FAQs zur Datenschutz-Grundverordnung (DSGVO) Stand: 20.03.2019

Allgemeines

Diese FAQs fußen auf dem derzeitigen Informationsstand zur Datenschutz-Grundverordnung. Da derzeit noch keine gerichtlichen oder verwaltungsbehördlichen Entscheidungen für diesen Bereich vorliegen und die Datenschutz-Grundverordnung in einigen wesentlichen Bereichen einen Interpretationsspielraum zulässt, kann die Ärztekammer für Niederösterreich keine Verantwortung oder Haftung für die Richtigkeit sowie Vollständigkeit der Inhalte übernehmen. Insofern kann die Ärztekammer für Niederösterreich für keinerlei Schäden, die sich aus der Nutzung des Inhalts ergeben können, haftbar gemacht werden.

Die vorliegenden Informationen werden regelmäßig aktualisiert und ergänzt.

Muss ich eine Datenschutzerklärung auf meine Homepage stellen?

Derzeitige Empfehlung: Ja.

Gemäß § 3b Abs. 2 Ärztegesetz 1998 sind Ärzte/innen insbesondere von den Informationspflichten nach Art 13 und Art 14 DSGVO betreffend Datenanwendungen, die im Ärztegesetz vorgesehen sind, befreit. Das Betreiben einer Homepage durch Ärzte fällte jedoch unseres Erachtens nicht unter diese Ausnahme. Wir empfehlen daher, eine Datenschutzerklärung auf der Homepage zu veröffentlichen. Ein Muster dafür finden Sie unter den Mustern zur DSGVO auf unserer Homepage. Dieses Muster wurde für Homepages erstellt, auf denen keine sonstigen Datenerhebungen (zB im Wege von Cookies oder Kontaktformularen) stattfinden.

Muss der Patient aufgrund der DSGVO seine ausdrückliche Einwilligung zur Übermittlung von (Blut-)Proben an Labors oder pathologische Institute sowie zur Rückübermittlung von Befunden an den Zuweiser geben?

Nein.

Gemäß Art. 9 Abs. 2 lit. h iVm Abs. 3 DSGVO ist die Übermittlung von Gesundheitsdaten für Zwecke der medizinischen Diagnostik und der Behandlung im Gesundheitsbereich aufgrund eines Vertrages mit einem Angehörigen eines Gesundheitsberufs zulässig, wenn diese Daten von Fachpersonal oder unter dessen Verantwortung verarbeitet werden und dieses Fachpersonal einem gesetzlichen Berufsgeheimnis unterliegt.

Zudem sind NÖ Labor- und pathologische Institute gemäß § 21 Abs. 3 NÖ KAG verpflichtet, einweisenden oder weiterbehandelnden Ärzten über Anforderung kostenlos Kopien von Krankengeschichten und ärztlichen Äußerungen über den Gesundheitszustand von Patienten zu übermitteln. Vergleichbare Regelungen existieren auch in den Landeskrankenanstaltengesetzen der anderen Bundesländer mit Ausnahme der Steiermark.

Gemäß § 51 Abs. 2 Ärztegesetz sind Ärzte zur Übermittlung von Patientendaten an andere Ärzte oder medizinische Einrichtungen, in deren Behandlung der Kranke steht, mit – auch schlüssiger – Einwilligung des Kranken berechtigt.

Vor diesem Hintergrund ist davon auszugehen, dass die ausdrückliche, allenfalls schriftliche Einwilligung des Patienten in die Übermittlung von (Blut-)Proben an Labors oder pathologische Institute und in die Rückübermittlung eines Befundes an den Zuweiser nicht erforderlich ist, da die diagnostische Abklärung entweder Teil des zwischen Zuweiser und Patienten geschlossenen Behandlungsvertrags oder Gegenstand eines zwischen dem Labor bzw. pathologischen Institut und dem Patienten abgeschlossenen Behandlungsvertrags ist und damit auch eine Einwilligung des Patienten vorliegt. Damit sind sowohl die Vorgaben der DSGVO als auch des Ärztegesetzes erfüllt.

