Geschäftsbereich
Recht, Zentrale Dienste

Nr. 07/2018

Newsletter Datenschutz

In dieser Ausgabe: Webseiten unterliegen neuen Anforderungen mit der DSGVO - Teil 1

Webseiten unterliegen neuen Anforderungen mit der DSGVO

Die Schonfrist ist abgelaufen, die Regeln der DSGVO (Datenschutzgrundverordnung) gelten seit dem 25. Mai 2018 einheitlich für alle im EU-Raum aktiven Unternehmen. Dies bedeutet: Soweit nicht Spezialregelungen (strittig bei TMG Telemediengesetz) greifen, sind die erhöhten Anforderungen der DSGVO zu beachten. Internetseiten unterliegen den datenschutzrechtlichen Bestimmungen, da dort stets personenbezogene Daten (z. B. eine IP-Adresse) verarbeitet werden. Dabei ist wichtig: Nach dem Datenschutzrecht ist eine Verarbeitung von Daten natürlicher Personen zunächst generell verboten, es sei denn ein Gesetz erlaubt dies ausdrücklich!

Für einen datenschutzkonformen Internetauftritt gibt es einiges zu beachten. Zum Beispiel ist eine rechtskonforme Datenschutzerklärung verpflichtend, die die nach DSGVO erweiterten Angaben beinhalten muss. Die folgenden Tipps helfen Unternehmen und Webseiten-Betreibern bei der Anpassung ihres Webauftritts an die neuen Regeln.

Tipps für gängige Website-Techniken und Tools

Die datenschutzrechtlichen Vorgaben der DSGVO gelten, sobald es sich bei den verarbeiteten, insbesondere erhobenen, Daten um personenbezogene Daten handelt. Nach Art. 4 Nr.1 DSGVO sind alle Informationen personenbezogen, die sich auf eine identifizierbare oder identifizierte natürliche Person beziehen. Zu diesen Daten gehören:

- Name und Anschrift
- Angaben wie Alter, Geschlecht und Einkommen
- Daten über das Surfverhalten wie Suchanfragen und Browserverlauf
- IP-Adressen und sonstige User-Daten
- E-Mails, Videos und Fotos
- Daten, die mithilfe von Tracking-Software entstehen
- Bestellverlauf in einem Online-Shop

Im Rahmen der DSGVO müssen Betreiber von Webseiten aller Art ihren Internetauftritt auf Konformität prüfen und gegebenenfalls auch das Newsletter-System, sofern dies in den Internetauftritt integriert ist.

Website-Hosting und Hoster

Unternehmen mit Internetauftritt speichern die dort anfallenden Daten meist nicht auf einem eigenen Server, sondern nutzen den Service eines externen Dienstleisters (IT-Hoster). Der Content auf der Website ist über die Server des Providers öffentlich abrufbar. Alternativ hosten Unternehmen mit eigener IT-Abteilung und Hardware ihren Internetauftritt auf einem eigenen Server.

Was ist das Problem bei der Nutzung von Website-Hosting?
Im Rahmen des Hostings bei einem Provider speichert dieser unter anderem die Inhalte der Website und im Falle eines Online-Shops zudem Kunden- und Zahlungsdaten auf seinen Servern ab. Zum Teil logt dieser auch Tracking-Daten über das Besucherverhalten auf der Website. Daher findet eine Verarbeitung, insbesondere Erhebung und Übermittlung, der personenbezogenen Daten statt.

Ist ein AV-Vertrag mit dem Hoster notwendig?
Ja, bei einer Auftragsverarbeitung lässt ein Unternehmen (Verantwortlicher) personenbezogene Daten durch eine andere externe Stelle verarbeiten. Das Unternehmen bestimmt allein über die Zwecke und Mittel der Verarbeitung. Ein IT-Hoster, der im Auftrag eines Unternehmens dessen Daten verarbeitet, insbesondere speichert, zählt zu Auftragsverarbeitern (weisungsgebundene Verarbeitung kundenbezogener Daten). Somit ist ein Vertrag über die Auftragsverarbeitung (AV-Vertrag) zu schließen.

Hinweis: Ebenso gelten Tätigkeiten wie Webdesign, Datenkonvertierung und das Erstellen von Back-ups im Sinne der DSGVO als Auftragsverarbeitung. Nur falls gar keine personenbezogenen Daten verarbeitet (z. B. erhoben) werden, handelt es sich nicht um einen Fall der Auftragsverarbeitung und es ist kein AV-Vertrag erforderlich.

