Die DSGVO 2018

Auswirkungen auf Ihre Website und Ihre Praxis

Liebe Frau Kollegin, lieber Herr Kollege,

am 25. Mai 2018 tritt EU-weit die neue DSGVO in Kraft. Sie verlangt nicht nur umfangreiche Änderungen auf Ihrer Website, sondern auch in Ihrer Praxis. Verstöße gegen die DSGVO können mit empfindlichen Bußgeldern geahndet werden. ***Nehmen Sie sich deshalb in Ihrem eigenen Interesse die Zeit, die folgenden Informationen zu lesen und dann umgehend zu handeln.***

Die Neuregelungen für Websites im Überblick:

- Jede Website, die ein Kontakt-Formular enthält, benötigt künftig ein sog. **SSL-Zertifikat**
- Die **Datenschutz-Erklärung (DSE)** muss wesentlich mehr Informationen für die Besucher als bisher beinhalten und allgemeinverständlich formuliert sein
- Wenn die Praxis einen **Datenschutzbeauftragten** benötigt (s.u.), muss dieser in der DSE genannt werden
- Im **Impressum** müssen zusätzliche Angaben zu den berufsrechtlichen Regelungen, zur Online-Streitbeilegung und ggf. zum Datenschutzbeauftragten gemacht werden
- **Kontakt-Formulare** sind datenschutzrechtlich nicht sicher und müssen durch die Angabe der Praxis-E-Mailadresse oder durch sichere Alternativen ersetzt werden
- Die **Statistik-Funktion der Website** muss deaktiviert werden, wenn der Website-Betreiber keine eigene Google Analytics-Tracking-ID besitzt und keinen Auftragsverarbeitungs-Vertrag mit Google abgeschlossen hat
- **Facebook Like- und Share-Buttons** sind nicht mehr erlaubt
- **Jameda-Siegel** könnten ein datenschutzrechtliches Problem sein
- und Einiges mehr (s.u.)

Höhere Strafen bei Verstößen

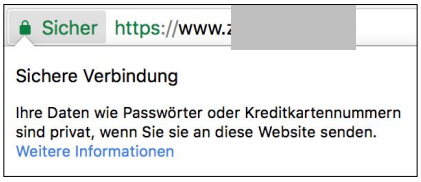
Verstöße gegen die DSGVO können von den Landesdatenschutz-Behörden mit **Strafen in Höhe von bis zu vier Prozent des Vorjahresumsatzes** geahndet werden. Bei einem durchschnittlichen Jahresumsatz von ca. 400.000 € wären das etwa 16.000 €. Zusätzlich können Verstöße kostenpflichtig abgemahnt werden.

Für die „Abmahn-Industrie", bestehend aus einer degenerierten Abart von „Rechtsanwälten" und manchmal auch missgünstigen „Kollegen", ist die neue DSGVO ein gefundenes Fressen.

Angesichts des deutlich gestiegenen Risikos für Geldbußen und Abmahnungen sollten Sie darauf hinarbeiten, dass Ihre Website möglichst bald DSGVO-konform ist!

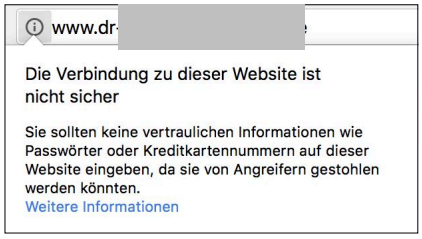
SSL-Zertifikat

SSL steht für „*Secure Sockets Layer*" und bedeutet, dass Daten, die über ein Kontakt-Formular (z.B. Patienten-Daten) **kryptografisch verschlüsselt und für andere nicht einsehbar** übermittelt werden.



Website mit SSL-Zertifikat: Erkennbar am „https" und am Schloss-Symbol

Unabhängig davon fordert Google schon seit Langem ein SSL-Zertifikat für jede Website und begünstigt zertifizierte Websites in den Suchergebnissen. Die DSGVO macht SSL-Zertifikate dann zur **Pflicht, wenn die Website ein Kontakt-Formular hat.**



Website ohne SSL-Zertifikat

Wir empfehlen zwar aus datenschutzrechtlichen Gründen, **keine Kontakt-Formulare** auf Websites zu verwenden, sondern nur die Praxis-E-Mailadresse anzugeben (s.u.). Wegen des besseren Google-Rankings sollte die Website aber ein SSL-Zertifikat besitzen.