Es ist jedoch dringend zu empfehlen, in der Ordination mittels Aushangs darauf hinzuweisen, dass (Blut-)Proben an – konkret anzuführende – externe Einrichtungen zur diagnostischen Abklärung übermittelt und die sich daraus ergebenden Befunde an die Ordination zurückgesendet werden.

Ich bin Facharzt, und mir wurde ein Patient überwiesen. Ist es mir gestattet, von mir erstellte Befunde unmittelbar an den Zuweiser zu übermitteln?

Ja. Es wird jedoch empfohlen, die (mündliche) Einwilligung des Patienten einzuholen. Diese kann entfallen, sofern auf der Überweisung ausdrücklich um Befundübermittlung an den Zuweiser ersucht wird.

Gemäß Art. 9 Abs. 2 lit. h iVm Abs. 3 DSGVO ist die Übermittlung von Gesundheitsdaten für Zwecke der medizinischen Diagnostik und der Behandlung im Gesundheitsbereich aufgrund eines Vertrags mit einem Angehörigen eines Gesundheitsberufs zulässig, wenn diese Daten von Fachpersonal oder unter dessen Verantwortung verarbeitet werden und dieses Fachpersonal einem gesetzlichen Berufsgeheimnis unterliegt.

Da der Patient mit dem Zuweiser und Ihnen in einem aufrechten Behandlungsverhältnis (Behandlungsvertrag) steht, ist die ausdrückliche Einwilligung des Patienten für die Übermittlung nicht erforderlich, um die Vorgaben der DSGVO einzuhalten.

Gemäß § 51 Abs. 2 Ärztegesetz sind Ärzte zur Übermittlung von Patientendaten an andere Ärzte oder medizinische Einrichtungen, in deren Behandlung der Kranke steht, jedoch nur mit Einwilligung des Kranken berechtigt.

Daher empfiehlt es sich, den Patienten zu befragen, ob er mit der Übermittlung an den Zuweiser einverstanden ist und dies zu dokumentieren.

Ist es datenschutzrechtlich zulässig, eine telefonische Befundauskunft zu erteilen?

In der Praxis ist es oftmals zweckmäßig, den Patienten einen zusätzlichen Weg in die Ordination zu ersparen und ihn telefonisch über das Ergebnis eines Befundes zu informieren. In diesem Fall sind vom persönlich anwesenden Patienten die Telefonnummer, über die er kontaktiert werden möchte, sowie seine zumindest mündliche Einwilligung über die telefonische Befundbesprechung einzuholen.

Beides ist im Patientenakt zu dokumentieren. Als zusätzliches Sicherheitskriterium kann mit dem Patienten ein Kennwort vereinbart werden, das er vor telefonischen Auskünften zu nennen hat.

Muss ich bauliche Maßnahmen setzen, um die Vertraulichkeit in meiner Ordination zu gewährleisten?

Patienten muss die Möglichkeit zu vertraulichen Gesprächen auch mit Ihren Angestellten etwa bei der Anmeldung, Terminvereinbarung, Abholung von Rezepten etc. gegeben werden. Patienten sollten daher auf Wunsch die Möglichkeit haben, Gespräche auch mit Ihren Mitarbeitern räumlich getrennt von anderen Patienten führen zu können. Auf diese Möglichkeit sollte mittels Aushangs hingewiesen werden. Es ist jedoch nicht erforderlich, dass der Anmeldebereich generell baulich von anderen Teilen der Ordination getrennt wird.

Dürfen Rezepte, Überweisungsscheine für einen Patienten durch Angehörige oder Vertrauenspersonen abgeholt werden?