Sie betreiben selbst einen Server?
Ein AV-Vertrag ist ebenfalls mit einem Dienstleister zu schließen, den Sie mit der Wartung Ihres Servers beauftragt haben, wenn dieser im Rahmen der Wartung auf personenbezogene Daten zugreifen kann. Die Möglichkeit des Zugriffs reicht bereits aus. Kann hingegen der Zugriff auf die personenbezogenen Daten vollumfänglich ausgeschlossen werden, liegt keine Auftragsverarbeitung vor.

Fazit
Webseiten-Hosting bedeutet, dass der Seitenbetreiber einen AV-Vertrag mit dem Hosting-Anbieter zu schließen hat. Die Provider stellen dafür AV-Verträge bereit.

SSL-Verschlüsselung (https)

Die SSL-Verschlüsselung ermöglicht die sichere Datenübertragung zwischen Client und Server, zum Beispiel sollten die Registrierung und der Einkauf bei einem Online-Shop über eine sichere Verbindung erfolgen.

Was ist das Problem bei nicht verschlüsselten Websites?
Füllt der Besucher einer Internetseite beispielsweise ein Kontaktformular aus und versendet dieses, findet die Datenübertragung vom Client des Anwenders zum Server statt. Geschieht die Datenübertragung unverschlüsselt über http, können zum Beispiel Cyberkriminelle die Daten abfangen und für kriminelle Zwecke missbrauchen.

Welche Lösungsansätze gibt es?
Zur sicheren Ende-zu-Ende-Datenübertragung zwischen Client und Server eignet sich daher die Möglichkeit zur Verschlüsselung. Empfohlen ist die Verschlüsselung mindestens mittels TLS 1.2 (Verfahren der Verschlüsselung) per https (SSL-verschlüsselte Transportverbindungen). Für die Verschlüsselung muss der Webseitenbetreiber ein SSL-Zertifikat erwerben. In der Regel ist ein solches Zertifikat kostenpflichtig oder im Angebot des Hosting-Providers enthalten.

Alternativ existieren zeitlich befristete Angebote von Dienstleistern, die Sie manuell verlängern müssen. Ein kostenloses und zeitlich limitiertes Zertifikat ist für Betreiber kleiner Websites mit begrenztem Budget interessant. Auf die Vertrauenswürdigkeit des Dienstleisters ist zu achten.

Fazit
Sobald Sie auf Ihrer Website personenbezogene Daten erheben, sollte der Datenaustausch per https abgesichert sein. Unter anderem ist die Verschlüsselung für Online-Shops verpflichtend, da Kontaktdaten und Zahlungsinformationen verarbeitet werden.

Log-Dateien auf dem eigenen Server

Mit Log-Dateien überwachen und protokollieren Webseitenbetreiber die Aktivitäten der Seitenbesucher. Es findet die Speicherung aller Anfragen und Zugriffe auf Unterseiten mit Statusmeldungen statt. Die gesammelten Daten haben für Administratoren großen Wert, denn mithilfe der Log-Dateien lässt sich jeder erfolgreiche und erfolglose Zugriff nachvollziehen. Die Protokollierung ist ein bewährtes Mittel, um Fehler aufzuspüren und zum Beispiel 404-Fehler zu beseitigen (wenn Besucher eine nicht existierende Unterseite öffnen möchten).

Was ist das Problem mit Log-Dateien?
Eine Log-Datei dient der Speicherung personenbezogener Daten, genauer werden folgende Daten protokolliert:

- Uhrzeit zum Zeitpunkt des Seitenzugriffs
- URL der besuchten Website
- Menge der übertragenen Daten in Byte
- Information über die Quelle, über die Besucher auf die Seite gelangen
- Angabe des Browsers
- Information zum Betriebssystem
- Speicherung der IP-Adresse des Besuchers (in anonymisierter Form)

Die Verarbeitung dieser Daten darf wie auch sonst nur erfolgen, sofern es hierfür eine Rechtsgrundlage gibt. Ein Beispiel ist das berechtigte Interesse für statistische Auswertungen.

Welche Lösungen gibt es für den Umgang mit Log-Dateien?
In der Datenschutzerklärung ist der Besucher der Website über die jeweilige Rechtsgrundlage zu informieren. Dabei gilt: Daten dürfen verarbeitet (insbesondere erhoben und ausgewertet) werden, wenn diese für die Sicherheit und Funktionsfähigkeit einer Website erforderlich sind. Derartige Daten dürfen nicht zur Auswertung der Verhaltensweisen der Besucher oder zur Profilbildung zum Einsatz kommen.

