Newsletter

Ausgabe Januar 2023

Liebe Leserin, lieber Leser,

nach einem hoffentlich guten Start in das neue Jahr erhalten Sie heute unseren ersten Newsletter für das Jahr 2023.

Unsere Themen und Quellen im Überblick:

- **Datenschutz in der Arztpraxis: Alles Wichtige im Überblick**
  https://www.dr-datenschutz.de/datenschutz-in-der-arztpraxis-alles-wichtige-im-ueberblick/

- **Der Dienstplan – Was darf drinstehen?**
  https://www.datenschutz-notizen.de/der-dienstplan-was-darf-drinstehen-2140366/

- **Mitarbeiter bleiben geheim!**
  https://www.datenschutz-notizen.de/mitarbeiter-bleiben-geheim-4640146/

- **Cookie-Banner bald nicht mehr irreführend?**
- https://www.datenschutzticker.de/2023/01/cookie-banner-bald-nicht-mehr-irrefuehrend/

- **Urteile**

- **weitere interessante Links**

Viel Spaß beim Lesen,

freundliche Grüße

Mario Barthel

➢ Datenschutz in der Arztpraxis: Alles Wichtige im Überblick

Gesundheitsdaten sind sensible Daten, die einen besonderen Schutzbedarf haben. Dies spiegelt sich durch die ärztliche Schweigepflicht und die besondere Bedeutung im Datenschutzrecht wider.

Sie erhalten hier einen Überblick, was besonders zu beachten ist:

1. **Empfang**
   - Diskretionsabstand bei der Anmeldung ist einzuhalten.
   - Für Telefonate empfiehlt sich eine räumliche Trennung zum Warte- und Behandlungsbereich.
   - Ein Zugriff oder Einblick auf Patientendaten darf nicht möglich sein.

2. **Die Verarbeitung von Gesundheitsdaten bedarf einer Rechtsgrundlage**
   - Die Verarbeitung von Gesundheitsdaten durch einen Arzt/eine Ärztin kann in aller Regel auf Art. 9 Abs. 2 lit. h), Abs. 3 DSGVO bzw. Art. 6 Abs. 1 lit. b) DSGVO gestützt werden.
   - Für zusätzliche Leistungen, die nicht unmittelbar mit dem Behandlungsvertrag in Verbindung stehen, bedarf es jedoch einer Einwilligung der Patienten nach Art. 9 Abs. 2 lit. a) DSGVO bzw. nach Art. 6 Abs. 1 lit. a) DSGVO.
   - Rechtsgrundlage für die Datenweitergabe der Arztpraxis an Krankenkassen ist § 284 SGB V.

3. **Online-Terminvereinbarungen**
   - Die Arztpraxis selbst und der Dienstleister sollten die erforderlichen technischen und organisatorischen Maßnahmen treffen, um die Sicherheit der sensiblen Daten gewährleisten zu können.
   - Die Übertragung der Daten muss sicher verschlüsselt sein, damit unbefugte Dritte nicht auf die Informationen zugreifen können, wann ein Patient aus welchen Gründen einen Termin vereinbart.
   - Die Arztpraxis muss einen Auftragsverarbeitungsvertrag mit dem externen Dienstleister (z. B. Doctolib) schließen, wenn die Software nicht rein lokal betrieben wird.

4. **E-Mailversand von sensiblen Daten an den Patienten**
   - Die Arztpraxis muss dafür Sorge tragen, dass unbefugte Dritte keinen Zugriff auf diese Daten erhalten.
   - Die Übermittlung der E-Mails muss verschlüsselt erfolgen.
   - Kann eine sichere Übermittlung nicht gewährleistet werden, sollte von dieser Methode sicherheitshalber Abstand genommen werden. Eine Einwilligung in eine unverschlüsselte Datenübermittlung ist nach Auffassung deutscher Aufsichtsbehörden nur in Einzelfällen und vertretbarem Umfang erlaubt, wenn der Wunsch vom Betroffenen ausgeht.

