Checkliste DSGVO

Wichtige Hinweise:

Die Datenschutzgrundverordnung verlangt, dass sich jeder, der personenbezogene Daten verarbeitet, persönlich mit der Umsetzung der DSGVO in seinem Verantwortungsbereich auseinandersetzt.

Bitte beachten Sie ferner, dass es sich bei dieser Checkliste und den angeschlossenen Unterlagen um einen Leitfaden handelt, der rechtlich unverbindlich ist und nicht die inhaltliche Auseinandersetzung mit dem Datenschutzrecht ersetzt.

Einführung:

Die Datenschutzgrundverordnung (kurz: DSGVO) verlangt, dass Sie als niedergelassener Arzt dokumentieren, wie und warum Sie personenbezogene Daten verarbeiten, welche Sicherheitsmaßnahmen Sie zum Schutz dieser Daten ergriffen haben und wie Sie die Rechte der betroffenen Personen wahrnehmen. Zur Erfüllung dieser Pflichten stellt die Österreichische Ärztekammer gemeinsam mit den Landesärztekammern das beiliegende Dokument zur Verfügung, sodass Sie diese Dokumentationspflichten ohne großen Aufwand erfüllen können.

Bitte beachten Sie, dass die Dokumente lediglich eine Empfehlung darstellen und die Ärztekammer keine Haftung für die Vollständigkeit und Korrektheit der Dokumente übernimmt.

Wer ist der Verantwortliche, wer die betroffene Person und wer der Auftragsverarbeiter?

Sie als niedergelassener Arzt sind als „*Verantwortlicher*" im Sinne der DSGVO verantwortlich für die korrekte Verarbeitung von personenbezogenen Daten und die Einhaltung der datenschutzrechtlichen Regeln.

Wann immer Sie Daten einer natürlichen Person (eines Menschen) verarbeiten, handelt es sich bei dieser Person um die „*betroffene Person*".

Sollten Sie personenbezogene Daten nicht selbst, sondern durch einen Dritten in Erfüllung Ihrer Pflichten oder zu Zwecken, die Sie festlegen, verarbeiten lassen, handelt es sich bei diesem Dritten um einen sogenannten „*Auftragsverarbeiter*" (Beispiele für Auftragsverarbeiter finden Sie am Ende dieses Dokuments).

Was müssen Sie tun?

Das beiliegende Dokument deckt die typischen Pflichten eines niedergelassenen Arztes ab, Sie müssen daher lediglich die für Ihre Praxis spezifischen Punkte ergänzen. Sollten Sie sich nicht sicher sein, ob einzelne Datenanwendungen in der angegebenen Form bei Ihnen vorhanden sind oder nicht, lassen Sie diese bestehen. Eine Datenanwendung „zu viel" schadet nicht.

Sämtliche Punkte, die Sie bearbeiten müssen, finden Sie **[in eckigen Klammern, halbfett, gelb hinterlegt].** Die meisten Punkte, die Sie ergänzen müssen, sind selbsterklärend. Gehen Sie daher wie folgt vor:

1. Ergänzen Sie auf den Seiten 1 und 3 im Dokument „Dokumentationspflicht DSGVO" die jeweiligen Kontaktinformationen. Ob Sie einen Datenschutzbeauftragten benötigen, hängt vom Einzelfall ab, wobei **ein einzelner Arzt jedenfalls keinen Datenschutzbeauftragten benötigt**. In der Gruppenpraxis oder bei gemeinsamer Patientenverwaltung in einer Apparate- oder Ordinationsgemeinschaft hängt die Bestellung eines Datenschutzbeauftragten davon ab, ob umfangreiche Daten verarbeitet werden. Als zahlenmäßige Orientierung ab wann von einer umfangreichen Datenverarbeitung ausgegangen werden kann, erachtet die Österreichische Ärztekammer 5.000 verschiedene Patienten pro Kalenderjahr jedenfalls als relevant.

