Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO

Gemäß Art. 5 Abs. 2 DS-GVO muss der für die Verarbeitung Verantwortliche die gesetzlich niedergelegten Grundsätze für die Datenverarbeitung einhalten und dies auch nachweisen können. Hieraus folgt eine umfassende Rechenschaftspflicht (engl.: „Accountability"), womit gegenüber dem bisherigen Recht zahlreiche zusätzliche Dokumentations- und Nachweispflichten entstehen. Die Accountability wird zukünftig einen gewichtigen Teil der betrieblichen Compliance darstellen.

Die Rechenschaftspflicht umfasst zunächst sämtliche Grundsätze des Art. 5 Abs. 1 DS-GVO:
>> „Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz" (lit. a)
>> „Zweckbindung" (lit. b)
>> „Datenminimierung" (lit. c)
>> „Richtigkeit" (lit. d)
>> „Speicherbegrenzung" (lit. e)
>> „Integrität und Vertraulichkeit" (lit. f)

Art. 5 DS-GVO wird ergänzt durch Art. 24 Abs. 1dDS-GVO, wonach der Verantwortliche unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen umsetzt, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung rechtmäßig erfolgt. Diese Maßnahmen werden erforderlichenfalls überprüft und aktualisiert (Quelle: https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_9.pdf).

Der Nachweis, dass die Grundsätze nach Art. 5 Abs. 1 DSGVO eingehalten werden, ist auf Anforderung gegenüber der zuständigen Datenschutzaufsichtsbehörde (in Bayern: Bayer. Landesamt für Datenschutzaufsicht (LDA) zu erbringen (www.lda.bayern.de).

Damit sich das LDA ein Bild von Ihrer Praxis machen kann, ist es empfehlenswert zunächst die Praxis verbal zu beschreiben, ggf. kann hier auch auf bereits vorhandene Unterlagen verwiesen werden:

- Personelle und technische Ausstattung (Hard- und Software mit der personenbezogene Daten verarbeitet werden (auch med. Geräte), WLAN, technische Anbindung von Zweigpraxen, Heimarbeitsplätzen u. ä.)
- Lage der Praxis
- Art der Tätigkeiten, die die Praxisinhaber ausüben und für die Technik der Praxis genutzt wird (z. B. Patientenbehandlung, Betriebsarzt, gutachterliche Tätigkeit)
- Einsatz von Kommunikationsmitteln (Brief, Fax, Telefon, E-Mail, Messenger-Dienste und sonstige Apps)
- Telemedizinische Dienste
- Bestellpflicht betrieblicher DSB ja/nein; Begründung
- Pflicht zur Datenschutzfolgeabschätzung ja/nein
- bestehende Auftragsverhältnisse
- Rechtsgrundlagen der Datenverarbeitung
  Patientendaten:
  Art. 6 Abs. 1 lit. b, ggf. auch lit. a und lit. f, 9 Abs. 2 lit h, ggf. lit a, c und f DSGVO, § 22 Abs. 1 BDSG
  Mitarbeiterdaten:
  Art. 6 Abs. 1 lit. b und f, 9 lit. b, f, § 26 BDSG

Beschreibung der Maßnahmen zur Umsetzung des Schutzes personenbezogener Daten und der Betroffenenrechte (Empfehlung: orientieren Sie sich dabei z. B. am Selbst-Check für Arzt-/Zahnarztpraxen der ULD, https://www.datenschutzzentrum.de/uploads/medizin/arztpraxis/SelbstcheckArztpraxisDSGVO2018-05-23.pdf), den wir nachstehend aufbereitet haben. Anstelle eines Ankreuzens (wie als Selbst-Check vorgesehen) erfordert die Rechenschaftspflicht eine konkrete Beschreibung der tatsächlich getroffenen Maßnahmen.

Empfangsbereich bzw. Anmeldung
Patientendaten sind im Empfangsbereich einer Arzt- bzw. Zahnarztpraxis vor neugierigen Ohren, Augen und Händen zu schützen.

Ist sichergestellt, dass Besucher die Praxis nicht unbemerkt betreten können?

