Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

POSTANSCHRIFT Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
Postfach 1468, 53004 Bonn

HAUSANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
FON (0228) 997799-0
E-MAIL Referat23@bfdi.bund.de
BEARBEITET VON
INTERNET www.bfdi.bund.de
DATUM Bonn, 16.05.2023
GESCHÄFTSZ. 23-501-10/017#0244

Bitte geben Sie das vorstehende Geschäftszeichen bei allen Antwortschreiben unbedingt an.

An
die behördlichen Datenschutzbeauftragten
der obersten Bundesbehörden
sowie deren nachgeordnete Bereiche

BETREFF **Rundschreiben Telemedien 01/2023: Tracking, Cookies, Banner**

Sehr geehrte Damen und Herren,

Webseiten der Behörden sind ein wichtiger Bestandteil der Öffentlichkeitsarbeit. § 3 des Gesetzes zur Förderung der elektronischen Verwaltung (EGovG) verpflichtet Behörden deshalb, über ihre Aufgaben, ihre Anschrift, Geschäftszeiten sowie Erreichbarkeiten im Internet zu informieren.

Webseiten können zwar grundsätzlich ohne den Einsatz einwilligungsbedürftiger Trackingtechnologien gestaltet werden, gleichwohl möchten viele Webseitenbetreiberinnen und -betreiber die Aktivitäten der Nutzenden bei dem Besuch ihrer Webseiten nachverfolgen, etwa um Statistiken zur Verbesserung der Nutzbarkeit des Telemedienangebots zu erheben. Dies ist auch bei den öffentlichen Stellen des Bundes zu sehen. In diesem Zusammenhang treten immer wieder Fragen hinsichtlich der datenschutzrechtlichen Vorgaben für Tracking, Cookies und Banner auf. Mir ist bewusst, dass diese Vorgaben nicht leicht zu verstehen sind. Deshalb und aufgrund des hohen Beratungsbedarfs möchte ich mit dieser Handreichung eine Einführung zu den wichtigsten Fragen rund um die Thematik mit der Bitte um Beachtung und ggf. Anpassung Ihrer Webseiten bereitstellen.

Meine Ausführungen berücksichtigen insbesondere die Wertungen, die sich aus der Orientierungshilfe Telemedien 2021 Version 1.1 (abrufbar unter https://www.bfdi.bund.de/DE/Buerger/Inhalte/Telemedien/Cookie-Banner.html) und dem Abschlussbericht der Cookie Banner Taskforce des Europäischen Datenschutzausschusses

(abrufbar unter https://edpb.europa.eu/system/files/2023-01/edpb_20230118_report_cookie_banner_taskforce_en.pdf) ergeben.

1. Welche datenschutzrechtlichen Regelungen müssen beim Einsatz von Trackingtechnologien beachtet werden?

Für den Einsatz von Trackingtechnologien sind aus datenschutzrechtlicher Sicht das Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG) und, soweit personenbezogene Daten verarbeitet werden, die Datenschutz-Grundverordnung (DSGVO) relevant. Das TTDSG ist, anders als die DSGVO, auf alle Informationen und damit auch auf nicht-personenbezogene Daten anwendbar. Im Verhältnis zur DSGVO gehen die Regelungen des TTDSG grundsätzlich vor.

Das TTDSG dient unter anderem dem Schutz der Privatsphäre bei Endeinrichtungen. Nutzende müssen nicht unbedingt erforderliche und unerwünschte Zugriffe auf ihre Endgeräte wie Computer, Tablets oder Handys nicht hinnehmen, und zwar unabhängig davon, ob mit dem Zugriff eine Verarbeitung ihrer personenbezogenen Daten verbunden ist.

Die DSGVO findet allein bei der Verarbeitung personenbezogener Daten Anwendung, also etwa bei einer Verhaltensanalyse oder Profilbildung. TTDSG und DSGVO gelten grundsätzlich für alle Trackingtechnologien wie Cookies, Skripte oder Fingerprints.

2. Wann müssen Einwilligungen von Nutzenden eingeholt werden?

Grundsätzlich fordert § 25 Absatz 1 TTDSG für den Einsatz von Cookies und anderen Trackingtechnologien eine Einwilligung – konkret für das Speichern von Informationen auf einem Endgerät und für den Zugriff auf Informationen, die bereits auf einem Endgerät gespeichert sind. Dieses Einwilligungserfordernis greift unabhängig davon, ob und wie eine Verarbeitung personenbezogener Daten stattfindet.

