Deutsche Gesellschaft für Alternative Medizin e.V.

Dachverband für humanistische Heilkunst und Gesundheitskultur

Als ob die DSGVO nicht schon schlimm genug ist, gab es, wie ich heute feststellen musste, auch noch technische Probleme im Mail-Versand letzte Woche. Entschuldigung für die doppelte Post an alle, die diese eMail schon letzten Freitag erhalten haben – es ist tatsächlich leichter und geht wesentlich schneller, noch einmal an alle zu versenden als herauszufinden, wer keine bekommen hat. In der Hoffnung auf Verständnis habe ich es nun so getan.

Herzliche Grüße aus dem DGAM Service Büro

Liebe Mitglieder,

Datenschutzgrundverordnung (DSGVO) zum Nächsten – diesmal Informationen rund um den Newsletterversand und die Anforderungen an den Datenschutz Offline, auch da gibt es einige zu beachtende Neuerungen.
Hier die Themen im einzelnen:

1. Datenschutz in der Praxis (inkl. IT-Sicherheit)
2. Einwilligung für Klienten zur Verarbeitung von Daten
3. Rechtssicherer Newsletterversand
4. Nachtrag zur Website für alle, die ein Kontaktformular nutzen

Die Neuerungen im Datenschutz in der Praxis drehen sich übrigens fast ausschließlich um Dokumentation von Prozessen, dem Anlegen von Verzeichnissen: einmal niederschreiben und getrost wieder vergessen ist die gute Nachricht hierzu.

1. Datenschutz in der Praxis

Datenschutzbeauftragter (oder nicht?)
In aller Regel ist nur dann ein Datenschutzbeauftragter zu benennen, wenn *mindestens 10 Personen* ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind – also wohl bei kaum einem zutreffend. Aber Achtung, eine zuständige Person muss dennoch benannt werden, sie muss aber nicht aktiv der zuständigen Datenschutzbehörde genannt werden, nur auf Anfrage.

Gibt es Auftragsdatenverarbeitung von externen Dienstleistern, an die personenbezogene Daten weitergegeben werden?
Falls ja: Die meisten Lohnabrechnungsbüros/Steuerbüros etc. sollten Vertragsmuster bereitliegen haben oder schon an Ihre Auftraggeber verschickt haben – falls (noch) nicht geschehen: einfach mal nachfragen und dann den Vertrag zur Auftragsdatenverarbeitung (neu) schließen. Sollte der externe Dienstleister tatsächlich keine Verträge bereitstellen, hier ein Link zu einer Mustervorlage des hessischen Datenschutzbeauftragten:
https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/Formulierungshilfe-Auftragsverarbeitungsvertrag%20nach%20DSGVO.pdf

Verzeichnis von Verfahrenstätigkeiten
Zunächst einmal ist es wichtig, alle Prozesse, bei denen Daten von Klienten oder Interessenten in irgendeiner Art und Weise verarbeitet werden, zu identifizieren und zu notieren (z.B. Aufnahme von persönlichen Daten in eine Datenbank bei Beginn einer Behandlung, Therapie, Geschäftsbeziehung o.ä.).
Nun müssen diese Prozesse in einem sogenannten ‚Verzeichnis von Verfahrenstätigkeiten' gem. Artikel 30 Abs. 1 DSGVO eingetragen bzw. beschrieben werden.
Ein konkretes Beispiel hierzu könnte so aussehen: Verarbeitungstätigkeit: Kundenverwaltung, Zuständiger: Maxine Musterpraktikerin, Datum der Einführung: 18.05.2018, Zweck der Verarbeitung: Verwaltung der Kunden, Kategorie betroffene Personen: Kunden, Kategorie von personenbezogenen Daten: Namen, Adressen, Erstkontakt, Art der Dienstleistung/Behandlung etc., Kategorie von Empfängern: keine (oder möglicherweise externe Dienstleister (Lohnabrechnung, Steuerberater…), Drittlandtransfer: keine (oder?), Löschfristen: die gesetzlichen Aufbewahrungsfristen angeben, Technische/organisatorische Maßnahmen: siehe IT-Sicherheitskonzept.
Hier ein Link zu einer Mustervorlage des Bayerischen Landesamtes für Datenschutzaufsicht:
https://www.lda.bayern.de/media/dsk_muster_vov_verantwortlicher.pdf
Achtung, auch der ‚Betrieb der Website' ist eine solche Verfahrenstätigkeit, die gerne vergessen wird.

