Digitale Gesellschaft e.V./Netzwerk Datenschutzexpertise/Deutsche Vereinigung für Datenschutz e. V./Digitalcourage e. V.

Beschwerde

bei den deutschen Datenschutz-Aufsichtsbehörden

wegen

VERHALTENSBASIERTER WERBUNG im Internet

und Aufforderung, hierzu Datenschutzleitlinien zu erarbeiten und zu veröffentlichen

---

A. Einführung & Zweck

1
Wir erheben in Absprache mit weiteren Organisation in Europa die unten stehende Beschwerde. Wer wir sind:

- Die Digitale Gesellschaft e.V. ist ein gemeinnütziger Verein, der sich seit seiner Gründung im Jahr 2010 für Grundrechte und Verbraucherschutz im digitalen Raum einsetzt.

- Das Netzwerk Datenschutzexpertise ist ein Zusammenschluss von DatenschutzexpertInnen mit dem Ziel, öffentliche Diskussionen über Fragen des Datenschutzes sowie generell des Schutzes von Menschenrechten und Grundrechten in der digitalen Welt zu initiieren und voranzubringen.

- Die Deutsche Vereinigung für Datenschutz e. V. (DVD) nimmt seit ihrer Gründung 1977 als gemeinnütziger Verein die Interessen der verdateten BürgerInnen wahr.

- Digitalcourage e. V. ist ein Zusammenschluss von Menschen, die Technik und Politik mit dem Ziel der Verwirklichung von Grundrechten und Datenschutz kritisch erkunden und menschenwürdig gestalten wollen.

2
Der Zweck der vorliegenden Beschwerde ist es, die deutschen Datenschutzaufsichtsbehörden um Maßnahmen zu bitten, welche den Einzelnen bzw. die Menschen allgemein vor weitreichenden und systematischen Datenschutzverstößen durch Google und ande-

re Internet-Unternehmen der Branche schützen. Die Beschwerde hat als Grundlage die Stellungnahme von Dr. Johnny Ryan (**Ryan-Bericht**).1

3
Es gibt zwei Hauptsysteme, die der verhaltensbasierten Onlinewerbung zugrunde liegen, die beide nach einer Spezifikation namens „Real Time Bidding“ (RTB) arbeiten:

• **OpenRTB** wird von praktisch jedem bedeutenden Unternehmen in der Online-Medien- und Werbebranche verwendet.

• **Authorized Buyers”** ist Googles proprietäres RTB-System, das vor Kurzem von „DoubleClick Ad Exchange“ (kurz „AdX“) in „Authorized Buyers“ umbenannt wurde.

4
Beide Systeme dienen dazu, personalisierte Werbung auf Websites bereitzustellen. Wie im Ryan-Bericht dargestellt, werden „jedes Mal, wenn eine Person auf eine Webseite geht, die automatisierte Werbung nutzt, und diese herunterlädt, persönliche Daten über sie an Dutzende – oder gar Hunderte – von Firmen übertragen“.

5
Es gibt drei zentrale, miteinander zusammenhängende Gründe für erhebliche Datenschutzbedenken beim Einsatz von verhaltensbasierter Internetwerbung.

Erstens Die Branche begann ursprünglich damit, personalisierte Werbung zu unterstützen. Inzwischen führt dies zu einer Übertragung von Massendaten, die

a. ein breites Spektrum an Informationen über Einzelpersonen umfasst, welches weit über den Bereich der Informationen hinausgeht, der für die Bereitstellung der relevanten Anzeigen erforderlich ist, und

b. einer Vielzahl von Dritten für eine Reihe von Anwendungen zur Verfügung gestellt werden, die weit über die Zwecke hinausgehen, welche eine betroffene Person verstehen kann und in die sie einwilligen oder gegen die sie Widerspruch einlegen kann. Es gibt keine rechtliche Grundlage für eine solche allgegenwärtige und invasive Profilerstellung und Verarbeitung personenbezogener Daten aus Profitgründen (Art. 22 Datenschutz-Grundverordnung – DS-GVO).

Zweitens Der praktizierte Mechanismus der Branche ermöglicht es nicht, die Kontrolle über die Verbreitung personenbezogener Daten nach deren Übertragung (bzw. überhaupt) zu behalten. Die schiere Anzahl der Empfänger solcher Daten führt dazu, dass die Sender weder ihre unbefugte Weiterverarbeitung verhindern, noch die betroffenen Personen über die Empfänger der Daten ordnungsgemäß informieren können. Die rechtskonforme Verarbeitung der personenbezogenen Daten kann nicht mehr gewährleistet werden, wenn diese einmal weitergegeben worden sind. Die technischen und organisatorischen Sicherheitsvorkehrungen, die getroffen wurden, bestätigen, dass Datenschutz-

1 https://brave.com/Behavioural-advertising-and-personal-data.pdf.

verletzungen dem Design der Branche inhärent sind. Dieses Problem besteht unabhängig davon, ob die Verarbeitung personenbezogener Daten und der Informationsaustausch im Rahmen der personalisierten Werbung durchgeführt werden. Eine Verarbeitung ohne ausreichende Sicherheitsvorkehrungen ist mit den Datenschutzbestimmungen nicht vereinbar.

Drittens Die Verarbeitung betrifft sehr oft besondere Kategorien personenbezogener Daten (Art. 9 Abs. 1 DS-GVO). Die besuchten Webseiten können Indikatoren enthalten, die über Sexualität, Ethnizität, politische Meinungen etc. Auskunft geben. Solche Aussagen, die als sensitive Daten anzusehen sind, können explizit erfolgen oder effektiv und leicht mit hoher Genauigkeit unter Verwendung moderner analytischer Techniken abgeleitet werden.[2] RTB erfolgt in Echtzeit, was zur Folge hat, dass solche sensitiven Daten ohne jegliches Einverständnis und ohne jegliche Kontrolle verbreitet werden können. Da solche Daten mit sehr hoher Wahrscheinlichkeit an zahlreiche Organisationen weitergegeben werden, die diese Daten wiederum mit anderen Daten verknüpfen, können extrem komplexe Profile von Personen erstellt werden, ohne dass die betroffene Person davon Kenntnis hat, geschweige denn ihr Einverständnis gegeben hätte. Die Industrie fördert diese Praxis und verzichtet auf adäquate Sicherheitsmechanismen, welche die Integrität der persönlichen Daten und auch solcher besonderer Kategorien gewährleisten könnten. Darüber hinaus ist es unwahrscheinlich, dass Einzelpersonen wissen, dass ihre persönlichen Daten auf diese Weise verbreitet und übertragen wurden, es sein denn, sie sind aus einem speziellen Grund in der Lage, bei einer Vielzahl von Unternehmen erfolgreiche Anträge auf Zugang zu persönlichen Daten zu stellen.[3] Es ist nicht zu erkennen, dass diese Unternehmen solchen Anfragen nachgekommen sind und dass dies nachweisbar wäre. Ohne Maßnahmen der Regulierungsbehörden ist es nicht möglich, die branchenweite Einhaltung der Datenschutzbestimmungen sicherzustellen.

6

Angesichts dieser anhaltenden Verstöße gegen die einschlägigen Vorschriften und Gesetze werden die Datenschutzaufsichtsbehörden um Folgendes ersucht:

i. Überprüfen Sie die detaillierten Beschwerdegründe, die hier und im Ryan-Bericht aufgeführt werden, und leiten Sie eine Untersuchung der speziellen Probleme in Bezug auf

2 Siehe Leitlinien für automatisierte individuelle Entscheidungsfindung und Profilerstellung im Sinne der Verordnung 2016/679 (wp251rev.01, S. 16): „Durch Profiling können Daten besonderer Kategorien erzeugt werden, indem aus Daten, die an sich keine besondere Datenkategorie bilden, dies aber in Kombination mit anderen Daten tun, Daten abgeleitet werden. So kann beispielsweise aus den Lebensmitteleinkäufen einer Person, die mit Daten zur Qualität und zum Energiegehalt von Lebensmitteln verknüpft werden, der Gesundheitszustand der betroffenen Person hergeleitet werden.“ Es sei auch darauf hingewiesen (wie vom CJEU in *Nowak* bestätigt wird), dass Daten, wie z. B. Schlussfolgerungen, die sich auf eine Person beziehen, aber unrichtig sind, personenbezogene Daten bleiben. Wäre dies nicht der Fall, könnte das „Recht auf Richtigstellung“ niemals eingefordert werden.

3 Dieses Problem wird verschärft durch die Tatsache, dass die Unternehmen weitgehend unbekannt und für die betroffene Person unzugänglich sind, da die für die Datenerfassung Verantwortlichen (Controller), welche die Daten zunächst sammeln, selten explizite Informationen über die Empfänger oder auch nur über Kategorien von Empfängern liefern, und die Empfänger die betroffenen Personen nicht gemäß ihren Verpflichtungen nach Art. 14 DS-GVO über den Erhalt dieser Daten informieren.

die Branche für verhaltensorientierte Werbung ein. Um gegen sie vorgehen zu können, ist es wichtig, die systematische Natur der in diesen Beschwerden aufgeführten Verstöße anzuerkennen.

ii. Leiten Sie eine breit angelegte Untersuchung zu den Datenschutzpraktiken der Branche ein. Wir fordern die Datenschutzaufsichtsbehörden auf, ihre Befugnisse nach Kapitel VII der Europäischen Datenschutz-Grundverordnung (DS-GVO) auszuüben, um in Zusammenarbeit mit anderen Datenschutzbehörden eine gemeinsame Untersuchung der genannten Geschäftspraktiken durchzuführen. Wie im Folgenden näher ausgeführt, wurden entsprechende Beschwerden bereits bei Datenschutzbehörden anderer EU-Mitgliedstaaten eingereicht.

iii. Darüber hinaus ersuchen wir die Datenschutzaufsichtsbehörden, die in dieser Beschwerde aufgeführten systematischen und weit verbreiteten Probleme und Bedenken gemäß deren gesetzlichen Auftrag nach § 40 Bundesdatenschutzgesetz (BDSG) zu untersuchen und eine Bewertung durchzuführen, ob die Branche die einschlägigen Datenschutzvorschriften einhält. Darüber hinaus fordern wir die Datenschutzaufsichtsbehörden auf, im Rahmen ihres Ermessens eine gemeinsame Prüfung der Branche vorzunehmen und geeignete Verhaltensregeln / Empfehlungen in Anlehnung an Art. 57 Abs. 1 lit. g, h DS-GVO zu erarbeiten und, falls erforderlich, Durchsetzungsmaßnahmen zu ergreifen.

7
Die von den Datenschutzaufsichtsbehörden geforderten Maßnahmen sind in den nachstehenden Ziffern 48 - 53 ausführlich beschrieben.

B. Hintergrund

8
Der Hintergrund der Branche ist in dem beigefügten Bericht von Dr. Ryan (Ryan-Bericht) dargestellt. Wir verweisen die Datenschutzaufsichtsbehörden für eine detaillierte Erklärung zur Branche, zu deren Vorgehensweise und zu den dem System innewohnenden Datenschutzbelangen auf diesen Bericht.

C. Richtlinien und Verfahren

9
Die Unternehmen sind in einem Branchenverband zusammengeschlossen, der Parameter und Anwendungsmuster festlegt: das Interactive Advertising Bureau (IAB). Die europäische Niederlassung des IAB, **IAB Europe**, hat mit der „Industry Standard Policy“ Verhaltensregeln und standardisierte Vorgehensweisen für Europa festgelegt. Wegen der marktbeherrschenden Stellung von Google handelt dieses Unternehmen mit *Authorized Buyers* nach eigenen Verfahren und Vorgehensweisen. Wir gehen nacheinander auf beides ein.

i. IAB Europe

10
IAB Europe hat das „Europe Transparency & Consent Framework“ geschaffen (Framework).4 Dieser Rahmen basiert auf der Idee, im Verlauf des RTB-Prozesses die Einwilligung von einer betroffenen Person für alle späteren Datenweitergaben an Dritte einzuholen.

11
Mit dem Design des Systems ist ein grundlegender Fehler verbunden. Das Framework erkennt ausdrücklich an, dass der für die Datenverarbeitung Verantwortliche, der „data controller“ (und damit auch die betroffene Person), unmittelbar jede Kontrolle über die Verwendung dieser Daten verliert, sobald die Daten einer natürlichen Person übertragen wurden. Tatsächlich akzeptiert das Framework, dass selbst für den Fall, dass ein Empfänger von Daten gegen Gesetze verstößt, diesem Empfänger weiterhin Daten zur Verfügung gestellt werden dürfen.5 Durch den Verzicht der „data controller“ auf die Kontrolle verzichtet die Branche insgesamt darauf, den Anschein eines Mechanismus aufrechtzuerhalten, in dem es eine Rolle spielt, wie die Daten verwendet werden. Einmal abgegeben, ist die Kontrolle über diese Daten im Äther des Datenhandels für immer verloren.

12
Diese Daten werden dann an ein umfangreiches Ökosystem von Data Brokern und Werbetreibenden weitergegeben. Diese Dritten können die Daten dann nach eigenem Ermessen verwenden, wobei die Betroffenen als die „Datensubjekte“ keinerlei Mitsprache, Kenntnis oder Kontrolle über diese nachfolgende Nutzung haben. Die Anwendungen für diese Daten sind umfangreich; sie können mit anderen Daten zusammengeführt werden oder die Daten können verwendet werden, um für viele unterschiedliche Zwecke ein Profil der betroffenen Person zu erstellen. Die letztliche Verwendung dieser Daten kann daher Bereiche umfassen, die vom ursprünglich Verantwortlichen in seiner Interaktion mit dem Kunden nicht erwähnt wurden. Solche Endverwendungen können für die betroffenen Personen bedenklich sein, wenn sie überhaupt davon Kenntnis erlangen.6 Tatsächlich gibt es keine Möglichkeit für den Verantwortlichen, alle möglichen Endanwendungen zu erwähnen, da diese nach der Übertragung der Daten nicht mehr in seiner Macht stehen. Dieses Problem ist dem Design der Branche inhärent.

---

4 http://www.iabeurope.eu/tcfdocuments/documents/legal/currenttcfpolicyFINAL.pdf.

5 Zitat aus dem Framework (Betonung nicht im Originaldokument): „Wenn ein CMP der festen Überzeugung ist, dass ein Verkäufer nicht mit der Spezifikation, den Richtlinien oder dem Gesetz übereinstimmt, muss er unverzüglich einen Bericht mit dem MO gemäß den MO-Verfahren einreichen und **kann**, wie in den MO-Verfahren vorgesehen, die Zusammenarbeit mit einem Verkäufer unterbrechen, solange die Angelegenheit untersucht wird“. Dies eröffnet dem für die Verarbeitung Verantwortlichen (Controller) einen vollständigen Ermessensspielraum bei der weiteren Verarbeitung und Verbreitung personenbezogener Daten, auch wenn diesem Controller bekannt ist, dass der Empfänger gegen die Datenschutzbestimmungen verstößt.

6 Im Ryan-Bericht (S. 5) wird dargestellt, dass die heute berüchtigte Firma Cambridge Analytica nur ein Beispiel für die Art der Endempfänger solcher Daten war.

13
Darüber hinaus können die zu verarbeitenden Daten, wie im Bericht von Dr. Ryan beschrieben, besondere Kategorien personenbezogener Daten, sog. sensitive Daten, enthalten. Dass solche Daten ohne jegliche Kontrolle weitergegeben werden, ist äußerst problematisch.

14
Ein weiteres Problem dieses Frameworks liegt darin, dass es darauf abzielt, die Kontrolle über personenbezogene Daten nach deren Übertragung zu beseitigen. Das Framework geht davon aus, dass diejenigen, die solche personenbezogenen Daten verbreiten, sie auch ohne Einwilligung der Betroffenen an Dritte weitergeben.

Das Framework besagt (Betonung nicht im Original): *„Ein Anbieter kann sich aus einem beliebigen Grund dafür entscheiden, keine Daten an einen anderen Anbieter zu übermitteln, aber ein Anbieter darf keine Daten an einen anderen Anbieter übermitteln, ohne dass eine* ***gerechtfertigte Grundlage für die Annahme*** *vorliegt, dass der Verkäufer über eine Rechtsgrundlage für die Verarbeitung der personenbezogenen Daten verfügt. Hat oder erhält ein Anbieter personenbezogene Daten und liegt keine Rechtsgrundlage für den Zugang zu diesen Daten und deren Verarbeitung vor,* ***sollte*** *der Verkäufer die Erhebung und Speicherung der Daten schnellstmöglich einstellen und von einer Datenweitergabe an andere Parteien auch dann absehen, wenn diese Parteien eine Rechtsgrundlage haben."*

15
Denjenigen, die personenbezogene Daten übertragen, wird folglich ein Ermessensspielraum eingeräumt, ob eine „gerechtfertigte Grundlage für die Annahme besteht, dass der Verkäufer über eine Rechtsgrundlage für die Verarbeitung personenbezogener Daten verfügt“. Im Umkehrschluss kann also die Einwilligungseinstellung einer betroffenen Person umgangen werden. Der Anbieter kann auf einer nicht näher spezifizierten „gerechtfertigten Grundlage“ seinen Ermessensspielraum nutzen um festzustellen, dass es einen rechtmäßigen Grund gibt, personenbezogene Daten an Dritte weiterzugeben, auch wenn eine Person die Zustimmung ausdrücklich verweigert hat. Das gesamte System stützt sich also auf das Ermessen und die Beurteilung des Anbieters auf Grundlage vager Begriffe mit unklar definierten Parametern und beruht nicht auf den Wünschen, der Kenntnisnahme oder der Zustimmung des Betroffenen.

16
Zusammenfassend lässt sich sagen, dass das Framework dem Verkäufer einen Ermessensspielraum einräumt, anstatt die Position des Betroffenen zu berücksichtigen. Dies steht im Widerspruch zu den gesetzlichen Anforderungen der DS-GVO. Das Framework versucht eine fiktive Zustimmung zu konstruieren, wobei sich die Verfasser darüber im Klaren sind, dass eine tatsächliche Zustimmung schwer zu erreichen ist. Angesichts der möglichen Verarbeitung von besonderen Kategorien personenbezogener Daten ist es durchaus verständlich, dass versucht wird, den Anbietern eine Form der Ermessensfreiheit einzuräumen. Bedauerlicherweise ist das Ergebnis nicht mehr als ein

Feigenblatt hinsichtlich der Rechte der einzelnen Personen an ihren Daten. Es gibt keine plausible Lesart des Frameworks, welche die individuellen Rechte angemessen berücksichtigt und schützt.

17
Wir stellen fest, dass IAB Europe kürzlich eine Presseerklärung veröffentlicht hat, in der eine Überarbeitung des Frameworks angekündigt wird. Diese Vorschläge werden aber nicht konkretisiert und die Ausführungen adressieren nicht die bestehenden Bedenken. Vielmehr weist die Presseerklärung darauf hin, dass es ein geeigneter Zeitpunkt für die Aufsichtsbehörden wäre, die gesamte Branche zu überprüfen, um eine konsistente und datenschutzkonforme Praxis zu erreichen.

ii. Authorized Buyers

18
Für *Authorized Buyers* gelten eine „Richtlinie“ (guideline)7 und Geschäftsbedingungen (terms of business). Die Richtlinie stößt auf eine Reihe von Bedenken.

19
Die Richtlinie verlagert die Verantwortung für den Datenschutz vom „Data Controller“ auf Dritte, nämlich diejenigen, welche die Daten erhalten. So wird in der Richtlinie Folgendes ausgeführt:

RTB Callout Data Restriction

Zur Auswertung von Seitenaufrufen und von Angeboten auf Basis von Benutzerdaten, die [der Käufer] zuvor erhalten hat, kann [dieser] die verschlüsselte Cookie-ID und die mobile Werbekennung speichern. Alle anderen Callout-Daten mit Ausnahme von Positionsdaten können vom Käufer nach der Beantwortung eines Anzeigenaufrufs und nur zum Zweck der Vorhersage der Verfügbarkeit von Lagerbeständen durch das Authorized Buyers Program gespeichert werden. [Der] Käufer darf die Callout-Daten nur für die Dauer, die zur Erfüllung der oben genannten Zwecke erforderlich ist, und in keinem Fall länger als 18 Monate aufbewahren. Außer wenn [der] Käufer [die Auktion für] einen bestimmten Seitenaufruf gewinnt, ist folgendes nicht erlaubt: (i) Callout-Daten verwenden um mit diesem Seitenaufruf Benutzerlisten oder Benutzerprofile zu erstellen; (ii) Callout-Daten für diesen Seitenaufruf mit Daten Dritter verbinden; oder (iii) Rate Card Daten in irgendeiner Form, einschließlich aber nicht beschränkt auf Zusammenfassungen, mit Dritten teilen.

Datenschutz

Wenn [der] Käufer auf von Google zur Verfügung gestellte personenbezogene Daten, die eine Person direkt oder indirekt identifizieren und die ihren Ursprung im Europäischen Wirtschaftsraum haben („persönliche Daten“), zugreift, sie verwendet oder verarbeitet, gilt folgendes für [den] Käufer:

7 https://www.google.com/doubleclick/adxbuyer/guidelines.html.

• *alle Datenschutz-, Datensicherheits- und Privatsphäregesetze, Richtlinien, Verordnungen und Regeln unter allen anwendbaren Gerichtsbarkeiten sind einzuhalten;*

• *Zugriff und Nutzung personenbezogener Daten ist nur für Zwecke gestattet, die mit der gegebenen Einwilligung der Person konform sind, deren personenbezogene Daten übermittelt wurden;*

• *Geeignete organisatorische und technische Maßnahmen zum Schutz der Mitarbeiter sind zu ergreifen, um die personenbezogenen Daten gegen Verlust, Missbrauch und unbefugten oder rechtswidrigen Zugriff, Offenlegung, Änderung und Vernichtung zu schützen; und*

• *es muss das gleiche Schutzniveau geboten werden, wie es die EU-US-Datenschutzrichtlinie (EU-US Privacy Shield Principles) vorschreibt.*

[Der] Käufer wird [die] Einhaltung dieser Verpflichtung regelmäßig überwachen und hat Google unverzüglich schriftlich zu benachrichtigen, wenn [der] Käufer nicht mehr in der Lage ist, dieser Verpflichtung nachzukommen (oder wenn es ein erhebliches Risiko gibt, dass [der] Käufer dieser Verpflichtung nicht mehr nachkommen kann) und in solchen Fällen wird [der] Käufer entweder die Verarbeitung personenbezogener Daten einstellen oder unverzüglich andere angemessene und geeignete Maßnahmen zur Behebung der Probleme, die einem angemessenen Schutzniveau im Wege stehen, ergreifen.

20
Der zitierte Abschnitt legt nahe, dass *Authorized Buyer*, sobald die personenbezogenen Daten an einen Käufer übermittelt werden, keine wirksame Kontrolle mehr darüber hat, wie diese Daten verwendet werden. Vielmehr wird akzeptiert, dass der Dritte (Käufer) befugt und in der Lage ist, diese Daten zu verwenden. Die einzigen Beschränkungen sind vertraglicher Natur und es ist unklar, inwieweit diese tatsächlich durchgesetzt werden oder werden könnten. Das Gleiche gilt für die „Google Ads Controller-Controller Data Protection Terms“ von Google.8

21
Darüber hinaus werden sogar die auferlegten Einschränkungen ausgehöhlt. Zum Beispiel wird aus der Guideline nicht klar, welche Einschränkungen einem erfolgreichen Bieter auferlegt werden, denn die Einschränkungen gelten für erfolglose Bieter:

Außer wenn [der] Käufer [die Auktion für] einen bestimmten Seitenaufruf gewinnt, ist Folgendes nicht erlaubt: („Unless buyer wins a given impression, it must not …“).

Das offensichtliche Fehlen von Kontrolle gibt Anlass zu ernsthaften Bedenken hinsichtlich der technischen und organisatorischen Sicherheit der relevanten Daten.

22

8 https://privacy.google.com/businesses/controllerterms/.

Darüber hinaus hängt die Wirksamkeit der Datenschutzpolitik allein von den Dritten ab, die Authorized Buyer-Verletzungen freiwillig melden sollen. Es gibt keine ausreichenden technischen Maßnahmen zum Schutz personenbezogener Daten.

D. Die Probleme: Rechtliche Bedenken bezüglich Framework und Guidelines

23
Der oben dargestellte Hintergrund verdeutlicht, dass die Verarbeitung durch die Branche ein erhebliches Risiko für anhaltende Verstöße gegen das Datenschutzrecht und insbesondere gegen die DS-GVO birgt. Datenschutzaufsichtsbehörden berücksichtigen normative Rahmen wie Branchen-Frameworks, wenn es darum geht zu entscheiden, ob regulatorische Maßnahmen ergriffen werden müssen.[9] Die Datenschutzbehörden werden daher ersucht, das IAB-Framework und Googles Guidelines bei der Prüfung der Notwendigkeit von Regulierungsmaßnahmen zu berücksichtigen.

24
Wir sind der Ansicht, dass eine Reihe der in Art. 5 DS-GVO genannten Datenschutzgrundsätze betroffen ist. In diesem Stadium und in Erwartung der Prüfung dieser Beschwerde werden unsere Bedenken hier nicht ausführlich dargelegt. Wir sind der Meinung, dass der Schwerpunkt in erster Linie auf der Prüfung der Rechtmäßigkeit der oben dargestellten Guidelines und Frameworks liegen sollte und nicht bei einzelnen Fällen und Verstößen. Wir fassen unsere wichtigsten Anliegen im Folgenden zusammen.

i. Integrität und Vertraulichkeit

25
Unsere Hauptsorge liegt darin, dass die derzeitigen Rahmenbedingungen und Regelungen der Branche keinen angemessenen Schutz gegen die unbefugte und potenziell unbegrenzte Weitergabe und Verarbeitung personenbezogener Daten bieten.

26
Gemäß Art. 5 Abs. 1 lit. f DS-GVO müssen die Daten „in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit")".

27

9 Für Großbritannien https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/security/.

Das Framework von IAB EUROPE und die Richtlinie von Google bieten insbesondere aus folgenden Gründen keine ausreichende „Integrität und Vertraulichkeit“ für personenbezogene Daten:

a. Sie verlangen nicht, dass die betroffenen Personen über die Verbreitung ihrer Daten oder über die Absicht oder Entscheidung, ihre Daten an Empfänger weiterzugeben, informiert werden.

b. Sie bieten Einzelpersonen keine Möglichkeit, sich bei Verkäufern / Empfängern von Daten dazu zu äußern, wie ihre personenbezogenen Daten verwendet werden dürfen.

c. Sie verweigern den betroffenen Personen ein formelles Recht auf Widerspruch gegen die Verwendung ihrer Daten durch Dritte.

d. Sie bieten keine oder keine ausreichende Kontrolle, um rechtswidrige und/oder genehmigte weitere Nutzungen zu kontrollieren.

ii. Rechtmäßigkeit und Fairness der Verarbeitung

28
Art. 5 Abs. 1 lit. a DS-GVO verlangt, dass personenbezogene Daten rechtmäßig und fair verarbeitet werden. Art. 6 DS-GVO beschreibt die Voraussetzungen einer rechtmäßigen Verarbeitung personenbezogener Daten. Nach Art. 6 Abs. 1 DS-GVO können nur zwei Rechtfertigungen für die Datenverarbeitung der Branche anwendbar sein:

i. die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben (lit. a) oder

ii. die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt (lit. f).

29
Die Zustimmung bzw. Einwilligung ist die zentrale Voraussetzung für eine rechtmäßige Datenverarbeitung. Es liegt in der Natur der Branche, dass sie nicht in der Lage ist, eine angemessene Einwilligung einzuholen. Dies wird auch im Framework anerkannt. Dies gilt insbesondere für Vermittler, die möglicherweise keinen direkten Kontakt mit den Betroffenen haben.

30
Jeglicher Verweis auf berechtigte Interessen wäre bei breit gestreuten RTB-Gebotsanfragen fehl am Platz. Ein solches berechtigtes Interesse gilt nicht absolut, sondern muss mit

den Interessen sowie Grundrechten und -freiheiten der Betroffenen abgewogen werden. Insbesondere wenn die personenbezogenen Daten an eine große Anzahl von Drittunternehmen weitergegeben werden, mit unbekannten Folgen und ohne angemessene Sicherheitsvorkehrungen, kann die Verarbeitung nicht als notwendig und/oder legitim gerechtfertigt werden, wenn man die möglichen Auswirkungen auf die Rechte und Freiheiten der betroffenen Personen berücksichtigt.