Eine Ausnahme gilt für Zugriffe, die technisch unbedingt erforderlich sind, um Nutzenden einen ausdrücklich gewünschten Telemediendienst bereitzustellen. Daher können ohne Einwilligung etwa Cookies gesetzt werden, die technisch erforderlich sind, damit Nutzende sich in einem Konto anmelden können. Die Ausnahme kann aber etwa nicht für Technologien gelten, mit denen die Aktivitäten Nutzender nachverfolgt werden, auch wenn das etwa zur Verbesserung der Webseite wünschenswert ist.

Die Ausnahme vom Einwilligungserfordernis greift auch nicht pauschal für mehrere Funktionen oder Inhalte einer Webseite. Vielmehr muss die Erwartungshaltung der Nutzenden

bei dem Aufruf der Webseite oder App berücksichtigt werden, sodass regelmäßig etwa Kontaktformular, Chatmöglichkeit oder Routenplaner eigenständige Telemediendienste darstellen. Die Zugriffe dürfen damit erst erfolgen, wenn die Nutzenden den spezifischen Dienst auch tatsächlich in Anspruch nehmen möchten (siehe hierzu auch Abschnitt 7.).

Zudem ist bei der technischen Ausgestaltung der Webseite unbedingt darauf zu achten, dass einwilligungsbedürftige Zugriffe erst nach erteilter Einwilligung erfolgen.

Soweit personenbezogene Daten verarbeitet werden, muss eine Ausnahme vom Verarbeitungsverbot des Artikel 6 Absatz 1 DSGVO die Datenverarbeitung rechtfertigen. Für die Weiterverarbeitung mithilfe Cookies oder anderer Trackingtechnologien erhobener personenbezogener Daten kann eine Einwilligung erforderlich sein, wenn keine andere Rechtsgrundlage des Artikels 6 Absatz 1 DSGVO einschlägig ist.

Schließlich möchte ich darauf hinweisen, dass die Weiterverarbeitung personenbezogener Daten nicht rechtmäßig sein kann, wenn eine nach TTDSG erforderliche Einwilligung nicht wirksam eingeholt wurde.

3. Können andere Rechtsgrundlagen der DSGVO den Einsatz von Trackingtechnologien rechtfertigen?

Die Verarbeitung personenbezogener Daten im Zusammenhang mit dem Einsatz von Trackingtechnologien kann in Einzelfällen auch auf Grundlage einer anderen Rechtsgrundlage als einer Einwilligung erfolgen. Für Bundesbehörden ist hier etwa an Artikel 6 Absatz 1 Buchstabe e, Absatz 3 DSGVO in Verbindung mit § 3 E-Government-Gesetz (EGovG) zu denken, wonach Datenverarbeitungen rechtmäßig sind, die für die Wahrnehmung der öffentlichen Aufgabe der Öffentlichkeitsarbeit im Internet erforderlich sind. Die Erforderlichkeit muss in jedem Einzelfall geprüft werden. Geht die Datenverarbeitung über das erforderliche Maß hinaus, kann nur eine Einwilligung der Nutzenden eingeholt werden.

Dies hilft allerdings nicht darüber hinweg, dass Trackingtechnologien regelmäßig mit Zugriffen auf Endgeräte einhergehen, die nach § 25 TTDSG grundsätzlich nur mit einer Einwilligung der Nutzenden zulässig sind (siehe hierzu Abschnitt 2 oben).

Vorbehaltlich Besonderheiten im Einzelfall können folgende Beispiele der Veranschaulichung der vorherigen Ausführungen dienen:

- Setzen eines Session-Cookies für die Abwehr von DoS-Attacken:
    - Nicht einwilligungsbedürftig nach § 25 Absatz 2 Nummer 2 TTDSG

    - Rechtfertigung der Datenverarbeitung über Artikel 6 Absatz 1 littera e DSGVO in Verbindung mit § 3 Absatz 1 E-Government-Gesetz (EGovG)
- Ausführen eines Javascripts zur Erhebung der Bildschirmgröße zum Zweck „Optimierung der Webseite“:
    - Einwilligungsbedürftig nach § 25 Absatz 1 TTDSG
    - Rechtfertigung der Datenverarbeitung über Artikel 6 Absatz 1 littera e DSGVO in Verbindung mit § 3 Absatz 1 EGovG, WENN für die konkrete Verarbeitungstätigkeit eine Erforderlichkeit für die öffentliche Aufgabenwahrnehmung bejaht werden kann, oder über eine Einwilligung nach Artikel 6 Absatz 1 littera a DSGVO

