Datenschutz im Gesundheitswesen

Juni | 2023

Wichtige Datenschutzinformationen für Ihr Unternehmen

CompuSaar

Inhalte | Datenschutzinformationen

Inhaltsverzeichnis

Begrüßung | Ihr Datenschutzbeauftragter vor Ort

Liebe Leserin, lieber Leser,

Informationen, die im Zusammenhang mit der Gesundheit einer Person stehen, zählen aus der Sicht des Datenschutzes zu den besonderen Arten personenbezogener Daten und werden nicht nur in der Datenschutzgrundverordnung (DSGVO) als sehr schützenswert eingestuft – vor allem weil der Verlust oder gar der Missbrauch solch sensibler Informationen, erhebliche Konsequenzen nach sich zieht. Beispielsweise könnte durch eine Veröffentlichung der Daten, Einfluss auf die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse eines Betroffenen genommen werden.

In den letzten Jahren gewinnt die Cyberkriminalität zudem an Bedeutung. Hier werden, beispielsweise durch den Einsatz von Ransomware, u. a. Krankenkassen, Kliniken, Pflegeeinrichtungen und Arztpraxen immer wieder in den Fokus genommen, um an sensible Gesundheitsdaten heranzukommen.

Aber nicht nur für Einrichtungen und Personen, die direkt im Gesundheitswesen tätig sind, ist im Umgang mit Gesundheitsdaten enorme Vorsicht geboten, sondern auch bei jedem verantwortungsbewussten Unternehmen. Auch hier gilt es, alle technischen Möglichkeiten zu nutzen, um ein höchstmögliches Sicherheitsniveau zu garantieren. Zudem sollten regelmäßige Schulungen dafür Sorge tragen, dass das Personal optimal auf alle Gegebenheiten vorbereitet ist, z. B. im Umgang mit riskanten E-Mails. Diese sollten eigenständig erkannt und eliminiert werden.

Um Ihnen einen ersten Überblick zu geben, was Gesundheitsdaten sind, wie man diese am besten schützt und welche Maßnahmen getroffen werden können, um beim Schutz dieser Daten auch alle Mitarbeiterinnen und Mitarbeiter mit einzubeziehen, haben wir uns in dieser Datenschutzzeitung dem Thema „Datenschutz im Gesundheitswesen“ gewidmet.

Sollten Sie darüber hinaus weitere Informationen benötigen oder eine ausführliche Beratung in Anspruch nehmen wollen, stehen wir Ihnen jederzeit sehr gerne zur Verfügung. Sie erreichen uns unter der Telefonnummer (06894) 38797-0 oder per E-Mail an datenschutz@compusaar.de.

Mit besten Grüßen

Alexander Eich

Christoph Hildmann

Christoph Hildmann

Externer Datenschutzbeauftragter (nach DIN EN ISO/IEC 17024)
Betrieblicher und externer Datenschutzbeauftragter (IHK)
Consultant für Datenschutz und Informationssicherheit

Was versteht man unter Gesundheitsdaten?

Um festzulegen wie Gesundheitsdaten definiert sind, schauen wir uns zuerst einmal den Art. 4 der Datenschutzgrundverordnung (DSGVO) an. Unter der Nummer 15 steht zur Begriffsbestimmung von Gesundheitsdaten folgendes:

> *„… personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen …“*

Hinzu können genetische Daten kommen, die unter Nummer 13 definiert sind.

> *„…personenbezogene Daten zu den ererbten oder erworbenen genetischen Eigenschaften einer natürlichen Person, die eindeutige Informationen über die Physiologie oder die Gesundheit dieser natürlichen Person liefern und insbesondere aus der Analyse einer biologischen Probe der betreffenden natürlichen Person gewonnen wurden…“*

Zudem muss der Art. 9 DSGVO (Verarbeitung besonderer Kategorien personenbezogener Daten) Abs. 1 in die Überlegungen mit einbezogen werden. Hier steht:

> *„… Die **Verarbeitung personenbezogener Daten**, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, **Gesundheitsdaten** oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person **ist untersagt**. …“*

Durch diese Artikel wird bestimmt, was Gesundheitsdaten im Allgemeinen sind und dass sie zu einer „besonderen Kategorie“ gehören. Das macht Gesundheitsdaten besonders schützenswert und somit dürfen diese ohne ausdrückliche Einwilligung der Betroffenen nicht so einfach verarbeitet und gespeichert werden.

