Die neue Datenschutz-Grundverordnung ab 24.05.2018

1. **Hinweis:**

Rechtsberatungen sind bestimmten Berufsgruppen vorbehalten.

Ich bin keine Rechtsanwältin und Sie erhalten hier lediglich eine Zusammenstellung der Informationen, die ich in Eigenrecherche aus unterschiedlichen vorhandenen Quellen zusammengetragen habe. Auch fließt mein eigenes Verständnis für die anstehenden Änderungen mit ein.

Diese Zusammenstellung erhebt keinen Anspruch auf Vollständigkeit und ich kann für die Inhalte auch keine Haftung übernehmen.

Diese Übersicht ersetzt keine rechtliche Beratung. Um Ihren Einzelfall zu prüfen, holen Sie sich bitte bei geeigneter Stelle, Rechtsberatung ein.

Sabine Niederreuther

Creative Webdesign NieSa.net

Westliche Gleisbgerstr. 40

76831 Billigheim-Ingenheim

Tel 0172-7648332

Email Niederreuther@niesa www.niesa.net

Inhaltsverzeichnis

2. Neue Datenschutz-Grundverordnung (DSGVO) ab 25. Mai 2018

Die ab dem 25. Mai 2018 anwendbare Datenschutz-Grundverordnung regelt europaweit den Umgang mit personenbezogenen Daten und ist dann geltendes Recht. Deshalb ist es wichtig, dass sich alle Betroffenen gut auf die Änderungen vorbereiten und handeln. [1]

Auch Sie, als Webseitenbetreiber sind davon betroffen!

Auch schon bei kleinen und einfach strukturierten Webseiten werden **IP-Adressen der Besucher** an den Webserver übertragen. Die IP Adressen sind **als personenbezogene Daten einzustufen**. Daher fallen auch diese Webseiten unter den Geltungsbereich der DSGVO und es müssen die entsprechenden Vorgaben beachtet werden. Verschärfte Regelungen greifen insbesondere bei Nutzung von Komponenten wie Kontaktformularen, Analyse-Werkzeugen oder Social-Media-Plug-Ins (Facebook, Twitter, Xing etc.). Hier gibt es ab Mai zusätzliche Informationspflichten. [2]

Ihre Webseiten-Besucher müssen über **datenschutzrelevante Aktivitäten** informiert werden, die über die einfache Erfassung der IP-Adresse hinausgehen.
Dazu gehören insbesondere:

- Das Verwenden von Kontaktformularen
- E-Mail-Newsletter
- Cookies
- Analyse-Tools
- Verwendung von Social-Media-Plug-Ins [3]

Schauen wir uns die Bereiche genauer an.

2.1 Kontaktformulare

Bereits bei einfachen Kontaktformularen ist darauf zu achten, dass die Eingabe und Übermittlung der Daten **stets mit aktuellen Verschlüsselungsverfahren** erfolgt, denn nur so ist sichergestellt, dass die von der **DSGVO geforderte „angemessene Sicherheit“** der personenbezogenen Daten gewährleistet ist. Dies gilt umso mehr, wenn etwa im Zuge einer Bestellung in einem Online-Shop **besonders sensible und schützenswerte Daten** wie **Kontoinformationen** übertragen werden.

Zudem gilt bei allen erfassten Formulardaten der **Grundsatz der Datenminimierung bzw. Datensparsamkeit**. Es dürfen nur solche Daten erhoben werden, die für den jeweiligen Zweck auch benötigt werden.

[1] Vgl. Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, https://www.bfdi.bund.de/DE/Datenschutz/datenschutz-node.html am 22.03.2018
[2] Vgl. https://www.haufe.de/compliance/recht-politik/auswirkung-der-datenschutzgrundverordnung-auf-website-pflichten_230132_440812.html am 23.03.2018
[3] Vgl. https://www.haufe.de/compliance/recht-politik/auswirkung-der-datenschutzgrundverordnung-auf-website-pflichten_230132_440812.html am 23.03.2018

Für einen Newsletter etwa **wird nur die E-Mail-Adresse benötigt**, nicht aber weitere persönliche Daten. Felder zur Erfassung dieser Pflichtangaben sind eindeutig zu kennzeichnen. Dass weitere Angaben stets freiwillig sind, muss in den Formularen auch ersichtlich sein.[4]