2. Auf den Seiten 5 bis 26 müssen jeweils zwei Punkte ergänzt werden:

   a. Beim Punkt „Verarbeitung durch Auftragsverarbeiter" benennen Sie bei jeder Datenanwendung den externen Dienstleister (mit Namen), der Daten für Sie verarbeitet. Beispiele hierfür sind E-Maildiensteanbieter oder auch IT-Supportunternehmen. Ihr IT-Techniker kann Ihnen bei diesem Punkt helfen. Sollten Sie die Daten nicht extern verarbeiten, kann dieser Punkt leer bleiben.
   b. Beim Punkt „Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen" müssen Sie – sofern möglich – allgemeine technische und organisatorische Maßnahmen beschreiben. Etwa: *„Buchhaltungsdaten werden in der Software XY verarbeitet, der Zugriff ist nur nach Eingabe eines Benutzernamens oder Passwortes möglich."* Die genauen Maßnahmen müssen Sie hier **nicht** angeben. Sollte es hier keine eigenen Maßnahmen geben, darf dieser Punkt auch „leer" bleiben. Ihr IT-Techniker kann Ihnen bei diesem Punkt helfen.

   Beachten Sie: Die Nummern im Feld „an Empfänger" bezieht sich auf die Liste von möglichen Empfängern auf Seite 4.

3. Auf den Seiten 27 bis 36 (III. Technische und organisatorische Maßnahmen) finden Sie einen Vorschlag für technische und organisatorische Maßnahmen. Die hier zu ergänzenden Punkte kann Ihnen Ihr IT-Techniker beantworten.

4. Ergänzen Sie in Punkt IV.1 (Seite 37) Ihre Auftragsverarbeiter (Beispiele für Auftragsverarbeiter finden Sie am Ende dieses Dokuments).

5. Senden Sie an jeden Auftragsverarbeiter einen Auftragsverarbeitervertrag. Ein Muster des Auftragsverarbeitervertrags finden Sie unter Punkt IV.2 (Seite 37).

   Für jeden Auftragsverarbeiter müssen Sie einen eigenen Vertrag erstellen (sofern Ihnen der Auftragsverarbeiter nicht ohnedies bereits einen solchen Auftragsverarbeitervertrag gesendet hat). In dem Vertragsmuster ergänzen Sie folgende Punkte:

a. Zu Punkt 1.1: Beschreiben Sie den Zweck, der Verarbeitung der Daten

b. Zu Punkt 1.2: Beschreiben Sie die Dauer der Verarbeitung

c. Zu Punkt 1.3: Beschreiben Sie die Datenkategorien. Etwa: Patientendaten, Daten zu Zeitaufzeichnungen, E-Mailkommunikation

d. Zu Punkt 1.4: Beschreiben Sie die Kategorien der betroffenen Personen. Etwa: Patienten, Lieferanten, Mitarbeiter

6. Übersendung von Gesundheitsdaten (z.B. Befunde, Arztbriefe, Rezepte, Untersuchungstermine, udgl.)

   Wir empfehlen, Gesundheitsdaten nicht mittels unverschlüsselter Kommunikation (etwa via E-Mail) zu versenden. Die Nutzung von Messenger-Diensten (dazu zählt – Stand 04/2019 – auch etwa WhatsApp) ist aufgrund einer datenschutzrechtswidrigen Übermittlung von Kontaktdaten durch die Applikation an Dritte unzulässig.

   Dies betrifft nicht nur die Arzt-Patienten-Kommunikation über Gesundheitsdaten, sondern auch den Versand an andere Ärzte bzw. Angehörige von Gesundheitsberufen.

   a. Für die **Arzt-Patienten-Kommunikation** ist neben der Übersendung von Gesundheitsdaten mittels normaler Briefpost die Übersendung auf elektronischem Wege nur zulässig, wenn entweder die Gesundheitsdaten verschlüsselt (zum Beispiel mit Passwort verschlüsselter Anhang) übersendet werden oder ein System zur sicheren Datenbereitstellung (etwa: eine dem Stand der Technik entsprechende Befundplattform) genutzt wird.

      Der unverschlüsselte Versand ist auch unzulässig, wenn der Patient eingewilligt hat. Diese Empfehlung basiert auf einer aktuellen Entscheidung der Datenschutzbehörde (DSB-D213.692/0001-DSB/2018 vom 16.11.2018).

   b. Für die **Kommunikation zwischen Ärzten und Ärzten und Angehörigen von anderen Gesundheitsberufen** ist der Versand von Gesundheitsdaten im Wege der etablierten Befundübermittlungssysteme datenschutzkonform.

      Eine Übermittlung von Patientendaten an andere Ärzte oder medizinische Einrichtungen, in deren Behandlung der Kranke steht, ist wie bisher gemäß § 51 Abs 2 Z 2 Ärztegesetz (siehe Anhang) nur zulässig, wenn der jeweilige Patient einwilligt. Die Einwilligung muss nicht schriftlich oder ausdrücklich erfolgen; sie sollte jedoch dokumentiert werden.

