Bundesamt
für Soziale Sicherung

Bundesamt für Soziale Sicherung, Friedrich-Ebert-Allee 38, 53113 Bonn

An alle
bundesunmittelbaren
Sozialversicherungsträger

- per E-Mail -

HAUSANSCHRIFT
Friedrich-Ebert-Allee 38
53113 Bonn

TEL +49 228 619 1935
FAX +49 228 619 1872

referat116@bas.bund.de
www.bundesamtsozialesicherung.de

BEARBEITER(IN) HR. COLOMBIER

8. Juni 2020

AZ 116 – 820 – 402/2020
(bei Antwort bitte angeben)

nachrichtlich:
Bundesministerium für Arbeit und Soziales, Referat IVa 1
Bundesministerium für Gesundheit, Unterabteilung 52 sowie Referat 211
Bundesbeauftragter für den Datenschutz und die Informationsfreiheit, Referat 13
GKV-Spitzenverband, Stabsbereich Justiziariat
vdek, Justiziariat
Deutsche Gesetzliche Unfallversicherung e.V., Justitiariat / Allgemeines Recht

Informationstechnik im Aufsichtsbereich – hier: Rechtskonforme Gestaltung von Webseiten in der Sozialversicherung

Sehr geehrte Damen und Herren,

bei der Gestaltung und dem Betrieb von Webseiten sind seitens der Sozialversicherungsträger eine Reihe rechtlicher Anforderungen zu beachten. Neben den allgemeinen Anforderungen an die technische und organisatorische Sicherheit der Verarbeitung (Artikel 32 DSGVO) sind – insbesondere bei der Einbindung von Diensten Dritter (z. B. Cookies, Web-Plugins) – weitere Maßgaben zu berücksichtigen. Im Folgenden stellen wir unseren Prüfrahmen für zukünftige Prüfungen dar.

1. Allgemeine Anforderungen aus der Managementperspektive

Unter Berücksichtigung des Stands der Technik und insbesondere unter Abwägung des Risikos für die Rechte und Freiheiten der Betroffenen treffen die Verantwortlichen geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten (Artikel 32 Absatz 1 DSGVO). Dies gilt auch für die Verarbeitung personenbezogener Daten im Zusammenhang mit der Webseite. Insbesondere ergeben sich hieraus folgende Anforderungen:

a) **Dokumentation der organisationsspezifischen Regelungen zur Gestaltung und Betrieb der Webseite und spezieller Webanwendungen** (z. B. Gestaltungs- und Programmiervorgaben, Regelungen zum Umgang mit Funktionsbausteinen von Dritter Seite, Regelungen zur Einbindung von Diensten Dritter, Dokumentation der Verantwortlichkeiten),

b) **Etablierung eines Verfahrens zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen** (z. B. Aufnahme in die Prüfplanung der internen Kontrollinstanzen wie z. B. Datenschutz- und Informationssicherheitsbeauftragte sowie IT-Revision, Durchführung von Security-Audits oder Penetrationstest),

c) **Management der Auftragsverarbeitungen in diesem Kontext** (z. B. Verfahrensanweisungen zur Einbindung von Diensten Dritter, Abgrenzungshinweise für eine Auftragsverarbeitung, Muster und Hinweise für eine Vereinbarung der Auftragsverarbeitung, Überprüfung des Auftragsverarbeiters).

2. Besondere Anforderungen beim Einsatz von Verfahren zur Webanalysen

Der Begriff Webanalyse (in der Fachliteratur auch als Webtracking bezeichnet) ist weder gesetzlich einheitlich definiert noch wird er in der Praxis einheitlich verwendet. Im Kontext des vorliegenden Rundschreibens subsumieren wir hierunter sämtliche Verfahren zur Analyse von Daten, welche beim Betrieb von Online-Angeboten (beispielsweise Webseiten, mobilen Apps) erhoben werden. Verbreitete Methoden der Web-Analyse sind unter anderem die Protokolldaten-Analyse sowie der Einsatz von Cookies und Fingerprinting-Technologien. Verfahren zur Webanalyse werden für technische Aspekte des Webseitenbetriebs, beispielsweise zur Fehleranalyse sowie im Zuge der Umsetzung von sicherheitstechnischen Maßnahmen

genutzt. Darüber hinaus werden sie vielfach auch zur Analyse des Nutzerverhaltens, zur Reichweitenmessung sowie zur werblichen Optimierung verwendet.

Bei Verfahren der Webanalyse werden regelmäßig personenbezogene Daten im Sinne des Artikels 4 Nummer 1 DSGVO verarbeitet. In Zweifelsfällen sollte davon ausgegangen werden, dass ein Personenbezug der Analysedaten gegeben ist. Dies ergibt sich aus der grundsätzlich gebotenen weiten Auslegung des Begriffs des Personenbezugs sowie aus den in Erwägungsgrund 30 der DSGVO niedergelegten Maßgaben zu Online-Kennungen. Soweit diese Daten in einem fachlichen Zusammenhang zur sozialrechtlichen Aufgabenerfüllung stehen, handelt es sich um Sozialdaten im Sinne des SGB X, die eine sozialdatenschutzrechtlichen Verarbeitungsgrundlage erfordern (§§ 67 Absatz 2, 67b Absatz 1 SGB X). Die datenschutzrechtlichen Vorschriften des Telemediengesetzes (TMG) werden durch die Regelungen der DSGVO verdrängt und kommen nicht mehr zur Anwendung.
Vor diesem Hintergrund ergeben sich für unsere Prüfung u. a. folgende Anforderungen:

a) **Rechtmäßigkeit der Verarbeitung** (z. B. wirksame Einwilligung der Betroffenen oder Begründung eines berechtigten Interesses, bevor die Webanalyse startet; Berücksichtigung Koppelungsverbot),

b) **Nachweis der jeweiligen Verarbeitungsbefugnis** (aus der Rechenschaftspflicht gemäß Artikel 5 Absatz 2 DSGVO ergibt sich, dass der Verantwortliche die Rechtmäßigkeit der jeweiligen Verarbeitung nachvollziehbar dokumentieren muss),

c) **Informationspflichten gegenüber den Betroffenen** (gemäß Artikel 13 DSGVO sind die betroffenen Nutzer umfassend über den Zweck und die Inhalte der Verarbeitung zu informieren z. B. in der Datenschutzerklärung),

d) **Rechtsgrundlage für die Einbindung Dritter** (in der Regel im Rahmen einer Verarbeitung im Auftrag nach Artikel 28 DSGVO oder in Form einer gemeinsamen Verantwortung gemäß Artikel 26 DSGVO),

e) **Berücksichtigung der räumlichen Beschränkung der Verarbeitung im Sozialrecht** (aufgrund des regelmäßig höheren Schutzbedarfs bei der Verarbeitung von Sozialdaten beschränkt § 80 Absatz 2 SGB X die Verarbeitung auf Deutschland, andere Mitgliedsstaaten der EU, gleichgestellte Staaten sowie Staaten mit Angemessenheitsbeschluss nach Artikel 45 DSGVO)

3. Besondere Anforderungen beim Einsatz von sog. Cookies

Als Cookies werden im Kontext von Webseiten kleine Textdateien bezeichnet, in denen der Internet-Browser des Nutzers Informationen über den Besuch einer Webseite speichert, um die Navigation auf der Webseite zu erleichtern. Darüber hinaus können Cookies aber auch Werbezwecken dienen, in dem Nutzer einer Webseite „wiedererkannt“ werden und dadurch Werbeanzeigen personalisiert werden können. Durch das Auslesen von Cookies beim Besuch eine Webseite können auch Sozialdaten betroffen sein. In diesem Kontext ergeben sich u. a. folgende Anforderungen:

a) **Rechtmäßigkeit der Verarbeitung** (insb. Einwilligung, Vertrag oder berechtigtes Interesse; eine Einwilligung kann z. B. entbehrlich sein, wenn keine Daten an Dritte weitergegeben werden, keine Einbindung von Elementen Dritter erfolgt und ein berechtigtes Interesse begründet ist, vgl. hierzu auch die Orientierungshilfe der Datenschutzkonferenz für Anbieter von Telemedien, Stand März 2019),

b) **Rechtsgrundlage für die Einbindung Dritter** (in der Regel im Rahmen einer Verarbeitung im Auftrag nach Artikel 28 DSGVO oder in Form einer gemeinsamen Verantwortung gemäß Artikel 26 DSGVO),

c) **Rechtskonforme Gestaltung des Cookies-Banners bei Einwilligungserfordernis** (vgl. hierzu insbesondere das BGH-Urteil vom 28. Mai 2020, Az. I ZR 7/16, in dem u. a. klargestellt wird, dass ein voreingestelltes Häkchen keine wirksame Einwilligung darstellt).

d) **Informationspflichten gegenüber den Betroffenen** (gemäß Artikel 13 DSGVO sind die betroffenen Nutzer umfassend über den Zweck und die Inhalte der Verarbeitung zu informieren z. B. in der Datenschutzerklärung),

4. Besondere Anforderungen beim Einsatz von sog. Plugins

Als Plugins werden im Kontext von Webseiten in der Regel unselbständige Softwarebausteine bezeichnet, die Einbindung zusätzlicher Funktionalitäten ermöglichen. Ausprägungsformen sind z. B. auch die sog. Like- und Share-Button von Social-Media-Anbietern und Werbenetzwerken. In diesem Kontext ergeben sich insbesondere folgende Anforderungen:

a) **Rechtmäßigkeit der Verarbeitung und Rechtsgrundlage für die Einbindung Dritter** (gemäß Urteil des EuGH zu „Facebook-Fanpage“ und „Fashion ID“ kann von einer gemeinsame Verantwortung ausgegangen werden; in einer Vereinbarung mit den Dritten ist transparent festzulegen, wer welche Pflichten zu erfüllen hat - Artikel 26 Absatz 1 DSGVO),

b) **Datenschutzfreundliche Implementierung** (insbesondere muss sichergestellt sein, dass keine Informationen über das Nutzungsverhalten ohne Einwilligung an Dritte weitergegeben werden),

c) **Informationspflichten gegenüber den Betroffenen** (gemäß Artikel 13 DSGVO sind die betroffenen Nutzer umfassend über den Zweck und die Inhalte der Verarbeitung zu informieren z. B. in der Datenschutzerklärung),

Auf Basis der dargestellten Kernanforderungen zur Gestaltung und Betrieb von Webseiten in der Sozialversicherung wird das Bundesamt für Soziale Sicherung künftig den rechtskonformen Einsatz in seinem Aufsichtsbereich stichpunktartig prüfen.

Mit freundlichen Grüßen
Im Auftrag

(Thorsten Schlotter)