Das Aushändigen derartiger Unterlagen an andere Personen als den Patienten oder seinen gesetzlichen Vertreter stellt eine Übermittlung von (sensiblen) Daten dar. Diese ist im vorliegenden Fall nur aufgrund ausdrücklicher und nachweislicher Einwilligung des Patienten zulässig. In der Praxis stellt dies eine große organisatorische Herausforderung dar. Eine Möglichkeit, einen rechtskonformen Zustand zu erreichen, ist, Patienten Vertrauenspersonen oder Einrichtungen definieren zu lassen, an die Patientendaten weitergegeben werden dürfen.

Muss mit Ordinationsvertretern eine spezielle Vereinbarung über den Datenschutz geschlossen werden oder müssen die Patienten ihre ausdrückliche Einwilligung erteilen, dass Vertreter in die Patientendokumentation des Vertretenen Einsicht nehmen dürfen?

Nein.

Gemäß Art. 9 Abs. 2 lit. h iVm Abs. 3 DSGVO ist die Übermittlung von (darunter fällt auch die Einräumung der Möglichkeit der Einsichtnahme in) Gesundheitsdaten für Zwecke der medizinischen Diagnostik und der Behandlung im Gesundheitsbereich aufgrund eines Vertrags mit einem Angehörigen eines Gesundheitsberufs zulässig, wenn diese Daten von Fachpersonal oder unter dessen Verantwortung verarbeitet werden und dieses Fachpersonal einem gesetzlichen Berufsgeheimnis unterliegt.

Soweit der Patient über die Vertretung zB durch Aushang informiert wird, kommt in der Regel der Behandlungsvertrag zwischen dem Vertreter und dem Patienten zustande. Der Vertreter ist selbst datenschutzrechtlicher Verantwortlicher. Eine gesonderte Einwilligung des Patienten ist aufgrund der genannten speziellen Regelung in der DSGVO nicht erforderlich ist.

Gemäß § 51 Abs. 2 Ärztegesetz sind Ärzte zur Übermittlung von Patientendaten an andere Ärzte, in deren Behandlung der Kranke steht, jedoch nur mit Einwilligung des Kranken berechtigt. Diese kann jedoch auch schlüssig erfolgen.

Zusammenfassend gesagt: Mit dem Vertreter, der selbst Verantwortlicher im Sinne des Datenschutzrechts ist, muss keine Auftragsverarbeitungsvereinbarung geschlossen werden. Es ist auch nicht erforderlich, dass der Patient ausdrücklich einwilligt, dass der Vertreter in die vorhandene Dokumentation Einsicht nimmt. Vielmehr ist von einer ausreichenden schlüssigen Einwilligung auszugehen, wenn der Patient den Vertreter aufsucht.

Darf ich Patienten oder anderen (zB Apotheken) Befunde oder andere sensible Daten per (unverschlüsselter) E-Mail zusenden?

Der Versand per E-Mail stellt keinen sicheren Kommunikationsweg dar. Bei der Übermittlung der Daten per E-Mail ist es (unberechtigten) Dritten relativ leicht möglich, diese Informationen zu lesen und sogar Daten (unbemerkt) zu verändern.

Eine Übermittlung per E-Mail sollte daher – wenn überhaupt – nur nach Einholung einer ausdrücklichen, schriftlichen Einwilligung des Patienten erfolgen. Eine solche Vereinbarung finden Sie in den Mustern zu der DSGVO auf unserer Homepage. Es ist jedoch bis dato nicht abschließend geklärt, ob eine solche Einwilligung die Übermittlung von Befunden per E-Mail zulässig macht.

UPDATE vom 20.03.2019:

In einer Entscheidung (DSB-D213.692/0001-DSB/2018) hält die österreichische Datenschutzbehörde fest, dass die Einwilligung eines Patienten in die unverschlüsselte Übermittlung von Gesundheitsdaten per E-Mail nicht statthaft ist.