31
Ferner bedarf gemäß Art. 9 Abs. 2 DS-GVO die Verarbeitung „besonderer Kategorien personenbezogener Daten" der ausdrücklichen Einwilligung (lit. a), wenn diese Daten nicht durch den Betroffenen „offensichtlich öffentlich gemacht" wurden (lit. e) und keine anderen Ausnahmen gelten. Dem gegenüber ermöglichen es das IAB-Framework und die *Authorized Buyer-Richtlinie* der Branche, Daten ohne Einwilligung zu verarbeiten, einschließlich direkter oder abgeleiteter Daten über die rassische/ethnische Herkunft, politische Meinungen, religiöse/philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit, Sexualleben oder sexuelle Orientierung und zur eindeutigen Identifizierung verarbeitete biometrische sowie genetische Daten. Ohne ausdrückliche Einwilligung zu einer solchen Verarbeitung verstößt dieses Vorgehen gegen Art. 9 DS-GVO.

32
Darüber hinaus ist eine ausdrückliche Einwilligung erforderlich, wenn wesentliche, ausschließlich automatisierte Entscheidungen in Bezug auf eine Person getroffen werden. Die Artikel-29-Arbeitsgruppe legte fest, unter welchen Umständen davon ausgegangen werden muss, dass verhaltensorientierte Werbung, wie sie von der Branche durchgeführt wird, „erhebliche Beeinträchtigungen" im Sinne von Art. 22 DS-GVO zur Folge hat.10 Dies gilt insbesondere dann, wenn gefährdete Personen mit Dienstleistungen angesprochen werden, aus denen ihnen Nachteile erwachsen können, wie z. B. Glücksspiele oder bestimmte Finanzprodukte. Das Fehlen der Möglichkeit, die ausdrückliche Einwilligung einzuholen, ist eine Missachtung von Art. 22 DS-GVO.

33
Dementsprechend bestehen Bedenken, dass die Branche ohne wirksame Einwilligung persönliche Daten und speziell sensitive Daten verarbeitet. Das Framework sieht ein System vor, in dem Daten ohne Zustimmung der betroffenen Person verarbeitet und ver-

---

10Working Paper 251rev.01 (Fußnote 1) S. 10: „In vielen typischen Fällen wird die Entscheidung, auf Profiling beruhende gezielte Werbung zu präsentieren, Personen nicht in ähnlicher Weise erheblich beeinträchtigen, zum Beispiel wenn Werbung für einen Online-Shop eines Mainstream-Modehändlers angezeigt wird, die auf folgendem einfachen demografischen Profil beruht: „Frauen im Raum Brüssel im Alter von 25 bis 35 Jahren, die wahrscheinlich Interesse an Mode und bestimmten Bekleidungsartikeln haben".
Es ist allerdings möglich, dass es in Abhängigkeit von den jeweiligen Umständen doch zu erheblichen Beeinträchtigungen kommt, beispielsweise
• durch den eingreifenden Charakter des Profiling-Prozesses, wenn beispielsweise Personen über mehrere Websites, Geräte oder Dienste verfolgt werden;
• die Erwartungen und Wünsche der betroffenen Personen;
• die Art und Weise der Werbeanzeige oder
• die Ausnutzung von Schwachstellen der betroffenen Personen, an die sich die Anzeige richtet."

breitet werden dürfen. Dies ist nicht rechtmäßig. Eine solche Datenverarbeitung kann auf keinen Fall als „fair“ oder „transparent“ bezeichnet werden.

iii. Angemessenheit, Relevanz und Timing

34
Wir haben Bedenken, ob die Verarbeitung der Daten durch die Branche den Anforderungen aus Art. 5 Abs. 1 lit. c DS-GVO entspricht, der verlangt, dass personenbezogene Daten „dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt“ verarbeitet werden. Die Anzahl der Empfänger der personenbezogenen Daten und die Möglichkeit, dass diese personenbezogenen Daten von den Empfängern weiterverwendet werden, kann schwerwiegende negative Konsequenzen nach sich ziehen.

35
Art. 5 Abs. 1 lit. e DS-GVO schreibt ferner vor, dass personenbezogene Daten, die für einen bestimmten Zweck oder bestimmte Zwecke verarbeitet werden, nicht länger aufbewahrt werden dürfen, als dies für diesen Zweck oder diese Zwecke erforderlich ist. Die Guidelines von *Authorized Buyers* sehen vor (auch wenn sie es aufgrund der fehlenden Kontrolle nicht garantieren können), dass personenbezogene Daten über einen längeren Zeitraum ohne identifizierbaren Zweck aufbewahrt werden.

iv. Data protection by design and default

36
Verhaltensbasierte Werbung hängt von der Fähigkeit ab, Menschen durch die Verwendung digitaler Identifikatoren, die an Geräte gebunden sind (die sich heute zumeist auf eine einzelne Person beziehen), auszusondern oder Verbindungen zu Personen über Geräte und Kontexte hinweg herzustellen. Zu diesen Identifikatoren gehören Web-Fingerabdrücke, die sich auf die eindeutige Einrichtung von Einzelgeräten und Cookies auf Geräten beziehen, so wie dies im Bericht von Dr. Ryan erläutert wird. Diese Identifikatoren sind für Einzelpersonen schwer nachvollziehbar oder abrufbar, um ihre Aufzeichnungen bei den Verantwortlichen, die ihre Informationen speichern, zu kontrollieren. Dies führt zu einem erheblichen Ungleichgewicht und stellt eine erhebliche Barriere für die betroffenen Personen dar, die es ihnen unmöglich macht, wichtige Datenschutzrechte durchzusetzen, wie z. B. die Rechte auf Auskunft, Löschung, Widerspruch, Einschränkung der Verarbeitung und Portabilität.