Wie können Sie nachprüfen, ob Ihre Website ein solches hat? Wenn links von der Browserzeile (im Bildschirm oben links) ein kleines **Schloss-Symbol** zu sehen ist und „**https**" Ihrer Domain vorangestellt ist, ist Ihre Website **sicher** (siehe obere Abbildung rechts) und Sie haben in dieser Hinsicht keinen Handlungsbedarf.

Wenn nur ein kleines **„i"-Symbol** zu sehen ist und evt. nur „**http**" ihrer Domain vorangestellt ist (siehe untere Abbildung rechts), ist Ihre Website **nicht sicher.** Falls Ihre Website ein Kontakt-Formular enthält, müssen Sie Ihren Webdesigner bitten, umgehend ein SSL-Zertifikat einzurichten. Das kann mit Kosten von ca. 50 - 80 Euro pro Jahr verbunden sein.

Info für Kunden von zahnarzterfolg.de:

Alle von uns gestalteten Websites haben schon seit Jahren und ohne Zusatzkosten ein SSL-Zertifikat. Wenn Sie also eine Website von uns haben, brauchen Sie in dieser Hinsicht nichts zu unternehmen.

Wenn Sie Ihre Praxis-Website selbst gestaltet haben, können und sollten Sie das SSL-Zertifikat bei Ihrem Web-Host (Provider) selbst einrichten.

Erweiterte Datenschutzerklärung (DSE)

Die DSE fällt künftig wesentlich umfangreicher aus und muss anders als bisher allgemeinverständlich formuliert sein. Sie muss Website-Besucher, Patienten, Mitarbeiter und Bewerber nicht nur umfangreich über die Verwendung ihrer Daten informieren. Sie muss ihnen u.a. auch die Möglichkeit einräumen

- ihre bei Ihnen gespeicherten **Daten einzusehen**
- die **Löschung zu verlangen** (sofern dieser nicht gesetzliche Aufbewahrungsfristen entgegenstehen)
- und die **Daten an sie selbst oder Dritte übertragen** zu lassen

Ihre Website-Besucher müssen außerdem die Möglichkeit haben, mit einem Mausklick die Erfassung ihres Besucherverhaltens durch *Google Analytics* oder andere Analyse-Programme zu statistischen Zwecken zu blockieren, falls Ihre Website die Statistik-Funktion nutzt.

Zusätzlich fordert die DSGVO, dass bei *Google Analytics* die sog. ***IP-Anonymisierung*** aktiviert ist, damit die Analyse-Daten keiner konkreten Person zugeordnet werden können.

Wenn in die Website sog. **Widgets** bzw. **Plugins** (kleine Programmschnipsel) fremder Anbieter eingebettet sind, muss in der DSE darauf hingewiesen und über die Verwendung der Daten durch diese Anbieter informiert werden. Dazu gehören unter anderem eingebettete

- Maps (**Karten**) von Google und anderen Anbietern
- Fonts (**Schriftarten**) von Google und anderen Anbietern
- **Videos** von YouTube und anderen Anbietern
- **Analyse (Statistik) Tools** von Google und anderen Anbietern
- **Like- und Share-Buttons** von Facebook und anderen Anbietern (s.u.)
- **Empfehlungs-Buttons** von Jameda und anderen Anbietern (s.u.)

Info für Kunden von zahnarzterfolg.de:

Wir haben mit ***eRecht24*** einen Agentur-Vertrag abgeschlossen. Dieser ermöglicht es uns, die Texte für die Datenschutzerklärung, das Impressum, den Haftungs-Ausschluss (Disclaimer) und weitere geforderte Texte für unsere Kunden dort generieren zu lassen und in die Kunden-Websites einzufügen. Zusätzlich dürfen wir mit ***eRecht24-Siegeln*** in den Websites unserer Kunden dokumentieren, dass die Inhalte rechtskonform sind (s.u.).