Legen Sie die anhand dieser Checkliste erstellten Dokumente ab und prüfen Sie diese regelmäßig auf Vollständigkeit und Korrektheit. Die Ärztekammern werden Sie regelmäßig über relevante datenschutzrechtliche Änderungen informieren.

Bitte beachten Sie, dass auch die Dokumente im Anhang lediglich eine Empfehlung darstellen und die Ärztekammern keine Haftung für die Vollständigkeit und Korrektheit der Dokumente übernimmt.

Beispiele für Auftragsverarbeiter und Verantwortliche

Auftragsverarbeiter:

- IT-Support Unternehmen, die Zugriff auf personenbezogene Daten haben
- Arztsoftwarehersteller, wenn diese Zugriff auf personenbezogene Daten haben
- E-Mailprovider
- Unternehmen, die Direktwerbung anbieten (etwa: E-Mailversand)
- Callcenter
- Online Terminvereinbarungen

Verantwortliche:

- Ärzte
- Krankenhäuser
- Apotheken
- Therapeuten
- Anbieter von Telefonleitungen
- Anbieter von Internetleitungen
- Post
- Rechtsanwälte
- Steuerberater
- Notare
- Behörden
- Banken
- Sozialversicherungsanstalt

Mit Verantwortlichen muss kein Auftragsverarbeitervertrag geschlossen werden.

Fragen im Zusammenhang mit der Datenschutzgrundverordnung:

1. **Was ist die Datenschutzgrundverordnung und für wen gilt sie?**

   Die Datenschutzgrundverordnung - Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung – kurz DSGVO - ist seit **27.4.2016** in Kraft. Die ursprüngliche Richtlinie aus dem Jahr 1995 (Richtlinie 1995/46/EG) musste in den einzelnen Mitgliedstaaten durch eigene Datenschutzgesetze umgesetzt werden. Obwohl die Datenschutzgrundverordnung nunmehr unmittelbar in jedem Mitgliedstaat gilt, haben die Mitgliedstaaten der EU dennoch die Möglichkeit, (eingeschränkt) Sonderregeln zu erlassen. Beispielsweise hat Deutschland Regeln festgelegt, ab wann ein Verantwortlicher einen Datenschutzbeauftragten benötigt.

   Die Regeln der Datenschutzgrundverordnung müssen seit dem 25.5.2018 angewendet werden.

2. **Für welche Art von Daten ist die DSGVO anwendbar?**

   Die DSGVO muss bei der Verarbeitung sämtlicher personenbezogener Daten beachtet werden, egal ob diese in Papierform oder automationsunterstützt (elektronisch) verarbeitet werden.

3. **Was ist ein Verantwortlicher?**

   Bei einem Verantwortlichen handelt es sich um jene Person, die personenbezogene Daten für gewisse Zwecke verarbeitet. Der Verantwortliche entscheidet, was mit den Daten passiert. Er ist der „Herr" über die Daten. Der Arzt, der gemäß § 51 Ärztegesetz Aufzeichnungen über jede zur Beratung oder Behandlung übernommene Person erfasst, ist ein Verantwortlicher im Sinne der Datenschutzgrundverordnung.

4. **Was ist ein Auftragsverarbeiter?**

   Der Auftragsverarbeiter verarbeitet personenbezogene Daten im Auftrag des Verantwortlichen. Das bedeutet, dass der Verantwortliche zwar über den Zweck der Verarbeitung die Entscheidung trifft, der Auftragsverarbeiter jedoch entscheidet, welche Mittel für die Verarbeitung eingesetzt werden.

   Beachten Sie: Auftragsverarbeiter (gerade große Unternehmen) wollen einen Auftragsverarbeitervertrag mit Ihnen abschließen, da diese sich ebenso einer Strafdrohung von 20 Millionen Euro oder 4% des Jahresumsatzes aussetzen. Viele Internetkonzerne verlangen diese Erklärungen bereits von ihren Nutzern.

5. **Wer ist ein Betroffener?**

   Der Betroffene ist derjenige, dessen personenbezogene Daten verarbeitet wer-

den. Es handelt sich dabei immer um eine natürliche Person (einen Menschen). Datenschutzrechtliche Betroffene sind nicht nur Patienten, sondern auch Mitarbeiter oder Lieferanten.

