Rechtsanwalt Dr. Martin Bahr

Updates in Sachen Tracking, Cookies, Pseudonyme und Nutzerprofile

Die Datenschutzkonferenz (DSK) hat im März 2019 ein neues Dokument zu der kontrovers diskutierten Frage herausgegeben, inwieweit unter der DSGVO der Einsatz von Tracking-Technologien noch erlaubt ist. Das Dokument umfasst 25 Seiten und ist sehr praxisbezogen. So wird anhand eines konkreten Beispiels auf drei Seiten der Einsatz eines Tracking-Pixels erläutert.
Jedem Webseiten-Betreiber, der Tracking-Technologien einsetzt, kann daher nur dringend angeraten werden, sich das Papier einmal näher anzuschauen. Die Äußerungen sind in mehrfacher Hinsicht sehr lesenswert.

A. Neues Papier der Datenschutzkonferenz

Die Datenschutzkonferenz (DSK) ist der Zusammenschluss der Datenschutzbehörden in Deutschland. Die Stellungnahmen dieses Gremiums haben zwar keinen verbindlichen Rechtscharakter, offenbaren aber, in welche Richtung die Behörden die DSGVO auslegen. Ob die Interpretation dann richtig oder falsch ist, werden die Gerichte entscheiden.

Bereits im April 2018, kurz vor Inkrafttreten der DSGVO, hatte die DSK eine Orientierungshilfe zum Tracking veröffentlicht.[1] Dieses Papier war vonseiten der meisten Internet-Unternehmen heftig kritisiert worden. Nicht nur die theoretischen Ausführungen eckten an, sondern auch die extrem restriktive Interpretation nervte viele User.

Nun hat die DSK nachgelegt und im März 2019 ein neues Papier veröffentlicht.[2] Es trägt den Namen *„Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien“* und umfasst 25 Seiten. Die Ausführungen sind – anders als im vorherigen Dokument – sehr praxisbezogen. So erläutert das Gremium beispielsweise den Einsatz eines Tracking-Pixels auf mehr als drei Seiten.

Jedem Webseiten-Betreiber, der Tracking-Technologien einsetzt, kann daher nur dringend angeraten werden, sich das Papier einmal näher anzuschauen. Die Äußerungen sind in mehrfacher Hinsicht sehr lesenswert.

Bevor wir im Nachfolgenden inhaltlich auf das Dokument eingehen, noch ein wichtiger Hinweis: Wie immer bei Stellungnahmen der DSK ist es wichtig, im Hinterkopf zu behalten, dass die Aussagen keine rechtsverbindliche Wirkung haben. Vielmehr werden die im Zweifelsfall angerufenen Gerichte das letzte Wort haben. Der Ausgang eines Gerichtsverfahrens ist damit nicht selten vollkommen offen. Die Standpunkte der DSK sind keineswegs in Stein gemeißelt, sondern es gilt, sie kritisch zu hinterfragen und zu überprüfen.

B. Das Dokument im Einzelnen

1. §§ 12, 15 TMG außer Kraft

Auch in ihrer neusten Stellungnahme bleibt die DSK dabei: §§ 12 und 15 des Telemediengesetzes (TMG) sind durch die DSGVO verdrängt und finden somit keine Anwendung mehr. Dies bedeutet: Die im Netz übliche Praxis, die Erstellung von Pseudonymen auf § 15 Abs. 3 TMG zu stützen, ist damit nicht mehr möglich.

Ob diese Ansicht der DSK wirklich zutreffend ist, kann bezweifelt werden. Denn es sprechen zahlreiche und gute Argumente für die Anwendbarkeit des TMG auch weiterhin nach dem 25.05.2018. Jedem Webseiten-Betreiber sollte aber klar sein, dass für ihn ein nicht unerhebliches Risiko besteht, wenn er seine Datenverarbeitung weiterhin auf diese Norm stützt.