2.1.1. SSL (*Secure Sockets Layer)* Verschlüsselung für Sicherheit im www

Um den verschlüsselten Datenverkehr zu garantieren, benötigt man normalerweise für jede Domain ein SSL-Zertifikat.[5] Pflicht ist es beispielsweise für OnlineShops oder Banken, die mit personenbezogenen Daten arbeiten. Für eine Webseite, auf der keine personenbezogenen Daten erhoben werden, ist eine SSL Verschlüsselung keine Pflicht. Allerdings stuft Google ihre Webseite ohne SSL Verschlüsselung direkt als „unsicher“ ein. Dies wirkt sich negativ auf das Ranking bei der Google Suche aus.

Sie erkennen, ob eine Internetseite verschlüsselt ist daran, dass anstatt **http** in der Eingabezeile **https** steht (Abbildung 1) . Auch wird ein kleines (meist) grünes **Schloss** angezeigt (Abbildung 2). Wenn Sie dieses anklicken, erhalten Sie Infos zur Identifizierung der Webseite.

Beispiel einer verschlüsselten Website: www.arbeitsagentur.de

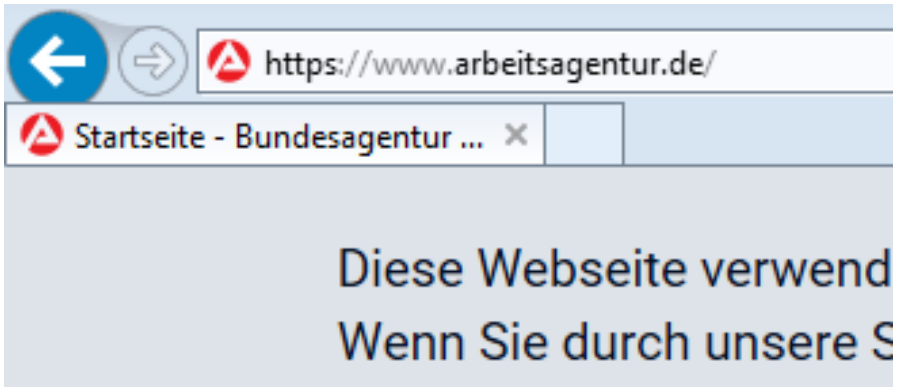

Abbildung 1: Website der Arbeitsagentur – eigenes Foto

[4] https://www.haufe.de/compliance/recht-politik/auswirkung-der-datenschutzgrundverordnung-auf-website-pflichten_230132_440812.html am 23.03.2018

[5] Vgl. GERWAN™ GmbH, Bonn, https://ssl.de/ssl-faq/braucht-jede-domain-ein-eigenes-ssl-zertifikat.html am 23.03.2018

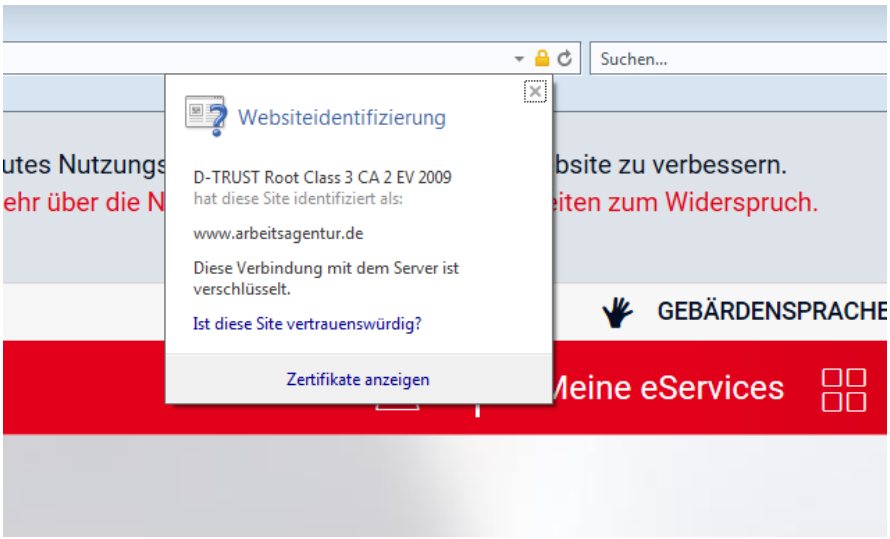

Abbildung 2: Website der Arbeitsagentur – eigenes Foto

Fazit: Auch für kleine Seiten, auf denen keine persönlichen Daten erhoben werden (und die somit kein SSL verwenden müssen), wirkt sich SSL auf jeden Fall positiv aus. **SSL schafft Vertrauen, Sicherheit und Datenschutz.**