4. Was ist zu beachten, wenn rechtmäßig erhobene personenbezogene Daten zu anderen Zwecken verarbeitet werden sollen?

Werden personenbezogene Daten zu anderen Zwecken weiterverarbeitet, als zu denen sie erhoben wurden, müssen zusätzlich die Anforderungen an die Zweckänderung des Artikel 6 Absatz 4 DSGVO beachtet werden. Der Verantwortliche muss dann unter Berücksichtigung der in Artikel 6 Absatz 4 Buchstaben a bis e DSGVO aufgelisteten Belange die Zweckvereinbarkeit positiv feststellen und dokumentieren, außer die Weiterverarbeitung beruht auf einer Einwilligung oder einer qualifizierten Rechtsgrundlage im Sinne des Artikel 23 DSGVO.

Zu einer solcher Zweckänderung kann es etwa bei der Analyse der Server-Logfiles kommen, die Aktivitäten von Nutzenden auf Webseiten protokollieren, sofern nicht ohnehin eine Einwilligung eingeholt wird oder werden muss. Solche Daten wurden insbesondere erhoben, um die Webseite bereitzustellen und die Sicherheit zu gewährleisten. Sollen diese Daten nachträglich etwa zu Zwecken der Optimierung der Webseite genutzt werden, muss eine Rechtsgrundlage nach Artikel 6 Absatz 1 DSGVO vorliegen und die Anforderungen der Zweckbindung eingehalten werden.

5. Wie sind Einwilligungsbanner zu gestalten?

Einwilligungen, die nach TTDSG und ggf. nach DSGVO erforderlich sind, werden auf Webseiten üblicherweise mit sogenannten Einwilligungsbannern eingeholt. Die Banner sind Fenster, die einer Webseite vorgeschaltet sind und in denen Nutzende ihr informiertes Einverständnis zu Zugriffen auf ihr Endgeräte und ggf. für die Verarbeitung ihrer personenbezogenen Daten geben oder ablehnen können. Das TTDSG verweist für die Anforderungen an die Einwilligung und die Information auf die DSGVO, sodass sich diese im Kern nicht unterscheiden.

Die Einwilligungen nach TTDSG und DSGVO können gebündelt im Banner abgefragt werden, wenn dies aus der Abfrage eindeutig erkennbar wird.

Grundsätzlich sollte der Banner nur die, aber auch nicht weniger, Informationen enthalten, die für die Abfrage der konkreten Einwilligungen erforderlich sind. Informationen, die für die Einwilligung nicht relevant sind, etwa zu technisch unbedingt erforderlichen Cookies für die keine Einwilligung erforderlich ist, gehören daher grundsätzlich nicht in das Banner.

Wie umfangreich die Informationen konkret sein müssen, die im Banner angezeigt werden, ist immer eine Frage des Einzelfalls und bedarf einer Abwägung zwischen den Anforderungen der Transparenz und der Verständlichkeit. Hierbei kann es zulässig sein, bestimmte Informationen auch erst auf einer zweiten Ebene des Cookies-Banners anzuzeigen.

Nutzenden müssen bei Erteilung der Einwilligung – und damit auf erster Ebene des Cookies-Banners – zumindest folgende Informationen bereitgestellt werden:

- Tragweite der Entscheidung in verständlicher Form; insbesondere, ob eine Einwilligung für die Speicherung oder den Zugriff auf ihrem Endgerät und ggf. in die Verarbeitung personenbezogener Daten abgefragt wird
- Identität des Telemedienanbieters und des oder der Verantwortlichen
- Zwecke der Zugriffe und der Datenverarbeitungsvorgänge
- Jederzeitige Widerrufbarkeit der Einwilligung(en) und wie das Widerrufsrecht geltend gemacht werden kann
- ggf. Profilbildung oder Datenübermittlung in Drittländer

Weitere erforderliche Informationen können meiner Auffassung nach auch auf zweiter Ebene verortet werden, wie etwa

- die Angabe der Rechtsgrundlage(n),
- die verwendeten Cookies oder ähnliche Technologien und deren Gültigkeitsdauer,
- die konkret verarbeiteten Datenkategorien,
- die Speicherdauer personenbezogener Daten, oder
- ggf. weitere Empfänger.