2. Definition von Tracking

Die DSK definiert erstmalig auch, was sie überhaupt unter Tracking versteht:

„... Datenverarbeitung zur – in der Regel websiteübergreifenden – Nachverfolgung des individuellen Verhaltens von Nutzern.“

DER AUTOR

Die **Kanzlei Dr. Bahr** *(http://www.Dr-Bahr.com)* ist auf den Bereich des Rechts der Neuen Medien und den gewerblichen Rechtsschutz (Marken-, Urheber- und Wettbewerbsrecht) spezialisiert. Unter *Suchmaschinen-und-Recht.de* betreibt sie seit 2005 ein eigenes Themenportal zur rechtlichen Dimension von Suchmaschinen.

[1] Positionsbestimmung der DSK v. 26.04.2018, Download: https://bit.ly/2r8Iq06. .
[2] Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien, Download: https://bit.ly/2GPTGrn.

3. Alle DSGVO-Rechtfertigungsgründe sind gleich

In ihren bisherigen Äußerungen hatten die deutschen Datenschutzbehörden immer den Erlaubnistatbestand der berechtigten Interessen (Art. 6 Abs. 1 f.) DSGVO) sehr stiefmütterlich behandelt und den Standpunkt vertreten, dass nur die Einwilligung eine Rechtsgrundlage für das Tracking darstellen könne.

Diese Ansicht hat das Gremium aufgegeben. Nunmehr steht der Rechtfertigungsgrund der berechtigten Interessen gleichberechtigt neben den Möglichkeiten der Einwilligung und des Vertrages. Dies bedeutet, dass die DSK nunmehr anerkennt, dass Tracking oder das Setzen von Cookies auch durch den Anwendungsfall der berechtigten Interessen gerechtfertigt sein können. Dies hatte die DSK bislang anders gesehen.

4. Ausführungen zur Einwilligung

Die DSK macht ganz konkrete Ausführungen zur Einwilligung:

„Insbesondere wenn bei der betroffenen Person erhobene Daten von dem jeweiligen Diensteanbieter (inkl. eingebundener Dienste) website-übergreifend zusammengeführt und ausgewertet werden, ist zu berücksichtigen, dass die betroffenen Personen für eine wirksame Einwilligung vorab über jegliche Form der durchgeführten Datenverarbeitung sowie sämtliche Empfänger ausführlich informiert werden und die Möglichkeit erhalten müssen, in die einzelnen Formen der Datenverarbeitung spezifisch einzuwilligen.

In Fällen, in denen sich mehrere (gemeinsame) Verantwortliche auf die ersuchte Einwilligung stützen wollen, oder in denen die Daten an andere Verantwortliche übermittelt oder von anderen Verantwortlichen verarbeitet werden sollen, müssen diese Organisationen sämtlich genannt und die Verarbeitungsaktivitäten der einzelnen Organisationen hinreichend beschrieben werden.“

Nach Meinung der DSK ist somit zwingende Voraussetzung für eine wirksame Einwilligung:

- **Nennung sämtlicher Empfänger**
- **ausführliche Aufklärung über Inhalt und Reichweite der jeweiligen Erklärung**
- **bereichsspezifische Einwilligung**

In der Praxis ist diese Voraussetzung aus mehreren Gründen nicht erfüllbar. Beispielsweise beim Retargeting ist unklar, welche Unternehmen genau die Daten erhalten. Dies bedeutet für die Praxis: Auf die Möglichkeit der Einwilligung werden sich nur die Webseiten-Betreiber berufen können, die lediglich begrenzt auf ihre Page die Daten verarbeiten. Alle Unternehmen, die hingegen das übliche webseitenübergreifende Tracking einsetzen, werden sich auf die Einwilligung nicht berufen können.