37
Dies wiederum unterstreicht ein breiteres Anliegen im Zusammenhang mit dem übergreifenden Grundsatz von Treu und Glauben in der DS-GVO (Art. 5 Abs. 1 lit. a): Die Verantwortlichen haben einfachen Zugang zu den Identifikatoren für einzelne Personen, während diese Personen selbst nicht wirklich in der Lage sind, die Identifikatoren zu verwenden oder zu kontrollieren. Dies führt insbesondere zu Bedenken im Hinblick auf Art.

25 DS-GVO, der den Verantwortlichen eine aktive Verpflichtung auferlegt, Datenschutzvorkehrungen wie z. B. für den Datenzugang oder für den Widerspruch in ihre Verfahren und Systeme aufzunehmen.

v. Datenschutz-Folgenabschätzung

38
Angesichts der Streuweite der personenbezogenen Daten und der besonders sensitiven Daten sowie der Vielzahl der Empfänger dieser Daten muss davon ausgegangen werden, dass die Verarbeitung zu einem „hohen Risiko für die Rechte und Freiheiten natürlicher Personen“ führt. Dementsprechend verlangt Art. 35 DS-GVO jeweils eine angemessene Datenschutz-Folgenabschätzung. Nach unserem Kenntnisstand wurde bisher keine ordnungsgemäße Folgenabschätzung durchgeführt oder veröffentlicht.

E. GERICHTSBARKEIT

39
Die Datenschutzaufsichtsbehörden sind für die Aktivitäten zuständig, die in dieser Stellungnahme angesprochen und im Ryan-Bericht beschrieben werden.

i. Verarbeitung personenbezogener Daten

40
Artikel 4 Nr. 1 DS-GVO definiert personenbezogene Daten als „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person“ beziehen. Dazu gehört auch „eine Online-Kennung“, wenn sie es ermöglicht, eine Person direkt oder indirekt zu identifizieren. Der Europäische Gerichtshof (EuGH) hat bestätigt, dass IP-Adressen personenbezogene Daten darstellen können.11 Darüber hinaus werden „pseudonymisierte“ Daten zu einer Person weiterhin als personenbezogene Daten behandelt.

41
Die Verarbeitung und Verbreitung der personenbezogenen Daten einer betroffenen Person während des RTB-Prozesses umfasst auch die Verarbeitung von IP-Adressen oder detaillierterer personenbezogener Daten wie zum Beispiel Standortdaten.

ii. Gerichtsbarkeit

42
Die sich vorliegend beschwerenden Nichtregierungsorganisationen, die Digitale Gesellschaft, das Netzwerk Datenschutzexpertise, die Deutsche Vereinigung für Datenschutz sowie Digitalcourage haben ihren Sitz in der Bundesrepublik Deutschland und vertreten die Grundrechtsinteressen von Internet-Nutzenden in Deutschland.

11 EuGH 19.10.2016 – C-582/14 (Breyer).

43
Gemäß Art. 3 Abs. 2 lit. b DS-GVO gilt die Verordnung für Verantwortliche außerhalb der EU, wenn sich ihre Datenverarbeitung auf die Beobachtung des Verhaltens von Betroffenen in der EU bezieht.

44
Die Branche ist bestrebt, Werbeanzeigen für Kunden im jeweiligen Gebiet anzubieten; daher ist der Ort der Niederlassung der verschiedenen beteiligten Unternehmen für den Geltungsumfang der DS-GVO und die Zuständigkeit der deutschen Aufsichtsbehörden irrelevant.

45
Gemäß Art. 51 DS-GVO und § 40 BDSG sind die Datenschutzaufsichtsbehörden der Bundesländer die zuständige Aufsichtsbehörden in Deutschland. Die Aufgaben der Aufsichtsbehörden sind in Art. 57 DS-GVO beschrieben und umfassen die Überwachung und Durchsetzung der DS-GVO. Um dieser Aufgabe gerecht zu werden, haben sie gemäß Art. 58 Abs. 1 lit. b DS-GVO die Befugnis, „Untersuchungen in Form von Datenschutzüberprüfungen durchzuführen“.

46
Die Datenschutzaufsichtsbehörden sind mit der Bearbeitung von Beschwerden betraut, die von einer betroffenen Person gemäß Art. 77 DS-GVO eingereicht werden. Diese Beschwerde wird von den für die genannten Nichtregierungsorganisationen unterzeichnenden Personen auch im eigenen Namen eingereicht.

47
Eine entsprechende Beschwerde wurde beim irischen Datenschutzbeauftragten erhoben; weitere Beschwerden werden derzeit bei anderen nationalen Aufsichtsbehörden eingereicht. Angesichts der europaweiten Dimension der in dieser Beschwerde aufgeworfenen Fragen und Unternehmen erscheint es sinnvoll, dass die Aufsichtsbehörden dieses Thema gemeinsam prüfen. Wir fordern die deutschen Aufsichtsbehörden deshalb auf, mit anderen nationalen Aufsichtsbehörden zusammenzuarbeiten, um eine gemeinsame Untersuchung gemäß Art. 62 DS-GVO durchzuführen.

F. Anfragen

48
Die Datenschutzaufsichtsbehörden erhalten individuelle Beschwerden von Frau Elisabeth Niekrenz, Herrn Thilo Weichert, Herrn Frank Spaeing und Herrn Friedemann Ebelt. Alle vier genannten Unterzeichnenden nutzen das Internet und sind von der in dieser Beschwerde genannten verhaltensbasierten Werbung betroffen. Zusätzlich zur Prüfung der individuellen Beschwerde und deren Bescheidung bitten wir die Aufsichtsbehörden, im Rahmen ihrer Befugnisse und ihres Mandats weitere Schritte zu unternehmen.

