EDV-Unternehmensberatung
Floß GmbH

Infoblatt
Webseiten und die
EU-Datenschutzgrundverordnung (DSGVO)

Mit der EU-Datenschutzgrundverordnung (DSGVO) ergeben sich bestimmte Anforderungen an eine rechtskonforme Verarbeitung personenbezogener Daten über Webseiten. Daher müssen sich Webseitenbetreiber genau überlegen, wie sie diese Anforderungen erfüllen. Rechtliche und faktische Voraussetzungen betreffen nicht nur die ohnehin immer geltenden Datenschutzprinzipien wie Verfügbarkeit, Integrität oder Vertraulichkeit, sondern auch besondere Informationspflichten gegenüber den Seitenbesuchern.

Jeder Webseitenbetreiber ist für die Einhaltung der Datenschutzanforderungen verantwortlich. Verstöße - auch durch Unterlassungen – können mit einem Risiko eines Bußgeldes durch eine Datenschutzaufsichtsbehörde oder der Gefahr einer Schadensersatzforderung durch einen Betroffenen verbunden sein. In Bezug auf die Geldbußen können die Aufsichtsbehörden seit Inkrafttreten der DSGVO Bußgeldbeträge bis zu 20 Mio. EUR bzw. 4% des Vorjahresumsatzes festsetzen, was das Risiko für Unternehmen deutlich erhöht.

Daher beraten wir Sie als unsere Kunden regelmäßig in Fragen rund um eine DSGVO konforme Webseite. Dennoch wollen wir Ihnen mit diesem Dokument ein paar generelle Tipps für den Bau und Unterhalt einer datenschutzkonformen Webseite an die Hand geben.

Bitte beachten Sie jedoch hierbei, dass es sich nur um einen groben Überblick mit den wichtigsten Prüfkriterien handelt. Dies ersetzt keine datenschutzrechtliche Beratung in einem konkreten Einzelfall. Kommen Sie daher gerne auf uns zu, wenn Sie eine neue Webseite oder den Umbau einer bestehenden Webpräsenz planen.

Wir helfen Ihnen dann gerne und mit Sachverstand weiter.

Ihr Floß Team

Inhaltsverzeichnis

Stand des Dokuments: 02.09.2022

1. Korrekte und vollständige Datenschutzerklärung auf der Webseite

Jeder Betreiber einer eigenen Webseite muss eine korrekte und vollständige Datenschutzerklärung mit Hinweisen zur Verarbeitung der (personenbezogenen) Daten bei Aufruf der Webseite zugänglich machen. Diese sollte von jeder Unterseite der Webseite aus zugänglich sein, weshalb es sich anbietet, die Datenschutzerklärung stets in der Fußzeile jeder Webseite zu verlinken. Folgende Inhalte sollte die Erklärung aufweisen:

I. Name bzw. Firmenname, Adresse und Kontaktdaten des Verantwortlichen
   - Name und Kontaktdaten des bestellten Datenschutzbeauftragten (soweit vorhanden)

II. Hosting
   - Wer betreibt den Webserver + wo wird der Webserver betrieben (Name, Adresse sowie ggf. Hinweis, dass ein AV-Vertrag abgeschlossen wurde (verpflichtend, wenn personenbezogene Daten über die Webseite verarbeitet werden (z. B. durch Kontaktformular))

III. Beschreibung der Datenverarbeitung über diese Webseite*
   - Welche Daten werden über die Webseite verarbeitet – z. B. bei Besuch der Webseite und deren Unterseiten, bei einer Anmeldung zum Newsletter über die Seite oder bei Verwendung eines Kontaktformulars

IV. Zwecke und Rechtsgrundlagen der Verarbeitung*

V. Empfänger oder Kategorien von Empfängern
   - Es sind die einzelnen Empfänger und -kategorien sowie der Zweck und die entsprechenden Rechtsgrundlagen für die Datenweitergabe zu benennen
   - Hinweis bei Empfängern in unsicheren Drittländern hinsichtl. notwendiger Garantien und Prüfungen (z. B. EU-Standardvertragsklauseln, Transferfolgenabschätzung)

VI. Cookies, Tracking und Co.*
   - Beschreibung welche Arten von Cookies und Analyse-Tools eingesetzt werden
   - Erklärung welche Plug-Ins, Verlinkungen etc. zu Social Media Plattformen bestehen und welche Daten für welchen Zweck übermittelt werden

VII. Speicher-/Löschfristen für verarbeitete Daten oder Kriterien, die eine Frist bestimmen*

VIII. Betroffenenrechte
   - Aufführen der Rechte nach Art. 15 – 18 DSGVO sowie Art. 21 DSGVO
   - Information über Beschwerderecht bei einer Datenschutzaufsichtsbehörde

** Es ist durchaus sinnvoll bei konkreten Verarbeitungsvorgängen, wie z. B. dem Kontaktformular, die mit dem * gekennzeichneten Informationen in einem Absatz zu formulieren. Das heißt, dass z. B. sodann entsprechend darüber informiert wird, welchen Zweck das Kontaktformular erfolgt, auf welcher Rechtsgrundlage die (personenbezogenen) Daten verarbeitet werden, die lange diese gespeichert werden und ob diese ggf. weitergeleitet werden.*

2. Interne Dokumentation von Verfahren und Rechtsgrundlagen

Nach Artikel 30 DSGVO sind Verantwortliche einer Datenverarbeitung in der Regel verpflichtet, ein **Verzeichnis aller Verarbeitungstätigkeiten mit personenbezogenen Daten** zu führen. Dieses Verzeichnis war vor dem Inkrafttreten der DSGVO nach altem Recht bereits unter den Begrifflichkeiten Verfahrensverzeichnis, Verfahrensbeschreibung oder Dateibeschreibung bekannt. Auch Auftragsverarbeiter haben nach dieser Norm bestimmte Dokumentationspflichten in Bezug auf Verfahren, bei den sie Daten im Auftrag eines Verantwortlichen verarbeiten.

Diese Dokumentationspflicht von Verantwortlichen und Auftragsverarbeitern gilt auch im Hinblick auf Webseiten und den damit verbundenen Verarbeitungsvorgängen mit personenbezogenen Daten von Webseitenbesuchern. Sie ist ein wesentlicher Baustein des unternehmensinternen Datenschutz- und Informationssicherheitsmanagements. Dabei verschafft diese Datenschutzdokumentation dem Unternehmen die Möglichkeit, seiner Rechenschaftspflicht im Sinne von Artikel 5 Abs. 2 DSGVO nachzukommen. Das Verzeichnis der Verarbeitungstätigkeiten sollte schriftlich geführt werden, eine digitale Führung ist möglich. **Das Verzeichnis der Verarbeitungstätigkeiten sollte stets die nachfolgenden Informationen pro Verfahren enthalten:**

- Bezeichnung, Titel oder Name des jeweiligen Verfahrens
- Name und Kontaktdaten des Verantwortlichen
- Zweck der Datenverarbeitung
- Verständliche und nachvollziehbare Beschreibung der Verarbeitung
- Rechtsgrundlage der Datenverarbeitung
    - In Fällen, bei denen auf das berechtigte Interesse nach Art. 6 Abs. 2 lit. f) DSGVO abgestellt wird, muss hierbei auch die Dokumentation der nach dieser Norm erforderlichen Abwägungsprüfung enthalten sein.
- Kategorien der verarbeiteten personenbezogenen Daten
- Kategorien der von der Verarbeitung betroffenen Personen
- Empfänger der personenbezogenen Daten
- Empfänger der Daten in einem Drittland oder einer internationalen Organisation
- Beschreibung der vorgenommenen Schutzmaßnahmen bei der Übermittlung in Drittländer
- Speicherdauer der Daten bzw. die vorgesehenen Löschfristen für die einzelnen Datenkategorien
- Beschreibung der technischen und organisatorischen Maßnahmen (TOMs) zum Schutze der Daten
- Entscheidung zur Notwendigkeit einer Datenschutzfolgenabschätzung
- Verweise auf Referenzdokumente und sonstige Anmerkungen

3. Dienstleister (Auftragsverarbeiter) sorgfältig wählen und Verträge schließen

Selten setzt ein Unternehmen seine Firmenwebseite komplett allein auf. Vielmehr ist es oft so, dass Dienstleister eingesetzt, werden, die z. B. für die visuelle und inhaltliche Gestaltung/Betreuung der Webseite oder für das Hosting eingesetzt werden. Ferner werden oft Dienstleistungen im Rahmen des Besuchertracking (z. B. für Statistiken/Marketing) oder für das Aufsetzen von Kontaktformularen bzw. der Newsletter-Anmeldung implementiert.

Alle für die Webseite eingesetzten Dienstleistungsanbieter, die personenbezogene Daten erhalten sollen, müssen vorab auf Datenschutzkonformität **geprüft** sein. Grundsätzlich muss bei der Weitergabe von über die Webseite erhobenen personenbezogenen Daten eine datenschutzrechtliche Absicherung der Dienstleistung erfolgen. Dies wird in den meisten Fällen den Abschluss eines **Auftragsverarbeitungsvertrags** erforderlich machen. Ohne diesen wird die Weitergabe personenbezogener Daten in der Regel verboten sein. Ein Verstoß dürfte in jedem Fall bußgeldbewehrt sein.

Dieser Auftragsverarbeitungsvertrag (AVV) sollte mindestens Folgendes regeln:

- Gegenstand und Dauer der Vereinbarung,
- Art und Zweck der Verarbeitung personenbezogener Daten,
- Weisungsgebundenheit des Auftragnehmers,
- Rechte und Pflichten des Auftraggebers,
- Pflichten des Auftragnehmers,
- Regelung von Unterauftragnehmerverhältnissen,
- Dokumentations- und Mitwirkungspflichten, Gerichtsstand und
- technische und organisatorische Maßnahmen.

Es lohnt sich, darauf hinzuwirken, mit dem jeweiligen, ins Auge gefassten zukünftigen Dienstleistungsanbieter einen DSGVO-konformen AVV abzuschließen.

Weitere Anforderungen ergeben sich, wenn der Dienstleister in einem Drittland außerhalb der EU oder des europäischen Wirtschaftsraumes sitzt oder als EU-Niederlassung eine Konzernmutter in einem Drittland hat. In diesen Fällen muss vor dem Einsatz geprüft werden, ob das Drittland ein angemessenes Datenschutzniveau hat.
Ist dies nicht der Fall (wie z. B. bei den USA), muss das notwendige Schutzniveau auf andere Weise sichergestellt werden, etwa durch die **Standardvertragsklauseln der europäischen Kommission**.
Zudem müssen ggf. **ergänzende Garantien** (vertraglich, technisch, organisatorisch) implementiert und eine **Transferfolgenabschätzung** durchgeführt werden.

4. Augen auf bezüglich des Trackings von Webseitenbesuchern!

Viele Unternehmen möchten auf Ihrer Webseite die Möglichkeit haben, die Webseitenbesucher und deren Verhalten auf der Seite auswerten und analysieren zu können. Jedoch dürfen Tracking-Werkzeuge wie zum Beispiel Google Analytics, etracker oder Matomo (vormals Piwik) nur dann eingesetzt werden, wenn diese auch den strengen Vorgaben der DSGVO und des deutschen Bundesdatenschutzgesetzes entsprechen. Ein eindeutig datenschutzkonformer Einsatz ist nicht einfach umsetzbar.

Im Oktober 2019 hat der Europäische Gerichtshof entschieden, dass ein **Tracking von Webseitenbesuchern zu Analysezwecken nur noch nach vorheriger und ausdrücklicher Zustimmung** durch den jeweiligen Webseitenbesucher zulässig ist (Az. C-673/17). Dies dürfte nicht nur (wie im Urteil behandelt) für Cookies, sondern auch für alle anderen Tracking-Technologien entsprechend gelten. Eine **Einwilligung** ist **immer einzuholen, wenn Tracking für Statistiken und Marketingzwecke** eingesetzt wird, z.B. um Nutzerprofile für personalisierte Werbung und Anzeigen zu erstellen. Seit der Verabschiedung des neuen Telekommunikations-Telemedien-Datenschutzgesetzes (TTDSG, seit Mai 2021) gilt diese **Einwilligungspflicht** beim Zugriff auf das Endgerät vom Webseitenbesucher (z. B. zur Ablage von Cookies) **unabhängig vom Personenbezug** der erhobenen bzw. gespeicherten Daten. Eine solche Einwilligung wird üblicherweise über ein sogenanntes Consent-Banner eingeholt. Bitte beachten Sie hierzu auch unsere Tipps im nächsten Abschnitt 5: „Cookies und Cookie-Banner bzw. Consent-Banner richtig einbinden“.

Hiervon **nicht betroffen sind rein funktionale Cookies**, die zwingend notwendig sind, um die Webseite funktional und sicher zu betreiben (wie etwa zur Seitennavigation oder Session-Cookies für Anmelde-Bereiche). Letztere dürfen weiterhin ohne Einwilligung gesetzt werden.

Viele Drittanbieter-Werkzeuge zum Besuchertracking übermitteln personenbezogene Daten der Webseitenbesucher an den Anbieter selbst. In diesem Fällen muss darauf geachtet werden, dass je nach Aufteilung der Verantwortlichkeit entweder ein **Auftragsverarbeitungsvertrag oder ein Vertrag zur gemeinsamen Verantwortlichkeit mit dem Trackingtool-Anbieter** abgeschlossen wird.

Zudem sollte die Übermittlung der Daten pseudonymisiert, bestenfalls sogar anonymisiert erfolgen. Einige Anbieter bieten hierfür schon eigene Funktionalitäten, jedoch ist dabei Vorsicht geboten, ob diese auch wirklich die Anforderungen erfüllen. So bietet zwar beispielsweise Google die Funktion anonymizeIP für Google Analytics an, allerdings wird beim Laden der relevanten Scripts von Google-Servern doch zunächst die vollständige IP-Adresse eines Website-Besuchers erfasst und wird erst in einem weiteren Schritt nur teilweise maskiert. Eine echte Anonymisierung, wie sie Google bewirbt, findet zudem noch nicht statt, da neben der IP-Adresse weitere Nutzungsdaten erhoben werden, die personenbeziehbar bleiben.

Insgesamt wird ein Einsatz speziell von Google Analytics durch die deutschen und europäischen Datenschutzaufsichtsbehörden immer kritischer gesehen. Diese gehen zunehmend davon aus, dass ein rechtskonformer Einsatz nicht möglich ist, da aufgrund der Datenweitergabe an die Google Konzernzentrale in den USA die allgemeinen Grundsätze der Datenübermittlung in ein Drittland verletzt werden. Eine Verwendung von Google Analytics geht somit derzeit mit einem hohen Risiko in Bezug auf aufsichtsbehördliche Sanktionen bzw. Betroffenenklagen einher.

Wird eine Trackinglösung selbst gehostet und findet keine Datenübermittlung an den Anbieter statt, so ist der Abschluss eines Auftragsverarbeitungsvertrags nicht erforderlich.

Zu bedenken ist auch, dass in der **Datenschutzerklärung** der Webseite umfänglich über die Erhebung, Verwendung (Zwecke), Speicherdauer und Weitergabe der Daten im Kontext von Tracking informiert werden muss. Zudem muss ein **Widerruf der Einwilligung** für die Webseitenbesucher **jederzeit möglich** sein.

5. Cookies und Cookie-Banner bzw. Consent-Banner richtig einbinden

Oft werden auf Webseiten sogenannte Cookies eingesetzt. Dies sind kleine Textdateien, die über den Webbrowser eines Webseitenbesuchers auf dessen Gerät gespeichert werden. Cookies enthalten Informationen, die zu einem späteren Zeitpunkt vom Webserver wieder ausgelesen werden können. Sie werden entweder von den Webseitenbetreibern selbst oder von Drittanbietern, deren Dienste auf der Webseite des Betreibers eingebunden wurden, gesetzt. Hierbei ist zu beachten, dass auch die Einbindung von Drittanbieter-Plug-Ins oder Zählpixel aus Social Media Netzwerken in der Regel das Setzen von Cookies erfordert.

Typische Zwecke für das Setzen von Cookies sind:

- **Speicherung von Einstellungen** für die Webseite, wie etwa die Sprache oder das Aussehen der Webseite
- **Speicherung eines Warenkorbinhalts** beim Online-Shopping, damit dieser zu einem späteren Zeitpunkt wieder aufgerufen werden kann
- **Wiedererkennung eines Webseitenbesuchers**, solange dieser sich eingeloggt auf allen Unterseiten einer Webseite bewegt (sog. Session Cookies). So müssen sich zum Beispiel in einem sozialen Netzwerk oder in einem Online-E-Mail-Account angemeldete Nutzer nicht bei jedem Aufruf einer Unterseite neu anmelden.
    - Dies bedeutet allerdings auch, dass Cookies auch vertrauliche Daten wie Anmeldedaten mit Passwörtern für solche Anmeldedaten enthalten können
    - **Analyse des Surfverhaltens des Webseitenbesuchers**, ggf. mit Bildung eines Nutzerprofils zu verschiedenen Einzelzwecken, wie etwa Erstellung von Seitenstatistiken oder für Werbe- und Marketingzwecke

Aus datenschutzrechtlicher Sicht ist relevant, ob es sich um sogenannte technisch notwendige (funktionale) Cookies handelt, oder nicht.

Funktionale Cookies sind jene, die zwingend notwendig für das Funktionieren der Webseite sind. Hierzu gehören etwa Session Cookies oder Cookies zur Speicherung eines Warenkorbinhalts oder von Log-In Daten. Diese werden meist automatisch gelöscht, sobald der Internetbrowser geschlossen wird.

- Für das Setzen funktionaler Cookies, ohne deren Speicherung die Darstellung der Website gar nicht möglich wäre, können Webseitenbetreiber als Rechtsgrundlage ihr **berechtigtes Interesse** an dem sicheren und störungsfreien Betrieb ihrer Webseite im Sinne von Artikel 6 Abs. 1 lit. f) DSGVO geltend machen. Die einzigen Webseitenwerkzeuge, die ebenfalls mit einem berechtigten Interesse begründet werden dürfen, sind jene, die anonymisiert die Seitenaufrufe zu statistischen Zwecken zählen. Immer ist in der Datenschutzerklärung über die Widerspruchsmöglichkeit des Betroffenen zu informieren.

Für alle anderen – nicht funktionalen - Cookies muss eine Einwilligung im Sinne der Artikel 6 Abs. 1 lit. a) und 7 DSGVO sowie Art. 25 Abs. 1 TTDSG eingeholt werden. Hier kommt das sogenannte Cookie- oder Consent-Banner der Webseite ins Spiel. Dessen konkrete Ausgestaltung unterliegt bestimmten datenschutzrechtlichen Anforderungen. Bitte beachten Sie hierbei auch, dass bei Webseiten, die sich (auch) an **Minderjährige** richten, eine Einwilligung für nicht funktionale Cookies nicht möglich ist. Eine zulässige bzw. rechtswirksame Einwilligung ist nach Art. 8 Absatz 1 S. 1 DSGVO erst bei Personen ab 16 Jahren möglich. Richten sich Webseiten daher an Minderjährige, sollten nur funktionale Cookies eingesetzt werden. Ferner nicht möglich sind (nach §§ 3, 5 Abs. 1 S. 2 Nr. 2, 8 Abs. 1, Abs. 3 Nr. 1 UWG) auch **Cookie-gesteuerte**, mehrfache und hintereinander geschaltete **Rabattaktionen** auf der Webseite. Dies betrifft Fälle, wo beim ersten Besuch eines Kunden auf einer Webseite ein Cookie auf seinem Rechner hinterlassen wird, auf Grund dessen die Webseite den Kunden bei dessen zweiten Besuch der Seite erkennt und diesem sodann keine weitere Rabattaktion mehr angezeigt wird. Nach aktueller Rechtsprechung (vgl. OLG Köln, Urteil vom 3.12.2021, Az. 6 U 62/21) dürfte diese Vorgehensweise unzulässig sein.

Die Anforderungen an ein DSGVO-konformes Cookie- bzw. Consent-Banner sind:

1. **Prominente Platzierung des Banners**
   Das Cookie- oder Consent-Banner sollte direkt zu Beginn des Aufrufs der Website angezeigt werden. Es sollte gut sicht- und lesbar sein, dabei aber wichtige Bereiche der Seite wie etwa das Impressum, die AGB oder die Datenschutzerklärung nicht verdecken. Diese Bereiche müssen stets anklickbar und lesbar sein, auch wenn der Webseitenbesucher über das Cookie-Banner noch keine Entscheidung zu Cookies getroffen hat.
2. **Setzen nicht funktionaler Cookies niemals vor Zustimmung des Webseitenbesuchers**
   Solange der Webseitenbesucher noch keine Entscheidung darüber getroffen hat, ob er Cookies zustimmt oder diese ablehnt, dürfen keinesfalls irgendwelche nicht funktionalen Cookies gesetzt werden. Das Setzen solcher Cookies muss daher bis zur Abgabe einer Einwilligung technisch unterbunden sein.
3. **Gestaltung des Cookie-Banners mit echter Wahlmöglichkeit für den Webseitenbesucher**
   Das Cookie-Banner muss dem Webseitenbesucher nicht nur die Möglichkeit geben, dem Setzen nicht funktionaler Cookies zuzustimmen, sondern dieses auch auf ebenso einfache Weise abzulehnen. Somit muss mindestens ein „Cookies akzeptieren“ wie auch ein „Alle Cookies ablehnen“ Button vorhanden sein. Eine differenzierte Abstufung mittels einer dritten Möglichkeit in der Art von „Individuelle Einstellungen vornehmen“ ist möglich und im Sinne umfänglicher Betroffeneninformation sogar wünschenswert.
4. **Aktives Zustimmen des Webseitenbesuchers**
   Die Einwilligung muss in einer aktiven Zustimmungshandlung des Webseitenbesuchers bestehen (sog. Opt-in, vgl. Erwägungsgrund 32 Satz1 DSGVO). Dies wäre etwa der Fall, wenn der Besucher vorhandene Checkboxen zur Zustimmung aktiv anklickt. Ein Anzeigen von bereits vom Webseitenbetreiber vorausgefüllten Checkboxen ist unzulässig (kein

Opt-out)! Enthalten Checkboxen bereits ein Häkchen, fehlt es regelmäßig an der Freiwilligkeit der Einwilligung im Sinne von Artikel 7 DSGVO, die Einwilligung kann in solchen Fällen daher unwirksam sein. Leere Checkboxen sind daher erfahrungsgemäß der praktischste Weg, die Zustimmung für Cookies einzuholen.

5. **Möglichkeit der differenzierten Entscheidung über die einzelnen Arten von Cookies**
   Es ist empfehlenswert, dem Webseitenbesucher die Möglichkeit zu geben, Details über einzelne Cookies oder zumindest Arten von Cookies zu erfahren und entsprechend differenziert zuzustimmen bzw. abzulehnen. Hierbei gibt es die Möglichkeit, entweder direkt alle Cookies einzeln aufzuführen oder über einen Klick (Aufklappmenü) einzublenden. Sinnvoll ist eine Information über die Cookies mittels einer Ansicht in Kategorien von Cookie-Arten, wie funktional (technisch erforderlich, immer an), Cookies zu Statistikzwecken und Cookies zu Werbe-/Marketingzwecken (jeweils Zustimmung erbeten). Es sollte möglich sein, für die einzelnen Cookies weitere Information aufzurufen, wie etwa Name des Cookies und des Drittanbieters mit Link zu dessen Datenschutzerklärung, dem Zweck sowie der Speicherdauer. Eine differenzierte Entscheidungsmöglichkeit mit Checkbox pro Cookie wäre optimal, da ein Webseitenbesucher beispielsweise durchaus mit einem Cookie des Webseitenbetreibers zu Statistikzwecken einverstanden sein kann, ohne ein Cookie von einem Drittanbieter (wie z. B. Google, Facebook) zulassen zu wollen.
6. **Keine entscheidungsbeeinflussende optische Gestaltung des Cookie-Banners**
   Die Farbe und Größe der Schaltflächen (Buttons) sollten gleichwertig und gut lesbar sein. Nicht zulässig ist eine alleinige optische Hervorhebung des „Zustimmen“ oder „Akzeptieren“ Buttons durch Farbe, Größe oder Beschriftung. Gleiches gilt, wenn die Ablehnungsmöglichkeit in einer weiteren (untergeordneten) Klickebene versteckt ist. Werden Webseitenbesucher durch optisch unattraktive Gestaltung der Ablehnungsmöglichkeit beeinflusst, ist dies unzulässig, was rechtlich zur Unwirksamkeit einer gegebenen Einwilligung führen kann.
7. **Hinweis auf Widerrufsmöglichkeit**
   Das Cookie-Banner sollte den Webseitenbesucher direkt darüber informieren, dass die Möglichkeit des späteren Widerrufs einer gegebenen Einwilligung besteht. Im Idealfall kann das Cookie-Banner jederzeit für eine erneute Entscheidung von jeder Seite/Unterseite der Webseite neu aufgerufen werden. Zumindest aber sollte die Möglichkeit an einer auffindbaren Stelle, z. B. am Anfang der Datenschutzerklärung, abgebildet bzw. möglich sein.
8. **Verweis auf die Datenschutzerklärung**
   Das Cookie-Banner sollte auf die Datenschutzerklärung der Webseite verlinken. Soweit beim Setzen von Cookies eine Datenübermittlung in Drittländer (wie z. b. USA) stattfindet, sollte bereits im Consent-Banner darauf hingewiesen werden.
9. **Sorgfältige Auswahl des Anbieters für Cookie-Banner**
   Meist werden externe Anbieter eingesetzt, die für die Webseite Funktionalitäten eines Cookie-Banners bereitstellen. Hierbei sollte wie bei allen anderen Dienstleistern für die

Webseite auch sorgfältig der Anbieter gewählt werden. Dessen Produkt sollte in der Lage sein, die o. g. Anforderungen zu erfüllen. Eine Drittlandübermittlung sollte vermieden und ein Auftragsverarbeitungsvertrag abgeschlossen werden.*

**Die meisten Anbieter setzen Unterauftragnehmer mit einer Verbindung oder dem Sitz in einem nichtsicheren Drittland, wie z. B. die USA ein. Oftmals wird AWS mit Standort in Deutschland oder innerhalb der EU angegeben. Aber Achtung! Dennoch ist eine Datenweitergabe an die Konzern-Mutter in den USA möglich und nicht ausgeschlossen!*

6. Kontaktformular – was ist zu beachten?

In vielen Fällen kann es sinnvoll sein, ein Kontaktformular auf der firmeneigenen Webseite zu unterhalten. Auch dazu sollten dann **Informationen in der Datenschutzerklärung** enthalten sein. In für den durchschnittlichen Webseitenbesucher leicht verständlicher Sprache sollte erläutert sein, welche Daten in solchen Fällen zu welchen Zwecken erhoben und verarbeitet werden. Auch alle anderen notwendigen Angaben in einer Datenschutzerklärung (siehe Abschnitt 1 oben) wie z. B. Speicherfristen, Rechtsgrundlagen und Datenweitergabe an dienstleistende Drittanbieter sollten enthalten sein.

Die Datenschutzerklärung sollte **direkt unter dem Formularfeld verlinkt** sein. Über eine **anklickbare Checkbox** sollte der Webseitenbesucher seine Bestätigung der Kenntnisnahme und Einwilligung zur Verarbeitung dieser Daten explizit geben können.

Die **Formularseite** sollte zur Gewährleistung der Sicherheit und Vertraulichkeit mit einem TSL- bzw. SSL-Zertifikat **verschlüsselt** sein. Sehen Sie hierzu bitte auch in diesem Dokument den Abschnitt 11 (Verschlüsselte Übertragung einrichten).

Grundsätzlich sollte dem **Grundsatz der Datensparsamkeit** entsprochen werden. Dies bedeutet, dass von den Seitenbesuchern über die Formularmaske nur die personenbezogenen Daten erhoben werden, die für den Zweck des Anliegens zwingend notwendig sind. Somit muss im Vorfeld der Implementierung geprüft werden, welche Datenangaben zu Pflichtfeldern erklärt werden sollen. Eine deutliche optische Unterscheidung zu optionalen Angaben muss vorhanden sein (z. B. durch Kennzeichnung mit einem „*“ oder dem Hinweis „*Pflichtfeld“).

Soweit eine **E-Mail-Adresse** nur zu dem Zweck erhoben wird, dem Seitenbesucher nach Absenden des ausgefüllten Formulars eine Bestätigungsmail zu senden, sollte die Adresse danach (gemäß dem Zweckbindungsgrundsatz) gelöscht werden.

Der **Zweckbindungsgrundsatz** gilt auch dann, wenn die über das Formular erhobenen Daten zunächst nur in einer Datenbank gespeichert und danach in einer E-Mail an den Seitenbetreiber übermittelt werden. Dann sollte daran gedacht werden, die Daten nach dem Versand dieser E-Mail aus der als Zwischenspeicher genutzten Datenbank zu löschen.

Die beschriebenen Anforderungen gelten dementsprechend nicht nur für Kontaktformulare, sondern auch für andere Formularseiten auf der Webseite, wie beispielsweise für Newsletter-Anmeldungen, Log-Ins, Webshop-Checkouts, Bewerbungsformulare oder dergleichen. Siehe hierzu auch die beiden nächsten Abschnitte für Kommentarfunktionen und Newsletter-Anmeldungen. **Bei Online-Bewerbungen** sollte zudem eine sichere Möglichkeit angeboten werden, Dokumente verschlüsselt zu übermitteln. Es ist auf entsprechende Datenschutzhinweise für Bewerber hinzuweisen.

7. Kommentarfunktionen – was ist zu beachten?

Eine Kommentarfunktion ist häufig dort erwünscht, wo sich der Webseitenbetreiber Interaktion erhofft, sei es bezüglich der Seitenbesucher untereinander oder mit dem Seitenbetreiber. Doch ebenso wie bei dem Kontaktformular gilt auch hier der **Grundsatz der Datensparsamkeit**. Dies bedeutet, dass nur die personenbezogenen Daten von den kommentierenden Seitenbesuchern erhoben werden sollten, die zwingend zur Zweckerfüllung notwendig sind. So reicht es für viele Zwecke der Kommentarfunktionen völlig aus, dass diese Kommentare im Idealfall anonym abgegeben werden können. Denkbar ist aber auch, auf freiwilliger Basis minimale Angaben wie Name (Pseudonym reicht) und E-Mail-Adresse (nur für Seitenbetreiber sichtbar) vom Kommentierenden abzufragen. Die Protokollierung der IP-Adresse dürfte in der Regel nicht erforderlich sein.

Soweit personenbezogene Angaben erhoben oder sogar eine Registrierung auf der Seite verlangt werden, dürfen diese nur für die Zwecke der Kommentarfunktion erhoben werden. Ist der Zweck erfüllt, sind die Angaben zu löschen.

Für die Datenverarbeitung der Kommentarfunktion muss von dem Webseitenbesucher vorab die Einwilligung im Sinne von Art. 6 Abs. 1 lit. a DSGVO eingeholt werden. Dies kann durch die **Verlinkung der Datenschutzerklärung unter dem Kommentarfeld mit Checkbox zur Bestätigung der Kenntnisnahme und Einwilligung** in die Datenverarbeitung erfolgen.

In der **Datenschutzerklärung** muss genauso wie bei dem Kontaktformular transparent und leicht verständlich erläutert werden, welche Daten zu welchen Zwecken für wie lange und auf welcher Rechtsgrundlage im Rahmen der Kommentare verarbeitet werden. Ebenso muss angegeben werden, wenn Daten an Drittanbieter weitergegeben werden.

Neben dem Datenschutzrecht sollte beachtet werden, dass bei der Einbindung von Kommentarfunktionen in Webseiten auch noch andere gesetzliche Vorgaben eine Rolle spielen könnten. Beispiele hierzu wären etwa Hassrede im Internet, ehrverletzende, beleidigende oder jugendgefährdende Inhalte sowie Inhalte, die eventuell Urheberrechte verletzen. Webseitenbetreiber sollten sich daher genau überlegen ob bei ihnen die Ressourcen vorhanden sind, eine hinreichende Inhaltsmoderation von Kommentaren sicherzustellen. Ist dies nicht der Fall, sollte eine Kommentarfunktion gar nicht erst angeboten werden. Entscheiden Sie sich als Webseitenbetreiber für eine Kommentarfunktion, sollten Sie sich zu diesen Themen unbedingt im Vorfeld entsprechenden Rechtsrat einholen, damit Sie wissen, wie eine rechtskonforme Content-Moderation umzusetzen ist.

8. Newsletter-Anmeldung über die Webseite – was ist zu beachten?

Soweit eine Anmeldung zu einem Newsletter auf der Webseite ermöglicht wird, gilt auch wieder der Grundsatz der **Datensparsamkeit**; in der Regel sollte hierfür die **E-Mail-Adresse** ausreichen. Wichtig ist hierbei, dass der Zweck eines Newsletters im Regelfall Werbung bzw. Marketing ist. Daher gelten hier neben der DSGVO noch **zusätzliche gesetzliche Vorgaben**, die zu beachten sind. Dazu zählen etwa das Telemediengesetz (TMG), das Telemedien-Telekommunikations-Datenschutzgesetz (TTDSG) für die Impressumspflicht sowie das Gesetz gegen unlauteren Wettbewerb (UWG).

Zunächst ist wieder in einer **Datenschutzerklärung** transparent über die Datenverarbeitung zu informieren. Auch hier sollte nicht vergessen werden, darüber zu informieren, wenn der Newsletter-Versand über einen Drittanbieter stattfindet. Ein entsprechender Auftragsverarbeitungsvertrag sollte geschlossen worden sein.

Bei elektronischer Werbung über einen Newsletter gilt zudem nach § 7 Abs. 2 Nr. 3 UWG, dass in der Regel die **Einwilligung des Betroffenen einzuholen** ist. Anderenfalls gelten unaufgefordert zugesandte Newsletter als wettbewerbswidrige unzumutbare Belästigung, also als Spam. Abhängig davon, ob die Einwilligungserklärung durch Klick auf einen Button („Newsletter abonnieren“ oder Ähnliches) oder über eine Checkbox erfolgt, sollte immer ein entsprechender **kurzer Begleittext** dabeistehen, der den Seitenbesucher darauf hinweist, dass er durch die entsprechende Aktion – jederzeit widerruflich –den E-Mail-Newsletter erhält und bestätigt, die Datenschutzerklärung mit weiteren Details zur Kenntnis genommen zu haben. Der **Zweck des Newsletters** ist hierbei zu benennen, etwa für die Information über Angebote und Aktionen des Unternehmens in regelmäßigen Abständen.

