# DATENVERARBEITUNGSVERZEICHNIS

**für freiberuflich tätige**
**Angehörige der gehobenen medizinisch-technischen Dienste**
**als datenschutzrechtlich Verantwortliche für die Datenverarbeitung**
**in Entsprechung des Art 30 Abs 1 DSGVO**

**Verantwortliche:**
**Eva Felbermayr**
**Physiotherapeutin**
**Leonfeldnerstr. 202, 4040 Linz**

**INHALTSVERZEICHNIS**

# I. Stammdatenblatt: Allgemeine Angaben zur Verantwortlichen:

1. **Name der Verantwortlichen:**
   **Eva Felbermayr**

2. **Berufsbezeichnung**
   **Physiotherapeutin**

3. **Berufssitz entsprechend der aufrechten Meldung gem. § 7a MTD-G (gem. § 8 MTD-G jener Ort an dem oder von dem aus die berufliche Tätigkeit als beruflich Tätige erfolgt).**
   **Leonfeldnerstr. 202, 4040 Linz**

4. **Kontaktdaten**
   **O699/10954763**
   **ef@ef-physiotherapie.at**
   **Leonfeldnerstr. 202, 4040 Linz**

# II. Verzeichnis der Datenverarbeitungen, Datenverarbeitungszwecke und jeweiligen gesetzlichen Grundlagen der Datenverarbeitungen

## A) Patientenverwaltung und Honorarabrechnung

**Zweck der Datenanwendung:**

Führung von Patienten-/Klientenkarteien zur Dokumentation (§ 11a MTD-G), Erfüllung der Berufspflichten (§11ff MTD-G), Erstellung von Gutachten (soweit die rechtlichen Voraussetzungen für die Erstellung eines Gutachtens vorliegen) und Honorarverrechnung im Rahmen der freiberuflichen/selbständigen Berufsausübung durch Angehörige der gehobenen medizinisch-technischen Dienste einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie z.B. Korrespondenz) in diesen Angelegenheiten.

**Rechtsgrundlagen der Anwendung sind insbesondere die folgenden Gesetze und Verordnungen** (in der geltenden Fassung)**:**

Bestimmungen über die freiberufliche/selbständige Ausübung des Berufes als Berufsangehörige/r der gehobenen medizinisch-technischen Dienste, §§7a. 11. 11a und 11b Bundesgesetz über die Regelung der gehobenen medizinisch-technischen Dienste, BGBl 1992/460 idgF (MTD-G).

**Höchstdauer der zulässigen Datenaufbewahrung:**

Die Daten der Patienten/Klienten sind gemäß § 11a Abs 3 MTD-G mindestens 10 Jahre hindurch aufzubewahren. Darüber hinaus gelten in Institutionen die jeweiligen gesetzlichen Aufbewahrungspflichten. Weiters ist es zulässig, die Daten bis zur Beendigung von allfälligen Rechtsstreitigkeiten, bei denen die Daten als Beweis benötigt werden, aufzubewahren. Daraus ergibt sich die zulässsige Aufbewahrungsfrist von 30 Jahren.

**Sonstige Hinweise:**
Die Datensicherheitsmaßnahmen gemäß Art. 32 DSGVO sind zu beachten. Insbesondere hat die Übermittlung der Datensätze an den Empfänger in gesicherter, verschlüsselter Form zu erfolgen. Die Verwendung der Daten aufgrund der Ausübung des Berufes eines gesetzlich geregelten Gesundheitsberufes erfordert die Berücksichtigung der entsprechenden gesetzlichen Anforderungen an die Übertragung von Gesundheitsdaten als besonderer Kathegorien personenbezogener Daten gem. Art. 9 DSGVO.
Die Anforderungen gem. Gesundheitstelematikgesetz 2012 (GtelG) an die gesicherte, verschlüsselte Übermittlung von Gesundheitsdaten unter Gesundheitsdiensteanbietern (GDA) wie insbesondere Sozialversicherungsträgern, Krankenanstaltenn und niedergelassenen Gesundheitsberufen sind zu beachten.

| Betroffene Personengruppen: | Nr: | Datenarten: | Empfängerkreise: |
|---|---|---|---|
| | 01 | Patienten-/Klientennummer, Protokollnummer | 1 - 5 |
| | 02 | Vor- und Familienname, akad. Grad / Titel, frühere Namen (Namensteile) | 1 - 6 |
| | 03 | Anschrift | 1 - 6 |
| | 04 | Telefon- und Faxnummer und andere zur Adressierung erforderliche Informationen, die sich durch moderne Kommunikationstechniken ergeben | 1 - 6, soweit nicht vom Betroffenen ausdrücklich untersagt |
| | 05 | Geburtsdatum | 1 - 6 |
| | 06 | Staatsangehörigkeit | 1, 4 |
| | 07 | Geschlecht | 1 - 6 |
| | 08 | Personenstand | --- |
| | 09 | Soziale Verhältnisse (z.B. Beruf) | --- |
| | 10 | Sozialversicherungsnummer | 1 - 6 |
| | 11 | Sozialversicherungsträger | 1 - 3, 5, 6 |

| | | | |
|---|---|---|---|
| Patienten/Klienten des Verantwortlichen sowie Patienten/ Klienten von zuweisenden Gesundheitsdienste-anbietern | 12 | Sonstige Daten zur Sozialversicherung (insbesonders der Name, das Geburtsdatum und die Sozialversicherungsnummer des Hauptversicherten sowie das Verwandtschaftsverhältnis zum Hauptversicherten bei mitversicherten Patienten und Daten des Antrages auf Kostenzuschusss für die Weiterführung der Behandlung/Therapie) | 1 - 3, 5, 6 |
| | 13 | Daten zu einem privaten Versicherungsverhältnis (Versicherer, Polizzennummer, usw.) | 1 - 3, 5 |
| | 14 | Daten sonstiger Kostenträger | 1 - 3, 5 |
| | 15 | Daten über die Erklärung der Kostenübernahme durch einen Kostenträger | 1 - 3, 5 |
| | 16 | Inanspruchnahme des Verantwortlichen (Anlass, Datum, Art und Zahl der Beratungen/ Behandlungen/Therapieeinheiten) | 1, 2, 5, 6 |
| | 17 | Daten zur Verwaltung von Terminen und Wartelisten | --- |
| | 18 | Zustand der Person bei Übernahme der Beratung oder Behandlung | 3 - 5 |
| | 19 | Anamnese (Familien,- und Eigenanamnese, Berufsanamnese) | --- |
| | 20 | Vorbehandlungen | --- |
| | 21 | Diagnosen (auch Fremddiagnosen) zu Behandlungsbeginn und bei Beendigung | 1, 3 - 6 |
| | 22 | Besondere Risikofaktoren, z.B. Allergien, tätigkeitsbedingte Einflüsse, familiäre Disposition | 3 - 5 |
| | 21 | Vorgeschichte der Erkrankung und dazugehörige Befunde | 3 - 5, 7, 8 |
| | 23 | Gutächtliche Äusserungen des Verantwortlichen (z.B. gegenüber Auftraggebern von Gutachten) | 4 |

| | | | |
|---|---|---|---|
| | 24 | Behandlungs,-/Beratungsverlauf, besondere Vorkömmnisse während der Behandlung | 3 - 5 |
| | 25 | