Europäische Datenschutzverordnung praktische Tipps für Webseiten – nicht nur im Bereich der Medizin

Am 25. Mai 2018 tritt die europaweit gültige Datenschutzgrundverordnung (kurz DSGVO) in Kraft. Sie ersetzt zukünftig die bislang geltende EU-Datenschutzrichtlinie aus dem Jahr 1995. Die Datenschutzverordnung gilt für alle Firmen, auch für Praxen und Kliniken unabhängig vom Firmensitz, von ihrer Größe, wenn sie Geschäfte mit EU-Bürgern machen wollen.

Die Datenschutzverordnung ist vor allem deshalb in aller Munde, weil sie die Strafen bei Verstoß gegen die Verordnung empfindlich erhöhen. Bis zu 20 Mio. Euro Bußgelder sind nach dem Gesetz möglich.

Die zahlreichen Änderungen, die die DSGVO mit sich bringt, treffen jeden Unternehmer und Webseitenbetreiber: Webstatistiken, Kundendaten, Newsletter, Werbung auf Facebook, die eigene Datenschutzerklärung, vieles ändert sich durch die Neuregelungen. **Es gibt in fast allen Bereichen des Datenschutzrechts umfangreiche Neuregelungen. Einige sind relativ einfach umzusetzen, andere sind sehr komplex.**

Unser DSGVO-Special – das wir als eRecht24 Agenturpartner in Zusammenarbeit mit eRecht24 für Sie zur Verfügung stellen – hilft Ihnen dabei, einen Überblick über die Anforderungen der DSGVO zu erhalten und zeigt Ihnen, wie Sie diese einfach und schnell für Ihre Webseite umzusetzen.

Gern unterstützen wir Sie in der DSGVO-konformen Umsetzung Ihrer Webseite. Sprechen Sie uns an: Tel. 07150-9789000 oder schmietainski@altamedinet.de.

Änderungen auf Ihrer Webseite

Auf Ihrer Webseite sind drei Bereiche betroffen:

- Aktualisierung Ihrer Datenschutzerklärung
- Besonderheiten beim Einbinden von Google-Analytics und anderen Statistiken
- Gesicherte Datenübertragung und Hinweis auf die Verarbeitung der Daten, wann immer Kundendaten erfasst werden

Schon seit 2016 benötigte eine Webseite einen Punkt „Datenschutz“, der getrennt vom Impressum von jeder Seite der Webseite erreichbar sein musste. Wir hatten seinerzeit bereits dazu informiert.

Eine DSGVO-konforme Datenschutzerklärung bedeutet:

- Einfache und verständliche Sprache
- ggf. eine vorgeschaltete, allgemein-zusammenfassende Erklärung
- Kontaktdaten des Seitenbetreibers
- Datenschutzbeauftragter mit Kontaktdaten, wenn vorhanden
- Die Rechtsgrundlage der jeweiligen Datenerhebung/Verarbeitung (gesetzliche Regelung oder Einwilligung) muss konkret benannt werden

Die folgenden Punkte muss eine Datenschutzerklärung nach DSGVO mindestens enthalten:

- Nennung aller Datenverarbeitungsvorgänge auf der Webseite
- Wie wird mit Kunden- / Bestelldaten umgegangen
- Welche Statistiktools, Cookies, Social Media oder datenverarbeitende Erweiterungen werden verwendet
- Gibt es einen Newsletter, wurden Verträge zur Auftragsdatenverarbeitung mit den Dienstleistern abgeschlossen
- Dauer der Speicherung der Daten, Löschungsfristen
- Information über das Recht des Besuchers bezüglich Auskunft, Berichtigung, Löschung, Widerspruch seiner Daten
- Hinweis auf das Recht auf Datenherausgabe und Übertragbarkeit

Ihr Impressum kann bleiben, wie es ist, hier sind keine Änderungen notwendig.

Die bereits auf vielen Webseiten am oberen oder unteren Bildschirmrand sichtbaren Hinweise auf die Verwendung von Cookies und die Möglichkeit, diese auszuschließen, sind noch nicht verbindlich. Hier werden Regelungen im Rahmen der ePricacy-Verordnung (ePV) ab 2019 erwartet. Wir empfehlen dennoch, diese im Rahmen der jetzt notwendigen Änderungen gleich mit einzufügen.

