**[Bearbeitungshinweis:**

**Praktisch jede verantwortliche Stelle (Praxis) ist gem. Art. 30 DSGVO verpflichtet, ein Verzeichnis von Verarbeitungstätigkeiten zu führen. Verwenden Sie diese Vorlage, um ein solches Verzeichnis für Ihre Praxis zu erstellen.**

**Diese Vorlage ist in zwei Teile gegliedert. Das Vorblatt mit den Stammdaten, die Kategorien der Betroffenen Daten, der Kategorien der Empfänger und die Liste mit den Auftragsverarbeitern.**

**Anschließend folgen die einzelnen Verfahren, angeführt von der Übersicht über die einzelnen Verfahren.**

**Gehen Sie wie folgt vor:**

1. **Passen Sie die Stammdaten (gelb markierte Stellen) auf Ihre Praxis an**
2. **Überprüfen Sie, ob bei den Kategorien der verarbeiteten Daten alle angegebenen Daten bei Ihnen in der Praxis verarbeitet werden oder ob davon welche gestrichen werden müssen. Streichen Sie ggf. überflüssige Daten.**
3. **Prüfen Sie, ob es ggf. Kategorien von Daten gibt, die noch nicht aufgeführt sind und ergänzen Sie diese entsprechend.**
4. **Verfahren Sie ebenso mit den Kategorien der Empfänger von Daten.**
5. **Tragen Sie alle Auftragsverarbeiter in die Liste für die Auftragsverarbeiter ein.**
6. **Gehen Sie anschließend alle einzelnen Verarbeitungstätigkeiten (Verfahren) durch und überprüfen Sie, ob diese bei Ihnen zu Anwendung kommen. Überprüfen Sie anschließend, ob es ggf. weitere Verarbeitungstätigkeiten in Ihrer Praxis gibt, die noch nicht aufgeführt sind und ergänzen Sie diese entsprechend.**
7. **Überprüfen Sie die einzelnen Verarbeitungstätigkeiten jeweils inhaltlich. Gehen Sie diese Punkt für Punkt durch und passen sie jeweils an, wenn dies nötig ist.**
8. **Passen Sie die Übersicht über die in Ihrer Praxis angewandten Verfahren an.**
9. **Löschen Sie ganz am Ende bitten den gesamten Bearbeitungshinweis.**

**Erläuterung zum Format der Verarbeitungstätigkeiten:**

**[Achtung: Die folgende Tabelle ist NUR die Erläuterung. Bitte nutzen Sie für das Verfahrensverzeichnis Ihrer Praxis ausschließlich die im zweiten Abschnitt befindlichen Tabellen.]**

|  |  |
| --- | --- |
| Name der Verarbeitungstätigkeit | |
| **Verantwortlicher**  **Ansprechpartner:** | Nennen Sie hier die Person, welche für diese Verarbeitungstätigkeit zuständig ist. Wenn Sie sich nicht sicher sind, dann geben Sie hier einfach an: Die Praxisleitung |
| **Angelegt:**  **Letzte Änderung:** | 15.05.2018 (Datum an dem Sie dieses Verfahren angelegt haben)  15.05.2018 (Datum an dem Sie dieses Verfahren zuletzt geändert haben)  (Die Daten werden am Anfang gleich sein |
| **Auftragnehmer** | Werden im Rahmen der Verarbeitungstätigkeit Auftragsverarbeiter nach § 28 DSGVO tätig (z.B. freie Mitarbeiter) sollten diese hier genannt werden. Ansonsten können Sie einfach schreiben: Keine, da nur intern |
| **Beschreibung** | Dies ist eine allgemeine Beschreibung der Verarbeitungstätigkeit. |
| **Zwecke der  Verarbeitung** | Hier sollten alle Zwecke der Verarbeitungstätigkeit genannt werden. Geben Sie hier an, „warum“ Sie diese Verarbeitungstätigkeit/Verfahren in Ihrer Praxis haben.  a) Befunderhebung zur Therapiewahl und Festlegung des Therapieziels  b) Erfüllung des Behandlungsvertrages  c) Dokumentation der Behandlung (§ 630 f BGB) |
| **Kategorien betroffener Personen (Zwecke)** | Geben Sie hier alle Kategorien von Betroffenen an, deren Daten im Rahmen dieser Verarbeitungstätigkeit verarbeitet werden. Z.B. Patienten. |
| **Betroffene Kategorien von Daten** | Geben Sie hier an, welche Kategorien von Daten im Rahmen dieser Verarbeitungstätigkeit verarbeitet werden. Gehen Sie am besten die Liste am Anfang des Verzeichnisses von Verarbeitungstätigkeiten durch, und prüfen Sie bei jeder Kategorie von Daten, ob diese im Rahmen dieser Tätigkeit verarbeitet werden. Geben Sie hinter jeder Kategorie von Daten an, zu welchem Zweck (vgl. oben) sie verarbeitet werden. Bspw:  Stammdaten der Patienten (a, b, c)  Krankheitsdaten (a, b, c)  Körperliche Daten (a, b, c)  Sozialanamnetische Daten (a, b, c)  Behandler (a, c) |
| **Legitimation der Datenverarbeitung** | Geben Sie hier an, auf Grund welcher Rechtsgrundlage die Verarbeitungstätigkeit ausgeübt wird.  - Behandlungsvertrag Art. 6 Abs. 1 b DSGVO  - Art. 9 Abs. 2 h i.V.m Abs. 3 DSGVO, § 22 BDSG n.F.  - § 630 f BGB für Buchst. c |
| **Empfänger /  Offenlegung** | Geben Sie hier in diesem Feld an, welchen Kategorien von Empfängern im Rahmen dieses Verfahrens Daten übermittelt werden. Denken Sie daran, dass Sie hier keine Empfänger mit Namen benennen müssen.  Intern (Anmeldekräfte)  Verordnender Arzt  Krankenversicherung  Rechenzentrum |
| **Löschfristen** | Geben Sie in diesem Feld an, wie lange die Daten jeweils gespeichert werden. Wenn Sie sich nicht sicher sind, können Sie auch einfach schreiben: Die gesetzlichen Aufbewahrungsfristen werden beachtet. Nicht mehr benötigte Daten werden gelöscht.  Die Aufbewahrungsfristen von zehn Jahren nach Abschluss der Behandlung gem. § 630 f Abs. 3 BGB werden beachtet. Nicht mehr benötigte Patientenakten werden gelöscht. |
| **Verfahrensspezifische TOMs** | Hier sollte der folgende Textbaustein stehen:  „Die verfahrensübergreifenden technischen und organisatorischen Maßnahmen der verantwortlichen Stelle bieten die notwendigen Garantien, um den Schutz der Rechte und Freiheiten der betroffenen Personen angemessen sicherzustellen.“  Haben Sie spezifische technische oder organisatorische Maßnahmen eingeführt, um Daten im Rahmen eines bestimmten Verfahrens/Verarbeitungstätigkeit zu schützen, können Sie dies hier vermerken. Beispielsweise:  „Zum besonderen Schutz von Patientenakten bei der Mitnahme zu Hausbesuchen werden diese ausschließlich in eigens dafür bereitgehaltenen verschließbaren Aktentaschen transportiert. Es besteht die dienstliche Anweisung gegenüber allen Mitarbeitern, die Hausbesuche durchführen, Patientenakten nicht sichtbar im Auto liegen zu lassen.“ |
| **Informationspflichten** | Hierbei handelt es sich um Textbausteine, die in den meisten Fällen für Sie zutreffend sein werden. Hier sollten nur bei Abweichung Änderungen vorgenommen werden.  Die Datenerhebung für alle für dieses Verfahren erforderlichen Daten erfolgt ausschließlich beim Betroffenen selbst gem. Art. 13 DSGVO.  Alle Patienten erhalten bei Aufnahme der Patientendaten die Datenschutzinformation gem. Art. 13 DSGVO. |
| **Risikobewertung** | Hier sollte der nachfolgende Textbaustein stehen:  Die Verarbeitungstätigkeit hat voraussichtlich kein hohes Risiko für die Rechte und Freiheiten zur Folge. Eine Datenschutz-Folgenabschätzung ist nicht erforderlich. |

