-media/. Zugriff: 01.07.2021.

BVDW. (2015). Browsercookies und alternative Tracking-Technologien: technische und datenschutzrechtliche Aspekte. Online: https://www.bvdw.org/fileadmin/bvdw/upload/publikationen/data_economy/whitepaper_targeting_browsercookies-und-alternative-trackingtechnologien_2015.pdf, Zugriff: 04.06.2021.

Cahn, A., Alfeld, S., Barford, P., & Muthukrishnan, S. (2016). An empirical study of web cookies. *25th International World Wide Web Conference, WWW 2016*, 891–901. https://doi.org/10.1145/2872427.2882991

Schmidt, C. (2019). Was ist eigentlich die Open Digital Rights Language?. Online: https://www.canto.com/de/blog/open-digital-rights-language/, Zugriff: 19.08.2021.

Cxense. (2021). About Us. Online: https://www.cxense.com/about-us, Zugriff: 16.08.2021.

Cxense. (2021a). Website Privacy Policy. Online: https://www.cxense.com/about-us/privacy-policy, Zugriff: 16.08.2021.

Dabrowski, A., Merzdovnik, G., Ullrich, J., Sendera, G., & Weippl, E. (2019). Measuring Cookies and Web Privacy in a Post-GDPR World. In D. Choffnes & M. Barcellos (Hrsg.), *Passive and Active Measurement* (Bd. 11419, S. 258–270). Springer International Publishing. https://doi.org/10.1007/978-3-030-15986-3_17

Degeling, M., Utz, C., & Urban, T. (2020). Effekte der DSGVO auf Websiten und die Entwicklung der ePrivacy-Verordnung. *Zeitschrift für Bürgerrechte und Gesellschaftspolitik*, 59(3-4), 77-86.

Degeling, M., Utz, C., Lentzsch, C., Hosseini, H., Schaub, F. & Holz, T. (2019). We Value Your Privacy ... Now Take Some Cookies: Measuring the GDPR's Impact on Web Privacy. In *Proc. NDSS 2019.* Internet Society. https://doi.org/10.14722/ndss.2019.23378

Domaintechnik. (2021). DNS-Lookup. Online: https://www.domaintechnik.at/dns-lookup.html, Zugriff: 22.08.2021.

Duden. (2021). Heuristik. Online: https://www.duden.de/rechtschreibung/Heuristik, Zugriff: 31.07.2021.

DSGVO. (2016). Datenschutz-Grundverordnung, 2016/119. Online: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679&from=DE, Zugriff: 30.03.2021.

Eckersley, Peter. (2010). How Unique Is Your Web Browser? In *Privacy Enhancing Technologies* (Vol. 6205, pp. 1–18). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-14527-8_1

EDPS. (2016). EDPS Opinion on Personal Information Management Systems. Online: https://edps.europa.eu/sites/edp/files/publication/16-10-20_pims_opinion_en.pdf, Zugriff: 19.08.2021.

Europäische Kommission. (2019). Nur jeder zehnte Deutsche liest Datenschutzerklärungen vollständig durch. Online: https://ec.europa.eu/germany/news/20190613-datenschutz_de, Zugriff: 24.08.2021.

Europäische Kommission. (2021). Worum handelt es sich bei einem Verantwortlichen bzw. einem Auftragsverarbeiter?. Online: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_de, Zugriff: 13.08.2021.

F5. (2014). Caching Behaviour of Web Browsers. Online: https://www.f5.com/de_de/services/resources/white-papers/caching-behavior-of-web-browsers, Zugriff: 19.06.2021.

Facebook. (2021). Company-Info. Online: https://about.facebook.com/company-info/, Zugriff: 16.08.2021.

Facebook. (2021a). Facebook Reports Fourth Quarter and Full Year 2020 Results. Online: https://s21.q4cdn.com/399680738/files/doc_news/Facebook-Reports-Fourth-Quarter-and-Full-Year-2020-Results-2021.pdf, Zugriff: 16.08.2021.

Facebook. (2021b). Was ist die Datenschutz-Grundverordnung (DSGVO)?. Online: https://de-de.facebook.com/business/gdpr, Zugriff: 16.08.2021.

Facebook. (2021c). Datenrichtlinie. Online: https://de-de.facebook.com/policy.php, Zugriff: 16.08.2021.

Fox, D. (2010). Webtracking. *Datenschutz und Datensicherheit - DuD*, *34*(11), 787–787.

Geradin, D, & Katsifis, D. (2020). Taking a Dive Into Google's Chrome Cookie Ban. TILEC Discussion Paper. Arttikel DP2020-042. https://doi.org/10.2139/ssrn.3541170

Google. (2021). Programmrichtlinien für Ad Manager und Ad Exchange - Häufig gestellte Fragen zur DSGVO. Online: https://support.google.com/admanager/answer/9035987?hl=de, Zugriff: 13.08.2021.

Google. (2021a). Datenschutzerklärung. Online: https://policies.google.com/privacy?hl=de, Zugriff: 16.08.2021.

Google. (2021b). Nutzungsbedingungen. Online: https://policies.google.com/terms?hl=de, Zugriff: 16.08.2021.

Gradow, L., & Greiner, R. (2021). *Quick Guide Consent-Management: Einwilligungen marketingoptimiert und DSGVO-konform einholen, verwalten und dokumentieren*. Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-33021-7

Heberlein, J. (2017). *Datenschutz im Social Web: Materiell-rechtliche Aspekte der Verarbeitung personenbezogener Daten durch Private in sozialen Netzwerken.* Nomos Verlagsgesellschaft mbH & Co. KG. https://doi.org/10.5771/9783845287737

Hiersche, A., & Mayer, A. T. (2017). Die Ermittlungen der Europäischen Kommission gegen Google: Auf der Suche nach dem Produktmarkt, Marktmacht und Missbrauch – Teil 3. *Österreichische Zeitschrift für Kartellrecht*, *2017*(2), 53–58.

Hillebrand, R.-T. (2018). *Online-Kommunikation für Verbände*. Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-13267-5

Hils, M., Woods, D. W., & Böhme, R. (2020). Measuring the Emergence of Consent Management on the Web. In *Proceedings of the ACM Internet Measurement Conference* (S. 317–332). Association for Computing Machinery. https://doi.org/10.1145/3419394.3423647

Holland, H. (Hrsg.). (2021). *Digitales Dialogmarketing: Grundlagen, Strategien, Instrumente*. Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-28959-1

IAB. (2021). IAB Europe Transparency & Consent Framework Policies. Online: https://iabeurope.eu/iab-europe-transparency-consent-framework-policies/, Zugriff: 10.08.2021.

itmagazine. (2021). Google verschiebt Cookie-Bann auf 2023. Online: https://www.itmagazine.ch/Artikel/74939/Google_verschiebt_Cookie-Bann_auf_2023.html, Zugriff: 01.07.2021.

Jakobi, T., Seufert, A.-M., Stevens, G. & Becker, M., (2019). Webtracking im neuen Datenschutzrecht - Gestaltungspotentiale an der Schnittstelle von Rechtswissenschaften und HCI. In: Alt, F., Bulling, A. & Döring, T. (Hrsg.), *Mensch und Computer 2019 - Tagungsband.* (S. 309-319) New York: ACM. https://doi.org/10.1145/3340764.3340790

Krämer, J., Dewenter, R., Zimmer, D., Henseler-Unger, I., Arnold, R., Hildebrandt, C., & Knieps, G. (2016). Wettbewerbspolitik in der digitalen Wirtschaft. *Wirtschaftsdienst*, *96*(4), 231–248. https://doi.org/10.1007/s10273-016-1964-6

Kreipl, C. (2020). Compliance Management. In C. Kreipl (Hrsg.), *Verantwortungsvolle Unternehmensführung: Corporate Governance, Compliance Management und Corporate Social Responsibility* (S. 129–217). Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-28140-3_3

Morrison, S. & Molla, R. (2020). Google Chrome's cookie ban is good news for Google — and maybe your privacy. Online: https://www.vox.com/recode/2020/1/16/21065641/google-chromecookie-ban-advertisers. Zugriff am 02.06.2021.

Mertins, K., Kempf, S., & Siebert, G. (1995). Benchmarking Techniques. In A. Rolstadås (Hrsg.), *Benchmarking—Theory and Practice* (S. 223–229). Springer US. https://doi.org/10.1007/978-0-387-34847-6_25

Müller, U. (2019). Talententdeckung und -förderung im Zeitalter von Big Data. In M. Ahlers, L. Grünewald-Schukalla, M. Lücke, & M. Rauch (Hrsg.), *Big Data und Musik: Jahrbuch für Musikwirtschafts- und Musikkulturforschung 1/2018* (S. 153–173). Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-21220-9_7

Neumann, N., Tucker, C. E. & Whitfield, T. (2019). Frontiers: How Effective Is Third-Party Consumer Profiling? Evidence from Field Studies. Marketing Science (Providence, R.I.), 38(6), 918–926. https://doi.org/10.1287/mksc.2019.1188

Onlinemarketing-Praxis. (2021). Definition Semantisches Targeting. Online: https://www.onlinemarketing-praxis.de/glossar/semantisches-targeting, Zugriff: 01.06.2021.

Papadopoulos, P., Kourtellis, N., & Markatos, E. (2019). Cookie Synchronization: Everything You Always Wanted to Know But Were Afraid to Ask. *The World Wide Web Conference*, 1432–1442. https://doi.org/10.1145/3308558.3313542

Possekel, M., & Schiemann, S. (2020). Data-driven Marketing als Risiko. *Controlling & Management Review*, *64*(2), 52–57. https://doi.org/10.1007/s12176-019-0079-5

Ravichandran, D. & Vassilvitskii, S. (2021). Evaluation of Cohort Algorithms for the FLoC API. Online: https://github.com/google/ads-privacy/blob/master/proposals/FLoC/FLOC-Whitepaper-Google.pdf, Zugriff: 20.05.2021.

Rodriguez-Garcia, M., Batet, M., Sánchez, D., & Viejo, A. (2021). Privacy protection of user profiles in online search via semantic randomization. *Knowledge and information systems*. https://doi.org/10.1007/s10115-021-01597-x

Roßnagel, A. (2007). *Datenschutz in einem informatisierten Alltag*. Stabsabteilung der Friedrich-Ebert-Stiftung. Berlin.

Roßnagel, A. & Müller, J. (2004). *Ubiquitous Computing – neue Herausforderungen für den Datenschutz* (8. Aufl.). Computer und Recht. Berlin.

Ryte. (2021). Ryte Wiki – Metadaten. Online: https://de.ryte.com/wiki/Metadaten, Zugriff: 11.04.2021.

Schallaböck, J. (2014). Verbraucher-Tracking. Online: https://www.gruene-bundestag.de/fileadmin/media/gruenebundestag_de/themen_az/digitale_buergerrechte/Tracking-Bilder/Verbraucher_Tracking, Zugriff: 10.06.2021.

Schärer, W. (2021). Cookies und die Herausforderungen für Web-Analytics. Online: https://www.blueglass.ch/blog/cookie-herausforderung-fuer-web-analytics, Zugriff: 13.05.2021.

Schelinski, T., & Feuerhake, J. (2019). Intellectual Property/IT-Recht/Medienrecht. In D. Graewe (Hrsg.), *Wirtschaftsrecht* (S. 563–650). Springer Fachmedien. Wiesbaden. https://doi.org/10.1007/978-3-658-23080-7_6

Schneider, T. (2018). *Wirkungsvolle Compliance*. Springer Berlin. Heidelberg. https://doi.org/10.1007/978-3-662-55941-3

Schott, A. (2014). Online-Marketing-Technologie. In H. Holland (Hrsg.), *Digitales Dialogmarketing: Grundlagen, Strategien, Instrumente* (S. 571–590). Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-02541-0_21

Siegert, G., & Brecheis, D. (2017). Werbung in der Medien- und Informationsgesellschaft (3. Aufl.). Springer Fachmedien. Wiesbaden. https://doi.org/10.1007/978-3-658-15885-9

Statcounter. (2021). Browser Market Share. Online: https://gs.statcounter.com/browser-market-share, Zugriff: 18.05.2021.

Statista. (2021). Statistiken und Daten rund um Google. Online: https://de.statista.com/themen/651/google/, Zugriff: 15.08.2021.

Solomos, K., Ilia, P., Ioannidis, S., & Kourtellis, N. (2019). Clash of the Trackers: Measuring the Evolution of the Online Tracking Ecosystem. ArXiv1907.12860, 1-10. http://arxiv.org/abs/1907.12860

Tinnefeld, M., Buchner, B., Petri, T. & Hof, H. (2019). *Einführung in das Datenschutzrecht: Datenschutz und Informationsfreiheit in europäischer Sicht*. Berlin, Boston: De Gruyter Oldenbourg. https://doi.org/10.1515/9783110630336

Traverso, S., Trevisan, M., Giannantoni, L., Mellia, M., & Metwalley, H. (2017). Benchmark and comparison of tracker-blockers: Should you trust them?. In: *2017 Network Traffic Measurement and Analysis Conference (TMA)*, (S. 1-9). IEEE.

TrustedTargeting. (2021). Cookieless Tracking – Beginn einer Ära ohne Cookies. Online: https://www.trustedtargeting.com/blog/cookieless-tracking, Zugriff: 19.06.2021.

Urban, T., Tatang, D., Degeling, M., Holz, T. & Pohlmann, N. (2020). Measuring the Impact of the GDPR on Data Sharing in Ad Networks. In ASIA CCS '20: *Proceedings of the 15th ACM Asia Conference on Computer and Communications Security*, 222–235. http://dx.doi.org/10.1145/3320269.3372194

Voigt, P. & von dem Bussche, A. (2019). Konzern In: Voigt, P. & von dem Bussche, A., Konzerndatenschutz, Verarbeitungsübersicht, Rn. 7.

Voigt, P. & von dem Bussche, A. (2018). *EU-Datenschutz-Grundverordnung (DSGVO)*. Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-662-56187-4

W3C. (2021). API for persistent data storage of key-value pair data in Web clients, URL: https://www.w3.org/TR/webstorage, Zugriff am 20.06.2021.

W3C. (2021a). GDPRtEXT. Online: https://www.w3.org/community/dpvcg/wiki/GDPRtEXT, Zugriff: 05.08.2021.

Wenhold, C. (2018). *Nutzerprofilbildung durch Webtracking: Zugleich eine Untersuchung zu den Defiziten des Datenschutzrechts im Zeitalter von Big Data-Anwendungen* (1. Aufl., Bd. 37). Nomos Verlagsgesellschaft mbH & Co. KG. https://doi.org/10.5771/9783845293264

Wirtschaftslexikon. (2018). Aggregation. Online: https://wirtschaftslexikon.gabler.de/definition/aggregation-30653/version-254230, Zugriff: 13.08.2021.

Woitke, T. (2003). Web-Bugs – Nur lästiges Ungeziefer oder datenschutzrechtliche Bedrohung?, *Multimedia und Recht*, 5(6), 310-314.

Anhang

Anhang 1 | Exposee Master These

Familienname, Vorname	Haaf, Moritz Philipp
eMail-Adresse	mm191802@fhstp.ac.at
Telefonnummer	+43 664 1582 252 9
Datum der Abgabe	06.01.2021
Name Betreuer*in	FH-Prof. Mag. Dr. Tassilo Pellegrini
Arbeitstitel	DSGVO-Compliance von alternativen Webtracking Methoden
Fragestellung der Master-These	Problemstellung: Aufgrund der jüngsten Urteile des EuGHs und der Einführung der DSGVO sowie der geplanten Einführung der ePrivacy Verordnung steht das klassische Webtracking mit Cookies vor dem Aus. Beim Webtracking handelt es sich um eine Technologie, die bei öffentlichen Dienstleistern im Internet zum Einsatz kommt, um User-Interaktionen zu erfassen. Durch die verschärften Datenschutzbestimmungen stehen Publisher und Werbetreibende vor enormen Herausforderungen, um ihr Geschäftsmodell weiterhin bedienen zu können. (vgl. Jakobi et al. 2019, S. 311) Zielsetzung: Diese Arbeit hat zum Ziel die unterschiedlichen Möglichkeiten des Cookieless Trackings zu analysieren und deren Vereinbarkeit mit der DSGVO zu untersuchen. Dadurch sollen geeignete Alternativen herausgearbeitet werden, die das klassische Cookie Tracking in der Zukunft ablösen könnten. Zentrale Forschungsfrage: „Inwieweit sind alternative Webtracking-Methoden mit der DSGVO zu vereinbaren?“
Wissenschaftliche und praktische Relevanz	**Wissenschaftliche Relevanz:** Durch die Reformen in der Rechtsprechung für Datenschutz ist auch in der Forschung ein Trend erkennbar, bei dem vermehrt nach Alternativen zum klassischen Cookie Tracking gesucht wird. Hierbei werden verschiedenste Technologien und Methoden untersucht, die es zum einen Websitenbetreibern ermöglichen sollen, ein Nutzerprofil anhand der erhobenen User Daten zu erstellen, aber gleichzeitig auch den neuesten Datenschutzbestimmungen entsprechen. Der Fokus der Forschung liegt aktuell darauf, welche Tracking Methoden momentan eingesetzt werden und ob diese rechtskonform im Zusammenhang mit der Datenschutzreform sind (vgl. Solomos et al. 2019, S. 2 ff). Genau

	an diesem Punkt soll diese Arbeit anknüpfen und die unterschiedlichen Technologien sollen miteinander in Vergleich gesetzt werden, um geeignete Möglichkeiten für die Praxis herauszuarbeiten. **Praktische Relevanz:** Aus der Sicht des Autors sind die verschiedenen Methoden des Cookieless Trackings aufgrund der Aktualität bislang in der Praxis erst wenig erprobt, da sich der Großteil der Publisher und Werbetreibenden im digitalen Marketing noch inmitten des Transformationsprozesses befindet weg vom klassischen Cookie Tracking. Diese Arbeit hat daher zum Ziel praktikable Trackingalternativen zu finden und diese unter Berücksichtigung der gegebenen Rahmenbedingungen im Rechtsraum der Europäischen zu evaluieren. Durch ein geeignetes Compliance Management Konzept soll Website-Betreibern dabei geholfen werden beim Einsatz von Tracking- Tools die Datenschutzbestimmungen einzuhalten.
Aufbau und Gliederung	Inhaltsverzeichnis Masterarbeit – Ehrenwörtliche Erklärung – Inhaltsverzeichnis – Abstract/ Zusammenfassung – Abbildungsverzeichnis/Tabellenverzeichnis/Abkürzungsverzeichnis 1. Einleitung 1.1 Problemstellung 1.2 Ableitung der Forschungsfrage 1.3 Zielsetzung und Methode der Arbeit 1.4 Forschungsstand 2. Compliance Management für Website-Betreiber*innen 2.1 Rechenschaftspflicht beim Einsatz von Tracking-Tools 2.2 Compliance Ziele 2.3 Monitoring und Verbesserung 3. Webtracking 3.1 Darstellung der rechtlichen Rahmenbedingungen 3.1.1 Grundsätze der Verarbeitung von personenbezogenen Daten 3.1.2 Auswirkungen der DSGVO auf das Webtracking 3.1.3 Mögliche Änderungen durch die geplante Einführung der ePrivacy Verordnung 3.2 Nutzungspotenziale und Funktionsweise von Webtracking 3.2.1 Recht auf Privacy auf Nutzerseite 3.2.2 Notwendigkeit der Interaktion zwischen Publisher und User 3.3 Formen des klassischen Cookie Trackings 3.2.3 Anwendungsfeld First Party Cookies 3.2.4 Anwendungsfeld Third Party Cookies 3.4 Alternative Webtracking Methoden und deren Funktionsweise

	3.4.1 Semantisches Targeting 3.4.2 Fingerprinting 3.4.3 Authentication Cache 3.4.4 ETag 3.4.5 Digitrust Universal ID 3.4.6 DOM Storage 4. Methodik 4.1 Desk Research - Alternative Webtracking Technologien 4.2 Benchmarking - Eigenschaften Webtracking Technologien 4.3 Auswertung 4.4 Handlungsempfehlungen 5. Fazit 5.1 Fazit Ergebnisse und Erhebungsmethode 5.2 Limitationen 5.3 Forschungsausblick Literaturverzeichnis Anhang
Methodenwahl	Empirische Methode: Im Rahmen dieser Arbeit wird ein heuristischer Ansatz gewählt. Mittels Desk Research sollen qualitative Kategorien herausgearbeitet werden, um die alternativen Tracking Methoden und die DSGVO zueinander in Beziehung stellen. Die Auswertung der explorativ erhobenen Ergebnisse soll beispielsweise nach der qualitativen Inhaltsanalyse nach Philipp Mayring erfolgen (vgl. Mayring & Fenzl, 2019, S. 633 ff.). Anschließend werden die einzelnen Tracking Methoden anhand der ausgearbeiteten Kategorien analysiert und mittels einer Likert-Skala gewichtet (z. B. niedrigster Wert 1 bis höchster Wert 5). **Begründung Methodenwahl:** Durch die Gewichtung der Kategorien können die verschiedenen Trackingverfahren mittels Benchmark Analyse miteinander verglichen und einheitlich analysiert werden. Die vorangehende Sekundärforschung dient zur Ausarbeitung geeigneter Merkmale und Kategorien ausgearbeitet, um die unterschiedlichen Webtracking Technologien miteinander sowie den relevanten Datenschutzbestimmungen in Relation zu setzen. Mithilfe dieser Herangehensweise sollen neue Denkansätze für zukünftige Forschung geschaffen werden.
	Empirische Methode: Im Rahmen dieser Arbeit wird ein heuristischer Ansatz gewählt. Mittels Desk Research sollen qualitative Kategorien herausgearbeitet werden, um die alternativen Tracking Methoden und die DSGVO zueinander in Beziehung stellen. Die Auswertung der explorativ erhobenen Ergebnisse soll beispielsweise mithilfe der qualitativen Inhaltsanalyse nach Philipp Mayring erfolgen. (vgl. Mayring & Fenzl, 2019, S. 633 ff.) Anschließend werden die einzelnen Tracking Methoden anhand der ausgearbeiteten Kategorien analysiert und mittels einer Likert-Skala gewichtet (z. B. niedrigster Wert 1 bis höchster Wert 5). **Begründung Methodenwahl:** Durch die Gewichtung der Kategorien können die verschiedenen