- Zwischen dem Endgerät (Client) und dem Webserver ausgetauschte Informationen werden **mit SSL/TLS Ende-zu-Ende verschlüsselt**. Das bedeutet, ein Dritter kann nicht ohne weiteres auslesen, welche Informationen ausgetauscht werden.
- Die **Identität vom Server wird zusätzlich bestätigt**. Das bedeutet, ein Dritter kann nicht ohne weiteres Kommunikation zwischen Client und Server abfangen und manipulieren.
- Eine **Zertifizierungsstelle (CA)** tritt als **vertrauenswürdige Instanz** zusätzlich mit ein, überprüft die Identität des Zertifikatsinhabers und stellt sicher, dass das Zertifikat zum Server, zu dem eine Verbindung aufgebaut werden soll, passt. [6]

2.1.2 Google und SSL / SEO und SSL

Google hat bereits 2014 darüber informiert, dass es künftig **HTTPS als Ranking-Signal** wertet. Das bedeutet für SEOs, dass die eigene Webseite – sofern sie über HTTPS ausgeliefert ist – einer in allen übrigen Ranking-Kriterien gleichwertigen Konkurrenz-Webseite überlegen ist und in den Suchergebnisse von Google höher platziert werden wird.

In der Praxis ist das **HTTPS Ranking-Signal** derzeit ein untergeordnetes – das bedeutet, nur durch die Anschaffung von einem eigenen SSL-Zertifikat und Umstellung der Webseite auf HTTPS wird man in Google nicht auf Platz 1 katapultiert. Jedoch ist ein klarer Trend abzulesen, dass Google auf die **Vorteile von SSL Zertifikaten** setzt.

[6] Vgl. Blue2Media UG (haftungsbeschränkt http://sslwebhosting.de/vorteile-ssl-zertifikat-warum-google-ssl-positiv-bewertet am 23.03.2018

Mit Blick auf die übrigen **Vorteile einer sicheren HTTPS-Verbindung** sind die kleinen SEO-Vorteile somit ein Mitnahmeeffekt für Webmaster, die sich bereits heute dafür entscheiden, auf HTTPS umzustellen. Gleichzeitig ist **Zukunftssicherheit** gegeben, sollte Google künftig das HTTPS Ranking-Signal stärker gewichten.[7]

Hier können Sie sich umfassend zu dem Thema SSL informieren:

https://ssl.de/ssl.html

2.2 Newsletterversand

Das sagt die DSGVO dazu:

Eine Einwilligung „könnte etwa durch Anklicken eines Kästchens beim Besuch einer Internetseite, durch die Auswahl technischer Einstellungen für Dienste der Informationsgesellschaft oder durch eine andere Erklärung oder Verhaltensweise geschehen, mit der die betroffene Person in dem jeweiligen Kontext eindeutig ihr Einverständnis mit der beabsichtigten Verarbeitung ihrer personenbezogenen Daten signalisiert. Stillschweigen, bereits angekreuzte Kästchen oder Untätigkeit der betroffenen Person sollten daher keine Einwilligung darstellen.“

Was bedeutet dies nun für den Webseitenbetreiber?

Der E-Mail Empfänger muss vor dem Versand eines Newsletters genaue Information erhalten, in was er einwilligt und er muss über seine Widerrufmöglichkeiten informiert werden. Die Einwilligung erfolgt freiwillig und ist zu protokollieren. Nicht als Einwilligung z.B. durch ein vorausgewähltes Häkchen, das man übersehen kann. [8]

Diese Einwilligung muss freiwillig und in unmissverständlicher Weise erfolgen. Dabei müssen Versender auch **darüber informieren**,

- in welchem Umfang,
- zu welchem Zweck
- und von wem die hier anfallenden **personenbezogenen Daten verarbeitet** werden.[9]

Es muss immer **auf die Möglichkeit zum Widerruf hingewiesen werden**.