Können Patienten ihre Anliegen schildern, ohne dass neugierige Ohren mithören (Diskretionszone, Einzelabfertigung, Verwendung von Anamnesebögen, …)?

Wird dem Patienten erklärt, wofür eine Telefonnummer oder die E-Mail-Adresse benötigt wird, und dass diese Angaben grundsätzlich freiwillig sind?

Kann das Personal Telefongespräche mit sensiblen personenbezogenen Inhalten führen, ohne dass Unbefugte zuhören?

Sind Patientenunterlagen wie Karteikarten und Terminkalender vor dem Zugriff und der Einsicht durch Unbefugte geschützt?

Sind Telefaxgeräte und Bildschirme so aufgestellt, dass sie nicht von Unbefugten eingesehen werden können?

Ist der Empfang deutlich vom Wartebereich getrennt („Keine Wartestühle für Patienten am Empfang.“)?

Achtung! Wird eine Online-Anmeldung bzw. Online-Termin-Vereinbarung angeboten, sind die im Abschnitt „Informationstechnik“ aufgezeigten Fragen zur Datensicherheit zu beachten.

Wartebereich

Ist der Wartebereich vom Empfang und Behandlungsbereich so getrennt, dass wartende Patienten nicht unbefugt Kenntnis von Patientendaten erhalten? Ist z. B. die Tür zum Wartezimmer normalerweise geschlossen?

Ist der Wartebereich derart gestaltet, dass wartende Patienten nicht hören können, was am Empfang besprochen wird?

Achtung! Keine Wartestühle vor den Behandlungsräumen, wenn Arzt-Patienten-Gespräche zu hören oder Behandlungen bei geöffneter Tür zu sehen sind. Patienten dürfen mit ihrem Namen aufgerufen werden.

Behandlungsbereich
Ärztliche Behandlungen müssen diskret, hinter verschlossenen Türen und in gesicherten Behandlungsbereichen erfolgen. Es darf keine unbefugten Zuschauer oder Zuhörer geben; Patientenunterlagen sind in den Behandlungsräumen vor einem unbefugten Zugriff zu sichern.

Ist sichergestellt, dass, wenn sich Patienten in Behandlungsbereichen unbeaufsichtigt aufhalten, Patientenunterlagen, wie Karteikarten, gegen unbefugten Zugriff geschützt sind?

Sind Patientenunterlagen in den Behandlungsräumen auch gegen eine zufällige unbefugte Kenntnisnahme geschützt (Achtung, Patienten können lesen, ein kurzer Blick kann reichen!)?

Ist sichergestellt, dass Patienten in den Behandlungsbereichen keinen Zugang zu ungesicherten Praxisrechnern haben?

Sind Behandlungsräume so gestaltet, dass bei Untersuchungen, Behandlungen und vertraulichen Arzt-Patienten-Gesprächen neugierige Augen und Ohren ausgeschlossen werden?

Sind z. B. die Behandlungsräume ausreichend schallisoliert, so dass Unbefugte nicht „vor der Tür“ mithören können?

Wird z. B. auch sichergestellt, dass Behandlungen und Gespräche grundsätzlich nicht in Bereichen erfolgen, die nur durch einen Vorhang geschützt sind, wenn Unbefugte mithören könnten?

Wird darauf geachtet, dass während einer Behandlung oder eines Gesprächs Türen geschlossen bleiben, wenn nicht anderweitig ausgeschlossen werden kann, dass Unbefugte ansonsten „Einblick erhalten“ würden? Auch wenn das Praxispersonal Behandlungsräume betritt oder verlässt, müssen neugierige Ohren und Augen ausgesperrt bleiben!

Werden in Behandlungsbereichen vertrauliche Telefonate nur geführt, wenn Unbefugte nicht mithören?

Wird von einem Patienten nur dann ein Foto gemacht, wenn dieses Foto für die Behandlung erforderlich ist und der Patient zuvor gefragt wird, ob er damit einverstanden ist?

Achtung! Grundsätzlich haben Patienten Anspruch darauf, nicht im Beisein anderer Patienten behandelt zu werden.