49

Gemäß Art. 58 Abs. 1 lit b DS-GVO sind die Aufsichtsbehörden befugt, Datenschutzüberprüfungen durchzuführen. Die Verantwortlichen sind gemäß § 40 Abs. 4 BDSG verpflichtet, hierfür alle erforderlichen Auskünfte zu erteilen. Die Aufsichtsbehörden sind befugt, Einblick in relevante Dokumente zu nehmen und die stattfindende Datenverarbeitung zu überprüfen. Die Aufsichtsbehörden haben die Beschwerdeführer über die Ergebnisse der Überprüfung gemäß Art. 77 Abs. 2 DS-GVO zu unterrichten. Hierbei sollte auf folgende Umstände eingegangen werden:

a. Es fehlen geeignete Garantien für Sicherheit und Integrität der genannten Daten.

b. Personenbezogene Daten und besondere Kategorien personenbezogener Daten werden verarbeitet.

c. Es ist fragwürdig, ob den Verarbeitungen wirksame Einwilligungen zugrunde liegen.

d. Es fehlt an einer Datenschutz-Folgenabschätzung.

50
Wir fordern die Datenschutzaufsichtsbehörden auf, ihre Befugnisse sowohl gegenüber dem *IAB Europe* Framework als auch im Hinblick auf Googles *Authorized Buyers* auszuüben. Da es einzelnen Betroffenen, nicht zuletzt wegen des Umfangs und der Komplexität der genannten Geschäftspraktiken, nicht möglich ist zu bewerten, inwieweit die gesamte Branche die rechtlichen Verpflichtungen allgemein einhält, geschweige denn diese Einhaltung sicherzustellen, ist der Sachverhalt der verhaltensbasierten Werbung eine vorrangige Aufgabe für die Datenschutzaufsicht.

ii. Verhaltenscodex (Code of practice)

51
Art. 40 DS-GVO sieht vor, dass Verbände und andere Vereinigungen Verhaltensregeln ausarbeiten können, die präzisierend eine „faire und transparente Verarbeitung“ mit einer Vielzahl von Vorkehrungen regeln. Diese sollen von den Aufsichtsbehörden gefördert werden und sind letztlich von diesen zu genehmigen. Es ist wünschenswert, dass für personalisierte Werbung derartige mit den Anforderungen der DS-GVO konforme Verhaltensregeln ausgearbeitet und dass deren Einhaltung im Rahmen regulierter Selbstregulierung überwacht wird.

52.
Es steht außer Frage, dass die öffentlich dokumentierten Aktivitäten der Branche, wie sie im Bericht von Dr. Ryan dargelegt werden, Leitlinien (good practice guidance) für diese Branche notwendig machen, um sicherzustellen, dass das Datenschutzrecht eingehalten wird und dass so die Rechte der Betroffenen gewahrt bleiben. Einzelfallklagen von Betroffenen werden nicht ausreichen, um den weitreichenden Bedenken hinsichtlich der Praktiken der Branche im Sinne des öffentlichen Interesses Rechnung zu tragen. Die Datenschutzaufsichtsbehörden werden dringend aufgefordert, Maßnahmen zu ergreifen

und Leitlinien speziell für diesen Teil des Profiling-Sektors zu erstellen.

iii. Einvernehmliche Prüfung (*Consensual audit)*

53
Den Aufsichtsbehörden ist es erlaubt, einvernehmliche Prüfungen durchzuführen. Angesichts der weitreichenden und systematischen Probleme, die in der vorliegenden Beschwerde sowie in dem Bericht von Dr. Ryan aufgezeigt wurden, ersuchen wir die Aufsichtsbehörden, im Rahmen ihrer Befugnisse einvernehmliche Prüfungen bei den beteiligten Unternehmen anzustreben, um in der gesamten Branche eine gute Praxis durchzusetzen. Werden die Untersuchungs- und Abhilfebefugnisse der Datenschutzaufsicht nicht umfassend wahrgenommen, so erscheint es unwahrscheinlich, dass die tief verwurzelten und sich weiter verschlimmernden Probleme gelöst werden können. Parallel zu den vorliegenden Beschwerden werden *IAB Europe* und *Google Authorized Buyers* angeschrieben und dabei aufgefordert, einer solchen Untersuchung freiwillig zuzustimmen und diese aktiv zu unterstützen.

G. Nächste Schritte

54
Aus den oben genannten Gründen werden die Datenschutzaufsichtsbehörden gebeten, eine allgemeine Untersuchung der Tätigkeiten der Branche einzuleiten und die in dieser Vorlage beschriebenen Maßnahmen zu ergreifen.

55
Eines der großen Probleme bei den oben beschriebenen Formen der Datenverarbeitung ist, dass sie so umfangreich und komplex sind, dass sie jede und jeden zu jeder Zeit betreffen können. Es betrifft Individuen, einschließlich schutzbedürftiger Personen, in allen Lebensbereichen und in der gesamten Europäischen Union. Wir fordern die deutschen Datenschutzaufsichtsbehörden daher auf, mit den Kollegen in den anderen Mitgliedstaaten zusammenzuarbeiten, um eine gemeinsame Untersuchung gemäß Art. 62 DS-GVO durchzuführen. Wir behalten uns das Recht vor, diese Beschwerde gegebenenfalls durch weitere Beweise und Argumente zu ergänzen. In der Zwischenzeit zögern Sie bitte nicht, uns zu kontaktieren, wenn wir Ihnen weiterhelfen können. Wir wären Ihnen dankbar, wenn Sie uns gemäß Art. 77 Abs. 2 DS-GVO über die als Reaktion auf diese Beschwerde ergriffenen Maßnahmen auf dem Laufenden halten würden.

Elisabeth Niekrenz, Digitale Gesellschaft, Groninger Straße 7, 13347 Berlin

Thilo Weichert, Netzwerk Datenschutzexpertise, Waisenhofstr. 41, 24103 Kiel

Frank Spaeing, Deutsche Vereinigung für Datenschutz, Reuterstraße 157, 53113 Bonn

Friedemann Ebelt, Digitalcourage, Marktstraße 18, 33602 Bielefeld

Berlin, Kiel, Bonn, Bielefeld **4. Juni 2019**