Wir werden alle unsere Kunden-Websites vor Inkrafttreten der DSGVO auf die neuen Anforderungen umstellen, sofern Sie uns den Auftrag dafür erteilen.

Alle unsere neu gestalteten Websites erfüllen von vornherein die Anforderungen der DSGVO.

Diese Siegel dürfen nur Vertragspartner von eRecht24 auf den Websites ihrer Kunden verwenden. zahnarzterfolg.de gehört dazu.

Ergänzungen im Impressum

Neben den bereits bisher geforderten Angaben im Impressum sollten Sie darauf achten, dass künftig die *richtige* Zahnärztekammer und die *richtigen* Aufsichtsbehörden angegeben sind. I.d.R. sind das die **Landes**-Zahnärztekammern und (neben anderen) die **Landes**-KZVen und nicht, wie auf vielen Kollegen-Websites zu sehen, die Bezirks-Verbände.

In Bayern sind die **Regierungen von Oberbayern und Unterfranken** - abhängig vom Standort der Praxis - und nicht die KZVen die Aufsichtsbehörden! Außerdem hat sich in Bayern die Adresse der Landeszahnärztekammer geändert, die deshalb auch im Impressum bayerischer Kollegen-Websites geändert werden muss.

Das Impressum muss künftig einen **Link auf die berufsrechtlichen Regelungen** enthalten, die üblicherweise auf einer entsprechenden Seite der jeweiligen Landeszahnärztekammer aufgeführt werden.

Info für Kunden von zahnarzterfolg.de:

Wir werden das Impressum aller unserer Kunden-Websites vor Inkrafttreten der DSGVO auf die neuen Anforderungen umstellen, sofern Sie uns den Auftrag dafür erteilen.

Bei **bayerischen Kollegen** aktualisieren wir (sofern nicht bereits geschehen) die Aufsichtsbehörde und die Adresse der Bayerischen Landeszahnärztekammer.

Wenn die Praxis einen **Datenschutzbeauftragten** benötigt, muss dessen E-Mailadresse im Impressum angegeben werden. Falls ein Praxis-Mitarbeiter zum Datenschutzbeauftragten ernannt wird, benötigt dieser eine **eigene** E-Mailadresse!

Zusätzlich muss ein **Link zur Plattform für Online-Streitbeilegung der Europäischen Kommission** im Impressum aufgeführt werden und angegeben werden, ob die Praxis bereit oder verpflichtet ist, an **Streitbeilegungsverfahren** vor Verbraucherschlichtungsstellen teilzunehmen. (Sorry für das Bürokraten-Deutsch, aber so ist es nun einmal...)

Haftungsausschluss (Disclaimer)

Unterhalb des Impressums sollte der sog. Disclaimer aufgeführt werden, der die Praxis von verschiedenen Haftungsansprüchen freistellen soll. Dazu gehören z.B. die Inhalte von anderen Websites, auf welche die Praxis-Website verlinkt.

Datenschutz-Risiko Kontakt-Formulare

Die üblichen Kontakt-Formulare auf Websites sind datenschutzrechtlich nicht sicher und dürfen nicht mehr verwendet werden. Auch wenn eine Website ein SSL-Zertifikat hat und Daten verschlüsselt übertragen werden, werden die in das Kontakt-Formular eingetragenen Daten als reiner Text unverschlüsselt per E-Mail übertragen: Vom Kontakt-Formular an den Web-Host, von dort an den E-Mail-Provider und von diesem an den Empfänger (die Praxis).

Auf allen drei „Strecken" kann die Sicherheit der Daten nicht garantiert werden. Juristisch gesehen handelt es sich dabei um eine **„Datenschutz-Panne"**, **die an die Datenschutz-Behörden gemeldet werden müsste!**

Aus diesem Grund empfehlen wir, zum gegenwärtigen Zeitpunkt **keine Kontakt-Formulare** auf der Website zu verwenden, sondern statt dessen **nur die Praxis-E-Mailadresse** anzugeben.