Um den Nachweis zu erbringen, dass der Nutzer einer E-Mail-Adresse einen Newsletter tatsächlich auch abonniert hat und nicht etwa ein Dritter diesen Newsletter angefordert hat bzw. es durch Tippfehler bei der angegebenen Adresse zu unerwünschten Zustellungen

[7] Vgl. Blue2Media UG (haftungsbeschränkt http://sslwebhosting.de/vorteile-ssl-zertifikat-warum-google-ssl-positiv-bewertet am 23.03.2018
[8] Vgl. Händlerbund Management AG, Leipzig https://www.haendlerbund.de am 23.03.2018
[9] Vgl. https://www.haufe.de/compliance/recht-politik/auswirkung-der-datenschutzgrundverordnung-auf-website-pflichten_230132_440812.html am 23.03.2018

gekommen ist, muss **vor dem Versand des Newsletters** eine **Rückfrage bei der angegebenen E-Mail-Adresse mittels einer Bestätigungs-Mail** erfolgen.

Dies entspricht dem **Double-Opt-In-Prinzip**. Erst nachdem der Nutzer die Newsletter-Bestellung durch Anklicken des Bestätigungs-Links akzeptiert, darf der Newsletter-Versand erfolgen.[10]

2.3 Cookies

Auch die Nutzung von Cookies auf den Webseiten fällt unter die Vorgaben der DSGVO, da hierüber - was auch Sinn und Zweck der Maßnahme entspricht - die **Nutzer durch entsprechende Techniken wiedererkennbar werden.** Mit einer Zustimmung der Nutzer ist man daher immer auf der richtigen Seite.

- Andererseits erlaubt die DSGVO aber auch die Verarbeitung personenbezogener Daten, wenn dies zur Wahrung berechtigter Interessen des Verantwortlichen notwendig ist
- und sofern dabei die Interessen und Grundfreiheiten der betroffenen Nutzer gewahrt bleiben.

Daraus lässt sich schließen, dass solche **Cookies, die die Nutzerfreundlichkeit** auf einer Website **erhöhen** bzw. einige Dienste erst ermöglichen, durchaus auch ohne Hinweis möglich sein müssten. Erst auf Cookies, die zu anderen Zwecken, etwa der **Analyse der Besucherströme,** verwendet werden, müsste dann explizit hingewiesen werden.

In jedem Fall unverzichtbar für alle Cookies ist jedoch ein **Widerspruchsrecht**, das allen Website-Besuchern eingeräumt werden muss.[11]

2.4 Analysetools

Viele Anbieter wissen gar nicht, dass sie im Hintergrund viele persönliche Daten ihrer Besucher und Kunden abgreifen und an Dritte übermitteln. Beim Einsatz von sogenannten Analysetools sind dem Webseiten-Besucher folgende Informationen mitzuteilen:

- ob persönliche Daten erhoben werden
- an wen sie übermittelt werden
- wofür sie verwendet werden

Hier bedarf es für jedes einzelne Tool einer ergänzenden Regelung in der Datenschutzerklärung, da jeder Anbieter anders arbeitet. [12]

[10] https://www.haufe.de/compliance/recht-politik/auswirkung-der-datenschutzgrundverordnung-auf-website-pflichten_230132_440812.html am 23.03.2018
[11] Vgl. https://www.haufe.de/compliance/recht-politik/auswirkung-der-datenschutzgrundverordnung-auf-website-pflichten_230132_440812.html am 23.03.2018
[12] https://www.haufe.de/compliance/recht-politik/auswirkung-der-datenschutzgrundverordnung-auf-website-pflichten_230132_440812.html am 23.03.2018

Webanalyse-Tools sollten daher unter folgenden Voraussetzungen zum Einsatz kommen:

- In einer Klausel in der Datenschutzerklärung wird für jedes Tool gesondert die Funktionsweise, der Empfänger, das Widerspruchsrecht und die Datennutzung erklärt.
- Es muss eine automatische Anonymisierung der Besucher-ID stattfinden, insbesondere bei Google Analytics.
- Der Webseitenbesucher muss die jederzeitige Widerspruchsmöglichkeit haben.
- Außerdem bestehen allgemeine Informationspflichten [13]