6. Benötige ich einen Datenschutzbeauftragten?

Der einzelne Arzt ist nicht verpflichtet, einen Datenschutzbeauftragten zu bestellen. Das Datenschutzrecht legt die Kriterien, ab welcher Praxisgröße ein Datenschutzbeauftragter zu bestellen ist, nicht klar dar, weshalb offen ist, ab welcher Praxisgröße der Verantwortliche einen Datenschutzbeauftragten bestellen muss.

Im Falle von ärztlichen Kooperationen, wie Gruppenpraxen und Primärversorgungseinrichtungen, aber auch im Falle der Anstellung eines Arztes in der Einzelordination, empfehlen wir, bei der Entscheidung über die Bestellung eines Datenschutzbeauftragten auf das Kriterium der Patientenzahlen pro Jahr abzustellen. Dies gilt auch für Ordinations- und Apparategemeinschaften, wenn die Patientenverwaltung gemeinsam erfolgt.

Sollten durchschnittlich mehr als 5.000 verschiedene Patienten pro Jahr betreut werden, empfehlen wir auf Basis der Kriterien der DSGVO die Bestellung eines Datenschutzbeauftragten.

Daraus folgt: Für Gruppenpraxen und Primärversorgungseinrichtungen empfehlen wir aufgrund der Annahme einer höheren Patientenzahl und des daraus folgenden Datenumfangs, einen Datenschutzbeauftragten zu bestellen.

Sollten Sie einen Datenschutzbeauftragten bestellt haben, müssen Sie dessen Kontaktdaten der Aufsichtsbehörde (Österreichische Datenschutzbehörde, Barichgasse 40-42, 1030 Wien, E-Mail: dsb@dsb.gv.at) melden.

7. Was ist eine Datenanwendung im Sinne der DSGVO?

Grundsätzlich dürfen personenbezogene Daten nur für einen gewissen Zweck erhoben und verarbeitet werden. Dabei kommt es insbesondere darauf an, dass der sogenannten „Datenminimierungspflicht" Rechnung getragen wird. Diese Pflicht sieht vor, dass nur so viele Daten verarbeitet werden dürfen, wie zum Erfüllen des jeweiligen Zwecks notwendig sind.

Eine „Datenanwendung" im Sinne der DSGVO hat nichts mit Technik zu tun. Eine Datenanwendung liegt vor, wenn der Verantwortliche personenbezogene Daten für einen gewissen Zweck verarbeitet.

8. Was ist ein Verzeichnis von Verarbeitungstätigkeiten und wofür benötige ich dieses?

Damit die Behörde prüfen kann, ob der Verantwortliche die Grundregeln der DSGVO einhält, muss dieser sämtliche Datenanwendungen dokumentieren. Dabei muss der Verantwortliche angeben, für welche Zweck dieser die Daten

verarbeitet, welche **Kategorien** von Betroffenen von der Verarbeitung betroffen sind, sowie welche Kategorien von Daten der Verantwortliche verarbeitet.

Dabei müssen Sie sämtliche Personengruppen, deren Daten Sie verarbeiten, bekanntgeben. So müssen Sie bei der Patientendokumentation auch die „Mitarbeiter" als Kategorien von Betroffene angeben, da in der Patientenakte vermerkt sein kann, welcher Mitarbeiter welche Leistung erbracht hat.

9. Benötige ich eine Datenschutzfolgenabschätzung und was ist das?

Eine Datenschutzfolgenabschätzung ist eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und die Zwecke der Verarbeitung samt einer Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf deren Zweck. Darüber hinaus muss der Verantwortliche eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen vornehmen und die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, sodass der Schutz der personenbezogenen Daten sichergestellt ist.

Aufgrund der Ausnahmeverordnung zur Pflicht zur Datenschutzfolgenabschätzung (vgl. BGBl. II Nr. 108/2018) trifft den einzelnen Arzt für die Patientenverwaltung und für die Honorarabrechnung keine Pflicht zur Durchführung einer Datenschutzfolgenabschätzung. Diese Ausnahme gilt nicht für Gruppenpraxen, Primärversorgungseinheiten, sonstige ärztliche Kooperationsformen (wie Ordinations- und Apparategemeinschaften) oder Einzelordinationen, in denen mehrere Ärzte beschäftigt sind, und damit eine erhöhte Patientenzahl (mehr als 5.000 verschiedene Patienten pro Jahr) verbunden ist.