Falls Sie weitere Aspekte oder Sachverhalte, die in der Vorlage noch nicht abgebildet sind, in die Vorlage aufnehmen möchten, wenden Sie sich gerne an uns

Sollten Sie Fragen haben, zögern Sie bitte nicht, sich an uns zu wenden.

DATA*privat* GmbH

horbach@dataprivat.de

0241-99 77 6 88 3

**Ihr DATA*privat* Team**

**Ende des Bearbeitungshinweises]**

**Verzeichnis von Verarbeitungstätigkeiten**

|  |
| --- |
| Name oder Firma der verantwortlichen Stelle  **Physiopraxis Mustermann**  Musterstraße 1, 12345 Berlin  Tel. …  Fax …  info@praxis.de |
| Leiter der verantwortlichen Stelle und der Datenverarbeitung; Datenschutzbeauftragter   * Praxisinhaber: Herr Mustermann * Datenschutzbeauftragter (extern):   **DATAprivat GmbH, Schönrath Str. 85, 52066 Aachen**  **Ansprechpartner: Rainer Horbach, Horbach@dataprivat.de** |

|  |  |
| --- | --- |
| Kategorien der in der verantwortlichen Stelle verarbeiteten personenbezogen Daten | |
| Patientendaten | **Stammdaten der Patienten**  Umfasst sind alle Daten, die für die Aufrechterhaltung des Kontaktes mit dem Patienten erforderlich sind. Dies umfasst insbesondere: Namen, Adresse, E-Mail-Adresse, Telefonnummer, etc..  **Versicherungsstatus**  Umfasst sind alle Daten, die für die Abrechnung von Leistungen gegenüber den gesetzlichen Krankenkassen erforderlich sind. Dies sind insbesondere: Versicherung, Versicherungsnummer, Befreiung von der Zuzahlungspflicht gem. § 32 Abs. 2 S. 1 i.V.m. § 61 SGB V, Anspruch auf Beihilfeleistungen, etc.  **Rechnungsdaten (Privatpatienten)**  Umfasst sind alle Daten, die im Rahmen der Rechnungstellung gegenüber Privat-patienten verarbeitet werden. Dies umfasst auch die Angabe des abgegebenen Heilmittels, die Zeiten der Abgabe und den Rechnungsbetrag.  **Krankheitsdaten**  Umfasst sind alle Daten, die sich auf pathologische Zustände der Patienten beziehen, wie beispielsweise Diagnosen und Befunde. Umfasst sind nicht nur die Krankheitsdaten, welche sich aus der im Zusammenhang mit der Abgabe des konkreten Heilmittels durchgeführten Befunderhebung ergeben. Oftmals ist die Erfassung weiterer Krankheitsdaten für die erfolgreiche Abgabe eines Heilmittels erforderlich, auch wenn diese nicht im unmittelbaren Zusammenhang mit der Therapie stehen. Erfasst sind daher auch chronische Leiden oder Gebrechen der Patienten.  Krankheitsdaten sind als Gesundheitsdaten gem. Art. 4 Nr. 15 DSGVO Daten besonderer Kategorien gem. Art. 9 DSGVO und unterliegen dem besonderen Schutz der Rechtsordnung. Eine Verarbeitung ist nur zulässig soweit eine ausdrückliche Einwilligung der Betroffenen vorliegt oder die Verarbeitung im Rahmen von Heilbehandlungen erfolgt und von Fachpersonal, welches dem Berufsgeheimnis unterliegt oder unter dessen Aufsicht durchgeführt wird. Hierzu zählen alle Ärzte und Heilmittelerbringer, sowie deren Angestellte.  **Körperliche Daten**  Umfasst sind alle Daten über körperliche Zustände und Eigenschaften, die nicht im engeren Sinne pathologischer Art sind. Dies können körperliche Besonderheiten sein, wie angeborene Fehlbildungen oder besondere Sensibilität auf bestimmte Behandlungsformen oder Stoffe. Erfasst in dieser Kategorie sind beispielsweise auch Allergien. Auch Gewicht, Größe, etc., sind von dieser Kategorie umfasst.  **Sozialanamnetische Daten**  Umfasst sind biographische Daten aus dem Leben der Patienten. Auch Freizeitaktivitäten wie beispielsweise sportliche Aktivitäten sind umfasst.  **Behandler (Therapeuten, Ärzte, Krankenhäuser, etc.)**  Umfasst sind alle Behandler, die mit der Behandlung der diagnostizierten Leiden, für welche das Heilmittel verordnet wurde, befasst waren. Dies sind insbesondere der verordnende Arzt und der das Heilmittel abgebende Therapeut der Praxis selbst.  **Zeiterfassungsdaten (Patienten)**  Umfasst sind alle mit der Praxis zur Abgabe von Heilmitteln vereinbarte Termine. Auch private Zeitdaten der Patienten können erfasst sein, wie bspw. Urlaubszeiten. Erfasst sind auch Terminabsagen oder Nichterscheinen zu einem Termin.  **Begleitpersonen und Angehörige von Patienten**  Umfasst sind alle Kontaktdaten von Angehörigen oder Begleitpersonen von Patienten. Im Falle von betreuten Patienten werden ggf. auch die Kontaktdaten von den Betreuern verarbeitet und gespeichert. |
| Kundendaten | **Stammdaten der Kunden**  Umfasst sind alle Daten, die für die Aufrechterhaltung des Kontaktes mit dem Kunden erforderlich sind. Dies umfasst insbesondere: Namen, Adresse, E-Mail-Adresse, Telefonnummer, etc..  **Krankheitsdaten**  Umfasst sind alle Daten, die sich auf pathologische Zustände der Kunden beziehen, soweit dies für die Bestimmung, ob eine sonstige Leistung (Prävention, Gesundheitsvorsorge, Wellness, etc.) abgegeben werden darf, erforderlich ist.  **Körperliche Gesundheitsdaten**  Umfasst sind alle Daten über körperliche Zustände und Eigenschaften, die nicht im engeren Sinne pathologischer Art sind. Dies können körperliche Besonderheiten sein, wie angeborene Fehlbildungen oder besondere Sensibilität auf bestimmte Behandlungsformen oder Stoffe. Erfasst in dieser Kategorie sind beispielsweise auch Allergien. Auch Gewicht, Größe, etc., sind von dieser Kategorie umfasst.  **Rechnungsdaten (Kunden)**  Umfasst sind alle Daten, die im Rahmen der Rechnungstellung gegenüber Kunden verarbeitet werden. Dies umfasst auch die Angabe der abgegebenen Leistung, die Zeiten der Abgabe und den Rechnungsbetrag.  **Zeiterfassungsdaten (Kunden)**  Umfasst sind alle mit der Praxis zur Abgabe von Leistungen vereinbarte Termine. Erfasst sind auch Terminabsagen oder Nichterscheinen zu einem Termin. |
| Mitarbeiter daten | **Stammdaten der Mitarbeiter**  Umfasst sind alle Daten, die für die Aufrechterhaltung des Kontaktes mit dem Mitarbeiter erforderlich sind. Dies umfasst insbesondere: Namen, Adresse, E-Mail-Adresse, Telefonnummer, etc.. Ebenfalls umfasst sind auch Daten wie z.B. Familienstand, Kirchenzugehörigkeit, Schwerbehindertenstatus, etc..  **Lohndaten und Bankdaten**  Umfasst sind alle Daten, die für die Lohnbuchhaltung und Lohnzahlung erforderlich sind. Dies umfasst neben der Kontoverbindung auch den Beschäftigungsstatus bei geringfügig Beschäftigten. Daten über Lohnpfändungen unterfallen dieser Kategorie.  **Berufliche Qualifikationen**  Umfasst sind alle Daten über die berufliche Qualifikation des Mitarbeiters. Dies sind insbesondere der berufsqualifizierende Abschluss und Nachweise für Fortbildungen.  **Bewerbungsunterlagen / Personalakte**  Umfasst sind alle Daten, wie sie sich aus den Bewerbungsunterlagen der Mitarbeiterinnen und Mitarbeiter ergeben sowie der Inhalt der Personalakte i.S. § 83 BetrVG.  **Zeiterfassungsdaten (Urlaub, Krankschreibungen, etc.)**  Umfasst sind alle Daten über die Arbeitszeiten der Mitarbeiterinnen und Mitarbeiter. Dies sind insbesondere: Dienstzeiten, wie sie sich aus den Dienstplänen ergeben, Urlaubszeiten, Krankheitstage, Mutterschutz, etc.. |
| Sonstige Daten | **Ärzte und Behandler**  Erfasst sind die Daten von verordnenden Ärzten, Zahnärzten oder Heilpraktikern  **Lieferanten**  Erfasst sind alle Daten von Lieferanten und sonstigen Geschäftspartnern der Praxis |