Bereits vor dieser Entscheidung haben wir in unseren FAQs darauf hingewiesen, dass nicht abschließend geklärt ist, ob eine solche Einwilligung die Übermittlung von Gesundheitsdaten per E-Mail zulässig macht. Aufgrund dieser Entscheidung sollte in Zukunft von der Einholung derartiger Einwilligungen und der Übermittlung von Gesundheitsdaten per E-Mail abgesehen werden.

Ist der Versand von Erinnerungen zu Untersuchungen (Recall-System) per Mail oder SMS zulässig. Wie sieht es bei Erinnerungen zu einem bereits vereinbarten Termin aus?

Der Versand einer Erinnerung im Rahmen eines Recall-Systems oder der Erinnerung an einen bereits vereinbarten Termin erfordert die vorherige nachweisliche Einwilligung des Patienten. Zudem sollte darauf geachtet werden, dass möglichst wenige Informationen, insbesondere kein konkreter Hinweis auf den zuletzt wahrgenommenen Termin, übermittelt werden.

Auch der Versand von Informationen via SMS weist gewisse Sicherheitsrisiken auf (Stichwort SS7-Hack). Dennoch ist das Sicherheitsniveau hier als wesentlich höher zu qualifizieren als beim Versand von E-Mails. Insofern ist dem Versand von SMS der Vorzug zu geben.

Ist die Verwendung eines Faxgerätes zur Übermittlung von Gesundheitsdaten zulässig?

Die Übermittlung von Daten per Fax erfolgt unverschlüsselt, sodass sich hier ein ähnliches Problem wie beim E-Mail-Versand ergibt. Derzeit liegt jedoch für das Verwenden von Faxgeräten bei der

Übermittlung von Gesundheitsdaten noch eine ausdrückliche gesetzliche Regelung vor, die die Nutzung bis auf weiteres unter bestimmten Voraussetzungen erlaubt.

Im Gesundheitstelematikgesetz (§ 27 Abs. 12f.) findet sich folgende Regelung zur Verwendung von Telefax:

„Die Weitergabe von Gesundheitsdaten darf unter den Voraussetzungen des Abs. 10 Z 1 bis 3 (d.h. insbesondere vorheriger telefonischer Kontakt) ausnahmsweise auch per Fax erfolgen, wenn 1. die Faxanschlüsse (einschließlich Ausdruckmöglichkeiten zu Faxanschlüssen, die in EDV-Anlagen installiert sind) vor unbefugtem Zugang und Gebrauch geschützt sind, 2. die Rufnummern, insbesondere die verspeicherten Rufnummern, regelmäßig, insbesondere nach Veränderungen der technischen Einrichtung sowie nach der Neuinstallation von Faxgeräten nachweislich auf ihre Aktualität geprüft werden, 3. automatische Weiterleitungen, außer an die jeweiligen Gesundheitsdiensteanbieter selbst, deaktiviert sind, 4. die vom Gerät unterstützten Sicherheitsmechanismen genützt werden und 5. allenfalls verfügbare Fernwartungsfunktionen nur für die vereinbarte Dauer der Fernwartung aktiviert sind.

Die erleichterten Bedingungen (…) können nicht in Anspruch genommen werden, wenn die Verwendung von Gesundheitsdaten entsprechend den Bestimmungen des 2. Abschnitts (insb. verschlüsselte Übermittlung) mit Bedachtnahme auf den Stand der technischen Möglichkeiten und auf die wirtschaftliche Vertretbarkeit (§ 14 Abs. 1 DSG 2000) zumutbar ist.“

Darf ich Gesundheitsdaten (zB Kopien von Honorarnoten) meiner Patienten an den Steuerberater übermitteln? Muss ich den Namen der Patienten oder die Diagnosen schwärzen?