	Trackingverfahren mittels Benchmark Analyse miteinander verglichen und einheitlich analysiert werden. Die vorangehende Sekundärforschung dient zur Ausarbeitung geeigneter Merkmale und Kategorien ausgearbeitet, um die unterschiedlichen Webtracking Technologien miteinander sowie den relevanten Datenschutzbestimmungen in Relation zu setzen. Mithilfe dieser Herangehensweise sollen neue Denkansätze für zukünftige Forschung geschaffen werden.
Literaturhinweise	**Zitierte Quellen Master Exposé:** Mayring, P., & Fenzl, T. (2019). Qualitative Inhaltsanalyse. In N. Baur & J. Blasius (Hrsg.), Handbuch Methoden der empirischen Sozialforschung (S. 633–648). Wiesbaden: Springer Fachmedien. https://doi.org/10.1007/978-3-658-21308-4_42 Jakobi, T., Seufert, A.-M., Stevens, G. & Becker, M., (2019). Webtracking im neuen Datenschutzrecht - Gestaltungspotentiale an der Schnittstelle von Rechtswissenschaften und HCI. In: Alt, F., Bulling, A. & Döring, T. (Hrsg.), Mensch und Computer 2019 - Tagungsband.(S. 309-319) New York: ACM. https://doi.org/10.1145/3340764.3340790 Solomos, K., Ilia, P., Ioannidis, S., & Kourtellis, N. (2019). Clash of the Trackers: Measuring the Evolution of the Online Tracking Ecosystem. ArXiv1907.12860, 1-10. **Kernquellen für die Masterarbeit:** Agogo, D. (2020). Invisible market for online personal data: An examination. *Electronic Markets*. https://doi.org/10.1007/s12525-020-00437-0 Dabrowski A., Merzdovnik G., Ullrich J., Sendera G., Weippl E. (2019) Measuring Cookies and Web Privacy in a Post-GDPR World. In: Choffnes D., Barcellos M. (Hrsg.) Passive and Active Measurement. PAM 2019. Lecture Notes in Computer Science, vol 11419. Springer, Cham. https://doi.org/10.1007/978-3-030-15986- 3_17 Hils, M., Woods, D. W., & Böhme, R. (2020). Measuring the Emergence of Consent Management on the Web. In Proceedings of the ACM Internet Measurement Conference (S. 317-332). Jakobi, T., Stevens, G., Seufert, A. M., Becker, M., & von Grafenstein, M. (2020). Web Tracking Under the New Data Protection Law: Design Potentials at the Intersection of Jurisprudence and HCI. *i-com*, *19*(1), 31-45. Nabbosa, V. L., & Iftikhar, R. (2019). Digital Retail Challenges within the EU: Fulfillment of Holistic Customer Journey Post GDPR. In *Proceedings of the 2019*

3rd International Conference on E-Education, E-Business and E-Technology (S.
51-58).
N. Nikiforakis, A. Kapravelos, W. Joosen, C. Kruegel, F. Piessens and G. Vigna,
"Cookieless Monster: Exploring the Ecosystem of Web-Based Device Fingerprinting," 2013 IEEE Symposium on Security and Privacy, Berkeley, CA,
2013, 541-555. https://doi.org/10.1109/SP.2013.43.