|  |
| --- |
| Kategorien von Empfängern personenbezogener Daten |
| Therapeutisches Personal der Praxis |
| Bürokräfte der Praxis |
| Ärzte, Krankenhäuser, Heilpraktiker |
| Begleitpersonen und gesetzliche Vertreter von Patienten |
| Steuerberater |
| Gesetzliche Krankenkassen (Primärkassen, Ersatzkassen, etc.) |
| Rechenzentrum (Abrechnungsstelle) |
| Rechtsanwalt |
| Kreditinstitute |
| IT-Dienstleister |
| Medizinischer Dienst der Krankenversicherung (MDK) |
| Gesundheitsamt (örtlich zuständiges) |
| Berufsgenossenschaft |
| Rentenversicherungsträger |
| Berufsfachverband (z.B. VPT, VDB, ZVK) |

|  |  |
| --- | --- |
| Liste der Auftragsverarbeiter der Praxis | |
| Pflege und Wartung EDV | … |
| Fernwartung  Praxissoftware | Bsp. Sovdwaer Gmbh, Franckstraße 5, Ludwigsburg |

|  |
| --- |
| in der Verantwortlichen STelle angewandte Verarbeitungstätigkeiten |
| Abgabe von Heilmitteln |
| Aufnahme Patientendaten und Verwaltung |
| Leistungsabrechnung |
| Primäre Prävention und Gesundheitsförderung |
| Medizinische Trainingstherapie |
| abgabe von Wellness-leistungen |
| Erweiterte Ambulante Physiotherpie |
| Personalverwaltung |
| Veröffentlichung von Lichtbildern |
| Videoüberwachung |

|  |  |
| --- | --- |
| Abgabe von Heilmitteln | |
| **Verantwortlicher**  **Ansprechpartner:** | Die Praxisleitung |
| **Angelegt:**  **Letzte Änderung:** | 15.05.2018  15.05.2018 |
| **Auftragnehmer** | Keine, da nur intern |
| **Beschreibung** | Die Durchführung von Heilbehandlungen in der Form der Abgabe von Heilmitteln ist die Kerntätigkeit der verantwortlichen Stelle. Dieses Verfahren umfasst alle Verarbeitungsvorgänge, die im Zusammenhang mit der Abgabe von Heilmitteln stehen.  **[ACHTUNG! Bitte bei Ergotherapie oder Logopädie den nachfolgenden Absatz entsprechend anpassen.]**  Dies sind insbesondere die Befundung durch den Masseur/medizinischen Bademeister oder Physiotherapeuten und die anschließende Therapiewahl einschließlich der Zeitvorgaben für Folgetermine. Zu den Hauptaufgaben des Masseurs/medizinischen Bademeisters oder Physiotherapeuten gehört im Rahmen der Abgabe von Heilmitteln die Befundung. Erst wenn diese erfolgt ist, kann der Therapeut die Therapiewahl treffen und mit dem Patienten gemeinsam ein Therapieziel festlegen. Das Verfahren umfasst nicht nur die Erhebung von Daten beim Patienten selbst; etwa durch Befragung oder durch manuelle Untersuchung. Daten werden auch aus Dokumenten (Rezepte, Patientenakte, etc.) erhoben und schließlich in der Patientenakte im Rahmen der Dokumentation gespeichert. Umfasst sind insbesondere:   * Befragung des Patienten im Rahmen der Anamnese * Ggf. Auswertung der Krankengeschichte, wie sie sich aus Unterlagen insb. der Patientenakte ergibt. * Durchführung der Sozialanamnese durch den Therapeuten * Ggf. Kontrolle ob Infektionskrankheiten vorliegen * etc. |
| **Zwecke der  Verarbeitung** | a) Befunderhebung zur Therapiewahl und Festlegung des Therapieziels  b) Erfüllung des Behandlungsvertrages  c) Dokumentation der Behandlung (§ 630 f BGB) |
| **Kategorien betroffener Personen (Zwecke)** | Patienten |
| **Betroffene Kategorien von Daten** | Stammdaten der Patienten (a, b, c)  Krankheitsdaten (a, b, c)  Körperliche Daten (a, b, c)  Sozialanamnetische Daten (a, b, c)  Behandler (a, c) |
| **Legitimation der Datenverarbeitung** | - Behandlungsvertrag Art. 6 Abs. 1 b DSGVO  - Art. 9 Abs. 2 h i.V.m Abs. 3 DSGVO, § 22 BDSG n.F.  - § 630 f BGB für Buchst. c |
| **Empfänger /  Offenlegung** | Intern (Anmeldekräfte)  Verordnender Arzt  Krankenversicherung  Rechenzentrum |
| **Löschfristen** | Die Aufbewahrungsfristen von zehn Jahren nach Abschluss der Behandlung gem. § 630 f Abs. 3 BGB werden beachtet. Nicht mehr benötigte Patientenakten werden gelöscht. |
| **Verfahrensspezifische TOMs** | Die verfahrensübergreifenden technischen und organisatorischen Maßnahmen der verantwortlichen Stelle bieten die notwendigen Garantien, um den Schutz der Rechte und Freiheiten der betroffenen Personen angemessen sicherzustellen. |
| **Informationspflichten** | Die Datenerhebung für alle für dieses Verfahren erforderlichen Daten erfolgt ausschließlich beim Betroffenen selbst gem. Art. 13 DSGVO.  Alle Patienten erhalten bei Aufnahme der Patientendaten die Datenschutzinformation gem. Art. 13 DSGVO. |
| **Risikobewertung** | Die Verarbeitungstätigkeit hat voraussichtlich kein hohes Risiko für die Rechte und Freiheiten zur Folge. Eine Datenschutz-Folgenabschätzung ist nicht erforderlich. |

|  |  |
| --- | --- |
| Aufnahme Patientendaten und verwaltung | |
| **Verantwortlicher**  **Ansprechpartner:** | Die Praxisleitung |
| **Angelegt:**  **Letzte Änderung:** | 15.05.2018  15.05.2018 |
| **Auftragnehmer** | Keine, da nur intern |
| **Beschreibung** | Zur Durchführung der Heilbehandlungen und für die Abgabe von Heilmitteln ist die Aufnahme von Patientendaten erforderlich und auch gesetzlich vorgeschrieben. Das Verfahren dient insbesondere auch der terminlichen Organisation. Mit Patienten müssen Termine vereinbart und ggf. auch abgestimmt werden, wenn es auf der Seite der Praxis zu Unpässlichkeiten kommt oder wenn Patienten Termine absagen. Zu diesem Verfahren gehört unter anderem:  - Aufnahme der Stammdaten (Name, Adresse, Telefonnummer, E-  Mail, etc.) der Patienten in die Patientenakte  - Eintragung von Terminen in den Praxiskalender  - Kontakt zu Patienten via Telefon, E-Mail, Fax, Post  - Löschung von Terminen aus dem Terminkalender |
| **Zwecke der**  **Verarbeitung** | 1. Sicherstellung des Kontaktes zum Patienten 2. Interne Praxisorganisation / Raumplanung 3. Vorbereitung des Forderungsmanagements 4. Vorbereitung Zahlungsaufforderung gem. § 43 c SGB V 5. Vorbereitung Leistungsabrechnung 6. Terminvergabe und Verwaltung 7. Kommunikation verordnendem Arzt |
| **Kategorien betroffener Personen** | Patienten  Ärzte |
| **Betroffene Kategorien von Daten** | Stammdaten der Patienten (a, b, c, d, e, f)  Versicherungsstatus (c, d, e)  Krankheitsdaten (b, e, f, g)  Behandler (g)  Begleitpersonen von Patienten (a, b)  Rechnungsdaten (Privatpatienten) (c, d) |
| **Legitimation der Datenverarbeitung** | - Behandlungsvertrag Art. 6 Abs. 1 b DSGVO  - Art. 9 Abs. 2 h i.V.m Abs. 3 DSGVO, § 22 BDSG n.F.  - § 43 c Abs. 1 S. 2 SGB V für Buchst. d  - § 7 GKV-Rahmenvertr. Physiotherapie für Buchst. g |
| **Empfänger /  Offenlegung** | Nur Intern (Anmeldekräfte)  Ärzte |
| **Löschfristen** | Die Aufbewahrungsfristen von zehn Jahren nach Abschluss der Behandlung gem. § 630 f Abs. 3 BGB werden beachtet. Nicht mehr benötigte Patienten-akten werden gelöscht. |
| **Verfahrensspezifische TOMs** | Die verfahrensübergreifenden technischen und organisatorischen Maßnahmen der verantwortlichen Stelle bieten die notwendigen Garantien, um den Schutz der Rechte und Freiheiten der betroffenen Personen angemessen sicherzustellen. |
| **Informationspflichten** | Die Datenerhebung für alle für dieses Verfahren erforderlichen Daten erfolgt ausschließlich beim Betroffenen selbst gem. Art. 13 DSGVO.  Alle Patienten erhalten bei Aufnahme der Patientendaten die Datenschutz-information gem. Art. 13 DSGVO. |
| **Risikobewertung** | Die Verarbeitungstätigkeit hat voraussichtlich kein hohes Risiko für die Rechte und Freiheiten zur Folge. Eine Datenschutz-Folgenabschätzung ist nicht erforderlich. |