2.4.1 Google Analytics

Google Analytics muss so verwendet werden, dass die **erfassten IP-Adressen anonymisiert** werden, wozu Google eine entsprechende Erweiterung anbietet. Vor der Verwendung muss ein schriftlicher Vertrag zur Auftragsverarbeitung mit Google abgeschlossen werden. [14]

Hier können Sie den Vertrag downloaden:

http://www.google.com/analytics/terms/de.pdf

Google Analytics und Datenschutz sind eigentlich ein Widerspruch. Nach jahrelangen Streitigkeiten hat sich der Suchmaschinenkonzern aber mit den Datenschützern auf eine rechtskonforme Nutzung von Google Analytics geeinigt. Seitenbetreiber müssen hier aber eine ganze Menge tun, um Google Analytics und Google Universal Analytics rechtssicher und ohne Angst vor Abmahnungen nutzen zu können. Erecht24 zeigt Ihnen Schritt für Schritt wie es geht.[15]

https://www.e-recht24.de/artikel/datenschutz/6843-google-analytics-datenschutz-rechtskonform-nutzen.html

Schnellcheck:

https://www.e-recht24.de/check/google-analytics-check.html

[13] Vgl. https://www.haendlerbund.de/de am 23.03.2018
[14] Vgl. https://www.haufe.de/compliance/recht-politik/auswirkung-der-datenschutzgrundverordnung-auf-website-pflichten_230132_440812.html am 23.03.2018
[15] Vgl. erecht24.de https://www.e-recht24.de/artikel/datenschutz/6843-google-analytics-datenschutz-rechtskonform-nutzen.html am 27.03.2018

2.5 Social Media Plugins

Social-Media-Plug-Ins enthüllen Surfverhalten der Nutzer
Sollen auf den Webseiten die sogenannten Social-Media-Plug-Ins eingebaut werden, mit denen die Besucher andere **Seiten** - beispielsweise **aus Soziale Netzwerke - empfehlen oder teilen können,** wird künftig eine ausdrückliche Einwilligung der Nutzer verlangt.

- Denn über diese Erweiterungen sammeln die sozialen Netzwerke, ähnlich wie mit anderen Analyse- und Tracking-Werkzeugen,
- **Daten mit Hinweisen um Surfverhalten der Nutzer** und können daraus **Nutzerprofile erstellen.** [16]

Bei dem Facebook Like-Button besteht das zusätzliche Problem, dass allein die Einbindung des Buttons in eine Website dazu führt, dass Nutzerdaten an Facebook übermittelt werden. **Die Datenübermittlung erfolgt also auch ohne Betätigung des Buttons** – der Nutzer muss noch nicht einmal bei Facebook angemeldet sein. Entsprechendes gilt für andere Share-Buttons, wie die von Twitter und Google Plus.[17]

Hier empfiehlt sich der Einsatz solcher Lösungen, bei denen die Besucher zunächst frei entscheiden können, ob ihre Daten durch die Plug-Ins an die Sozialen Netzwerke übertragen werden sollen oder nicht. Realisiert werden kann dies beispielsweise durch zusätzliche Schaltflächen, durch deren Anklicken erst die **Zustimmung zur Nutzung der Plug-Ins** erteilt wird.[18]

Erecht24.de stellt mit dem „Safe Sharing Tool“ eine Möglichkeit bereit, Social Media abmahnsicher auf der eigenen Webseite einzubinden.

Was kann das eRecht24 Safe Sharing Tool?

- Mehr Reichweite: ihre Inhalte werden weiterhin über soziale Netzwerke verbreitet
- Keine Abmahnungen: datenschutzkonformes Teilen von Inhalten auf Facebook etc
- Zufriedene Nutzer: keine automatische Weitergabe von Nutzerdaten an Facebook etc
- Keine Programmierung: fertige Plugins für Wordpress, Joomla und Typo 3
- Korrekter Datenschutzerklärung: Über den Datenschutz-Generator gleich die passende Datenschutzerklärung erzeugen. [19]