Praxisverwaltung

Fehlendes Wissen, fehlende technische und organisatorische Maßnahmen, aber auch mangelnde Sensibilität im Umgang mit Patientendaten und der tägliche Arbeitsstress können das Patientengeheimnis gefährden.

Sind Mitarbeiterinnen und Mitarbeiter über ihre Befugnisse und gesetzlichen Pflichten bei der Wahrung der Schweigepflicht ausreichend informiert?

Sind schriftliche Patientenunterlagen, wie z. B. Karteikarten und Patientenakten, vor dem Zugriff und der Einsicht durch Unbefugte geschützt?

Sind abschließbare Aktenschränke vorhanden? Werden diese bei Dienstschluss verschlossen?

Ist die Aufbewahrung von „alten Akten“ sicher organisiert (kein „offener Keller“)?

Sind die Praxisräume, in denen sich Patientendaten/Abrechnungsdaten befinden, ausreichend gegen Einbruch geschützt?

Ist sichergestellt, dass das Reinigungspersonal keinen Zugang zu Patientendaten hat?

Werden in der Praxis ausschließlich Shredder für die Aktenvernichtung entsprechend der DIN 66399-1/2 der Partikelgröße P-5 (vormals Sicherheitsstufe 4) verwendet?

Informationstechnik

Ärzte unterliegen vielfältigen Dokumentationspflichten. Die Patientenverwaltung und die Abrechnung mit Kassen und Privatversicherten erfordern viel „Schreibkram". Moderne Informationstechnik (IT) erleichtert die Arbeit. Auch in der Diagnostik ist die IT kaum noch zu ersetzen. Mit einer automatisierten Datenverarbeitung steigen jedoch nicht nur die Möglichkeiten, sondern auch die Risiken für die Datenverarbeitung.

Wird sichergestellt, dass für die Verarbeitung von Patientendaten ausschließlich autorisierte Hardware, also keine privaten Notebooks oder Smartphones, verwendet wird?

Werden in der Praxis ausschließlich autorisierte Verfahren und Programme für die Verarbeitung von Patientendaten eingesetzt, die in einem Verzeichnis der Verarbeitungstätigkeiten (Art. 30 DSGVO) erfasst sind?

Sind Computer mit Patientendaten, die mit dem Internet verbunden sind, tatsächlich ausreichend geschützt (gewartete „Firewall", KV-Safenet)?

Sind auf den Computern Virenschutzprogramme installiert, und werden diese täglich aktualisiert?

Existiert ein Notfall-Handlungskonzept für den Fall eines Sicherheitsvorfalls (z. B. Virenbefall, Datenverlust) oder eines Datenschutzvorfalls (z. B. Diebstahl))?

Sind ausreichende Sicherheitsvorkehrungen getroffen worden, wenn WLAN verwendet wird (Verschlüsselung (WPA2), starkes Passwort für den WLAN-Router, Deaktivierung der Übertragung des Funknetznamens (SSID) im Router, …)?

Wird eine Praxis-Software verwendet, die Patientendaten verschlüsselt speichert, soweit dies möglich ist?

Werden für die Speicherung von Patientendaten Verfahren genutzt, die die Möglichkeit einer Löschung dieser Daten vorsehen?

Wird regelmäßig eine verschlüsselte Sicherungskopie der Daten gefertigt (möglichst jeden Tag, mindestens einmal die Woche)?

Werden diese Sicherungskopien ausreichend gegen Diebstahl, Brand etc. geschützt?

Wird insbesondere in großen Praxen durch ein Berechtigungskonzept sicher-gestellt, dass Ärzte und Praxismitarbeiter nur auf die für ihre Aufgabe erforderlichen Daten zugreifen können (eingeschränktes Benutzerprofil)?

Werden lesende und ändernde Zugriffe auf Patientendaten protokolliert?

Sind Drucker und Faxgeräte vor unbefugtem Zugriff geschützt?

Ist der Zugang zu den eingesetzten Computern geschützt (z. B. durch ein Passwort)?

Wenn Passwörter verwendet werden: Entspricht das Passwort dem aktuellen Sicherheitsstandard (mindestens 8 Stellen, bestehend aus Buchstaben, Zahlen und Sonderzeichen)? Ist es technisch vorgesehen, dass das Passwort nach einer gewissen Zeit geändert werden muss?