|  |  |
| --- | --- |
| Leistungsabrechnung | |
| **Verantwortlicher**  **Ansprechpartner:** | Die Praxisleitung |
| **Angelegt:**  **Letzte Änderung:** | 15.05.2018  15.05.2018 |
| **Auftragnehmer** | Keine, da nur intern |
| **Beschreibung** | Das Verfahren dient der Abrechnung von abgegebenen Leistungen und Heilmitteln gegenüber den gesetzlichen Krankenkassen und der Einziehung der gesetzlichen Zuzahlungsbeträge gem. §§ 32 Abs. 2, 61 Abs. 3 SGB V unter Einhaltung des Zahlungsweges gem. § 43c Abs. 1 SGB V. Es umfasst auch die Übermittlung der Heilmittelverordnungen / Rezepten im Original an das Rechenzentrum, sofern eines in Anspruch genommen wird.  Ebenfalls umfasst ist die Abrechnung gegenüber Privatpatienten und das Forderungsmanagement.  Das Verfahren umfasst insbesondere die folgenden Verarbeitungstätigkeiten:  - Übersendung der Rezepte an das Rechenzentrum im Original  - Anschreiben der Zuzahlungsverpflichteten Patienten zur  gesonderten schriftlichen Aufforderung zur Zahlung  - Anzeige der gesonderten Aufforderung zur Zuzahlung gegenüber  der GKV bei Nichtzahlung  - Erteilung von Quittungen für entgegengenommene  Zuzahlungsbeträge  - Rechnungsstellung gegenüber Privatpatienten |
| **Zwecke der**  **Verarbeitung** | 1. Abrechnung der Leistungen gegenüber der GKV der Patienten 2. Einziehung und Erinnerung an Zuzahlung 3. Leistungsabrechnung der Privatpatienten 4. Steigerung der Effizienz der Praxis durch Abrechnung über Rechenzentrum |
| **Kategorien betroffener Personen** | Patienten |
| **Betroffene Kategorien von Daten** | Stammdaten der Patienten (a, b, c, d)  Versicherungsstatus (a, b, d)  Rechnungsdaten (c)  Krankheitsdaten (a, c, d) |
| **Legitimation der Datenverarbeitung** | - Behandlungsvertrag Art. 6 Abs. 1 b DSGVO  - Art. 9 Abs. 2 h i.V.m Abs. 3 DSGVO  - § 43 c Abs. 1 S. 2 SGB V  - Art. 6 Abs. 1 f DSGVO i.V.m. § 302 Abs. 2 S. 2 SGB V für die Weitergabe  an die Abrechnungsstelle (Rechenzentrum)  Die Praxis nimmt für die Abrechnung von Kassenleistungen gegenüber den gesetzlichen Krankenkassen ein Rechenzentrum (z.B. azh, Optica, Arni, rzh) i.S.v. § 302 Abs. 2 S. 1 SGB V in Anspruch. Die Inanspruchnahme des Rechenzentrums ist zur Wahrung der berechtigten Interessen der Praxis erforderlich.  Das Interesse der Praxis an der Inanspruchnahme des Rechenzentrums ergibt sich insbesondere aus der Notwendigkeit der Vereinfachung der innerbetrieblichen Verfahrensabläufe. Der Praxis steht eine Vielzahl gesetzlicher Krankenkassen gegenüber, mit welchen sie grundsätzlich jeweils einzeln abrechnen müsste. Durch die Inanspruchnahme der Leistungen des Rechenzentrums kann die Praxis die für die Abrechnung notwendigen Schritte auf einen Empfänger konzentrieren.  Die Praxis übermittelt die Verordnungen von abgegebenen Heilmitteln im Original an das Rechenzentrum, welches sodann die eigentliche Abrechnung gegenüber den gesetzlichen Krankenversicherungen übernimmt. Als weitere Serviceleistung erhält die Praxis in regelmäßigen Abständen von dem Rechenzentrum Statistiken über die in der Praxis abgegebenen Heilmittel. Diese stellen ein wertvolles Instrument zur betriebswirtschaftlichen Kontrolle der Praxis dar.  Überwiegende Interessen der Betroffenen, die einer Datenweitergabe an das Rechenzentrum entgegenstehen könnten, sind nicht erkennbar. Vor dem Hintergrund, dass nahezu ausnahmslos alle Heilmittelerbringer über ein Rechenzentrum abrechnen, dürfen Patienten regelmäßig damit rechnen, dass eine Praxis ein solches in Anspruch nimmt. Die Rechenzentren unterliegen zudem gem. § 302 Abs. 2 S. 3 SGB V besonders strengen datenschutzrechtlichen Anforderungen und stehen unter der Aufsicht der BaFin. Für die übermittelten Daten ist daher kein hohes Risiko zu besorgen.  Die Patienten werden vor der Behandlung über die Datenweitergabe an das Rechenzentrum informiert. |
| **Empfänger /**  **Offenlegung** | Intern (Bürokräfte der Praxis)  Rechenzentrum |
| **Löschfristen** | Die Aufbewahrungsfristen von zehn Jahren nach Abschluss der Behandlung gem. § 630 f Abs. 3 BGB werden beachtet. Nicht mehr benötigte Patienten-akten werden gelöscht.  Die Speicherfristen gem. § 147 AO werden beachtet. Daten, die nicht weiter gespeichert werden müssen, werden gelöscht. |
| **Verfahrensspezifische TOMs** | Die verfahrensübergreifenden technischen und organisatorischen Maßnahmen der verantwortlichen Stelle bieten die notwendigen Garantien, um den Schutz der Rechte und Freiheiten der betroffenen Personen angemessen sicherzustellen. |
| **Informationspflichten** | Die Datenerhebung für alle für dieses Verfahren erforderlichen Daten erfolgt ausschließlich beim Betroffenen selbst gem. Art. 13 DSGVO. Die Patienten werden entsprechend informiert.  Insbesondere werden die Patienten darüber informiert, dass ihnen bezüglich der Datenweitergabe an das Rechenzentrum ein Recht auf Widerspruch zusteht. |
| **Risikobewertung** | Die Verarbeitungstätigkeit hat voraussichtlich kein hohes Risiko für die Rechte und Freiheiten zur Folge. Eine Datenschutz-Folgenabschätzung ist nicht erforderlich. |

|  |  |
| --- | --- |
| Primäre Prävention und Gesundheitsförderung | |
| **Verantwortlicher**  **Ansprechpartner:** | Die Praxisleitung |
| **Angelegt:**  **Letzte Änderung:** | 15.05.2018  15.05.2018 |
| **Auftragnehmer** | Keine, da nur intern |
| **Beschreibung** | Zu den Leistungen der gesetzlichen Krankenkassen gehören gem. § 20 SGB V auch Leistungen für die sog. primäre Prävention und Gesundheitsförderung. Auch Heilmittelerbringer können – sofern sie die Voraussetzungen erfüllen – als Leistungserbringer für Prävention und Gesundheitsförderung auftreten.  Die Leistungen werden vorwiegend in der Form von Gruppenkursen angeboten, an welchem die Versicherten der gesetzlichen Krankenkassen als Kunden der Praxis teilnehmen. Die Abrechnung der Leistungen erfolgt gegenüber den Kunden direkt, welche wiederum eine Kostenerstattung von ihrer Krankenversicherung erhalten.  Ebenso können Präventionsleistungen abgegeben werden, die nicht unter § 20 SGB V fallen.  Die Gruppe der Kunden, welche Präventionskurse und Angebote der Gesundheitsförderung in Anspruch nehmen, ist von der Gruppe der Patienten zu trennen, da sie im Gegensatz zu letzterer keine Heilbehandlungen in Anspruch nimmt. Zur Durchführung der Präventionskurse und sonstigen Angebote der Gesundheitsförderung gehört daher auch die Erhebung von Gesundheitsdaten bei den Kunden durch die Praxis. Sind krankhafte Zustände festzustellen, darf die Prävention nicht durchgeführt werden. |
| **Zwecke der**  **Verarbeitung** | 1. Aufnahme von Kontaktdaten 2. Abfrage krankhafter Zustände 3. Führen von Teilnehmerlisten 4. Abgabe der Leistung 5. Datenweitergabe an Träger 6. Leistungsabrechnung und Forderungsmanagement |
| **Kategorien betroffener Personen** | Patienten  Kunden |
| **Betroffene Kategorien von Daten** | Stammdaten der Kunden / Patienten (a, c, d, e)  Krankheitsdaten (b)  Körperliche Gesundheitsdaten (d)  Rechnungsdaten (Kunden / Patienten) (f) |
| **Legitimation der Datenverarbeitung** | - Behandlungsvertrag Art. 6 Abs. 1 b DSGVO  - Art. 9 Abs. 2 h i.V.m Abs. 3 DSGVO, § 22 BDSG n.F. |
| **Empfänger /  Offenlegung** | Nur Intern (Anmeldekräfte)  Gegebenenfalls Träger der Präventionsleistung |
| **Löschfristen** | Die Aufbewahrungsfristen von zehn Jahren nach Abschluss der Behandlung gem. § 630 f Abs. 3 BGB werden beachtet. Nicht mehr benötigte Patienten-akten werden gelöscht. |
| **Verfahrensspezifische TOMs** | Die verfahrensübergreifenden technischen und organisatorischen Maßnahmen der verantwortlichen Stelle bieten die notwendigen Garantien, um den Schutz der Rechte und Freiheiten der betroffenen Personen angemessen sicherzustellen. |
| **Informationspflichten** | Die Datenerhebung für alle für dieses Verfahren erforderlichen Daten erfolgt ausschließlich beim Betroffenen selbst gem. Art. 13 DSGVO.  Alle Teilnehmer erhalten bei Aufnahme der Patientendaten die Datenschutz-information gem. Art. 13 DSGVO. |
| **Risikobewertung** | Die Verarbeitungstätigkeit hat voraussichtlich kein hohes Risiko für die Rechte und Freiheiten zur Folge. Eine Datenschutz-Folgenabschätzung ist nicht erforderlich. |