Fazit
Log-Dateien verarbeiten Informationen wie die IP-Adressen von Seitenbesuchern. Über die Nutzung der Log-Dateien müssen Sie in der Datenschutzerklärung informieren. Die Erklärung unterrichtet über die Verwendungszwecke der Server-Logfiles und der dort protokollierten Daten.

Kontaktformulare in der Website

Das Kontaktformular ist ein verbreiteter Service und vereinfacht Seitenbesuchern die Kontaktaufnahme mit dem Kundenservice des Unternehmens bzw. Betreibers der Web-site. Da Daten wie Name und Kontaktdaten abgefragt werden, erheben Sie mit einem Kontaktformular persönliche Daten und müssen Seitenbesucher deshalb zu Beginn der Nutzung über Art, Umfang und Zweck der Datenerfassung informieren. Dabei gilt:

- nur notwendige Angaben abfragen (Grundsatz der Datenminimierung),
- bei der Abfrage optionaler Angaben diese als freiwillig kennzeichnen,
- Übermittlung der Daten möglichst über eine verschlüsselte Datenleitung („https“) vornehmen und
- Hinweis zu Kontaktformular in der Datenschutzerklärung geben.

Was gibt es bei Kontaktformularen nach DSGVO zu beachten?
Die Datenschutzvorschriften sind bei personenbezogenen Daten und damit für Kontaktformulare auf Websites relevant. Auf die richtige technische (eine verschlüsselte Datenverbindung) und inhaltliche Umsetzung ist zu achten.

Welche Lösungsansätze kommen infrage?
Die Verarbeitung personenbezogener Daten ist erlaubt, wenn es hierfür eine Rechtsgrundlage (z. B. Vertrag bzw. Vorvertrag oder Einwilligung) gibt (Art. 6 Abs. 1 DSGVO). Wie bisher sollte das Versenden der personenbezogenen Daten angemessen verschlüsselt per https erfolgen. Die Verschlüsselung über das SSL-Protokoll sollte dem aktuellen Stand der Technik entsprechen und mindestens per TLS 1.2 erfolgen.

Fazit
Betreiber einer Internetseite bieten Besuchern als Serviceleistung und Angebot (Rechtsgrundlage: vorvertragliches Schuldverhältnis) eine einfache Möglichkeit der Kontaktaufnahme. Hierbei sollten Websitebetreiber darauf achten, dass die Übertragung der persönlichen Daten über eine angemessen verschlüsselte Verbindung erfolgt. Die Datenschutzerklärung muss Informationen über die Zwecke sowie über Art und Weise der Datenverarbeitung enthalten.

Tracking- und Analyse-Software

Mithilfe von Tracking- und Analyse-Software wie Google Analytics und Matomo (ehemals Piwik) lernen Websitebetreiber viel über die Besucher ihrer Website und können ihren Internetauftritt zielgruppenspezifisch optimieren.

Was ist das Problem mit Tracking- und Analyse-Software?
Ist Software wie Google Analytics oder Matomo auf Ihrer Website aktiv, werden personenbezogene Daten (IP-Adressen) an Dritte übertragen. Damit sind die Datenschutzbestimmungen zu beachten. Um die Dienste rechtskonform zu gestalten, müssen Sie Folgendes beachten:

Wie lassen sich Tracking- und Analyse-Software datenschutzkonform einsetzen?
Wichtig ist die Einbindung eines Opt-Out-iFrames, damit Besucher das Tracken deaktivieren können. Für Google Analytics arbeiten Sie mit der Anleitung zum Deaktivieren des Trackings, Matomo bietet das Plugin „AnonymizeIP“ an, das der Admin aktivieren muss. In den FAQs von Matomo finden Sie weitere Informationen zum Opt-Out-Verfahren. Tracking-Tools zur Reichweitenmessung sind zur ausschließlich statistischen Analyse zulässig. Rechtsgrundlage hierfür ist ein „berechtigtes Interesse“ nach Art. 6 Abs. 1 f DSGVO, d. h. erforderlich sind zum einen eine Vorabinformation der Seitenbesucher (z. B. über Datenschutzerklärung) und eine Möglichkeit, einem anonymisierten Tracken zu widersprechen.