Hierbei gibt es natürlich Ausnahmen. Beispielsweise, dann wenn die Verarbeitung *„zum Schutz lebenswichtiger Interessen“ oder zum „Recht der sozialen Sicherheit“* durchgeführt werden muss. Weitere Ausnahmen können u. a. zum Zweck der Gesundheitsvorsorge gelten (z. B. *zur Beurteilung der Arbeitsfähigkeit,* § 22 BDSG).

Die Hürden sind allerdings hoch und somit muss bei einer möglichen Verarbeitung von Gesundheitsdaten immer eine Einwilligung der betroffenen Person oder eine Rechtsgrundlage vorliegen!

Reicht die ärztliche Schweigepflicht für ein angemessenes Schutzniveau?

Die ärztliche Schweigepflicht | § 203 Abs. 1 StGB

Die ärztliche Schweigepflicht wird durch den § 203 des Strafgesetzbuches (StGB) festgeschrieben. Hier wird im Abs. 1 StGB bestimmt, dass

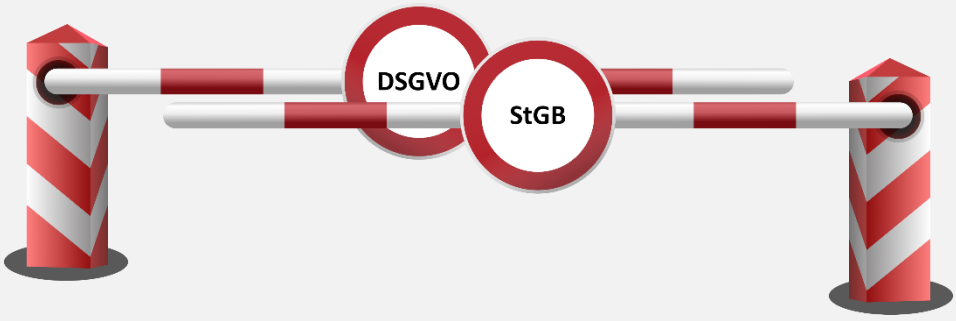
> *„… **derjenige, der unbefugt ein fremdes Geheimnis,** namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, **offenbart, das ihm als Arzt anvertraut oder sonst bekannt geworden ist, mit Freiheitsstrafe bis zu einem Jahr oder mit einer Geldstrafe bestraft wird**. …“*

Dies gilt zudem für berufsmäßig tätige Gehilfen und die zur Vorbereitung auf den Beruf tätigen Personen, was neben den Ärzten auch Apotheker, Krankenschwestern, Arzthelfer etc. miteinschließt. Ja sogar berufsnahe Gehilfen (Sekretariat, Sprechstundenhilfen uvm.) werden durch den § 203 StGB angesprochen.

Zudem wird die Schweigepflicht in der (Muster-)Berufsordnung (MBO) für in Deutschland tätige Ärztinnen und Ärzte im § 9 explizit hervorgehoben.

Reicht die ärztliche Schweigepflicht aus Sicht des Datenschutzes aus?

Diese Frage kann ganz klar mit „nein“ beantwortet werden.



Das Vorhandensein einer beruflichen Ethik, selbst wenn diese gesetzlich oder in einer Berufsordnung geregelt ist, entbindet nicht von der Pflicht, alle Datenschutzvorschriften zu beachten - „Zwei-Schranken-Prinzip“!

Somit ist die Schweigepflicht alleine keine ausreichende Grundlage, um Gesundheitsdaten zu erheben, zu verarbeiten oder zu speichern. Zulässig ist die Verarbeitung nur dann, wenn auch die DSGVO oder eine andere Rechtsvorschrift dies erlaubt oder vorschreibt, oder Betroffene selbst ihre Einwilligung erteilt haben.