5. **Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung (DSFA)?**
   - Bei Krankenhäusern und stationären Pflegeeinrichtungen mit einer Vielzahl an Patienten dürfte eine umfangreiche Verarbeitung schnell anzunehmen sein, eine Pflicht zur Durchführung einer DSFA also bestehen.
   - Bei kleinen Arztpraxen, die im erforderlichen und üblichen Umfang Gesundheitsdaten der Patienten verarbeiten, ist ein hohes Risiko daher eher der Ausnahmefall, in der Regel damit eine DSFA nicht durchzuführen.

6. **Braucht jede Arztpraxis einen Datenschutzbeauftragten?**
   - Hier bedarf es einer umfangreichen Verarbeitung sensibler Daten. Wovon bei einem einzelnen Arzt noch nicht ausgegangen werden kann.
   - Sind jedoch in der Regel mindestens 20 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt, ist – auch wie bei jedem Unternehmen – ein Datenschutzbeauftragter zu bestellen.
   - Ansonsten ist es eine Einzelfallfrage. Zudem muss eine Arztpraxis Datenschutzbeauftragten bestellen, wenn Datenverarbeitungsvorgänge vorgenommen werden, die einer DSFA unterliegen.

7. **Datenschutzerklärung**
   - Grundsätzlich hat die Arztpraxis als verantwortliche Stelle ihre Informationspflichten zu erfüllen. Aufsichtsbehörden empfehlen, die Datenschutzhinweise grundsätzlich schriftlich auszuhändigen.
   - Die Information kann auch durch einen Aushang in den Praxisräumen erfolgen, vor Verarbeitung der Patientendaten müssen diese aber auf den Aushang hingewiesen werden und auf Wunsch auch eine schriftliche Kopie erhalten.
   - Hat die Arztpraxis auch eine Website, muss diese ebenfalls eine Datenschutzerklärung enthalten.

Die Praxis sollte nach den Vorgaben der DSGVO gestaltet sein, um die sensiblen Gesundheitsdaten der Patienten zu schützen. Dies wirkt sich positiv auf das Vertrauensverhältnis aus und bewahrt vor möglichen Bußgeldern.

➢ Der Dienstplan – Was darf drinstehen?

Für die Personaleinsatzplanung ist ein Dienstplan häufig unerlässlich. Doch was genau darf hier erfasst werden und worauf ist datenschutzrechtlich zu achten?

Diese Zusammenfassung zeigt auf, was im Dienstplan stehen darf:

- Name bzw. ein Namenskürzel des Mitarbeitenden
- Die Information, wann dessen Dienst beginnt und endet.
- Ein „A“ für Abwesenheit, wobei hier kein Grund für die Abwesenheit angegeben werden darf. Eine Angabe wie „K“= krank oder „U“ = Urlaub ist unzulässig. Zulässig wäre noch die Verwendung des Buchstaben „B“, für Bereitschaft, wenn Mitarbeitende abwesend, aber bei Personalengpässen verfügbar sind und für andere ausgefallene Kollegen einspringen können.
- So wenig Angaben wie möglich – auch wenn hilfreich für die Planung sein kann, den Stundensaldo anzugeben, ist dies nicht erlaubt.

➢ Mitarbeiter bleiben geheim!

Das Auskunftsrecht ist ein wichtiges Betroffenenrecht und wir haben schon mehrfach darüber berichtet. Es umfasst das Recht auf Auskunft über gespeicherte personenbezogene Daten einer Person. Dies umfasst auch Informationen wie z. B. Verarbeitungszwecke, Herkunft der Daten und an welche Empfänger sie übermittelt wurden. In diesem Artikel geht es insbesondere um die Ausübung des Auskunftsrechts beim eigenen Arbeitgeber und die Klärung, ob Mitarbeiter des Verantwortlichen auch als „Empfänger“ anzusehen sind.