Checkboxen sollten niemals vorausgefüllt sein – vielmehr ist für eine wirksame Einwilligung immer ein **aktives Opt-In des Webseitenbesuchers** erforderlich. Bewährt hat sich bei Newslettern das sogenannte **„Double-Opt-In“-Verfahren**. Das bedeutet, dass der Webseitenbesucher bei Anmeldung seine Einwilligung abgibt und dieser dann einen **Bestätigungslink per E-Mail** erhält. Erst mit Anklicken des Links wird durch die betreffende Person verifiziert, dass dieser die Newsletter-Anmeldung auch tatsächlich veranlasst hat. Somit sollte ein Newsletter-Versand erst nach Betätigen des Aktivierungslinks durch den Inhaber der E-Mail-Adresse erfolgen.

Die Aktionen des Webseitenbesuchers – die Anmeldung auf der Webseite selbst wie auch das Anklicken des Bestätigungslinks sollten **protokolliert** werden, damit nachgewiesen werden kann, dass eine wirksame Einwilligung vorliegt.

Den Betroffenen steht ein jederzeitiges Widerrufsrecht in Bezug auf ihre abgegebene Einwilligung zu. Daher muss der Webseitenbesucher, der sich für einen Newsletter anmelden will, im Vorfeld darüber informiert werden, dass er diese **Einwilligung jederzeit mit Wirkung**

für die Zukunft widerrufen kann. Daher bietet es sich auch an, in jedem einzelnen Newsletter unten im Fußzeilenbereich einen deutlichen **Hinweis auf die Abbestellmöglichkeit mit einem entsprechenden Link** einzubauen. Ein Beispiel für einen Hinweis auf die Abbestellmöglichkeit in der Newsletter-E-Mail wäre etwa:

> *Sie erhalten diesen Newsletter, da Sie sich vormals für unseren Newsletter angemeldet hatten. Wenn Sie Ihre Einwilligung widerrufen und diesen Newsletter künftig nicht mehr erhalten möchten, können Sie ihn jederzeit abbestellen, indem Sie hier [Abbestell-Link einfügen] klicken. Alternativ können Sie uns auch eine E-Mail an [E-Mail-Adresse einfügen] senden oder uns dies über die in unserem Impressum angegeben Kontaktdaten mitteilen.*

Nur ausnahmsweise darf ein Newsletter auch ohne die vorherige Einwilligung versandt werden. Dies ist unter Umständen dann der Fall, wenn Ihr Unternehmen Bestandskunden anschreibt, die bereits in der Vergangenheit eine oder mehrere Käufe, Bestellungen o. ä. getätigt haben. Zwingende Voraussetzungen hierfür sind:

- Erhalt der E-Mail-Adresse des Kunden im Zusammenhang mit dem Verkauf einer Ware oder Dienstleistung
- **Information in der Datenschutzerklärung**
  - z. B. in der Datenschutzerklärung des Online-Shops, dass Bestandskunden Newsletter-Werbung zugesandt wird, einschließlich dem Hinweis auf das jederzeitige Widerrufsrecht.
- **Hinweis auf das Widerrufsrecht** für den Kunden bereits bei Erhalt und mit jedem (!) versandten Newsletter
  - Auch hier kann am Ende unten im Fußzeilenbereich jedes Newsletters ein deutlicher **Hinweis auf die Abbestellmöglichkeit mit einem entsprechenden Link** eingebaut werden.
  - Ein Beispiel für einen Hinweis auf die Widerspruchsmöglichkeit in der Newsletter-E-Mail wäre etwa:
    - Sie erhalten diesen Newsletter, weil Sie bei uns bereits eine Bestellung getätigt haben. *Wenn Sie diesen Newsletter künftig nicht mehr erhalten möchten, können Sie dem Versand jederzeit widersprechen und den Newsletter abbestellen, indem Sie hier [Abbestell-Link einfügen] klicken. Alternativ können Sie uns auch eine E-Mail an [E-Mail-Adresse einfügen] senden oder uns dies über die in unserem Impressum angegeben Kontaktdaten mitteilen.*
- **Verwendung dieser E-Mail-Adresse ausschließlich zur Werbung für eigene und ähnliche Waren oder Dienstleistungen**
  - Dies bedeutet, dass sich die einwilligungslose Newsletter-Werbung nur auf Waren oder Dienstleistungen bezieht, die mit denjenigen aus einem vorherigen Kauf oder einer vorherigen Bestellung **identisch oder vergleichbar** sind. Das bedeutet, dass nur generische Shop-Ankündigungen, Rabattaktionen oder Bewertungsaufforderungen für andere Waren-/Dienstleistungskategorien nicht ohne Einwilligung zulässig sind.
- **Kein vorliegender Widerspruch** des Kunden.

9. Vorsicht bei Social-Media Plug-Ins (z. B. Like- oder Teilen-Buttons)

Häufig möchte man als Unternehmen den Besuchern der eigenen Firmenwebseite die Möglichkeit geben, Inhalte zu liken oder über Soziale Medien zu teilen. Zu diesem Zweck binden viele Webseitenbetreiber sogenannte Social-Media-Buttons ein, so wie etwa den Facebook Like Button oder Share/Teilen Schaltflächen mit Verlinkung zu Twitter oder Instagram. Aus datenschutzrechtlicher Sicht ergibt sich hierbei das Problem, dass diese über Plug-Ins eingebetteten Social-Media Buttons eine direkte Verbindung zu den Servern der jeweiligen Social Media Plattformbetreiber unterhalten. Dies bedeutet, dass diese Plattformbetreiber über ihre Plug-Ins das Surfverhalten ihrer Nutzer nachverfolgen können. Dies gilt jedoch nicht nur für Personen, die bereits einen Account bei dieser Social Media Plattform haben und eingeloggt sind. Vielmehr werden über diese Plug-Ins auch Nutzer verfolgt, die nicht eingeloggt oder noch nicht einmal einen Account bei dieser Plattform haben.

Wenn ein solches Plug-In auf einer Webseite eingebettet ist, löst jeder Aufruf der Webseite eine Übermittlung von Nutzerdaten (wie z. B. die IP-Adresse) nicht nur an den Betreiber der Seite aus, sondern auch an den Anbieter der Social Media Plattform. Dabei werden diese Nutzerdaten in der Regel nicht anonymisiert, sondern vielmehr genutzt, um Profile zu Zwecken der Werbung und des Marketings zu erstellen.