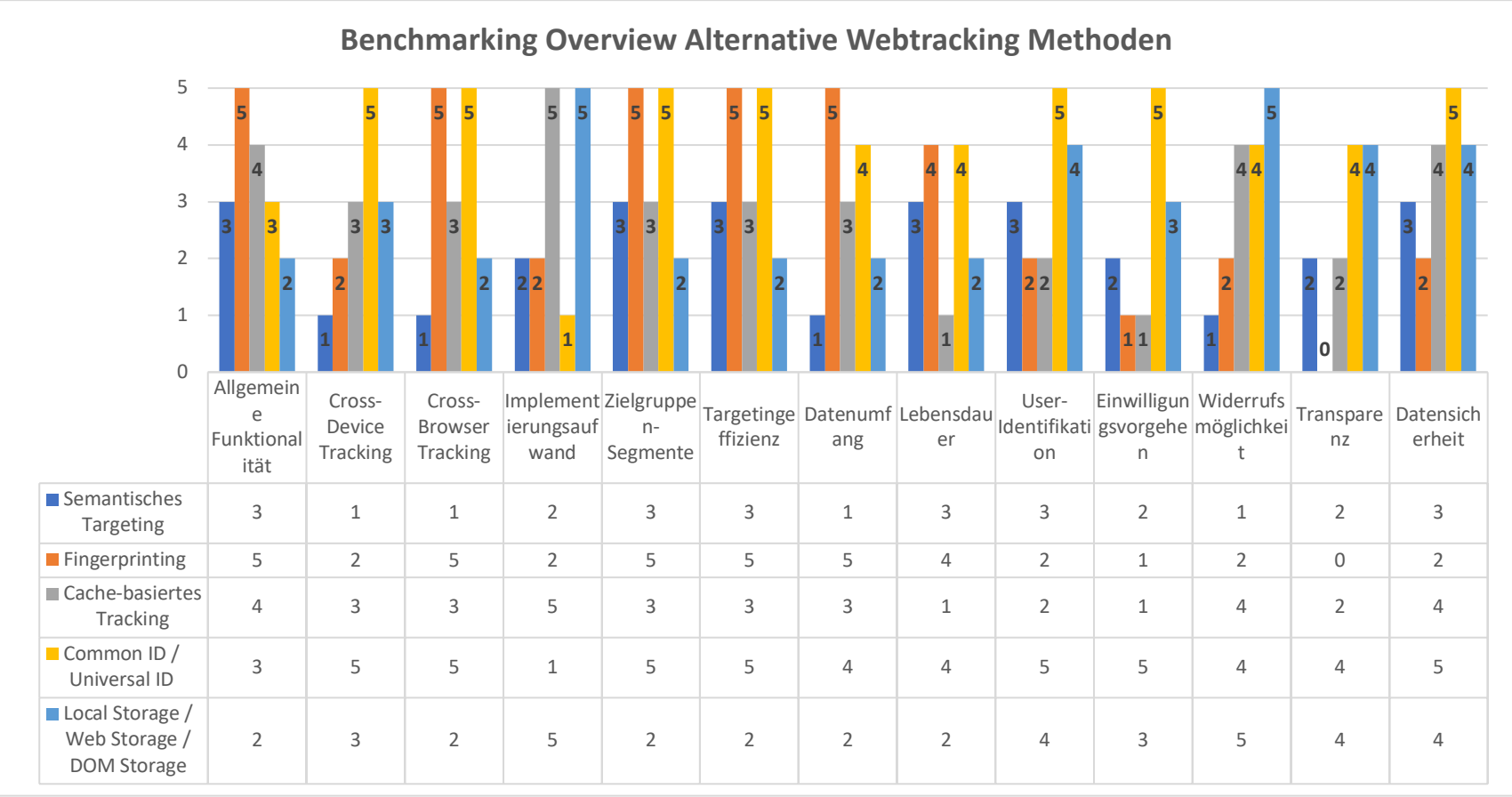
Possekel, M., & Schiemann, S. (2020). Data-driven Marketing als Risiko.
Controlling & Management Review, *64*(2), 52-57.
https://doi.org/10.1007/s12176-
019-0079-5
Sanchez-Rola, I., Dell'Amico, M., Kotzias, P., Balzarotti, D., Bilge, L., Vervier, P.
A., & Santos, I. (2019). Can I Opt Out Yet? GDPR and the Global Illusion of Cookie
Control. In Proceedings of the 2019 ACM Asia Conference on Computer and
Communications Security (S. 340-351).
Sy, E., Burkert, C., Federrath, H., & Fischer, M. (2019). A QUIC Look at Web
Tracking, Proceedings on Privacy Enhancing Technologies, 2019(3), 255-266.
https://doi.org/10.2478/popets-2019-0046

Sørensen, J., & Kosta, S. (2019, May). Before and after gdpr: The changes in third party presence at public and private european websites. In *The World Wide Web Conference, 2019,* 1590-1600.