Besonderheit Google-Analytics und andere Statistiken

Die gute Nachricht: die Verwendung des leistungsfähigen Statistiktools Google Analytics bleibt auch nach der DSGVO wie bisher „erlaubt“, wenn folgende Voraussetzungen erfüllt sind:

- DSGVO-konformen Vertrag zur Auftragsdatenhaltung mit Google abgeschlossen (geht jetzt auch elektronisch)
- IP Anonymisierung aktiviert
- Deutlicher Hinweis in der Datenschutzerklärung der Webseite, dass die erfassten Daten außerhalb des EU-Raumes verarbeitet werden (speziell bei Analytics)
- Opt-out Möglichkeiten für Desktop und Mobil (d.h. der Besucher kann verhindern, dass sein Benutzerverhalten aufgezeichnet wird)

Diese Regelungen gelten auch für alle anderen Statistiktools.

SSL – gesichertes Datenübertragen vorgeschrieben oder nicht,- Verweis auf Verarbeitung der Daten

Schon seit April letzten Jahres ist die gesicherte Datenübertragung vorgeschrieben, wenn auf einer Webseite Bestellungen getätigt werden können oder ein Kontaktformular angeboten wird. **Da SSL inzwischen auch für Google ein Rankingfaktor geworden ist, empfehlen wir inzwischen für jede Webseite, diese mit einer gesicherten Datenübertragung auszustatten, auch, wenn Sie kein Kontaktformular auf der Seite haben.** Je nach Art der übertragenen Daten kommen unterschiedliche Zertifikate zum Einsatz. Für ganz einfache Webseiten können wir seit Anfang dieses Jahres in der Zusammenarbeit mit Mittwald-Medien als Hoster nun auch kostenlose SSL-Zertifikate anbieten. Gern beraten wir Sie zu den verfügbaren Zertifikaten.

Werden Daten des Webseitenbesuchers erfasst – z.B. in Kontaktformularen oder Shops, muss auf die Verarbeitung dieser Daten hingewiesen werden.

Änderungen, wenn Sie Newsletter an Ihre Patienten oder Kunden verschicken

Grundsätzlich gilt: einen Newsletter dürfen Sie nur verschicken, wenn Sie dazu eine Erlaubnis haben und diese im Zweifel auch nachweisen können. In welcher Form diese erteilt wurde, ist nicht vorgeschrieben: handschriftlich in einer Liste auf einer Messe (hier ist die Unterschrift des Abonnenten wichtig), elektronisch auf der Webseite oder mündlich in einem Telefonat. Sie müssen nur nachweisen können, dass Sie die Erlaubnis erhalten haben.

Für die Anmeldung auf der Webseite hat sich in den letzten Jahren das Double Opt-in Prinzip bewährt, in dem der potentielle Newsletter-Empfänger seine Mail nach der Anmeldung bestätigt. Mit der Bestätigung wird verhindert, dass jemand anders die Mailadresse in einen Verteiler einträgt und der Nachweis des Eintragens in der Mailsoftware hinterlegt.

Eine gültige Einwilligung beinhaltet:

- Den Hinweis auf die Möglichkeit des Widerspruchs
- Einen Abmeldelink – auch auf der Anmeldeseite
- Einen Datenschutzlink auf der Anmeldeseite
- Revisionssicherere Speicherung der erteilten Erlaubnis zu Nachweiszwecken (Einwilligung wurde erteilt, wann wurde sie erteilt)
- Hinweis auf evtl. Statistiken und Auswertungen

Die Einwilligung muss dabei „freiwillig" erfolgen: das heißt, eine Kopplung mit anderen Angeboten ist nicht mehr zulässig - z.B. „…. Laden Sie dieses Dokument herunter und abonnieren Sie unseren Newsletter". Hier müssen sich viele Hersteller und Kliniken etwas Neues einfallen lassen, denn das war ein üblicher Weg, um neue Newsletter-Abonnenten zu gewinnen. Ein möglicher Weg könnte sein, die Argumentation herumzudrehen: „Abonnieren Sie unseren Newsletter und erhalten Sie als Dankeschön dieses Dokument". Hier wird sich erst anhand von Musterprozessen zeigen, wie die Gerichte das Gesetz auslegen.