Diese Übermittlung findet allerdings oft bereits statt, ehe ein Webseitenbesucher eine wirksame Einwilligung (etwa über ein Consent-Banner) geben kann. Die direkte Übermittlung von Nutzer- bzw. Besucherdaten im Wege der Social-Media Buttons ist in der Regel selbst bei einer ausführlichen Information über die Datenschutzerklärung der Webseite **nicht zulässig**. **In solchen Fällen besteht keine wirksame Einwilligung, da diese zu spät erfolgt.**

Es gibt hierfür zwei mögliche **Lösungen** auf technischer Ebene, nämlich entweder die sogenannte 2-Klick-Lösung oder der Shariff-Button. Die **2-Klick-Lösung** bedeutet, dass die Social-Media-Buttons so auf der Webseite eingebettet sind, dass die Plug-Ins zunächst inaktiv sind. Vielmehr ist anstelle dessen zunächst eine funktionslose Grafik des Buttons zu sehen, die erst proaktiv durch den Webseitenbesucher geklickt werden muss, um die Like- bzw. Teilen-Funktion des Plug-Ins in Gang zu setzen. Über diesen Vorgang kann somit dann auch über die Übermittlung informiert und die aktive Einwilligung des Webseitennutzers eingeholt werden. Knifflig ist hierbei allerdings für Unternehmen, dass zutreffend und vollständig über Umfang und Zweck der Datenübermittlung sowie der weiteren Verarbeitung informiert werden muss. Die **Shariff-Lösung** baut auf der Idee der 2-Klick-Lösung auf und besteht aus von den Seitenbetreibern individuell gestaltbaren HTML-Links direkt zu den Webseiten der jeweiligen Social-Media Plattformen in einem gesonderten Fenster des Browsers. Ab dort greifen daher die Informationspflichten des betreffenden Social-Media Plattformanbieters, so dass ein

Unternehmen, welches die Shariff-Lösung auf der eigenen Firmenseite einbindet, keine Einwilligung der Besucher für Social-Media-Buttons einholen muss.

10. Auch sonstige Drittanbieter-Plug-Ins + Skripte vorher prüfen (lassen)

Die meisten Webseiten haben jenseits der Social-Media Buttons auch noch weitere Drittanbieter-Plug-Ins, Bibliotheken und Add-Ons zu verschiedensten Zwecken eingebunden. Dies können beispielsweise **Schriftbibliotheken** (wie Google Fonts, siehe dazu unten Abschnitt Nr. 12), **Chat-oder Captcha-/Spamschutz-Funktonen**, oder auch Plug-Ins zum Einbetten **externer Karten** (wie Google Maps) **oder Videos** (wie YouTube oder Vimeo) sein.

Auch bei diesen externen Skripten muss auf die datenschutzrechtlichen Anforderungen geachtet werden. Häufig übermitteln diese genauso wie bei den Social-Media Buttons die IP-Adresse des Webseitenbesuchers schon beim Laden der Seite und unabhängig davon, ob der Besucher z. B. ein Video oder eine Karte anklickt.

Findet eine Übermittlung von Besucherdaten an den Drittanbieter statt, so muss hier die Zulässigkeit der Übermittlung stets geprüft werden. Eine Information in der Datenschutzerklärung muss erfolgen und zumeist auch die Einwilligung des Webseitenbesuchers eingeholt, mindestens aber das Widerspruchsrecht einzuräumen.

Es bietet sich an, **auch hier eine 2-Klick Lösung zu finden oder zumindest erweiterte Datenschutzeinstellungen bei der Einbettung des Skriptes** zu nutzen, falls der Drittanbieter diese bietet (so z. B. „erweiterter Datenschutzmodus“ bei YouTube, so dass kein Cookie gesetzt wird). Bei eigenen, kleineren Videodateien bietet es sich auch an, diese über Standard HTML-Skripte direkt lokal auf der Webseite einzubinden, so dass gar kein Drittanbieter notwendig wird. Alternativ kann auf der Webseite einfach ein Vorschaubild mit Link auf die Drittanbieter-Videoplattform eingesetzt werden. Die Weiterleitung auf die Drittwebsite sollte **deutlich** sichtbar sein!

Ist die Übermittlung grundsätzlich zulässig, sollte auch daran gedacht werden, mit dem Drittanbieter einen **Auftragsverarbeitungsvertrag** zu schließen.

11. Verschlüsselte Übertragung einrichten

Nach der DSGVO müssen Verantwortliche dafür sorgen, dass die Verarbeitung personenbezogenes Daten so erfolgt, dass ihre Sicherheit und Vertraulichkeit hinreichend gewährleistet ist.

Dazu gehört bei einer Webseite auch, sicherzustellen, dass Unbefugte keinen Zugang zu Daten bei der elektronischen Übertragung von Daten zwischen Computer und dem Server haben. Eine Datenübertragung findet immer dann statt, wenn eine Webseite aufgerufen wird. Wichtig sind hier vor allem die Fälle, wo Kontakt-, Bestell- oder Anmelde-/Registrierungsformulare online durch den Seitenbesucher ausgefüllt und abgesandt werden.

Fehlt eine hinreichende Verschlüsselung der Datenübertragung, besteht die Gefahr, dass sich Betrüger oder Hacker Zugang zu den Daten verschaffen. Nehmen wir einen Online-Shop als Beispiel, können dies unter anderem hochsensible Bezahldaten sein. Mit diesen können Betrüger dann problemlos weiter im Netz einkaufen – auf Kosten anderer.

In solchen Fällen bietet es sich an, auf der Webseite eine **Verschlüsselung der Übertragung** einzurichten, damit die abgeschickten Daten nicht frei zugänglich durch das Internet reisen. Eine solche Verschlüsselung kann mit einem sogenannten **Secure Socket Layer (SSL) Zertifikat oder mit einem Transport Layer Security (TLS) Zertifikat** realisiert werden. TLS ist hierbei nur eine neuere Version von SSL, die einige Sicherheitslücken in den früheren SSL-Protokollen behebt und leistungsfähiger ist. Im Idealfall sollte nach Möglichkeit die neuste TLS Version eingesetzt werden.

Alle Seiten, die ein solches Zertifikat haben, erkennt man daran, dass in der Adresszeile des Browsers am Anfang nicht nur „http“ (für „HyperText Transfer Protocol“) steht, sondern „**https**“ (das S steht für „Secure“). Ferner wird oft in dieser Browser Adresszeile zusätzlich ein kleines **Schloss-Symbol** angezeigt oder der Beginn der URL grün hinterlegt.

SSL- bzw. TLS Zertifikate bekommt man von zahlreichen Anbietern und werden oft kostenlos oder gegen eine nur geringe Gebühr angeboten. Nahezu all Webseiten-Baukästen unterstützen SSL oder TLS.

Neben der Sicherheit ist ein weiterer Vorteil, dass Webseiten mit SSL-/TLS-Verschlüsselung im Ranking von Suchmaschinen (z. B. Google) besser bewertet werden.

Zudem sollte beachtet werden, dass die Webseite keine veralteten SSL/TLS-Protokolle zulässt.

12. Google Fonts lokal einbinden

Google Fonts (früher Google Web Fonts) wird häufig von Webseitenbetreibern genutzt. Dieses ist ein interaktives Verzeichnis mit über 1400 Schriftarten, welche die Google LLC. zur freien Verwendung für Betreiber von Internetseiten bereitstellt. Allerdings ist die **dynamische Einbindung von Google Fonts**, wo die Schriftarten jeweils immer vom Google Server geladen werden, **datenschutzrechtlich bedenklich**. Sie ist **zudem derzeit mit einem hohen Risiko verbunden, von Betroffenen abgemahnt und auf Schadensersatz verklagt zu werden**.