|  |  |
| --- | --- |
| Medizinische Trainingstherapie | |
| **Verantwortlicher**  **Ansprechpartner:** | Die Praxisleitung |
| **Angelegt:**  **Letzte Änderung:** | 15.05.2018  15.05.2018 |
| **Auftragnehmer** | Keine, da nur intern |
| **Beschreibung** | Medizinische Trainingstherapie ist das gezielte körperliche Training unter physiotherapeutischer Aufsicht und Anleitung zum Zweck der Rehabilitation nach Verletzungen oder zur vorbeugenden Stärkung der Muskulatur.  Nach einer Einweisung und Aufnahme durch die Praxis führen die Patienten die festgelegten Übungen an den Trainingsgeräten weitestgehend selbständig unter Aufsicht der Therapeuten durch. Zu diesem Verfahren gehören insbesondere die folgenden Verarbeitungstätigkeiten:   * Erstellen der Trainingspläne * Zurverfügungstellung der Trainingspläne * Etc. |
| **Zwecke der**  **Verarbeitung** | 1. Aufnahme Kontaktdaten 2. Abfrage krankhafter Zustände 3. Leistungsabrechnung und Forderungsmanagement |
| **Kategorien betroffener Personen** | Kunden |
| **Betroffene Kategorien von Daten** | Stammdaten der Kunden (a, c)  Krankheitsdaten (b)  Körperliche Gesundheitsdaten (b)  Rechnungsdaten (Kunden) (c) |
| **Legitimation der Datenverarbeitung** | - Vertrag Art. 6 Abs. 1 b DSGVO |
| **Empfänger /  Offenlegung** | Nur Intern (Anmeldekräfte) |
| **Löschfristen** | Die Speicherfristen gem. § 147 AO werden beachtet. Daten, die nicht weiter gespeichert werden müssen, werden gelöscht. |
| **Verfahrensspezifische TOMs** | Die verfahrensübergreifenden technischen und organisatorischen Maßnahmen der verantwortlichen Stelle bieten die notwendigen Garantien, um den Schutz der Rechte und Freiheiten der betroffenen Personen angemessen sicherzustellen. |
| **Informationspflichten** | Die Datenerhebung für alle für dieses Verfahren erforderlichen Daten erfolgt ausschließlich beim Betroffenen selbst gem. Art. 13 DSGVO.  Alle Teilnehmer erhalten bei Aufnahme der Patientendaten die Datenschutz-information gem. Art. 13 DSGVO. |
| **Risikobewertung** | Die Verarbeitungstätigkeit hat voraussichtlich kein hohes Risiko für die Rechte und Freiheiten zur Folge. Eine Datenschutz-Folgenabschätzung ist nicht erforderlich. |

|  |  |
| --- | --- |
| Erweiterte ambulante Physiotherapie | |
| **Verantwortlicher**  **Ansprechpartner:** | Die Praxisleitung |
| **Angelegt:**  **Letzte Änderung:** | 15.05.2018  15.05.2018 |
| **Auftragnehmer** | Keine, da nur intern |
| **Beschreibung** | Die EAP ist eine Leistung der gesetzlichen Unfallversicherung und unterfällt nach der Rechtsprechung des Bundessozialgerichts nicht den ärztlichen Behandlungen und auch nicht den Heilmitteln im engeren Sinne des SGB V (BSG Urteil v. 17.2.2010, B 1 KR 23/09 R).  Bei der erweiterten ambulanten Trainingstherapie werden die klassischen und grundsätzlich isoliert angewendeten Heilmittel (Krankengymnastik, Klassische Massagetherapie, etc.) mit der medizinischen Trainingstherapie zusammengeführt und als Komplextherapie vereinigt. Die Leistungen der EAP fußen auf der Heilbehandlung der gesetzlichen Unfallversicherung (§ 40 SGB V, §§ 27 ff. SGB VII, § 42 SGB IX). |
| **Zwecke der**  **Verarbeitung** | 1. Aufnahme Kontaktdaten 2. Abfrage krankhafter Zustände 3. Leistungsabrechnung und Forderungsmanagement 4. Erstellung der Trainingspläne |
| **Kategorien betroffener Personen** | Kunden |
| **Betroffene Kategorien von Daten** | Stammdaten der Kunden (a, c)  Krankheitsdaten (b)  Körperliche Gesundheitsdaten (b)  Rechnungsdaten (Kunden) (c) |
| **Legitimation der Datenverarbeitung** | - Vertrag Art. 6 Abs. 1 b DSGVO |
| **Empfänger /  Offenlegung** | Nur Intern (Anmeldekräfte) |
| **Löschfristen** | Die Speicherfristen gem. § 147 AO werden beachtet. Daten, die nicht weiter gespeichert werden müssen, werden gelöscht. |
| **Verfahrensspezifische TOMs** | Die verfahrensübergreifenden technischen und organisatorischen Maßnahmen der verantwortlichen Stelle bieten die notwendigen Garantien, um den Schutz der Rechte und Freiheiten der betroffenen Personen angemessen sicherzustellen. |
| **Informationspflichten** | Die Datenerhebung für alle für dieses Verfahren erforderlichen Daten erfolgt ausschließlich beim Betroffenen selbst gem. Art. 13 DSGVO.  Alle Teilnehmer erhalten bei Aufnahme der Patientendaten die Datenschutz-information gem. Art. 13 DSGVO. |
| **Risikobewertung** | Die Verarbeitungstätigkeit hat voraussichtlich kein hohes Risiko für die Rechte und Freiheiten zur Folge. Eine Datenschutz-Folgenabschätzung ist nicht erforderlich. |