Fazit
Ein rechtskonformer Einsatz setzt Folgendes voraus:

- Hinweis in der Datenschutzerklärung,
- Anonymisierung der IP-Adresse,
- Möglichkeit zum Widerspruch gegen anonymisiertes Tracken,
- Auftragsverarbeitungsvertrag (sofern personenbezogene Daten auf Server des Tracking-Tool-Anbieters gespeichert werden).

Wir danken der IHK für München und Oberbayern für die Zurverfügungstellung des Textes.

Facebook-Fanpage: Wer haftet für die Datenverarbeitung auf der Plattform Facebook?

Der EuGH hat entschieden: Neben Facebook haftet auch der Betreiber einer Facebook-Fanpage für Datenschutzverstöße. Er muss im Rahmen seiner Datenschutzerklärung auf der Fanpage erklären, wo welche Daten für wen erhoben und wie lange sie aufbewahrt werden. Das dürfte ihm kaum gelingen, denn hier beginnt das Geschäftsgeheimnis von Facebook. Das Urteil setzt auf dem alten Datenschutzrecht auf, wahrscheinlich gilt dasselbe für die DSGVO.

Die deutschen Aufsichtsbehörden äußern sich dazu wie folgt:

- Wer eine Fanpage besucht, muss transparent und in verständlicher Form darüber informiert werden, welche Daten zu welchen Zwecken durch Facebook und die Fanpage-Betreiber verarbeitet werden. Dies gilt sowohl für Personen, die bei Facebook registriert sind, als auch für nicht registrierte Besucherinnen und Besucher des Netzwerks.
- Betreiber von Fanpages sollten sich selbst versichern, dass Facebook ihnen die Informationen zur Verfügung stellt, die zur Erfüllung der genannten Informationspflichten benötigt werden.
- Soweit Facebook Besucherinnen und Besucher einer Fanpage durch Erhebung personenbezogener Daten trackt, sei es durch den Einsatz von Cookies oder vergleichbarer Techniken oder durch die Speicherung der IP-Adresse, ist grundsätzlich eine Einwilligung der Nutzenden erforderlich, die die Anforderung der DSGVO erfüllt.

- Für die Bereiche der gemeinsamen Verantwortung von Facebook und Fanpage-Betreibern ist in einer Vereinbarung festzulegen, wer von ihnen welche Verpflichtung der DSGVO erfüllt. Diese Vereinbarung muss in wesentlichen Punkten den Betroffenen zur Verfügung gestellt werden, damit diese ihre Betroffenenrechte wahrnehmen können.

Für die Durchsetzung der Datenschutzvorgaben bei einer Fanpage ist die Aufsichtsbehörde zuständig, die für das jeweilige Unternehmen oder die Behörde zuständig ist, die die Fanpage betreibt. Die Durchsetzung der Datenschutzvorgaben im Verantwortungsbereich von Facebook selbst obliegt primär der irischen Datenschutzaufsicht im Rahmen der europäischen Zusammenarbeit.
Die deutschen Aufsichtsbehörden weisen darauf hin, dass nach dem Urteil des EuGH dringender Handlungsbedarf für die Betreiber von Fanpages besteht. Dabei ist nicht zu verkennen, dass die Fanpage-Betreiber ihre datenschutzrechtlichen Verantwortung nur erfüllen können, wenn Facebook selbst an der Lösung mitwirkt und ein datenschutzkonformes Produkt anbietet, das die Rechte der Betroffenen wahrt und einen ordnungsgemäßen Betrieb in Europa ermöglicht.

Praxistipp: Abzuwarten bleibt, wie die Entwicklung weitergeht und das Bundesverwaltungsgericht entscheidet. Bis dahin sollten Fanpagebetreiber auf jeden Fall eine Datenschutzerklärung auf die Fanpage einstellen.

Datenschutzfolgenabschätzung - Liste bei LfDI

Nach Art. 35 DSGVO muss bei gewissen Verarbeitungsvorgängen vorab eine Abschätzung der Risiken für die Rechte und Freiheiten der Betroffenen erfolgen (Datenschutzfolgenabschätzung, DSFA). In Art. 35 DSGVO werden zwar drei Regelbeispiele genannt, jedoch herrschte häufig Unsicherheit, welche Vorgänge nun konkret gemeint sind, sagt das Unabhängige Datenschutzzentrum Saarland:

https://datenschutz.saarland.de/themen/datenschutz-folgenabschaetzung/

Der Landesbeauftragte für Datenschutz und Informationsfreiheit Rheinland-Pfalz (LfDI) gibt Erklärungen zur DSFA stellt eine Liste für Unternehmen zur Verfügung, in der entsprechende Verarbeitungsvorgänge genannt sind. Diese ist hier einsehbar:

https://www.datenschutz.rlp.de/fileadmin/lfdi/Dokumente/Orientierungshilfen/DSFA_-_Muss-Liste_RLP_NOE.pdf

VERANSTALTUNGEN

„Haftungsklauseln und ihre Versicherbarkeit“
Dienstag, 21. August 2018, 18.00 bis 20.00 Uhr, IHK Saarland, Saalgebäude, Raum 1, Franz-Josef-Röder-Str. 9, 66119 Saarbrücken.