Ein Muster für eine Datenschutzfolgenabschätzung finden Sie in der Anlage.

10. Was sind besondere Kategorien von Daten?

Dabei handelt es sich um personenbezogene 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.

Die Verarbeitung dieser Daten ist nur zulässig, wenn der Betroffene entweder in die Verarbeitung eingewilligt hat oder eine gesetzliche Verpflichtung (wie etwa in § 51 Ärztegesetz) die Verarbeitung zulässig macht.

11. Was ergibt sich aus § 51 Ärztegesetz?

(Auszug) § 51. (1) Der Arzt ist verpflichtet, Aufzeichnungen über jede zur Beratung oder Behandlung übernommene Person, insbesondere über den Zustand der Person bei Übernahme der Beratung oder Behandlung, die Vorgeschichte einer Erkrankung, die Diagnose, den Krankheitsverlauf sowie über Art und Umfang der beratenden, diagnostischen oder therapeutischen Leistungen einschließlich der Anwendung von

Arzneispezialitäten und der zur Identifizierung dieser Arzneispezialitäten und der jeweiligen Chargen im Sinne des § 26 Abs. 8 des Arzneimittelgesetzes, BGBl. Nr. 185/1983, erforderlichen Daten zu führen und hierüber der beratenen oder behandelten oder zu ihrer gesetzlichen Vertretung befugten Person alle Auskünfte zu erteilen. In Fällen eines Verdachts im Sinne des § 54 Abs. 4 sind Aufzeichnungen über die den Verdacht begründenden Wahrnehmungen zu führen. Den gemäß § 54 Abs. 5 oder 6 verständigten Behörden oder öffentlichen Dienststellen ist hierüber Auskunft zu erteilen. Der Arzt ist verpflichtet, dem Patienten Einsicht in die Dokumentation zu gewähren oder gegen Kostenersatz die Herstellung von Abschriften zu ermöglichen.

(2) Ärzte sind zur automationsunterstützten Ermittlung und Verarbeitung personenbezogener Daten gemäß Abs. 1 sowie zur Übermittlung dieser Daten
1.an die Sozialversicherungsträger und Krankenfürsorgeanstalten in dem Umfang, als er für den Empfänger zur Wahrnehmung der ihm übertragenen Aufgaben eine wesentliche Voraussetzung bildet, sowie
2.an andere Ärzte oder medizinische Einrichtungen, in deren Behandlung der Kranke steht, mit Einwilligung des Kranken berechtigt.

12. Ist die Auskunft wirklich kostenlos zu erteilen?

Ja. Die DSGVO sieht vor, dass der Betroffene kostenlos eine Kopie sämtlicher beim Verantwortlichen gespeicherten Daten verlangen darf.

13. Was ist mit einer Videoüberwachung?

Auch diese muss im Rahmen des Verzeichnisses der Verarbeitungstätigkeiten dokumentiert werden. Dieser Leitfaden bildet diese jedoch nicht ab.

14. Was passiert, wenn ich die Regeln der Datenschutzgrundverordnung nicht einhalte?

Die Strafdrohung der Datenschutzgrundverordnung beträgt bis zu EUR 20 Mio. oder 4% des weltweiten Jahresumsatzes.

Auch wenn diese Strafen primär zur Abschreckung von Datenschutzverstößen bei multinationalen Unternehmen gedacht sind, werden die Strafen – in Zukunft – bei den einzelnen Verantwortlichen empfindlicher sein als in der Vergangenheit.

15. Wenn ich die vorliegenden Dokumente ausgefüllt habe, habe ich dann alle Pflichten erfüllt?

Die Datenschutzgrundverordnung sieht vor, dass die hier vorliegenden Dokumente aktuell gehalten werden müssen. Das bedeutet, dass die Dokumente an die tatsächlichen Gegebenheiten regelmäßig angepasst werden müssen.

Darüber hinaus gibt es noch viele Unklarheiten im Zusammenhang mit der Datenschutzgrundverordnung. Wir werden Sie laufend über Neuerungen informieren, in diesem Fall ist möglicherweise ein Anpassungsbedarf bei den einzelnen Dokumenten notwendig.

Daneben besteht natürlich die Pflicht, sich selbst laufend mit aktuellen Entwicklungen im Datenschutzrecht zu informieren.