|  |  |
| --- | --- |
| Abgabe von wellness-leistungen | |
| **Verantwortlicher**  **Ansprechpartner:** | Die Praxisleitung |
| **Angelegt:**  **Letzte Änderung:** | 15.05.2018  15.05.2018 |
| **Auftragnehmer** | Keine, da nur intern |
| **Beschreibung** | In der Praxis werden jedenfalls gelegentlich auch sog. Wellness-Leistungen abgegeben. Hierbei handelt es sich ausschließlich um Dienstleistungen zur Förderung des allgemeinen Wohlbefindens. Wellness-Leistungen sind keine Heilbehandlungen. |
| **Zwecke der**  **Verarbeitung** | 1. Aufnahme Kontaktdaten 2. Abfrage krankhafter Zustände 3. Leistungsabrechnung und Forderungsmanagement |
| **Kategorien betroffener Personen** | Kunden |
| **Betroffene Kategorien von Daten** | Stammdaten der Kunden (a, c)  Krankheitsdaten (b)  Körperliche Gesundheitsdaten (b)  Rechnungsdaten (Kunden) (c) |
| **Legitimation der Datenverarbeitung** | - Vertrag Art. 6 Abs. 1 b DSGVO |
| **Empfänger /  Offenlegung** | Nur Intern (Anmeldekräfte) |
| **Löschfristen** | Die Speicherfristen gem. § 147 AO werden beachtet. Daten, die nicht weiter gespeichert werden müssen, werden gelöscht. |
| **Verfahrensspezifische TOMs** | Die verfahrensübergreifenden technischen und organisatorischen Maßnahmen der verantwortlichen Stelle bieten die notwendigen Garantien, um den Schutz der Rechte und Freiheiten der betroffenen Personen angemessen sicherzustellen. |
| **Informationspflichten** | Die Datenerhebung für alle für dieses Verfahren erforderlichen Daten erfolgt ausschließlich beim Betroffenen selbst gem. Art. 13 DSGVO.  Alle Teilnehmer erhalten bei Aufnahme der Patientendaten die Datenschutz-information gem. Art. 13 DSGVO. |
| **Risikobewertung** | Die Verarbeitungstätigkeit hat voraussichtlich kein hohes Risiko für die Rechte und Freiheiten zur Folge. Eine Datenschutz-Folgenabschätzung ist nicht erforderlich. |

|  |  |
| --- | --- |
| Personalverwaltung | |
| **Verantwortlicher**  **Ansprechpartner:** | Die Praxisleitung |
| **Angelegt:**  **Letzte Änderung:** | 15.05.2018  15.05.2018 |
| **Auftragnehmer** | Keine, da nur intern |
| **Beschreibung** | Im Verfahren ‚Personalverwaltung‘ sind alle Verfahren zusammengefasst, welche in der Organisation der Mitarbeiterinnen und Mitarbeiter erforderlich sind. Es umfasst sowohl die Einstellung neuer Mitarbeiterinnen und Mitarbeiter als auch die Datenweitergabe an den Steuerberater sowie Führung der Personalakte. |
| **Zwecke der**  **Verarbeitung** | a) Durchführung von Bewerbungsverfahren  b) Einstellung neuer Mitarbeiterinnen und Mitarbeiter  c) Speicherung von Bewerbungsunterlagen  d) Führen der Personalakte  e) Personaleinsatzplanung und Kommunikation  f) Schlüsselliste  g) Abrechnung von Reisekosten  h) Lohn- und Gehaltabrechnung  g) Weitergabe von Qualifikationen an die gesetzlichen Krankenversicherungen |
| **Kategorien betroffener Personen** | Mitarbeiter |
| **Betroffene Kategorien von Daten** | Stammdaten der Mitarbeiter (a, b, c, d, e, f, g, h)  Berufliche Qualifikationen (a, b, d, h)  Bewerbungsunterlagen / Personalakte (a, b, c, d)  Lohn- und Bankdaten (g, h,)  Zeiterfassungsdaten (a, e, g, h) |
| **Legitimation der Datenverarbeitung** | * Vertrag und vorvertragliches Schuldverhältnis Art. 6 Abs. 1 b DSGVO i.V.m. mit den Arbeitsverträgen * Erfüllung eigener Geschäftszwecke Art. 6 Abs. 1 f DSGVO i.V.m. § 21 Abs. 2 S. 1 AGG für die Speicherung von Bewerbungsunterlagen abgelehnter Bewerberinnen und Bewerber zum Schutze vor ungerechtfertigten Klagen aus dem ‚Allgemeinen Gleichbehandlungsgesetz‘ (AGG).   Die Praxis hat grundsätzlich ein schutzwürdiges Interesse an der Erhaltung von Beweismöglichkeiten für den Fall, dass eine abgelehnte Bewerberin oder ein abgelehnter Bewerber gegen die Praxis ungerechtfertigt Ansprüche wegen Benachteiligung gem. § 21 Abs. 2 S. 1 AGG geltend macht. Insbesondere besteht ein berechtigtes Interesse zur Erhaltung von Beweismitteln zur Erschütterung der Vermutungsregel des § 22 AGG und damit zur Abwendung der Beweislastumkehr.  Abgelehnte Bewerberinnen oder Bewerber präkludieren gemäß § 21 Abs. 5 S. 1 AGG nach Ablauf von 2 Monaten nach Bekanntgabe der Entscheidung mit Ansprüchen wegen Benachteiligung. Unter Berücksichtigung des Laufes der Gerichtspost weiß der Arbeitgeber spätestens drei Monate nach Bekanntgabe der Entscheidung gegenüber der Bewerberin oder dem Bewerber, ob Ansprüche aus dem AGG beim zuständigen Arbeitsgericht anhängig gemacht worden sind. Die Unterlagen sind daher spätestens drei Monate nach Bekanntgabe der Entscheidung zu löschen.   * Art. 6 Abs. 1 f DSGVO für Weitergabe von Daten an Steuerberater. Die Inanspruchnahme der Dienstleistungen eines Steuerberaters und die damit notwendigerweise verbundene Datenübermittlung liegt im berechtigten Interesse der Praxis. Hiergegen ist kein überwiegendes Interesse der Betroffenen (Mitarbeiterinnen und Mitarbeiter) erkennbar. Die Inanspruchnahme eines Steuerberaters kann als allgemein sozialüblich betrachtet werden. Zudem unterliegt der Steuerberater der Geheimnispflicht gemäß § 203 StGB, weshalb ein hohes Risiko für die Betroffenen nicht zu besorgen ist. * Art. 6 Abs. 1 c DSGVO i.V.m. § 2 Abs. 5, § 4 Abs. 8, § 6 Abs. 2 der GKV-Rahmenverträge Physiotherapie für die Datenweitergabe von Mitarbeiterdaten an die gesetzlichen Krankenkassen. |
| **Empfänger /**  **Offenlegung** | Steuerberater, Krankenversicherungen, Berufsgenossenschaft, Finanzverwaltung |
| **Löschfristen** | Die Fristen nach § 147 AO werden beachtet.  Für Abmahnungen, die gegenüber Mitarbeiterinnen und Mitarbeitern ausgesprochen wurden ist eine Löschfrist von drei Jahren vorgesehen.  Arbeitszeitnachweise werden gem. § 16 ArbZG nach zwei Jahren gelöscht.  Bewerbungsunterlagen abgelehnter Bewerber werden drei Monate nach Mitteilung der Ablehnung gelöscht. |
| **Verfahrensspezifische TOMs** | Die Personalakten werden getrennt von übrigen Akten der Praxis in einem verschlossenen Schrank aufbewahrt. Nur die Praxisleitung hat einen Schlüssel und damit Zugang zu diesem Schrank.  Die verfahrensübergreifenden technischen und organisatorischen Maßnahmen der verantwortlichen Stelle bieten ansonsten die notwendigen Garantien, um den Schutz der Rechte und Freiheiten der betroffenen Personen angemessen sicherzustellen. |
| **Informationspflichten** | Die Datenerhebung für alle für dieses Verfahren erforderlichen Daten erfolgt ausschließlich beim Betroffenen selbst gem. Art. 13 DSGVO.  Die Mitarbeiterinnen und Mitarbeiter werden über ein Formblatt bei Aufnahme ihrer Tätigkeit entsprechend Art. 13 DSGVO informiert.  Bewerberinnen und Bewerber erhalten die notwendigen Informationen gem. Art. 13 DSGVO mit der Bestätigung des Eingangs der Bewerbungsunterlagen. |
| **Risikobewertung** | Die Verarbeitungstätigkeit hat voraussichtlich kein hohes Risiko für die Rechte und Freiheiten zur Folge. Eine Datenschutz-Folgenabschätzung ist nicht erforderlich. |