In dem bestimmten Fall hatte eine interne Untersuchung für einen Beschäftigten (und auch Kunden) eines finnischen Finanzinstituts zur Kündigung geführt. Er verlangte nun Auskunft über die Identität der Personen, die in diesem Rahmen seine personenbezogenen Daten erhalten haben. Das Finanzinstitut lehnte dies ab, woraufhin der Betroffene Klage beim Verwaltungsgericht Ostfinnlands erhob. Hierbei stellte sich die Frage, ob die in die Untersuchung involvierten Mitarbeiter des Finanzinstituts (Verantwortlichen) als Empfänger zu betrachten sind. Der Generalstaatsanwalt kommt aus folgenden Gründen zu dem Ergebnis, dass die involvierten Mitarbeiter nicht als „Dritte“ zu verstehen sind und auch sonst nicht als Empfänger zu kategorisieren:

- Der Ausdruck „Dritter“ bezeichnet eine „natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, **außer** der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und **den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten**.
- In bestimmten Wirtschaftszweigen stellen Mitarbeiterdaten aus Sicherheitsgründen ein besonders sensibles Datum dar. Beschäftigte im Bankensektor etwa, deren Aufgabe die Verhütung und Bekämpfung von Finanzstraftaten ist, könnten sonst der versuchten Ausübung von Druck oder der Beeinflussung durch Dritte ausgesetzt sein.
- Des Weiteren gilt, dass Betroffene grundsätzlich nur Auskunft bezüglich der eigenen personenbezogenen Daten verlangen können und die Rechte und Freiheiten anderer dadurch nicht beeinträchtigt werden dürfen. Die Identität der Mitarbeiter stellt jedoch aus Sicht des Betroffenen gerade personenbezogene Daten Dritter dar. Informationen über Beschäftigte sind demnach also nicht herauszugeben.

Eine Ausnahme stellt ein Mitarbeiterexzess dar. Hier ignoriert der Beschäftigte vom Verantwortlichen festgelegte Verfahren und verarbeitet eigenmächtig und unrechtmäßig Daten von Kunden oder Beschäftigten. Er handelt dann nicht im Auftrag des Verantwortlichen.

➢ Cookie-Banner bald nicht mehr irreführend?

Als Ergebnis einer Zusammenarbeit der Datenschutzbehörden im Rahmen des EDSA-Ausschusses für Cookie-Banner wurde von dem Arbeitskomitee ein Entwurf für einen Bericht über Cookie-Banner vorgelegt. Hier werden unter Berücksichtigung des rechtlichen Rahmen Mindeststandards für die Bewertung von Cookie-Bannern festgelegt.

Folgende Punkte sind demnach als rechtswidrig anzusehen:

- Fehlende Ablehn-Option auf derselben Ebene wie die Zustimmung
- Bereits angekreuzte Kästchen anstelle einer aktiven Zustimmung
- Eingebettete Textlinks zur Ablehnung
- Links außerhalb des Cookie-Banner zur Verweigerung der Zustimmung
- der Vorwand des berechtigten Interesses an der Installation nicht notwendiger Cookies
- Keine permanente Möglichkeit, die Zustimmung zu widerrufen

Verlangt wird in dem Bericht die Möglichkeit des Nutzers, die Einwilligung bereits auf der ersten Ebene nicht zu erteilen.

➢ Urteile

Bei DSGVO-Auskunft müssen konkrete Empfänger benannt werden

Bei einer normalen Datenschutzerklärung (z.B. auf einer Webseite) reicht es aus, die potenziellen Datenempfänger nach bloßen Kategorien zu benennen, ohne die konkreten Firmen zu erwähnen. Was aber gilt, wenn eine konkrete DSGVO-Auskunft von einem Betroffenen verlangt wird? Reicht es auch hier, lediglich Kategorien zu nennen?

Diese Frage hat der EuGH nun mit einem klaren "Nein" beantwortet. Bei einer individuellen DSGVO-Auskunft müssen grundsätzlich die Empfänger-Adressaten einzeln benannt werden. Eine Kategorien-Nennung ist hier nicht ausreichend.

Urteil des Europäischen Gerichtshofs vom 12. Januar 2023 - Az.: C-154/21

Eingesetzter Cookie-Banner auf Focus.de rechtswidrig

Der in der Vergangenheit eingesetzte Cookie-Banner auf Focus.de war rechtswidrig, da er durch seine Ausgestaltung keine wirksame Einwilligung des Users ermöglichte.