Deutliche Worte findet das Gremium auch zum üblichen Cookie-Banner-Wahnsinn auf vielen Seiten:

„Auch genügt es für eine Einwilligung i. S. d. DSGVO nicht, wenn, wie bei vielen einfachen Cookie-Bannern im Web, ein Hinweis auf das Setzen von Cookies zusammen mit einem ‚OK‘-Button erfolgt. In diesen Fällen fehlt es an der nach Art. 7 DSGVO erforderlichen Freiwilligkeit, wenn die betroffenen Personen zwar ‚OK‘ drücken können, aber keine Möglichkeit erhalten, das Setzen von Cookies abzulehnen.“

5. Berechtigte Interessen

Da – wie zuvor erläutert – die DSK bei der Einwilligung in der Praxis nicht erfüllbare Voraussetzungen verlangt, bleibt für den Webseiten-Betreiber nur noch der Erlaubnis-Tatbestand der berechtigten Interessen nach Art. 6 Abs. 1 f.) DSGVO über.

Das Gremium empfiehlt dabei eine dreistufige Zulässigkeitsprüfung:

1. **Stufe: Vorliegen eines berechtigten Interesses des Verantwortlichen oder eines Dritten**
2. **Stufe: Erforderlichkeit der Datenverarbeitung zur Wahrung dieser Interessen**
3. **Stufe: Abwägung mit den Interessen, Grundrechten und Grundfreiheiten der betroffenen Person im konkreten Einzelfall**

Als berechtigte Interessen im Rahmen der 1. Stufe nennt die Konferenz dabei u. a.:

- *„Bereitstellung besonderer Funktionalitäten, z. B. die Warenkorb-Funktion unter Verwendung eines sog. Session-Identifiers,*
- *Freie Gestaltung der Website auch unter Effizienz- und Kosteneinsparungserwägungen, z. B. Einbindung von Inhalten, die auf anderen Servern gehostet werden, Nutzung von Content Delivery Networks (CDN), Web Fonts, Kartendiensten, Social-Plugins, etc.*
- *Integrität und Sicherheit der Website; IT-Security-Maßnahmen sind bspw. das Speichern von LogDateien und insbesondere IP-Adressen für einen längeren Zeitraum, um Missbrauch erkennen und abwehren zu können,*
- *Reichweitenmessung und statistische Analysen,*
- *Optimierung des jeweiligen Webangebots und Personalisierung/Individualisierung des Angebots abgestimmt auf die jeweiligen Nutzer,*
- *Wiedererkennung und Merkmalszuordnung der Nutzer, z. B. bei werbefinanzierten Angeboten*
- *Betrugsprävention, Abwehr von den Dienst überlastenden Anfragen (Denial of Service-Attacken) und Bot-Nutzung“*

Im Rahmen der 2. Stufe merkt die DSK an, dass es wichtig sei, an das Merkmal der Erforderlichkeit strenge Voraussetzungen zu stellen:

„Allein das Vorliegen eines berechtigten Interesses reicht nicht aus, um die Datenverarbeitung zu legitimieren. Zwingend ist, dass die jeweilige Datenverarbeitung zur Wahrung dieses Interesses erforderlich ist. Erforderlichkeit meint, dass die Verarbeitung geeignet ist, das Interesse (Motiv/Nutzen der Verarbeitung) des Verantwortlichen zu erreichen, wobei kein milderes, gleich effektives Mittel zur Verfügung steht.

Das bedeutet, dass der Verantwortliche die Verarbeitung auf das notwendige Maß zu beschränken hat."

Konkret zum webseitenübergreifenden Tracking heißt es:

„Setzt der Website-Betreiber hierfür ein Analyse-Tool ein, welches Daten über das Nutzungsverhalten betroffener Personen an Dritte weitergibt (z. B. soziale Netzwerke oder externe Analysedienste, die Nutzungsdaten über die Grenze der Website hinweg mit Daten von anderen Websites zusammenführen), ist dies nicht mehr erforderlich.

Das Ziel – Reichweitenmessung – kann auch mit milderen, gleich geeigneten Mitteln erreicht werden, die deutlich weniger personenbezogene Daten erheben und diese nicht an Dritte übermitteln (z. B. ohne Einbindung Dritter über eine lokale Implementierung einer Analysesoftware)."