|  |  |
| --- | --- |
| veröffentlichung von lichtbildern | |
| **Verantwortlicher**  **Ansprechpartner:** | Die Praxisleitung |
| **Angelegt:**  **Letzte Änderung:** | 15.05.2018  15.05.2018 |
| **Auftragnehmer** | Keine, da nur intern |
| **Beschreibung** | Dieses Verfahren umschreibt Maßnahmen, welche der Förderung der Außendarstellung der Praxis dienen. Es umfasst insbesondere:   * Aushängen von Lichtbildern der Mitarbeiterinnen und Mitarbeiter innerhalb der Praxisräume * Veröffentlichung von Lichtbildern der Mitarbeiterinnen und Mitarbeiter auf der Internetseite der Praxis, ggf. Facebook-Seite der Praxis * Veröffentlichung von Lichtbildern von Patienten auf der Internetseite der Praxis * Veröffentlichen von Lichtbildern in Werbematerial (Flyer, Zeitungsanzeigen, etc.) |
| **Zwecke der**  **Verarbeitung** | a) Förderung der Außendarstellung der Praxis |
| **Kategorien betroffener Personen** | Mitarbeiter  Patienten |
| **Betroffene Kategorien von Daten** | Stammdaten der Patienten (a)  Stammdaten der Mitarbeiter (a)  Bewerbungsunterlagen / Personalakte (a) |
| **Legitimation der Datenverarbeitung** | * Qualifizierte schriftliche Einwilligung gem. Art. 6 Abs. 1 a, Art. 7 DSGVO i.V.m § 22 KUG |
| **Empfänger /**  **Offenlegung** | Veröffentlichung |
| **Verfahrensspezifische TOMs** | Die verfahrensübergreifenden technischen und organisatorischen Maßnahmen der verantwortlichen Stelle bieten die notwendigen Garantien, um den Schutz der Rechte und Freiheiten der betroffenen Personen angemessen sicherzustellen. |
| **Informationspflichten** | Eine Datenerhebung erfolgt ausschließlich bei den Betroffenen i.S.v. Art. 13 DSGVO. Die Betroffenen Personen werden in der vorgelegten schriftlichen Einwilligungserklärung umfassend gem. Art. 13 DSGVO aufgeklärt. |
| **Risikobewertung** | Die Verarbeitungstätigkeit hat voraussichtlich kein hohes Risiko für die Rechte und Freiheiten zur Folge. Eine Datenschutz-Folgenabschätzung ist nicht erforderlich. |

|  |  |
| --- | --- |
| Videoüberwachung | |
| **Verantwortlicher**  **Ansprechpartner:** | Die Praxisleitung |
| **Angelegt:**  **Letzte Änderung:** | 15.05.2018  15.05.2018 |
| **Auftragnehmer** | Keine, da nur intern |
| **Beschreibung** | Dieses Verfahren beschreibt den Einsatz von visuellen Überwachungssystemen |
| **Zwecke der**  **Verarbeitung** | a) Wahrnehmung des Hausrechts  b) Vorbeugung von Straftaten |
| **Kategorien betroffener Personen** | Mitarbeiter  Patienten  Kunden  Sonstige Besucher der Praxis |
| **Betroffene Kategorien von Daten** | Stammdaten der Patienten (a, b)  Stammdaten der Mitarbeiter (a, b) |
| **Legitimation der Datenverarbeitung** | * Interessenabwägung gem. Art. 6 Abs. 1 f DSGVO |
| **Empfänger /**  **Offenlegung** | keine |
| **Verfahrensspezifische TOMs** | Die Überwachungssysteme sind so voreingestellt, dass die internen Speicher nach 48h jeweils gelöscht werden.  Die Kamers sind zum Schutze der Mitarbeiterinnen und Mitarbeiter so ausgerichtet, dass weder die Eingangstüre zu den Toiletten noch Arbeitsplätze vom Anzeigebild erfasst sind. |
| **Informationspflichten** | Alle Besucher der Praxis werden über ein standardisiertes Bildsymbol gem. Art. 12 Abs. 7 S. 1 DSGVO über die Videoüberwachung informiert. |
| **Risikobewertung** | Die Verarbeitungstätigkeit hat voraussichtlich kein hohes Risiko für die Rechte und Freiheiten zur Folge. Eine Datenschutz-Folgenabschätzung ist nicht erforderlich. |

|  |  |
| --- | --- |
| Betreiben einer Internetseite | |
| **Verantwortlicher**  **Ansprechpartner:** | Die Praxisleitung |
| **Angelegt:**  **Letzte Änderung:** | 15.05.2018  15.05.2018 |
| **Auftragnehmer** | Keine, da nur intern  oder  Webdesign Mustermann |
| **Beschreibung** | Die Praxis betreibt eine Internetseite, um Patienten und Interessierten Personen Informationen über in der Praxis angebotene Behandlungsmethoden und Kontaktmöglichkeiten zu geben. Zudem nutzt die Praxis die Internetseite, um sich und das Team vorzustellen. |
| **Zwecke der**  **Verarbeitung** | a) Förderung der Außendarstellung der Praxis  b) Bereitstellung einer funktionsfähigen Website  c) Analyse zur Effizienzsteigerung der Website  d) Schaffung von Kontaktaufnahmemöglichkeiten  e) Einsatz von Cookies zur nutzerfreundlichen Websitegestaltung |
| **Kategorien betroffener Personen** | Mitarbeiter  Patienten  Kunden  Sonstige Besucher der Internetseite |
| **Betroffene Kategorien von Daten** | Stammdaten der Mitarbeiter (Name, beruflicher Lebenslauf) (a)  Lichtbilder der Mitarbeiter (a)  IP-Adresse der Besucher (a, b, c, e) |
| **Legitimation der Datenverarbeitung** | * Interessenabwägung gem. Art. 6 Abs. 1 f DSGVO * Einwilligung im Fall der Veröffentlichung von Fotos * Art. 6 Abs. 1 b DSGVO für das Kontaktformular |
| **Empfänger /**  **Offenlegung** | Ggf. Google (Wenn Google Analytics verwendet wird!) |
| **Verfahrensspezifische TOMs** | Zur sicheren Datenübertragung wird ein Verschlüsselungsprotokoll in Formeiner Secure Sockets Layer (SSL) Verbindung aufgebaut. |
| **Informationspflichten** | Die Datenschutzerklärung der Website ist über einen Link unmittelbar von der Startseite aus mit einem Click zu erreichen. (Informationsgabe nach Art .13 DSGVO.) |
| **Risikobewertung** | Die Verarbeitungstätigkeit hat voraussichtlich kein hohes Risiko für die Rechte und Freiheiten zur Folge. Eine Datenschutz-Folgenabschätzung ist nicht erforderlich. |