Wenn ein Website-Besucher der Praxis eine Mail senden möchte, muss er (auf eigenes Risiko und unabhängig von Ihrer Praxis-Website und damit datenschutzrechtlich unbedenklich für Sie) sein persönliches E-Mail-Programm aufrufen und über dieses versenden.

Info für Kunden von zahnarzterfolg.de:

Wir werden im Rahmen der DSGVO-Aktualisierung Ihrer Website(s) alle Kontakt-Formulare durch die einfache Angabe Ihrer Praxis-E-Mailadresse ersetzen.

Es gibt eine datenschutzkonforme Alternative zu den E-Mail-basierten Kontakt-Formularen, die allerdings einen höheren Einrichtungs-Aufwand erfordert und zusätzliche Kosten verursacht.

Wir werden Ihnen diese Alternative später anbieten, wenn wir alle von uns erstellten Websites in Bezug auf die DSGVO aktualisiert haben.

Statistik-Funktion der Website

Damit eine Website Statistiken über die Besucheranzahl, Seitenaufrufe und weitere Daten liefern kann, wird üblicherweise ***Google-Analytics*** eingesetzt. Dafür muss für die Website eine sog. Tracking-ID von Google verwendet werden. Die meisten Web-Hosts verwenden dafür ihre eigene Tracking-ID für alle Kunden-Websites. Das ist künftig nicht mehr erlaubt!

Wenn Sie künftig die Statistik-Funktion Ihrer Website nutzen möchten, müssen Sie bei Google **Ihre persönliche Tracking-ID** generieren und in Ihre Website(s) einfügen lassen. Außerdem müssen Sie mit Google einen sog. **Auftragsverarbeitungs-Vertrag** abschließen, den Sie im Falle einer Überprüfung vorlegen müssten. Solange beide nicht vorliegen, empfehlen wir Ihnen, die Statistik-Funktion Ihrer Website deaktivieren zu lassen.

Info für Kunden von zahnarzterfolg.de:

Wir werden im Rahmen der DSGVO-Aktualisierung Ihrer Website(s) die Statistik-Funktion deaktivieren.

Falls Sie Statistiken über Ihre Website erheben wollen, wenden Sie sich bitte zu einem späteren Zeitpunkt (ab Juni 2018) an uns.

Facebook Like-Buttons

Wenn solche Buttons auf einer Website vorhanden sind, können Besucher durch Anklicken die Inhalte der Website „liken“ (also positiv bewerten) oder mit anderen Nutzern teilen. Hinter all dem steckt ein handfestes datenschutzrechtliches Problem:

Technisch gesehen sind solche Buttons kurze Teile von Programmier-Code (Widgets), die von Facebook (oder auch anderen Anbietern) stammen. Sobald jemand eine Website mit solchen Widgets besucht, werden im Hintergrund automatisch Informationen über den Besucher via (Praxis-) Website auf Facebook bzw. andere Anbieter übertragen. Der Besucher bekommt davon nichts mit und kann das auch nicht beeinflussen.

Deshalb hat das Oberlandesgericht Düsseldorf am 9. März 2016 solche Like-Buttons in Deutschland verboten. Aus den o.g. Gründen sind sie auch nach der neuen DSGVO künftig EU-weit nicht mehr erlaubt.

Info für Kunden von zahnarzterfolg.de:

Wir verwenden schon seit Jahren keine Like-Buttons auf den von uns gestalteten Websites.

Statt dessen setzen wir sog. **Share-Buttons** und **einfache Links** zu Facebook und anderen Social Media-Portalen wie Twitter oder Google Plus. Diese sind datenschutzrechtlich unbedenklich, weil sie erst dann eine Verbindung zu den SM-Portalen herstellen, wenn der Besucher auf die Links klickt.

Falls Sie solche Like-Buttons auf Ihrer Praxis-Website verwenden, empfehlen wir Ihnen, diese umgehend löschen zu lassen und durch sog. **Share-Buttons oder einfache Links** auf die Social Media-Portale bzw. zu Ihren Profilen dort zu ersetzen. Solche Buttons und Links stellen erst dann eine Verbindung zu ihren Ziel-Websites her, wenn sie angeklickt werden und sind deshalb datenschutzrechtlich unbedenklich.