„... die Haftung für ... ist ausgeschlossen“ oder „... begrenzt ...“. Solche und ähnliche Klauseln lesen Sie oft in Verträgen. Hintergrund ist der Versuch, sich als Unternehmer vor der Inanspruchnahme für mittelbare, unmittelbare, direkte oder auch indirekte Schäden zu schützen. Aber: Sind solche Klauseln auch wirksam und wenn nicht, kann der Unternehmer sich durch den Abschluss von Versicherungen vor Haftung schützen?

Fragen, die Ihnen Herr Rechtsanwalt **Matthias Brombach,** teras Anwaltskanzlei Brombach & Partner | Rechtsanwälte Saarbrücken, gerne beantwortet. Abgerundet wird sein Vortrag durch Herrn **Joachim Lenoir,** Mitglied der Geschäftsleitung / Leiter Haftpflicht, BüchnerBarella Assekuranzmakler GmbH & Co. KG, Saarbrücken.

Anmeldungen bis **20. August 2018** unter E-Mail: rosemarie.kurtz@saarland.ihk.de

„Arbeiten 4.0 - anyplace - Alles rund um den Arbeitsort“
Donnerstag, 23. August 2018, 18.00 bis 20.00 Uhr, Raum 1, Saalgebäude, IHK Saarland, Franz-Josef-Röder-Str. 9, 66119 Saarbrücken.

Die Digitalisierung hält Einzug in der Arbeitswelt. Die moderne Technik mit Tablets, Laptops und Smartphones ermöglicht mobile und variable Arbeitsorte. Auch das Home-Office ergänzt bzw. ersetzt den Büroarbeitsplatz immer mehr.

Herr Rechtsanwalt **Frank Gust,** Training und Beratung im Arbeitsrecht, Saarbrücken, wird aufzeigen, welche Regelungen getroffen werden müssen, damit ortsunabhängiges Arbeiten für beide Seiten funktioniert - sowohl für den Arbeitgeber wie auch für seinen Arbeitnehmer. Von der auszugestaltenden Technik, dem Arbeitsschutz, der Wahrung des Geschäfts- und Betriebsgeheimnisses, dem Datenschutz bis hin zur Regelung der eventuell eintretenden Haftungsfragen für Schäden - alles bedarf einer klaren Regelung im Vorfeld.

Anmeldungen bis 22. August 2018 unter E-Mail:
rosemarie.kurtz@saarland.ihk.de

Verantwortlich und Redaktion:
Ass. iur. Heike Cloß, Tel.: (0681) 9520-600, Fax: (0681) 9520-690
E-Mail: heike.closs@saarland.ihk.de
IHK Saarland, Franz-Josef-Röder-Str. 9, 66119 Saarbrücken

Ihre Ansprechpartnerinnen:

Ass. iur. Heike Cloß
Tel.: (0681) 9520-600
Fax: (0681) 9520-690
E-Mail: heike.closs@saarland.ihk.de

Ass. iur. Kim Pleines
Tel.: (0681) 9520-640
Fax: (0681) 9520-690
E-Mail: kim.pleines@saarland.ihk.de

Die in dem Newsletter Datenschutz enthaltenen Angaben sind mit größtmöglicher Sorgfalt erstellt worden. Dennoch kann für Vollständigkeit, Richtigkeit sowie für zwischenzeitliche Änderungen keine Gewähr übernommen werden

Impressum:
IHK Saarland, vertreten durch Präsident Dr. jur. Hanno Dornseifer und Hauptgeschäftsführer Dipl.-Volkswirt Dr. Heino Klingen, Franz-Josef-Röder-Str. 9, 66119 Saarbrücken, E-Mail info@saarland.ihk.de, Tel. + 49 (0) 6 81/95 20-0, Fax + 49 (0) 6 81/95 20-8 88, UST.- Ident.- Nummer: DE 138117020