Hierzu besteht die allgemeine Empfehlung, nicht zuletzt auf Grund der DSGVO, Personenbezüge, wenn möglich, zu vermeiden. Nur dort, wo der Personenbezug zur Erfüllung einer rechtmäßigen Aufgabe notwendig ist, wie z.B. Mahnwesen im Rahmen der Buchhaltung, ist eine Übermittlung von personenbezogenen Daten statthaft. Allerdings nur jene Daten die zur Erfüllung der konkreten Aufgabe notwendig sind. Für das Beispiel des Mahnwesens im Rahmen der Buchhaltung sind nur Namen und Adresse des Patienten notwendig. Nicht jedoch z.B. Diagnosen bzw. Behandlungsschritte. Diese wären unkenntlich zu machen.

Haben externe Arbeitsmediziner eine zusätzliche Datenverarbeitung im Verzeichnis von Verarbeitungstätigkeiten zu dokumentieren oder ist dieser Bereich bereits im Musterdokument berücksichtigt?

Bei den personenbezogenen Aufzeichnungen über arbeitsmedizinische Untersuchung und die Durchführung von Schutzimpfungen, die mit der Tätigkeit der Arbeitnehmer im Zusammenhang stehen, handelt es sich um eine Patientendokumentation gemäß § 51 Ärztegesetz, die der ärztlichen Verschwiegenheitspflicht unterliegt. Das Führen dieser Aufzeichnung ist durch das Muster auf unserer Homepage abgedeckt. Sollten diese Daten im Betrieb verwahrt oder gespeichert werden, ist diesbezüglich in der Regel der Abschluss einer Auftragsverarbeitervereinbarung mit dem Betriebsinhaber erforderlich. Ein entsprechendes Muster finden Sie in den Unterlagen zur DSGVO (Dokumentationspflichten des Arztes) auf unserer Homepage.

Haben Schulärzte eine zusätzliche Datenverarbeitung im Verzeichnis von Verarbeitungstätigkeiten zu dokumentieren oder ist dieser Bereich bereits im Musterdokument berücksichtigt?

Bei den personenbezogenen Aufzeichnungen über schulärztliche Untersuchung und die Durchführung von Schutzimpfungen handelt es sich um eine Patientendokumentation gemäß § 51 Ärztegesetz, die der ärztlichen Verschwiegenheitspflicht unterliegt. Das Führen dieser Aufzeichnung ist durch das Muster auf unserer Homepage abgedeckt. Sollten diese Daten in der Schule verwahrt oder gespeichert werden, ist diesbezüglich in der Regel der Abschluss einer Auftragsverarbeitervereinbarung mit dem Schulerhalter erforderlich. Ein entsprechendes Muster finden Sie in den Unterlagen zur DSGVO (Dokumentationspflichten des Arztes) auf unserer Homepage.

Was muss ich im Zusammenhang mit meinen Angestellten beachten?

Auch die von Ihnen verarbeiteten personenbezogenen Daten über Angestellte Ihrer Ordination (zB im Zusammenhang mit der Lohnabrechnung oder mit Arbeitszeitaufzeichnungen) unterliegen der DSGVO. Zudem sollten Mitarbeiter/innen über den richtigen Umgang mit (Patienten-)Daten informiert bzw. geschult werden sowie eine Datenschutzerklärung unterfertigen. Unter den Mustern zur DSGVO auf unserer Homepage stellen wir ein Muster für eine Zustimmungserklärung zur Verwendung von Daten der Dienstnehmer sowie zu den Regeln über die Handhabung der IT-Systeme zur Verfügung. Dieses deckt auch die Veröffentlichung von Fotos Ihrer Mitarbeiter auf der Homepage ab.

Darüber hinaus stellt die Wirtschaftskammer Österreich ein generisches Muster für eine Datenschutzerklärung des Dienstgebers (Ordinationsinhabers) gegenüber seinen Mitarbeitern/innen zur Einhaltung der Informationspflicht gemäß DSGVO zur Verfügung: https://www.wko.at/service/wirtschaftsrecht-gewerberecht/dsgvo-muster-datenschutzerklaerung-mitarbeiter.html