IT-Sicherheitskonzept
Im obigen Verzeichnis von Verfahrenstätigkeiten nehmen wir unter ‚Technische/organisatorische Maßnahmen' darauf Bezug.
Auch hier wird zunächst der/die Verantwortlichen genannt, dann die Maßnahmen. Zum Beispiel:
-Automatische Updates im Betriebssystem, Browsern, Antivirussoftware und sonstiger relevanter Software
-verschlüsselter eMail-Verkehr, ggf. HTTPS-Verschlüsselung der Website (beides heutzutage Standard, sollte aber hier erwähnt werden)
-Standard-Gruppenverwaltung (z.B. in Windows, verschiedene Benutzerkonten)
-regelmäßige Backups (z.B. einmal wöchentlich auf externe Festplatte)
-Papieraktenvernichtung mit Standard-Shredder
-Welche Möglichkeiten zum Datenexport gibt es? (bzgl. des Auskunftsrecht von Kunden/Klienten/Patienten etc. – nach Anfrage hat man 4 Wochen Zeit dafür, aber schön, wenn man auch diesen Prozeß vorher schon geklärt hat)

Datenschutzerklärung zur Aushändigung an Interessenten, Kunden, Klienten, Patienten etc.
Im Grunde enthält die Datenschutzerklärung das Gleiche wie die auf einer Website (siehe letzte Rundmail zum Thema), außer allem, was direkt mit der Website zu tun hat (z.B. Tools, Plugins…), also

eine Beschreibung über Umgang mit personenbezogenen Daten und Aufklärung über die Rechte des Kunden. Einfach die nicht benötigten Passagen aus der ‚Online-Datenschutzerklärung' löschen.

Gibt es Mitarbeiter, Praktikanten etc.?
Wenn das so ist, müssen alle Mitarbeiter, die Kontakt zu personenbezogenen Daten haben, eine Verpflichtung auf die Beachtung datenrechtlicher Vorschriften unterschreiben.
Hier ein Link zu einer Mustervorlage des Bayerischen Landesamtes für Datenschutzaufsicht:
https://www.lda.bayern.de/media/info_verpflichtung_beschaeftigte_dsgvo.pdf

Handelt es sich um eine Praxisgemeinschaft?
Bei einer Praxisgemeinschaft muss sichergestellt werden, dass strikte Datentrennung herrscht und keine Einsicht in personenbezogene Daten von Klienten zwischen den Praxen möglich ist!

Gibt es Videoüberwachung?
Trifft wohl auf die wenigsten zu, aber wer weiß, also hier noch der Hinweis auf eine wichtige Änderung im Bundesdatenschutzgesetz:
Ein Schild muß nun auf diese Videoüberwachung hinweisen, BEVOR die betroffene Person in den Erfassungsbereich der Kamera gerät.

Außerdem auf das Schild gehören die Kontaktdaten des Verantwortlichen.

2. Einwilligung für Klienten zur Datenverarbeitung

Folgendes Musterbeispiel bezieht sich auf einen abzuschließenden Klientenvertrag, er kann natürlich auch abgeändert werden auf die reine Aufnahme von Daten eines Interessenten (zur weiteren Kontaktaufnahme oder Beschickung mit Informationen etc.):

Schriftliche Einwilligung gemäß Datenschutz

Die im Vertrag angegebenen personenbezogenen Daten, insbesondere Name, Anschrift, Telefonnummer, Bankdaten, die allein zum Zwecke der Durchführung des entstehenden Vertragsverhältnisses notwendig und erforderlich sind, werden auf Grundlage gesetzlicher Berechtigungen erhoben.
Für jede darüber hinausgehende Nutzung der personenbezogenen Daten und die Erhebung zusätzlicher Informationen bedarf es regelmäßig der Einwilligung des Betroffenen. Eine solche Einwilligung können Sie im Folgenden Abschnitt freiwillig erteilen.

Einwilligung in die Datennutzung zu weiteren Zwecken
Sind Sie mit den folgenden Nutzungszwecken einverstanden, kreuzen Sie diese bitte entsprechend an. Wollen Sie keine Einwilligung erteilen, lassen Sie die Felder bitte frei.
▢ Ich willige ein, dass mir Petra Praktikerin (Vertragspartner) postalisch Informationen und Angebote zum Zwecke der Werbung übersendet.
▢ Ich willige ein, dass mir Petra Praktikerin (Vertragspartner) per EMail/Telefon/Fax/SMS*Informationen und Angebote zum Zwecke der Werbung übersendet. (* bei Einwilligung bitte Unzutreffendes streichen)

[Ort, Datum]

[Unterschrift des Betroffenen]

Rechte des Betroffenen: Auskunft, Berichtigung, Löschung und Sperrung, Widerspruchsrecht.

Sie sind gemäß § 15 DSGVO jederzeit berechtigt, gegenüber Petra Praktikerin (Vertragspartner) um umfangreiche Auskunftserteilung zu den zu Ihrer Person gespeicherten Daten zu ersuchen.