> *Die zum Schutz von sensiblen Daten nötigen technischen und organisatorischen Maßnahmen (TOM) sind immer dort ohne Einschränkung umzusetzen, wo Gesundheitsdaten verarbeitet werden!*

Art. 32 der Datenschutzgrundverordnung | Sicherheit der Verarbeitung

Die Basis für technische und organisatorische Maßnahmen (TOM), die getroffen werden müssen, bildet der Art. 32 der DSGVO:

> *„Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter **geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten**“*

Hieraus kann ein erster Maßnahmenplan und somit eine erste Selbsteinschätzung erarbeitet werden, bei der die folgenden *grundlegenden Vorgaben erfüllt sein sollten:*

Datenschutz am Empfang (Diskretionszone)

Hier lauern viele datenschutzrechtliche Risiken, die oft gar nicht als solche eingeschätzt werden. Beispielsweise werden immer wieder Akten beim Empfang abgelegt, Terminpläne stehen offen und Notizen sind für jeden einsehbar.

Gleiches gilt für Gespräche die hier mit und über Betroffene geführt werden, sei es persönlich oder per Telefon. Hier sollten Dritte immer ausgeschlossen werden!

Folgende Mindestanforderungen sollten hier immer positiv beantwortet werden:

- Ist sichergestellt, dass alle Personen ihr Anliegen schildern können, ohne dass Wartende mithören?
- Kann das Personal Gespräche, sei es persönlich oder per Telefon, führen, ohne dass Wartende mithören?
- Sind alle Unterlagen, Terminpläne, Notizen und IT-Systeme vor der Ansicht Unbefugter geschützt?
- Sind alle Akten mit personenbezogenen Gesundheitsdaten zu 100% vor dem Zugriff Unbefugter geschützt?

Datenschutz im Wartebereich

- Ist der Wartebereich optisch und akustisch vom Empfang und den Behandlungsräumen getrennt?

Datenschutz im Behandlungsbereich

- Wird der Behandlungsbereich bei jeder Behandlung geschlossen?
- Sind auch bei Abwesenheit des behandelnden Personals alle Gesundheitsdaten gegen unbefugte Kenntnisnahme geschützt?

Datenschutz in der Verwaltung

- Sind abschließbare Aktenschränke vorhanden und wenn ja, werden diese bei Nichtnutzung immer geschlossen?
- Ist sichergestellt, dass das Reinigungspersonal keinen Zugang zu Gesundheitsdatendaten hat?

Grundlegende technische Maßnahmen - Informationstechnologie

- Ist der Zugang zu allen IT-Geräten durch Passwörter geschützt?
- Entsprechen die Passwörter dem aktuellen Sicherheitsstandard (Empfehlungen des BSI / IT-Grundschutz)?
- Werden IT-Systeme bei jedem Verlassen des Arbeitsplatzes gesperrt?
- Sind IT-Systeme, die mit dem Internet verbunden sind und den Zugriff auf sensible Daten erlauben, ausreichend geschützt („Firewall“)?
- Wird regelmäßig eine Datensicherung erstellt, um alle Daten vor Verlust oder Zerstörung zu schützen?
- Bietet die genutzte Software die Möglichkeit, Gesundheitsdaten verschlüsselt zu speichern?
- Wird der Schutz der Gesundheitsdaten auch dann gewahrt, wenn ein externer IT-Dienstleister Support leistet?

Grundlegende Maßnahmen - Personal

- Wird das Personal regelmäßig sensibilisiert, wie mit personenbezogenen Gesundheitsdaten umzugehen ist?
- Gibt es Maßnahmen zur Risikominimierung (z. B. zur Erkennung von schadhaften E-Mails, Awareness-Programm, …)?

Maßnahmen bei einer möglichen Datenübermittlung

Es gibt Situationen, bei denen Gesundheitsdaten an Dritte übermittelt werden müssen, z. B. an weitere Ärzte oder an privatärztliche Verrechnungsstellen. Hier sollten immer mind. folgende Punkte berücksichtigt werden:

- Ist bei der Versendung der Daten sichergestellt, dass ausschließlich Berechtigte Kenntnis erhalten (z. B. durch Versendung mit Ankündigung)?
- Datenreduzierung - ist sichergestellt, dass nur notwendige Daten übermittelt werden?
- Wurde einer Übermittlung (z. B. an eine privatärztliche Verrechnungsstelle) schriftlich zugestimmt?
- Wurden die betroffenen Personen über mit- und nachbehandelnde Ärzte informiert und wurden der Datenweitergabe zugestimmt?