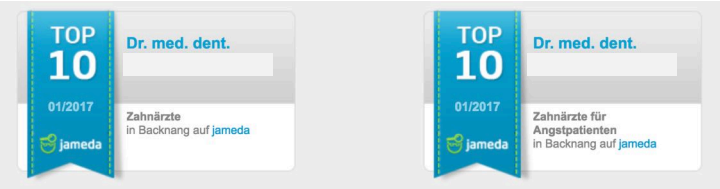
Abbildungen links und Mitte:

Beispiele für Share-Buttons auf Kollegen-Websites, die nicht mehr erlaubt sind.

Share-Buttons und Symbole mit einfachen Links zu den SM-Portalen, die erst durch Anklicken eine Verbindung herstellen, sind datenschutzrechtlich unbedenklich.

Jameda-Siegel

Jamdea-Siegel sind ebenfalls sog. Widgets, also Programmier-Code von Jameda, der in die Praxis-Website eingebettet wird.



Jameda-Siegel (Widgets) auf einer Praxis-Website: Datenschutzrechtlich fraglich

Wir konnten bisher noch nicht klären, ob über solche Siegel (wie z.B. bei Facebook Share-Buttons) ein sofortiger und automatischer Datenaustausch zwischen Website-Besucher und Jameda stattfindet. Wenn dem so sein sollte, müssten auch solche Buttons von Praxis-Websites entfernt werden. Wir werden das noch klären und unsere Kunden und Interessenten von zahnarzterfolg.de per E-Mail informieren.

Die vorläufig sicherere Vorgehensweise wäre, die Siegel durch einfache Links zum Jameda-Profil der Praxis zu ersetzen.

Datenschutzbeauftragter (DSB): Ja oder Nein?

Wer benötigt einen Datenschutzbeauftragten?

Alle Praxen (Einzelpraxen, Sozietäten), in denen regelmäßig zehn und mehr Personen (Vollzeit- und Teilzeitkräfte, Azubis) mit der Verarbeitung personenbezogener Daten (Leistungserfassung, Abrechnung, Terminverwaltung, Recall, Praxislabor) beschäftigt sind. Nicht mitgezählt werden Mitarbeiter, die nicht mit der Bearbeitung von Daten befasst sind (z.B. die Raumpflegerin). Ob der Praxisinhaber mitgezählt werden muss, ist zum gegenwärtigen Stand (2. Mai 2018) noch offen.

Welche Funktion hat der DSB?

Der Datenschutzbeauftragte ist der Praxisleitung direkt unterstellt, in der Wahrnehmung seiner gesetzlichen Aufgaben aber nicht weisungsgebunden. Er überwacht die Datenverarbeitungsprozesse in der Praxis, unterrichtet und berät die Praxisleitung und wirkt auf die Einhaltung des Datenschutzrechts hin.

Zudem soll er die an den Verarbeitungsvorgängen beteiligten Zahnärzte und Mitarbeiter sensibilisieren und schulen. Gibt es eine Beschwerde, ist der Datenschutzbeauftragte die erste Anlaufstelle für die Datenschutzbehörde (Quelle: Merkblatt Datenschutz BZÄK).

Wer kann zum DSB berufen werden?

Grundsätzlich benötigt ein DSB juristische und datentechnische Sachkunde. Wegen eines möglichen Interessenkonflikts können der Praxisinhaber und der IT-Administrator der Praxis **nicht** als DSB

fungieren, da sie sich selbst kontrollieren müssten. Wegen dieses Interessenkonflikts können auch wir von zahnarzterfolg.de als Website-Administratoren nicht als DSB fungieren.

Zum DSB können deshalb nur ausgewählte Mitarbeiter (angestellte Zahnärzte oder zahnmedizinische Assistenzberufe), Lebenspartner oder externe Kräfte berufen werden. Wenn Praxismitarbeiter zum DSB berufen werden, haben diese einen arbeitsrechtlichen Sonderstatus und genießen gleichen Kündigungsschutz wie Betriebsräte!