Werden auf den Bildschirmen (insbesondere in den Behandlungsräumen) Bildschirmschoner genutzt, die sich erst nach Passworteingabe oder durch ein Sicherheitstoken deaktivieren?

Sind die Bildschirme so aufgestellt, dass diese nicht durch Unbefugte eingesehen werden können?

Achtung!
Bei einer Administration der IT durch ein externes Unternehmen kann ein Zugriff auf Patientendaten durch den Dienstleister nicht ausgeschlossen werden. Rechte und Pflichten des externen Dienstleisters müssen in einem schriftlichen Vertrag definiert werden (Art. 28 DSGVO). Eine Fernwartung der IT durch ein externes Unternehmen darf nur dann vorgenommen werden, wenn diese nur nach Freigabe durch die Praxis erfolgt, die Fernwartung protokolliert und von einem Praxismitarbeiter kontrolliert wird.

Datenübermittlung – Datenaustausch
Patientendaten werden weitergegeben, ausgetauscht und offenbart. Eine Übermittlung von Patientendaten ist allerdings nur zulässig, wenn eine gesetzliche Befugnis oder die Einwilligung des Patienten („Schweigepflichtentbindungserklärung“) vorliegt. Die Verantwortung für die Zulässigkeit einer Übermittlung von Patientendaten trägt in der Regel der Arzt bzw. die Arztpraxis.

Ist sichergestellt, dass bei Zweifeln bzgl. der Zulässigkeit einer Übermittlung von Patientendaten vorab eine rechtliche Klärung erfolgt (z. B. über die Ärzte-/ Zahnärztekammer oder das LDA)?

Werden (geprüfte) Mustererklärungen zur Entbindung von der ärztlichen Schweigepflicht verwendet, in denen Patienten ausreichend erklärt wird, welche Daten für welche Zwecke an welche Empfänger weitergegeben werden? (Unter www.datenschutzzentrum.de/artikel/879-.html hat das ULD in einem Informationsbeitrag wichtige Hinweise und ein Muster einer Schweigepflichtentbindungserklärung veröffentlicht.)

Wird bei jeder Übermittlung von Patientendaten in der Patientendokumentation dokumentiert, welcher Empfänger welche Daten erhalten hat?

Wird darauf geachtet, dass bei der Übermittlung von Patientendaten die Empfänger nicht mehr Informationen erhalten, als sie zur Erfüllung ihrer spezifischen Aufgaben benötigen?

Wird sichergestellt, dass bei Anfragen von Dritten, z. B. privaten Versicherern geprüft wird, ob die geforderten Auskünfte, Berichte oder Bescheinigungen dem Patienten zur Weiterleitung ausgehändigt werden können?

Werden Patienten über mit- und nachbehandelnde Ärzte (auch Laborärzte) informiert und wird sich vergewissert, dass die Patienten keine Einwände gegen deren Einbeziehung und deren Unterrichtung, z. B. über Behandlungsergebnisse, haben?

Wird vor der Beauftragung einer privatärztlichen Verrechnungsstelle die schriftliche Einwilligung des Patienten eingeholt? Dies ist jedenfalls dann erforderlich, wenn die Honorarforderung an die Verrechnungsstelle abgetreten werden soll.

Erhalten Angehörige von Patienten grundsätzlich nur dann Auskunft, wenn der Patient sich hiermit (möglichst schriftlich) einverstanden erklärt hat?

Werden für die Übermittlung von Patientendaten sichere Übermittlungswege genutzt? Unverschlüsselte E-Mails sind unsicher und damit für die Übermittlung von Patientendaten grundsätzlich ebenso wenig zu empfehlen wie die Nutzung sozialer Medien wie Facebook, Instagram oder WhatsApp. Auch wenn der Patient einen unsicheren Übermittlungsweg wählt oder wünscht, verbleibt die datenschutzrechtliche Verantwortung bei dem Arzt bzw. der Arztpraxis (vgl. auch https://www.lda.bayern.de/media/baylda_report_07.pdf, Punkt 9.6).