Die hier dargestellten Fragen, stellen nur einen ersten kleinen Überblick dar. Sie müssten zur Vollständigkeit individuell angepasst und deutlich erweitert werden!

Risikominimierung und Sensibilisierung aller Mitarbeiter:innen

Hierzu empfehlen wir unserer Datenschutzzeitung zum Thema ***Mitarbeiter-Awareness*** (Ausgabe Juni 2022).

Weitergabe von Gesundheitsdaten

Dürfen Gesundheitsdaten weitergegeben werden?

Gesundheitsdaten unterliegen im besonderem dem Datenschutz und somit ist eine Weitergabe von Informationen erst einmal unzulässig. Zum einen gibt es hier datenschutzrechtliche Gründe, zum anderen greift die Schweigepflicht, der alle Beschäftigten unterliegen, die Kenntnisse zum Gesundheitszustand des Betroffenen erlangen. Hier könnten Verstöße sogar strafrechtliche Konsequenzen nach sich ziehen.

Somit ist bei einer potentiellen Weitergabe von Gesundheitsdaten nicht nur der Datenschutz, sondern im besonderen Maße auch die Schweigepflicht zu beachten!

Allerdings gibt es Ausnahmen, folgend eine kleine Auswahl:

Beispielsweise wäre Polizei und Staatsanwaltschaft zur Herausgabe von Gesundheitsdaten berechtigt, wenn hierdurch Gefahren abgewehrt werden könnten.

Bei meldepflichtigen Krankheiten wäre eine Weitergabe der Daten sogar verpflichtend. Möglicherweise könnten diese dann aber anonymisiert abgegeben werden.

Auch bei Geburten und Sterbefällen müsste eine Weitergabe der Daten an das zuständige Standesamt erfolgen.

Gleiches kann im Bedarfsfall u. a. auch für einen medizinischen Dienst, der zuständigen Krankenkasse, einer Berufsgenossenschaft oder einer Datenschutzbehörde gelten, wobei die zu übermittelten Daten hier immer verschiedenen Einschränkungen unterliegen und genau abgewogen werden sollte, ob und in welcher Form eine Übermittlung allen Anforderungen gerecht wird.

Um bei einer Übermittlung personenbezogener Daten, und vor allem bei Gesundheitsdaten, jegliches Risiko zu vermeiden, sollten alle Betroffene immer in alle Gegebenheiten (Sinn und Zweck einer möglichen Weitergabe der Daten, potentielle Empfänger, …) eingewiesen werden und idealerweise ihre Einwilligung erteilen. Dies könnte beispielsweise in Form einer Datenschutzerklärung, idealerweise mit einer Entbindung der Schweigepflicht, erfolgen.

Sind Auskünfte an Dritte (Verwandte, Arbeitgeber, …) gestattet?

Auch hier ist eine entsprechende Einwilligung die beste Lösung. Mit ihr kann der Betroffene selbst bestimmen, wer informiert werden soll und wer nicht. Ohne diese sind Auskünfte prinzipiell nicht möglich, da hier sowohl gegen die Schweigepflicht als auch gegen geltende Datenschutzbestimmungen verstoßen würde.

Eine Ausnahmesituation ergibt sich allerdings, wenn Betroffene nicht ansprechbar sind. Hier wären Ehegatten oder nahe Verwandte die ersten Ansprechpartner.

Um solchen Situationen vorzubeugen, wäre eine Patientenverfügung von Vorteil, weil man so selbstbestimmt und nach eigenem Willen handelt und niemanden vor ungewollte Entscheidungen stellt.

Die Elektronische Patientenakte (ePA) und Datenschutz

Die Elektronische Patientenakte (ePA)

Aktuell steht jedem Versicherten eine *elektronische Patientenakte (ePA)* zur Verfügung. Diese kann bei der zuständigen Krankenkasse beantragt werden und dient dazu, medizinische Befunde und Informationen aus vorhergehenden Untersuchungen bereitzustellen. Mit der ePA soll, u. a. bei einem Notfall, eine optimale Versorgung und Behandlung der Patienten und Patientinnen sichergestellt werden. Auch unnötig belastende Mehrfachuntersuchungen sollen so reduziert oder vermieden werden.

Die Nutzung ist von Seiten der Patienten freiwillig.