Hier geht es zum Download:

https://www.e-recht24.de/erecht24-safe-sharing.html

[16] Vgl. https://www.haufe.de/compliance/recht-politik/auswirkung-der-datenschutzgrundverordnung-auf-website-pflichten_230132_440812.html am 23.03.2018
[17] Vgl. Dr. Nils Christian Haag (V.i.S.d.P.)intersoft consulting services AG, Hamburg https://www.datenschutzbeauftragter-info.de/like-button-und-datenschutz-heise-shariff-verbessert-2-klick-loesung/ am 27.03.2018
[18] Vgl. https://www.haufe.de/compliance/recht-politik/auswirkung-der-datenschutzgrundverordnung-auf-website-pflichten_230132_440812.html am 23.03.2018
[19] Vgl. eRecht24 GmbH & Co. KG, 10117 Berlin, https://www.e-recht24.de/erecht24-safe-sharing.html am 27.03.2018

2.6. Löschansprüche

Eine weitere Neuerung betrifft die **Löschansprüche**, die Betroffene nach Art. 17 DSGVO nun unter Umständen auch **gegen Website-Betreiber** haben. Diese müssen bei derartigen berechtigten Ansprüchen zum einen die beanstandeten Datenquellen auf ihren Webseiten entfernen. Zum anderen sind sie sogar verpflichtet, angemessene Maßnahmen zu ergreifen, um Dritte über den Zwang zum Löschen von Links etc. zu informieren. Ebenfalls neu ist schließlich das **Recht auf Datenübertragbarkeit**, das es den Nutzern erlaubt, **bei Sozialen Netzwerken**, aber beispielsweise auch bei Online-Shops, sämtliche **ihn betreffende personenbezogene Daten anzufordern**.
Diese Daten müssen dann in einer strukturierten, gängigen und maschinenlesbaren Form ausgehändigt werden, damit sie anschließend an einen anderen Anbieter übertragen werden können, wenn der Nutzer dies wünscht.[20]

3. Gesetze und hilfreiche Quellen

E-Privacy

https://www.bfdi.bund.de/SharedDocs/Publikationen/DatenschutzKompaktBlaetter/ePrivacy.pdf?__blob=publicationFile&v=4

Gesetz

https://dsgvo-gesetz.de/

https://dsgvo-gesetz.de/bdsg-neu/

Video-Seminar zum neuen Datenschutzrecht
Der **Referent Prof. Dr. Boris Paal** erläutert die Auswirkungen des neuen Datenschutzrechts. Die Seminarinhalte sind:

- Überblick über die die DS-GVO und das BDSGneu,
- Anwendungsbereiche, Bußgelder und Sanktionen und
- Leitfaden Datenschutz 2018/Compliance-Management.

Videogebühr: 98 EUR zzgl. USt.

Hier können Sie das Video herunterladen.[21]

[20] Vgl. https://www.haufe.de/compliance/recht-politik/auswirkung-der-datenschutzgrundverordnung-auf-website-pflichten_230132_440812.html am 23.03.2018
[21] Vgl. https://www.haufe.de/compliance/recht-politik/auswirkung-der-datenschutzgrundverordnung-auf-website-pflichten_230132_440812.html am 23.03.2018

Quellenverzeichnis:

Blue2Media UG (haftungsbeschränkt) 20357 Hamburg
http://sslwebhosting.de/vorteile-ssl-zertifikat-warum-google-ssl-positiv-bewertet
am 23.03.2018

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Bonn
https://www.bfdi.bund.de/DE/Datenschutz/datenschutz-node.html am 22.03.2018

Dr. Nils Christian Haag (V.i.S.d.P.) intersoft consulting services AG, Hamburg
https://www.datenschutzbeauftragter-info.de/like-button-und-datenschutz-heise-shariff-verbessert-2-klick-loesung/ am 27.03.2018

eRecht24 GmbH & Co. KG, 10117 Berlin,
https://www.e-recht24.de/erecht24-safe-sharing.html am 27.03.2018

Händlerbund Management AG, Leipzig
https://www.haendlerbund.de am 23.03.2018

GERWAN™ GmbH, Bonn
https://ssl.de/ssl-faq/braucht-jede-domain-ein-eigenes-ssl-zertifikat.html am 23.03.2018

Haufe-Lexware GmbH & Co. KG , 79111 Freiburg
https://www.haufe.de/compliance/recht-politik/auswirkung-der-datenschutzgrundverordnung-auf-website-pflichten_230132_440812.html am 23.03.2018