Bei Telefon und Fax muss man sich davon überzeugen, dass die sensiblen Daten nur dem berechtigten Empfänger zur Kenntnis gelangen.

Der betriebliche Datenschutzbeauftragte (bDSB)
Die DSGVO bzw. das (neue) BDSG sehen vor, dass Arzt- und Zahnarztpraxen ab dem 25. Mai 2018 einen bDSB benennen müssen, wenn mindestens 20 Personen mit der automatisierten Verarbeitung von Patientendaten beschäftigt sind (§ 38 Abs. 1 BDSG).

Hinweis:
Der Bundestag hat am 27. Juni 2019 das sog. Zweite Datenschutz-Anpassungs- und Umsetzungsgesetz EU beschlossen.
Dies betrifft unter anderem die Regelung zur Benennungspflicht eines Datenschutzbeauftragten. Hierbei werden kleine Praxen künftig entlastet. Der Gesetzgeber hat die Pflicht, einen betrieblichen Datenschutzbeauftragten zu benennen, von zehn Mitarbeiter, die ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind, auf zwanzig erhöht (§ 38 Abs. 1 Satz 1 BDSG).
Der Bundesrat hat am 20. September 2019 diesem Gesetz zugestimmt und dieses wurde auch im Bundesgesetzblatt veröffentlicht.

Zum bDSB darf benannt werden, wer die zur Erfüllung seiner Aufgaben erforderliche berufliche Qualifikation, Fachwissen und Fähigkeit besitzt (Art. 37 Abs. 5 DSGVO).

Praxisleiter, Personalchef und IT-Leiter dürfen grundsätzlich nicht zum bDSB benannt werden („Interessenskonflikt der Aufgaben“). Eine Interessenskonflikt kann auch bei der Bestellung von Praxismanagern/-innen und Ehegatten/-innen bestehen.

Es besteht die Möglichkeit, einen externen bDSB zu benennen.

Der bDSB unterrichtet und berät das Praxisteam in datenschutzrechtlichen Fragen.

Der bDSB überwacht die Einhaltung datenschutzrechtlicher Vorschriften.

Dem bDSB ist das Verzeichnis der Verarbeitungstätigkeiten („Bestandsaufnahme der Verarbeitungsvorgänge“) nach Art 30 DSGVO zur Verfügung zu stellen.

Der bDSB überwacht die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme.

Der bDSB berät und unterstützt bei der Durchführung der Datenschutz-Folgenabschätzung und überwacht ihre Durchführung.

Der bDSB informiert, sensibilisiert und schult das gesamte Praxisteam in datenschutzrechtlichen Fragen.

Der bDSB wirkt bei der Erstellung eines Datenschutzkonzepts für die Praxis mit.

Der bDSB prüft die Einhaltung datenschutzrechtlicher Vorschriften mit Hilfe dieses Selbst-Checks.

Der bDSB hat ein Recht auf Fortbildung, genießt einen besonderen Kündigungsschutz und ist bei der Erfüllung seiner Aufgaben weisungsfrei.

Wurden die Kontaktdaten des bDSB veröffentlicht und der Aufsichtsbehörde mitgeteilt?

Achtung!
Wird entgegen der gesetzlichen Pflicht kein Datenschutzbeauftragter bestellt, droht eine Geldbuße in Höhe von bis zu 10.000.000 Euro (Art 83 Abs. 4 DSGVO).

Informationspflicht bei Datenschutzverstößen
Das Bayerische Landesamt für Datenschutzaufsicht (www.lda.bayern.de) als zuständige Aufsichtsbehörde und die betroffenen Patienten müssen bei einer Datenpanne u. U. informiert werden (Art. 33, 34 DSGVO).

Ist bekannt, wann, in welcher Zeit und wie das LDA und die Betroffenen im Fall einer Datenpanne zu unterrichten sind?

Achtung!
Wird die Aufsichtsbehörde über eine Datenpanne unterrichtet, können die mitgeteilten Informationen nicht mehr für die Durchführung eines Verfahrens nach dem Gesetz über Ordnungswidrigkeiten verwendet werden. Die Aufsichtsbehörde berät bei der Aufklärung der Datenpanne und unterstützt bei der Suche nach Sicherungsmaßnahmen.