Eingabe und Zugriff auf Gesundheitsdaten

Laut dem Bundesministerium für Gesundheit, hat alleinig der Patient, das Recht zu bestimmen, was in seiner elektronische Patientenakte vorgehalten wird. Zudem kann er frei bestimmen, wer Zugriff auf seine Daten bekommt und wie lange. Auch können die Daten selektiv freigegeben werden, so dass z. B. jeder behandelnde nur Zugriff auf seinen Fachbereich bekommt und möglicherweise auch nur für die Zeit der aktuellen Behandlung.

Welche Berufsgruppen sind (nach Freigabe) für den Zugriff zugelassen

- ✓ Krankenhäuser
- ✓ Ärzte und Zahnärzte
- ✓ Apotheken
- ✓ Therapeuten
- ✓ Leistungserbringer, die an der Behandlung beteiligt sind

Zudem werden kurzfristig Pflegepersonal, Hebammen, Physiotherapeuten, der öffentl. Gesundheitsdienst, Arbeitsmediziner sowie Reha-Kliniken eingebunden.

Gibt es datenschutzrechtliche Bedenken beim Einsatz der ePA?

Mit in Kraft treten des *Patientendaten-Schutz-Gesetz (PDSG)* wurde die Digitalisierung im Gesundheitswesen vorangetrieben und damit auch das wahrscheinlich größte Projekt dieses Gesetzes - die elektronische Patientenakte (ePA).

Zum Start wurde die ePA vom Bundesbeauftragten für Datenschutz und Informationsfreiheit sehr kritisch gesehen. Zum einen, weil Daten noch nicht selektiert werden konnten, zum anderen, weil es Personen gab, die kein eigenes geeignetes Gerät zur Einsicht in die Akte besaßen. Dies verstieß laut BfDi gegen die DSGVO.

Die selektive Freigabe ist zwischenzeitig gegeben. Das nicht alle ein geeignetes Endgerät zur Einsicht in die Akte besitzen, stellt immer noch ein Problem dar.

Ansprechpartner für alle Datenschutz-Fragen zur ePA ist der Datenschutzbeauftragte der zuständigen Krankenkasse.

Ist im Gesundheitswesen ein Datenschutzbeauftragter Pflicht?

Gibt es die Pflicht einen Datenschutzbeauftragten zu bestellen?

Auch wenn die Daten, die im Gesundheitswesen verarbeitet werden, als besonders schützenswert eingestuft sind, besteht keine zwingende Pflicht einen Datenschutzbeauftragten bestellen zu müssen, vorausgesetzt die Anzahl der Mitarbeiter:innen, die ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind, liegt unter der verpflichtenden Bestellungsgrenze. Somit gelten, auch im Gesundheitswesen, prinzipiell die gleichen DSGVO-Vorgaben wie bei Unternehmen.

Dennoch ist die Bestellung eines Datenschutzbeauftragten (intern, oder durch einen externen Dienstleister) zu empfehlen, da speziell im Gesundheitswesen sehr viele Datenschutzvorgaben erfüllt werden müssen und deren Nichtbeachtung schnell finanzielle Konsequenzen nach sich ziehen kann.

Gibt es Ausnahmen, bei denen zwingend ein Datenschutzbeauftragter bestellt werden muss?

Im Gesundheitswesen kann es besondere Umstände geben, bei denen eine ***umfangreiche Verarbeitung von Gesundheitsdaten*** vorliegt. Beispiele:

- Es kommen komplexe digitale Medizinprodukte im Sinne des Medizinproduktegesetzes zum Einsatz
- Die nicht nur gelegentliche Nutzung telemedizinischer Anwendungen
- Der Einsatz von Videotechnik im Behandlungsverfahren
- Hausarzt-, Kinderarzt- oder internistische Praxen, welche einen umfassenden, generationsübergreifenden Datenbestand zu einer Person oder Familie haben und diese Daten zur Auswertung miteinander abgleichen
- Überproportional großer Patientenstamm im Vergleich zu anderen Praxen selber Ausrichtung und Beschäftigtenzahl
- Nutzen von „Big Data“ Anwendungen (z. B. Auswertung großer Datenmengen von Patientendaten)
- Begleitende Forschungstätigkeit, wenn mehr Daten, als zur Behandlung erforderlich sind, erhoben werden

Hier kann eine Bestellung auch weit unter der verpflichtenden Bestellungsgrenze zur Pflicht werden. Gleiches gilt, wenn aufgrund eines hohen Risikos bei der Datenverarbeitung oder einer umfangreichen Datenverarbeitung eine Datenschutz-Folgenabschätzung durchzuführen ist.