Die Ausgestaltung des Cookie-Banners war wie folgt: Auf der Startseite erschienen die Auswahl *"Akzeptieren"* und *"Einstellungen"*. Bei Anklicken des Buttons *"Akzeptieren"* willigte der User in die umfangreiche Datenverarbeitung und Datenanalyse durch Drittunternehmen ein. Bei Aufruf von "Einstellungen" war dem Nutzer hingegen eine individuelle Einstellung für mehr als 100 Drittanbieter möglich. Zudem waren die Schaltflächen *"Alle akzeptieren"* und *"Auswahl speichern"* optisch hervorgehoben. Die Möglichkeit *"Alle ablehnen"* hingegen war in blasser Schrift in der rechten oberen Ecke des Fensters platziert.

Das LG München I ging bei dieser Ausgestaltung von keiner wirksamen Einwilligung des Nutzers aus und bewertete das Cookie-Banner daher als rechtswidrig.

Urteil des Landgerichts München I vom 29. November 2022 - Az.: 33 O 14766/19

➢ Weitere interessante Links

Neue Richtlinie zur Cybersicherheit veröffentlicht
Kurz nach Weihnachten, am 27. Dezember 2022 wurde eine neue Richtlinie zu „Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union“ veröffentlicht. Ziel dieser neuen Richtlinie ist der „Aufbau von Cybersicherheitskapazitäten“ und die „Eindämmung von Bedrohungen für Netz- und Informationssysteme[n]“.
https://www.datenschutzticker.de/2022/12/neue-richtlinie-zur-cybersicherheit-veroeffentlicht/

Datenschutz bei Online-Bewerbungen
Welche datenschutzrechtlichen Anforderungen hierbei zu beachten, wird in diesem Blogbeitrag dargestellt.
https://www.datenschutz-notizen.de/datenschutz-bei-online-bewerbungen-4239661/

DSGVO Strafen und Bußgelder

Bei Verstößen gegen die DSGVO drohen Unternehmen Bußgelder. Diese werden von den jeweiligen zuständigen Aufsichtsbehörden der Bundesländer verabschiedet. Da sie eine existenzbedrohende Höhe erreichen können, ist es wichtig zu wissen, wann ein Bußgeld droht und wie man dies vermeiden kann.
https://keyed.de/blog/dsgvo-strafen-und-bussgelder/

Die Weitergabe von Daten im Verein nach der DSGVO

Ein Überblick, wann eine Datenweitergabe stattfinden darf und was passiert, wenn diese widerrechtlich erfolgt, erhalten Sie in diesem Artikel.
https://www.dr-datenschutz.de/die-weitergabe-von-daten-im-verein-nach-der-dsgvo/

Praxisleitfäden zur Auftragsverarbeitung

Der Bitkom e.V. („Bitkom“) hat seinen beliebten Muster-Auftragsverarbeitungsvertrag aktualisiert und stellt diesen mit ergänzenden Informationen zum Download bereit.
https://www.bitkom.org/Themen/Praxisleitfaeden-zur-Auftragsverarbeitung

Übersicht der relevanten Aufbewahrungsfristen 2023

Damit Sie einfach und schnell überprüfen können, was datenschutzkonform vernichtet werden kann und was noch nicht, finden Sie hier eine Übersicht aller Dokumentenarten von A-Z mit den jeweils relevanten Aufbewahrungsfristen.
https://www.reisswolf.com/leistungsbereiche/aktenvernichtung-datenvernichtung/aufbewahrungsfristen/

Website rechtssicher erstellen – so geht’s!

Dieser Artikel stellt die wichtigsten Aspekte dar, die aus datenschutzrechtlicher Sicht beim Betreiben einer Website zu beachten sind.
https://www.dr-datenschutz.de/website-rechtssicher-erstellen-so-gehts/

GDD-Praxishilfe DS-GVO - ePrivacy und Datenschutz beim Onlineauftritt

Anlässlich des 17. Europäischen Datenschutztags am 28.01.2023 veröffentlicht die Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V. eine neue Praxishilfe zum aktuellen Thema "ePrivacy und Datenschutz beim Onlineauftritt".
https://www.gdd.de/downloads/praxishilfen/prax-praxishilfen-neustrukturierung/GDDPraxishilfeDSGVOePrivacyundDatenschutzbeimOnlineauftritt.pdf