Patientenrechte
Der Gesetzgeber schützt das Patientengeheimnis und er hat Patientenrechte definiert. Patienten können Akteneinsicht oder Auskunft verlangen. U. U. besteht auch ein Anspruch auf Korrektur und Löschung von Daten. Auch die Möglichkeit einer Gegendarstellung hat der Gesetzgeber für Patienten vorgesehen. Zudem sieht die DSGVO umfangreiche Informationspflichten vor.

Ist das Praxispersonal ausreichend über die Rechte von Patienten (Akteneinsicht, Aushändigung von Kopien, Auskunft, Korrektur unrichtiger Daten, Löschung von Daten etc.) informiert?

Ist bekannt, dass auch Erben und Angehörige von verstorbenen Patienten u. U. ein Recht auf Akteneinsicht haben (§ 630g Bürgerliches Gesetzbuch – BGB)?

Ist das Praxispersonal darauf vorbereitet, was zu veranlassen ist, wenn ein Patient z. B. Akteneinsicht beantragt und/oder Kopien aus der Patientenakte verlangt?

Ist bekannt, wann eine Akteneinsicht oder Auskunft verweigert werden darf bzw. muss?

Werden Patienten Informationen darüber zur Verfügung gestellt,
- zu welchem Zweck und auf welcher Rechtsgrundlage Daten erhoben werden,
- warum die Speicherung von Patientendaten erforderlich ist,
- wie lange Patientendaten gespeichert werden,
- gegebenenfalls, ob Patientendaten von Dritten bezogen wurden und welche Daten das sind,
- an welche Empfänger Daten u.U. übermittelt werden,
- ob Daten auch ins Ausland übermittelt werden,
- dass man sich bei dem LDA als zuständige Aufsichtsbehörde beschweren darf?

Denkbar ist ein Informationsflyer, der z. B. für weitergehende Informationen auf eine Darstellung auf der Homepage verweist.

Ist bekannt, dass Patienten – soweit sie es verlangen – darüber Auskunft zu geben ist, an welche Stellen welche Patientendaten zu welchem Zweck übermittelt wurden (Art. 15 DSGVO)?

Ist bekannt, dass Patientenunterlagen nur solange gespeichert werden dürfen, wie dies zur Aufgabenerfüllung erforderlich ist und danach, soweit einer Löschung gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen (z. B. nach der jeweiligen Berufsordnung der Ärztekammer und der Zahnärztekammer) entgegenstehen, gesperrt (Einschränkung der Verarbeitung, Art. 18 DSGVO) werden müssen?

Outsourcing/Beauftragung von Dienstleistern

Bei der Beauftragung eines externen Dienstleisters (Auftragnehmer), z. B. mit der Administration der IT oder der Aktenvernichtung kann oftmals ein Zugriff auf Patientendaten durch den Auftragnehmer nicht vollständig ausgeschlossen werden. In einem sogenannten Auftragsdatenverarbeitungsvertrag müssen insbesondere Umfang, Art und Weise der Dienstleistung, Rechte und Pflichten von Auftraggeber und Auftragnehmer sowie die erforderlichen technischen und organisatorischen Maßnahmen fixiert werden (Art. 28 DSGVO).

Wurden bestehende Auftragsdatenverarbeitungsverträge auf die ab dem 25. Mai 2018 geltenden Vorschriften der DS-GVO angepasst?

Ist bekannt, dass sowohl die Arztpraxis als Auftraggeber, als auch der Dienstleister als Auftragnehmer die Verantwortung für die Einhaltung datenschutzrechtliche Vorschriften tragen?

Ist bekannt, dass der Dienstleister als Auftragnehmer nach § 203 Abs. 4 Strafgesetzbuch (StGB) einer strafrechtlich sanktionierten Verschwiegenheitspflicht unterliegt und wurde dieser entsprechend verpflichtet?

Erfolgte die Auswahl der Auftragnehmer unter besonderer Berücksichtigung der Eignung und der von diesen getroffenen technischen und organisatorischen Maßnahmen zur Datensicherheit?