Muss im Gesundheitswesen ein Verzeichnis von Verarbeitungstätigkeiten geführt werden?

Laut Art. 30 Abs. 5 DSGVO sind Unternehmen und Institutionen mit weniger als 250 Mitarbeiter:innen von der Führung eines *Verzeichnisses von Verarbeitungstätigkeiten* ausgenommen, wobei man beachten muss, dass diese Befreiung nicht für alle Daten-Kategorien gilt und im speziellen nicht für Gesundheitsdaten.

Somit stellen Gesundheitsdaten eine konkrete Ausnahme dar und verpflichten zur Führung eines solchen Verzeichnisses.

Anonymisierung von Gesundheitsdaten

Dokumente mit Gesundheitsdaten zu anonymisieren, bringt viele Vorteile mit sich. Beispielsweise findet so das Datenschutzrecht keine Anwendung mehr und es würde selbst dann nichts passieren, wenn Dokumente veröffentlicht würden.

Allerdings ist hier Vorsicht geboten, weil die Anforderungen an eine Anonymisierung sehr streng gestaltet sind. Beispielsweise reicht es hier nicht, den Namen einfach nur durch eine Identifikationsnummer auszutauschen.

Ein aktueller Datenschutzverstoß im Gesundheitswesen

Bußgeld wegen mangelhafter TOM | 2022, Bußgeld: 105.000,00 EUR

Ein Unternehmen hatte unterlassen, geeignete technische und organisatorische Maßnahmen (TOM) zu treffen, um beim Versand von Arztbriefen durch Beschäftigte des Unternehmens ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

In der Folge wurden mehrfach Arztbriefe an eine Person versandt, die nicht die weiterbehandelnde Ärztin war. Erschwerend kam hinzu, dass die unberechtigte Empfängerin mehrfach auf den Fehlversand hingewiesen hat.