Werden Einwilligungen für mehrere Trackingtechnologien und Zwecke abgefragt, müssen diese granular auswählbar sein. Bereits angekreuzte Kästchen oder andere Opt-Out-Verfahren sind ungeeignet, wirksame Einwilligungen zu begründen.

Ferner ist darauf zu achten, dass die Gestaltung des Banners in der Gesamtheit nicht zu einer unzulässigen Verhaltenssteuerung (Nudging) führt. Dazu kann es insbesondere durch irreführende Informationen, bewusst verharmlosende Sprache oder Informationsüberlastung kommen.

Das Merkmal der Freiwilligkeit erfordert auch, dass das Banner eine Ablehnfunktion als gleichwertige Alternative zur Einwilligung enthält, die eindeutig erkennbar, leicht wahrnehmbar und unmissverständlich ist. Dies kann etwa durch die Verwendung der Begriffe „Einwilligen“ und „Weiter ohne Einwilligung“ oder „Ablehnen“ umgesetzt werden.

Schließlich ist wichtig, dass die Zugriffe auf das Endgerät erst stattfinden, wenn eine wirksame Einwilligung tatsächlich vorliegt.

6. Welche Informationen müssen außerhalb des Banners bereitgestellt werden?

Neben den Informationen im Banner, die für eine wirksame Einwilligung erforderlich sind, müssen Verantwortliche den betroffenen Personen weitere Informationen – etwa in einer Datenschutzerklärung – zur Verfügung stellen. Dazu gehören insbesondere nach Artikel 13 DSGVO erforderliche Informationen über die Verarbeitungen personenbezogener Daten, die aufgrund einer anderen Rechtsgrundlage als einer Einwilligung stattfinden, und Informationen zur Geltendmachung der Betroffenenrechte oder die Kontaktdaten der oder des Datenschutzbeauftragten. Ferner sollte hier über technisch unbedingt erforderliche Cookies und ähnliche Technologien informiert werden.

Zudem muss der Widerruf einer Einwilligung ebenso einfach möglich sein wie die Erteilung. Wird die Einwilligung unmittelbar bei der Nutzung einer Webseite erteilt, muss auch deren Widerruf auf diesem Weg möglich sein.

7. Was ist bei der Einbindung von Drittdiensten zu beachten?

Häufig möchten Webseitenbetreiberinnen und -betreiber Drittdienste einbinden wie Kartendienste, Routenplaner, Videoplattformen, Soziale Netzwerke, Fonts (Schriften, die von externen Servern geladen werden), Captcha-Dienste (Test zur Unterscheidung von Menschen zu Maschinen) oder Webanalysetools.

Hierbei gilt grundsätzlich das zuvor Gesagte zu Einwilligungen nach TTDSG und ggf. DSGVO entsprechend.

Da eine Einwilligung nur freiwillig erteilt ist, wenn die Nutzenden eine echte Wahlmöglichkeit haben, kann es erforderlich sein, eine ggf. datensparsamere Alternative eines Dienstes anzubieten. Das gilt insbesondere, wenn wichtige Informationen im Rahmen der Öffentlichkeitsarbeit über eingebundene Drittdienste bereitgestellt werden sollen.

Die Einbindung – und damit auch die Abfrage der Einwilligung – sollte erst dann erfolgen, wenn die Nutzenden den jeweiligen Dienst konkret anfordern, soweit dies technisch umsetzbar ist.

Schließlich sollte geprüft werden, ob Drittdienste über einen Proxy-Server (einen Kommunikationsvermittler) eingebunden werden können, um eine nicht erforderliche Weitergabe personenbezogener Daten an die Anbieter der Drittdienste zu verhindern.

Bitte überprüfen Sie die Gestaltung Ihrer Webseiten sowie Banner und passen diese zeitnah entsprechend an.

Für die Beachtung und Weiterleitung dieses Schreiben auch an die nachgeordneten Stellen Ihres Geschäftsbereichs danke ich Ihnen.

Mit freundlichen Grüßen
Im Auftrag