Genehmigt durch Studiengangsleitung

Anhang 2 | Benchmarking Auswertung

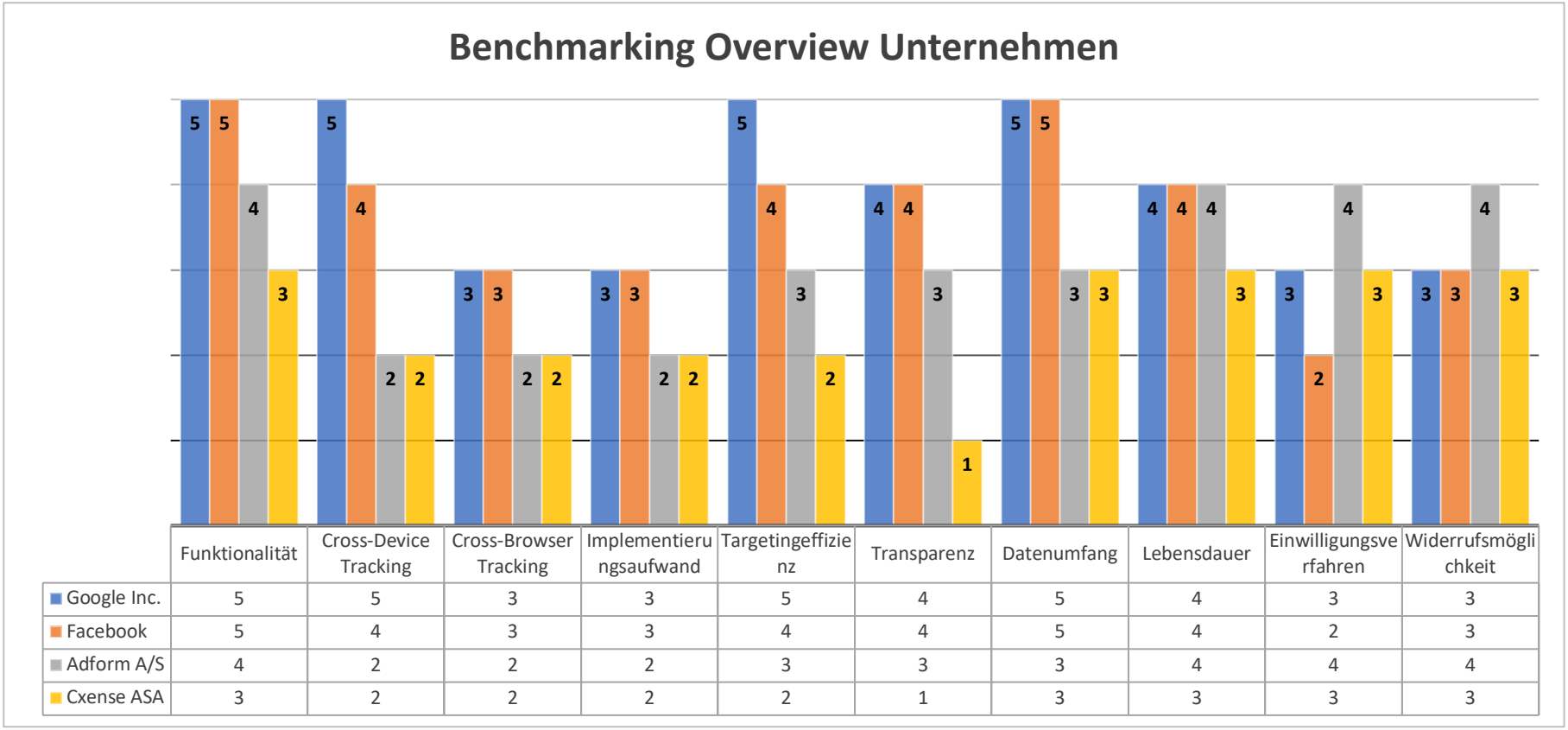
Alternative Methoden des Webtrackings – Benchmarking Übersicht



	Allgemeine Funktionalität	Cross-Device Tracking	Cross-Browser Tracking	Implementierungsaufwand	Zielgruppen-Segmente	Targetingeffizienz	Datenumfang	Lebensdauer	User-Identifikation	Einwilligungsvorgehen	Widerrufsmöglichkeit	Transparenz	Datensicherheit
Semantisches Targeting	3	1	1	2	3	3	1	3	3	2	1	2	3
Fingerprinting	5	2	5	2	5	5	5	4	2	1	2	0	2
Cache-basiertes Tracking	4	3	3	5	3	3	3	1	2	1	4	2	4
Common ID / Universal ID	3	5	5	1	5	5	4	4	5	5	4	4	5
Local Storage / Web Storage / DOM Storage	2	3	2	5	2	2	2	2	4	3	5	4	4

Abbildung 20: Eigene Darstellung - Benchmarking Overview Alt. Webtracking Methoden

Unternehmen im Bereich der Datenaggregation – Benchmarking Übersicht



	Funktionalität	Cross-Device Tracking	Cross-Browser Tracking	Implementierungsaufwand	Targetingeffizienz	Transparenz	Datenumfang	Lebensdauer	Einwilligungsverfahren	Widerrufsmöglichkeit
Google Inc.	5	5	3	3	5	4	5	4	3	3
Facebook	5	4	3	3	4	4	5	4	2	3
Adform A/S	4	2	2	2	3	3	3	4	4	4
Cxense ASA	3	2	2	2	2	1	3	3	3	3

Abbildung 21: Eigene Darstellung - Benchmarking Overview Unternehmen