Die Einwilligungen von Nutzern zum Newsletter-Versand, die bereits nach altem Recht wirksam eingeholt wurden (Double Opt-in) gelten grundsätzlich weiter. Es sei denn:

- Das Koppelungsverbot bei alten Einwilligungen wurde nicht beachtet
- Es fehlte das Widerspruchsrecht
- Einwilligungen durch Minderjährige (bis zum Alter von 16 Jahren müssen jetzt die gesetzlichen Vertreter unterschreiben)

Auswirkungen auf die Organisation des Datenschutzes in Ihrem Unternehmen/Ihrer Praxis oder Klinik

Die Datenschutzverordnung schreibt umfassende Maßnahmen vor, um im Unternehmen die Sicherheit der Verarbeitung von Daten zu gewährleisten:

- Die Gewährleistung der Hoheit des Kunden über seine Daten: Recht auf Auskunft, Löschung und Weitergabe
- Erstellung von Verarbeitungsverzeichnissen

- Abschluss von Verträgen zur Auftragsdatenverarbeitung mit allen Dienstleistern, die in Ihrem Auftrag Daten Ihrer Patienten/Kunden verarbeiten
- Umgang mit Mitarbeiterdaten
- Die Benennung eines Datenschutzverantwortlichen

Die Hoheit Ihres Kunden/Patienten über seine Daten

Mit der DSGVO haben Kunden das Recht, zu erfahren, welche Daten über sie gespeichert wurden. Damit er dazu in zumutbarer Zeit und mit vertretbarem Aufwand eine Antwort bekommen kann, müssen ggf. intern Vorkehrungen getroffen werden.

Achtung Löschpflicht - das Recht auf Vergessen-werden

Daten müssen gelöscht werden, wenn:

- der Erhebungszweck weggefallen ist,
- die Einwilligung widerrufen wurde (Newsletter-Abmeldung),
- ein Widerspruch des Nutzers erfolgt („Löschen Sie meine Daten“) und keine gesetzlichen Speicherpflichten entgegenstehen (Steuern und Buchhaltung)

Die Datenschutzverordnung schreibt vor, dass der Besitzer von Daten seine Daten auch zu einem anderen Dienstleister mitnehmen kann. Auch dafür müssen ggf. intern Vorkehrungen getroffen werden.

Verarbeitungsverzeichnisse

Die meisten Firmen benötigen ein Verarbeitungsverzeichnis, wenn Sie Daten „nicht nur gelegentlich verarbeiten“ und vor allem, wenn Sie besondere Datenkategorien verarbeiten – siehe „Besonderheiten in der Medizin“. Es ist aber noch nicht genau geklärt, was dies genau bedeutet. Bis die Voraussetzungen abschließend geklärt sind, sollten Sie im Zweifel ein solches Verzeichnis anlegen.

Beispiele und Aufbau eines solchen Verarbeitungsverzeichnisses finden Sie hier: https://www.bitkom.org/NP-Themen/NP-Vertrauen-Sicherheit/Datenschutz/FirstSpirit-1496129138918170529-LF-Verarbeitungsverzeichnis-online.pdf oder hier: https://lzk-bw.de/zahnaerzte/praxisfuehrung/eu-datenschutz-grundverordnung/kapitel-5-verzeichnis-von-verarbeitungstaetigkeiten/.

Auftragsdatenverarbeitung

Wenn das Erheben und Verarbeiten personenbezogener Daten durch ein „externes“ Unternehmen erfolgt (z.B. Newsletter-Tool, Abrechnungsstelle), muss dies – wie auch im alten Recht – vertraglich geregelt werden.

Beispiele

- Agentur führt Werbemaßnahmen aus
- Externer Newsletter-Anbieter
- Webhoster
- Externe Wartungsverträge

Muster für Ihre ADV-Verträge erhalten Sie z.B. bei Ihrem Dienstleister, bei eRecht24 oder hier: https://lzk-bw.de/zahnaerzte/praxisfuehrung/eu-datenschutz-grundverordnung/kapitel-2-auftragsverarbeitung/.

Wir werden in den nächsten Wochen auf unsere Kunden mit entsprechenden Verträgen zugehen.

Umgang mit Mitarbeiterdaten

Mit der DSGVO kommen auch Neuregelungen zum Mitarbeiterdatenschutz. Die neuen Vorschriften enthalten zahlreiche Pflichten und Obliegenheiten, die Arbeitgeber künftig einhalten müssen.

Es sollen nur die Daten erhoben werden, die „erforderlich" sind. Mitarbeiterdaten sollen nur dann verarbeitet werden, wenn dies für die Entscheidung über die Einstellung eines Bewerbers oder zur Durchführung, Ausübung oder Beendigung eines Arbeitsverhältnisses erforderlich ist.