In den meisten Fällen wird es praktikabel sein, auf externe Kräfte zurückzugreifen. Einen Link zur Website des **Berufsverbandes der Datenschutzbeauftragten Deutschlands (BvD) e.V.** finden Sie auf unserer Website **www.zahnarzterfolg.de/dsgvo**. Beim BvD haben Sie ein umfangreiches Verzeichnis von Datenschutzbeauftragten zur Auswahl.

Bezugsquelle:
https://www.spitta.de/shop.html

Wie kann man Mitarbeiter zum DSB weiterbilden ?

Entweder durch eine i.d.R. mehrtägige Fortbildung mit Zertifizierung an einer externen Institution (Bei Google nach "Ausbildung Datenschutzbeauftragter" suchen) oder autodidaktisch mit entsprechenden Lehrmitteln.

Der Spitta-Verlag hat dazu ein neues Loseblattwerk herausgebracht, das nicht nur als Lehrmittel dient, sondern auch Checklisten für die Datenschutz-Dokumentation und Datenschutz-Folgenabschätzung (s.u.) enthält.

DSB auf der Praxiswebsite aufführen!

Wenn Ihre Praxis einen DSB benötigt, muss dessen E-Mailadresse in der Datenschutz-Erklärung und im Impressum Ihrer Website aufgeführt werden. Wenn ein Praxismitarbeiter als DSB fungiert, benötigt er eine **eigene E-Mailadresse**, z.B. *datenschutz@zahnarzt-musterstadt.de.* Für ihn darf nicht die E-Mailadresse der Praxis verwendet werden.

Datenschutzbeauftragten an Behörde melden!

Sie müssen Ihren Datenschutzbeauftragten auch mit Namen und Kontaktdaten (einschließlich E-Mailadresse) an die zuständige Landesdatenschutzbehörde melden.

Umsetzung der DSGVO innerhalb Ihrer Praxis

Was Ihre **Website** anbelangt, können wir unseren Kunden (oder der Webdesigner Ihrer Praxis-Website) Ihnen alle Arbeit mit der Umsetzung der DSGVO abnehmen, was Ihnen schon einmal sehr viel Zeit spart.

Bei der Umsetzung in Ihrer **Praxis** können und dürfen wir Ihnen leider nicht helfen. Und da wird es noch einmal richtig heftig: Sie müssen **umfangreiche Dokumentationen** anlegen für

- die verschiedenen Datenverarbeitungsprozesse innerhalb Ihrer Praxis
- ergriffene Datenschutzmaßnahmen
- Datenschutz-Schwachstellen-Analysen
- und Einiges mehr

Bitte beachten Sie: Das alles gilt nicht nur für die Daten Ihrer Patienten, sondern auch für Daten von Mitarbeitern und BewerberInnen.

Merkblatt

„Das neue Datenschutzrecht“ der Bundeszahnärztekammer

Download:

www.zahnarzterfolg.de/dsgvo

Erste Details finden Sie im **Datenschutz-Merkblatt der BZÄK**, das Sie sich von unserer Website **www.zahnarzterfolg.de/dsgvo** herunterladen können. Für Checklisten und Mustervorlagen verweisen wir noch einmal auf den Spitta-Leitfaden Datenschutz.

Info für die Website-Kunden von zahnarzterfolg.de

Wir aktualisieren die Websites, die wir für Sie oder gemeinsam mit Ihnen im Workshop erstellt haben, nach den neuen Anforderungen der DSGVO, wenn Sie uns rechtzeitig Ihren Auftrag dazu erteilen. **Mehr Informationen dazu und das Auftragsformular finden Sie auf**

www.zahnarzterfolg.de/dsgvo

Verantwortlich für den Inhalt

Dr. Hartmut Sauer

Weithartstraße 6

88512 Mengen

Tel. 0172 88 55 470

Mail: dr.h.sauer@gmail.com

www.zahnarzterfolg.de

Stand: April 2018