Die Rechte des Betroffenen können hier auch gerne ausgeschrieben werden (siehe Datenschutzerklärung).

3. Rechtsicherer Newsletterversand

Im Prinzip sollte man vor dem nächsten Newsletterversand in jedem Fall die erneute Einwilligung der Interessenten bzw. Kunden einholen. Es gibt aber tatsächlich eine Ausnahme, die dann greift, wenn alle folgenden Punkte erfüllt sind:

- der Versender die E-Mail-Adresse eines Kunden im Zusammenhang mit dem Verkauf einer Ware oder Dienstleistung erhalten hat,
- er diese Adresse zur Direktwerbung (bspw. E-Mail-Marketing) für eigene ähnliche Waren oder Dienstleistungen verwendet,
- der Kunde der Nutzung seiner E-Mail-Adresse nicht widersprochen hat und
- der Kunde bereits bei Eingabe seiner E-Mail-Adresse und in jedem Newsletter klar und deutlich darauf hingewiesen wird, dass er der Verwendung jederzeit widersprechen kann, ohne dass hierfür andere als die Übermittlungskosten nach den Basistarifen

Wer sich unsicher ist, sollte besser erneut eine Einwilligung einholen.

Wichtig für alle, die einen Button oder ein Eingabefeld für eine eMail-Adresse zur Newsletterbestellung auf der Website haben:

Das einfache eingeben einer eMail-Adresse und das drücken eines Buttons reichen nicht mehr aus! Dadurch soll nur eine Antwort-eMail losgeschickt werden an die angegebene eMail-Adresse, die dann entweder durch eine Antwort oder das anklicken eines gesendeten Links bestätigt wird. Hintergrund hierzu ist schlicht, dass ja jeder auch irgendeine fremde eMail-Adresse angeben könnte, auf die er gar kein Zugriff hat, also daher die Zweitbestätigung (das sogenannte ‚Double-Opt-In'). Am unkompliziertesten ist es hier tatsächlich, um eine kurze Rückantwort per eMail zu bitten zur erneuten Bestätigung bzw. Einwilligung (diese eMails dann natürlich auch speichern).

Und nach wie vor gilt (das war auch schon vor der neuen DSGVO so, sei aber kurz erwähnt, da es wichtig ist):
Der Empfänger muss jederzeit widerrufen, d.h. abbestellen können und auch in jedem Newsletter darauf aufmerksam gemacht werden.

4. Nachtrag zum Datenschutz Online auf der Website

Nur nötig zu lesen, wenn ein sogenanntes Kontaktformular verwendet wird

Zusätzlich zur Beschreibung der Datennutzung in der Datenschutzerklärung (siehe letzte eMail zum Thema), sei hier noch empfohlen, eine Checkbox unter dem Kontaktformular einzurichten, damit der Interessent aktiv bestätigen muss, dass er die Hinweise zum Datenschutz gelesen hat. Einfach den

Ersteller der Website darum bitten, falls es nicht sowieso schon eine solche Checkbox gibt, damit ist man jetzt und vor allem auch zukünftig auf der (Datenschutz)sicheren Seite.

Wir hoffen sehr, nichts vergessen zu haben, können das natürlich nicht garantieren, aber sind sicher, dass bei Einhaltung dessen, was wir verschickt haben, erstmal kein Unheil droht – für alles, was Offline zu passieren hat, gibt es übrigens auch noch sogenannte Bearbeitungfristen. Niemand wird eine Verfahrensbeschreibung in 24 Stunden sehen wollen usw. – wichtige Ausnahme sind hierbei allerdings die Verträge mit Dienstleistern oder Mitarbeitern (siehe oben), die sollten tatsächlich bis zum 25.05. abgeschlossen worden sein.

Ansonsten sind hoffentlich nicht mehr allzu viele Fragen offen, ansonsten am besten per eMail in den nächsten Tagen, da ja Montag ein Feiertag ist und das Büro nicht besetzt sein wird.

Ein schönes langes Wochenende und frohe Pfingsten wünscht Ihr und Euer
DGAM Service Büro

Impressum & Kontakt

Die DGAM Infomail sendet Informationen von Mitgliedern für Mitglieder und Interessierte
Redaktionsteam: Gerhard Tiemeyer, Jörn Hingst
Impressum: ViSP ist Gerhard Tiemeyer.
Anschrift: DGAM Lister Meile 33 D-30161 Hannover.
E-Mail: service@dgam.de , Tel. 0511 - 5349479
Wenn Du keine DGAM Infomail erhalten möchtest - bitte hier klicken: Infomail abbestellen

Die Inhalte dieser Seiten wurden mit größter Sorgfalt erstellt. Für die Richtigkeit, Vollständigkeit und Aktualität der Inhalte können wir jedoch keine Gewähr übernehmen.