Erlaubt ist die Verarbeitung auch dann, wenn sie für die Erfüllung gesetzlicher Rechte und Pflichten, eines Tarifvertrags oder einer Betriebs- oder Dienstvereinbarung oder zum Zwecke der Strafverfolgung erforderlich ist. Ob und wann die Erhebung bestimmter Daten tatsächlich erforderlich ist, muss dabei immer anhand des konkreten Einzelfalls bestimmt werden.

Einwilligungen einholen

Wer sich den rechtlichen Unsicherheiten rund um die „Erforderlichkeit" entziehen will, kann freiwillig abgegebene Einwilligungen von seinen Arbeitnehmern einholen. Im Streitfall muss eine behauptete Freiwilligkeit der Einwilligung vom Arbeitgeber allerdings nachgewiesen werden.

Eine wirksame Einwilligung muss bestimmte formale Kriterien erfüllen. So muss sie grundsätzlich in Schriftform erfolgen, d. h. eigenständig unterschrieben werden. Da das allerdings nicht immer praktikabel ist, kann unter besonderen Umständen auch eine elektronische Einwilligung eingeholt werden. Zudem muss der Beschäftigte in geeigneter Form darauf hingewiesen werden, dass die Einwilligung jederzeit widerruflich ist. Schlussendlich müssen durch den Arbeitgeber bestimmte Voraussetzungen für die Widerrufserklärung geschaffen werden.

Datenschutzbeauftragter

Unternehmen, die in der Regel mindestens zehn Personen ständig mit der Verarbeitung personenbezogener Daten beschäftigen oder zu einer Datenschutz-Folgeabschätzung nach Artikel 35 DSGVO verpflichtet sind (Einzelheiten siehe „Besonderheiten in der Medizin"), müssen gegenüber den Behörden einen Datenschutzbeauftragten benennen und die Kontaktdaten zum Datenschutzbeauftragten in der Datenschutzerklärung aufzeigen.

Bei der Besetzung des Datenschutzbeauftragten dürfen keine Interessenkonflikte bestehen. **Daher kann ein Vorstandsmitglied, ein Geschäftsführer oder der Unternehmensinhaber nicht Datenschutzbeauftragter sein.** Diese Personen können im Fall von Konflikten zwischen den Unternehmensinteressen und den datenschutzrechtlichen Vorschriften nicht vermitteln.

Sie können auch einen externen Datenschutzbeauftragten bestellen, um Konflikte zu vermeiden.

Qualifikationen des Datenschutzbeauftragten
Der Datenschutzbeauftragte muss zuverlässig sein. Juristische sowie technische Fachkunde sind ebenfalls unumgänglich für die Position des Datenschutzbeauftragten.
Schulungen/Seminare inkl. Prüfung werden bundesweit angeboten, um die entsprechenden Qualifikationen zu erwerben, z.B. beim TÜV.

Besonderheiten in der Medizin - Datenschutz-Folgenabschätzung

Bestimmte Daten bedürfen eines besonderen Schutzes. Dazu gehören auch Gesundheitsdaten. In diesen Fällen sind Sie verpflichtet, die Folgen der Datenverarbeitung zu bewerten und dies in einer sog. Datenschutz-Folgenabschätzung festzuhalten

Wann und wie eine solche Datenschutz-Folgenabschätzung im Detail durchzuführen ist, können Sie im umfangreichen Whitepaper des „Forum Privatfreiheit“ nachlesen:
https://www.forum-privatheit.de/forum-privatheit-de/publikationen-und-downloads/veroeffentlichungen-des-forums/themenpapiere-white-paper/Forum_Privatheit_White_Paper_Datenschutz-Folgenabschaetzung_2016.pdf

Wichtiger Hinweis:
Dieses Dokument wurde nach besten Wissen und Gewissen erstellt. AltaMediNet darf keine Rechtsberatung durchführen und übernimmt keine Gewähr für die hier getroffenen Aussagen. Wir empfehlen, Details zu Ihrer Webseite mit Ihrem Rechtsanwalt abzuklären.

Quellen:

https://lzk-bw.de/zahnaerzte/praxisfuehrung/eu-datenschutz-grundverordnung/
https://www.gdd.de/gdd-arbeitshilfen/praxishilfen-ds-gvo/praxishilfen-ds-gvo
E-Recht24: DATENSCHUTZ, MARKETING UND DIE DS-GVO, www.e-recht24.de
https://www.e-recht24.de/artikel/abmahnung/10650-wichtige-gesetzesaenderungen-2018.html

Zusammengestellt von Dr. Anke Schmietainski
Stand 16.04.2018