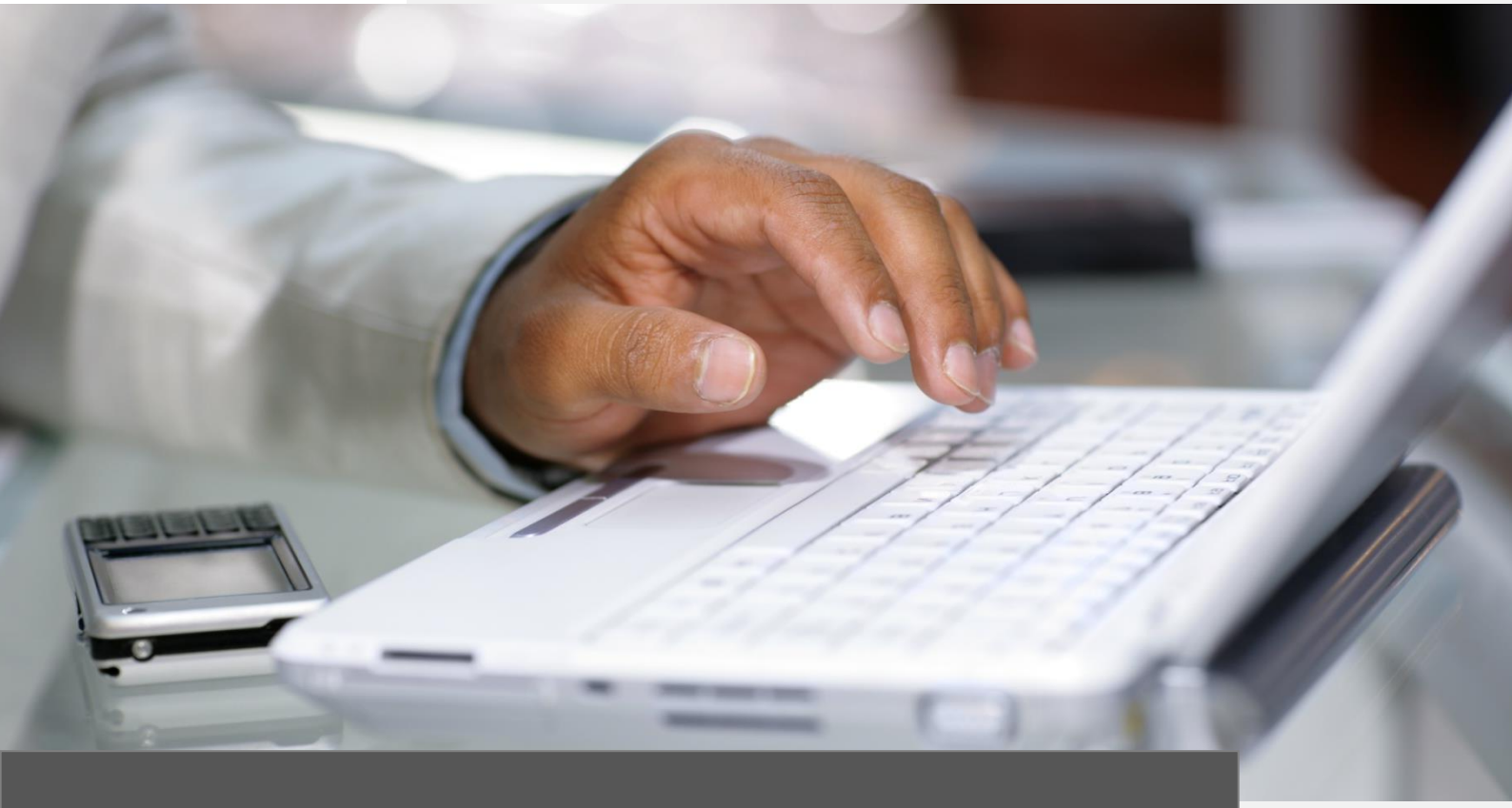
Das Unternehmen hatte die Adressatin nach deren Hinweisen mit einem Sperrvermerk im verwendeten Datenverarbeitungssystem versehen. Es hatte es dabei aber unterlassen, durch TOM sicherzustellen, dass der Sperrvermerk auch bei Software-Updates übernommen wird. So wurde nach einem Update der Sperrvermerk nicht übernommen und die Empfängerin bekam erneut Arztbriefe über Personen, die nicht ihre Patientinnen und Patienten waren. Der Fehlversand beruhte somit auf dem fehlenden Sperrvermerk und einer nicht mit der notwendigen Sorgfalt durchgeführten Auswahl der Adressatin durch die Beschäftigten des Unternehmens.

Dies stellt einen Verstoß gegen die Pflicht des Art. 32 Abs. 1 DSGVO dar.

Quellen: Tätigkeitsbericht 2021 des HmbBfDI
https://www.dsgvo-portal.de/dsgvo-bussgeld-datenbank/

> **!** Bei der Verarbeitung von Gesundheitsdaten von Patientinnen und Patienten müssen Unternehmen geeignete technische und organisatorische Maßnahmen (TOM) ergreifen, um diese Daten angemessen zu schützen. Bei einer unzureichenden Umsetzung von TOM drohen empfindliche Bußgelder!

Mai | 2023



Impressum

CS Hard- & Software Consulting GmbH
Saarbrücker Str. 72
66386 St. Ingbert
Tel.: +49 (6894) 38797 - 0
Fax: +49 (6894) 38797 - 99
Web: www.compusaar.de
E-Mail: datenschutz@compusaar.de

Amtsgericht St. Ingbert, HRB 13312
Ust-IdNr.: DE813536236
Geschäftsführerin: Ursula Doll

Redaktion
Alexander Eich

Bildnachweise | Bild (Seite 1) von Tung Nguyen auf Pixabay
Diese Unterlage wurde in unserem Auftrag von der Firma ITKservice GmbH & Co. KG, Fuchsstädter Weg 2, 97491 Aidhausen erstellt. Einige der dargestellten Bilder wurden von der ITKservice bei https://www.ccvision.de gekauft und lizensiert. Weitere stammen von https://pixabay.com/de/ einer Plattform für lizenzfreie Bilder.

CompuSaar