Am 20. Januar 2022 gab es ein Gerichtsurteil vom Landgericht München I (Az. 3 O 17493/20), bei dem eine Webseitenbetreiberin wegen dem dynamischen Einsatz von Google Fonts neben Unterlassung zu einem Schadensersatz in Höhe von 100 Euro verurteilt wurde. Die Webseitenbetreiberin holte vorab keine Einwilligung von den Webseitenbesuchern ein, sondern stützte die dynamische Einbettung der Google Fonts auf die Rechtsgrundlage des berechtigten Interesses nach Art. 6 Abs. 1 lit. f) DSGVO. Laut dem LG München I ist diese Rechtsgrundlage jedoch nicht verwendbar, da es an einem berechtigten Interesse der Webseitenbetreiberin i. S. d. Art. 6 Abs. 1 f) DSGVO fehle. Nach Auffassung des Gerichts sei dies der Fall, da Google Fonts auch genutzt werden kann, ohne dass beim Aufruf der Webseite eine Verbindung zu einem Google-Server hergestellt wird.

Der Hintergrund dessen ist, dass bei dem dynamischen Laden der Schriftarten von den Google Servern auch die IP-Adresse und weitere Nutzerdaten des jeweiligen Webseitenbesuchers an Google übermittelt werden. Google verwendet diese Informationen für Analysezwecke weiter, indem die aggregierten Nutzerzahlen dafür genutzt werden, um die Beliebtheit einer bestimmten Schriftart zu messen. Google veröffentlicht die Ergebnisse sodann in einer Statistik auf der Google Analyseseite. Diese Übermittlung lässt sich leider technisch nicht unterbinden.

Daher empfehlen wir, Google Schriftarten nur noch lokal auf Websites einzubetten. Dies können Sie umsetzen, indem Sie folgende Schritte ausführen:

1. Feststellung, welche Google Schriftarten genutzt werden
2. Ebendiese Schriftarten vom Google Server (https://fonts.google.com/) herunterladen
3. Heruntergeladene Schriftarten auf dem eigenen Webserver hochladen und die somit nun lokale Einbindung in die Webseite veranlassen
4. Webseitenverbindung zum Google Fonts Server deaktivieren und nochmal prüfen, ob nun alle Schriftarten wirklich nur lokal geladen werden
    - Bei Wordpress Seiten kann man eines von zahlreichen Plug-Ins nutzen, welche das dynamische Laden von Google Fonts deaktivieren. Eine Übersicht findet sich hier: https://de.wordpress.org/plugins/search/disable+google+fonts/
5. Nach jedem Update (auch von Plug-Ins) nachprüfen, ob die gewählten Einstellungen immer noch korrekt sind und Fonts weiterhin lokal geladen werden.

13. Sonstiges (auch an das Impressum denken)

Bei der Impressumspflicht handelt es sich im eigentlichen Sinne nicht um eine rein datenschutzrechtliche Anforderung an Webseiten. Jedoch darf dieses auch nicht vergessen werden. Die Pflicht zur Impressumsangabe erfüllt Zwecke der Transparenz, des Verbraucherschutzes und im Bedarfsfall der Erleichterung der Identitätsfeststellung, z. B. für etwaige Rechtsverfolgungen bei Straftaten und im Streitfalle. Ein Verstoß kann zu einer Abmahnfalle für Unternehmen werden.

Die Impressumspflicht ergibt sich aus § 5 Telemediengesetz (TMG) und richtet sich an Dienstanbieter von Telemedien. Damit sind alle Domaininhaber bzw. Betreiber von (privaten wie auch gewerbsmäßigen) Webseiten, (Werbe-/Newsletter-) E-Mails, Blogs oder Social-Media Profilseiten (z. B. auf Facebook, Twitter, YouTube etc.) oder Verkäuferprofilseiten auf Verkaufsplattformen (wie z. B. Amazon) gemeint. Kein Telemediendienstanbieter ist ein Betreiber reiner Datenübertragungsanlagen, wie zum Beispiel VoIP für Telefonie.
Generell kann man sich merken, dass nahezu alle Angebote im Internet Telemedien sind und alle geschäftsmäßigen Betreiber der Impressumspflicht unterfallen.

Diese müssen dann nach § 5 TMG ganz bestimmte Informationspflichten erfüllen. Die Rechtsnorm zählt hierbei ausdrücklich auf, welche Informationen z. b. für Webseitenbesucher in einem Impressum verfügbar sein müssen. Diese sind:

- Name und aktuelle Anschrift des Dienstanbieters
- Rechtsform und vertretungsberechtigte Personen
- Sofern Angaben über das Kapital der Gesellschaft gemacht werden, das Stamm- oder Grundkapital sowie, wenn nicht alle in Geld zu leistenden Einlagen eingezahlt sind, der Gesamtbetrag der ausstehenden Einlagen
- Mindestens eine E-Mail-Adresse für eine schnelle elektronische Kontaktaufnahme und unmittelbare Kommunikation. Ein Kontaktformular ist nicht ausreichend. Weiterhin sollte neben der E-Mail-Adresse eine weitere Kommunikationsmöglichkeit angegeben sein (dies ist oft die Postadresse).
- Wenn eine Umsatzsteueridentifikationsnummer nach § 27a Umsatzsteuergesetz oder eine Wirtschafts-Identifikationsnummer nach § 139c Abgabenordnung vorhanden ist, die Angabe dieser Nummer
- Online-Händler müssen seit dem 09.01.2016 auf die EU-Plattform zur Online-Streitbeilegung verlinken. Stellen Sie also nachfolgenden Text mitsamt anklickbarem Link auf die Plattform direkt unterhalb Ihrer Impressumsangaben dar (ohne die Anführungszeichen):
    - „Plattform der EU-Kommission zur Online-Streitbeilegung: www.ec.europa.eu/consumers/odr“
    - Nach jüngster Rechtsprechung muss der Teil der Information "www.ec.europa.eu/consumers/odr" als anklickbarer Hyperlink ausgestaltet sein. Eine bloße Verweisung unter Nennung des URL der Plattform reicht nicht!

- Je nach Unternehmensform sind ggf. weitere Informationen notwendig, wie z.B.:
  - Zuständige Aufsichtsbehörden
  - Das jeweils zuständige Handels-, Vereins-, Partnerschafts- oder Genossenschaftsregister mit der eingetragenen Registernummer
  - Inhaltlich Verantwortlicher, z. B. bei Anbietern, die journalistisch-redaktionelle Angebote bereithalten nach § 18 Abs. 2 Medienstaatsvertrag.

Grundsätzlich sollte das Impressum von jedem Bereich bzw. jeder Unterseite der Webseite aus unmittelbar erreichbar, leicht erkennbar und verfügbar sein. Daher bietet es sich an, das Impressum stets im Seitenmenü bzw. in der Fußzeile der Webseite zu verlinken. Eine Zusammenführung des Impressums mit dem Menüpunkt „Kontakt“ ist zulässig, eine eigene Bezeichnung als „Impressum“ bietet sich jedoch wegen der Unmissverständlichkeit an.