Enthält der Vertrag u. a. Festlegungen über Umfang, Art und Zweck der vorgesehenen Datenverarbeitung, über die vom Auftragnehmer zu treffenden Sicherheitsvorkehrungen, über Berichtigung, Löschung und Sperrung bzw. die Rückgabe von Daten und über die Kontroll- und Weisungsrechte des Auftraggebers?

Ist bekannt, dass sich der Auftraggeber vor Beginn und sodann regelmäßig beim Auftragnehmer von der Einhaltung der vereinbarten Sicherheitsvorkehrungen überzeugen muss?

Möglichkeiten einer Videoüberwachung in der Praxis

Eingangs-, Empfangs-, Warte- und Behandlungsbereiche einer Arzt- bzw. Zahnarztpraxis sind im Sinne des Gesetzes öffentlich zugängliche Räume. Die Beobachtung dieser Bereiche mit optisch-elektronischen Einrichtungen (Videoüberwachung) ist nur unter ganz besonderen Voraussetzungen zulässig. Nach Einschätzung der Datenschutzaufsichtsbehörden ist dies in Arzt- bzw. Zahnarztpraxen aus folgenden Gründen häufig nicht der Fall:

Es fehlt in der Regel an einem ausreichenden Zweck für die Videoüberwachung.

Die Videoüberwachung ist regelmäßig nicht erforderlich.

Beobachtung von Patienten und/oder Mitarbeitern ist nicht verhältnismäßig. Umfangreiche Informationen und eine bundesweit abgestimmte Orientierungshilfe „Videoüberwachung durch nicht-öffentliche Stellen“ stellt das ULD zur Verfügung unter www.datenschutzzentrum.de/plugin/tag/video.

Die Datenschutzfolgenabschätzung (DSFA) nach Art. 35 DS-GVO
Die DSFA ist ein Instrument zur Beschreibung, Bewertung und Eindämmung von Risiken, die durch die Verarbeitung ihrer Daten für die Patienten entstehen. Eine DSFA ist durchzuführen, wenn durch eine umfangreiche Verarbeitung von Gesundheitsdaten ein „hohes Risiko“ für die Rechte der Patienten besteht.

- Ist festgelegt, wer die DSFA durchführt (Festlegung eines DSFA-Team unter Beteiligung des betrieblichen Datenschutzbeauftragten)?
- Wurde geprüft und festgestellt, für welche Verarbeitungsvorgänge eine DSFA erfolgen muss (Risikoeinschätzung)?
- Ist bekannt, wie eine DSFA durchzuführen ist?
- Ist bekannt, dass eine DSFA kein einmaliger Vorgang ist, sondern zu überprüfen ist, wenn neue Risiken für die Datenverarbeitung entstehen bzw. erkannt werden?
- Wurden die Prüfung und Durchführung der DSFA sowie die getroffenen Sicherungsmaßnahmen dokumentiert? Die Ärztekammern, aber auch das ULD werden in Kürze Informationen, Anleitungen und Beispiele für eine DSFA zur Verfügung stellen.

Folgen einer Verletzung des Patientengeheimnisses

- Wer als Arzt, Zahnarzt oder Mitarbeiter einer Arzt-/Zahnarztpraxis unbefugt Patientendaten offenbart, dem droht eine Geldstrafe oder eine Freiheitsstrafe bis zu zwei Jahren (§ 203 Abs. 1 Nr. 1 Strafgesetzbuch – StGB). Auch Dienstleister, die im Auftrag einer Praxis Patientendaten verarbeiten, unterliegen dieser strafrechtlich sanktionierten Verschwiegenheitspflicht.
- Ein datenschutzrechtlicher Verstoß kann als Ordnungswidrigkeit mit einer Geldbuße bis zu 20.000.000 Euro oder 4 % des Jahresumsatzes geahndet werden (Art. 83 DSGVO).
- Bei einer Datenpanne muss die Praxis die Aufsichtsbehörde und jeden betroffenen Patienten unterrichten (Art. 33, 34 DSGVO).

Mitgeltende Dokumente und Unterlagen:
Verzeichnis der Verarbeitungstätigkeit
Patienteninformation nach Art. 13 DSGVO
Sonstige