Im Rahmen der 3. Stufe empfiehlt die DSK dann das nachfolgende Prüfungsschema:

a. *„Vernünftige Erwartung der betroffenen Personen und Vorhersehbarkeit/Transparenz*
b. *Interventionsmöglichkeiten der betroffenen Personen*
c. *Verkettung von Daten*
d. *Beteiligte Akteure*
e. *Dauer der Beobachtung*
f. *Kreis der Betroffenen (bspw. besonders schutzbedürftige Personen)*
g. *Datenkategorien*
h. *Umfang der Datenverarbeitung"*

6. Pseudonymisierung

Zur Pseudonymisierung merkt das Gremium an, dass in einer Vielzahl von Fällen gar keine wirkliche Pseudonymisierung vorliege, da die Daten weiterhin identifizierbar seien:

„Im Hinblick auf die Verwendung von Pseudonymen ist generell anzumerken, dass die Tatsache, dass die Nutzer etwa über IDs oder Kennungen bestimmbar gemacht werden, keine Pseudonymisierungsmaßnahme i. S. d. DSGVO darstellt. Zudem handelt es sich nicht um geeignete Garantien zur Einhaltung der Datenschutzgrundsätze oder zur Absicherung der Rechte betroffener Personen, wenn zur (Wieder-) Erkennung der Nutzer IP-Adressen, Cookie-IDs, Werbe-IDs, Unique-User-IDs oder andere Identifikatoren zum Einsatz kommen.

Denn, anders als in Fällen, in denen Daten pseudonymisiert werden, um die identifizierenden Daten zu verschleiern oder zu löschen, sodass die betroffenen Personen nicht mehr adressiert werden können, werden IDs oder Kennungen dazu genutzt, die einzelnen Individuen unterscheidbar und adressierbar zu machen. Eine Schutzwirkung stellt sich folglich nicht ein. Es handelt sich daher nicht um Pseudonymisierungen i. S. d. ErwGr 28, die die Risiken für die betroffenen Personen senken und die Verantwortlichen und die Auftragsverarbeiter bei der Einhaltung ihrer Datenschutzpflichten unterstützen.

Darüber hinaus ist zu berücksichtigen, dass sich Nutzer in den allermeisten Fällen früher oder später an irgendeiner Stelle im Web registrieren und in diesen Fällen auch eine Verknüpfung mit E-Mail-Adressen, Klarnamen oder Offline-Adressen möglich ist. Auf die Kenntnis des bürgerlichen Namens zur Identifikation von betroffenen Personen kommt es aber beim Personenbezug nicht an. Wenn die Nutzung des Webs, wie bei vielen Menschen, einen großen Teil der Lebenswirklichkeit widerspiegelt, dann ist es relevant, ob die Nutzer über ihre Online-Kennungen bestimmbar oder adressierbar sind. Die DSGVO geht davon aus, dass eine indirekte Identifizierung auch durch Aussondern erfolgen kann."

C. Ausblick in die Zukunft

Die DSK ist zunächst zu loben für die durchgehend praxisnahen, sehr lesenswerten Ausführungen in ihrem aktuellen Dokument. Jedem Unternehmen, das mit Tracking, Cookies oder Pseudonymen zu tun hat, kann das Paper nur wärmstens ans Herz gelegt werden.

Der Grundkonflikt zwischen Theorie und Praxis bleibt aber bestehen. Nach der restriktiven Ansicht der DSK ist webseitenübergreifendes Tracking, d. h. jedes Retargeting, nach der DSGVO nicht möglich, da die Voraussetzungen nicht erfüllbar sind. Gleichwohl setzen in Deutschland nach wie kommerzielle Unternehmensseiten eine Vielzahl unterschiedlichster Tracking-Technologien ein.

Dieser offensichtliche Widerspruch ist ein großes Dilemma im deutschen Datenschutzrecht und hat sich durch die DSGVO nicht verbessert. Es bleibt abzuwarten, ob und wie die Aufsichtsbehörden ihren Standpunkt durchsetzen werden. ¶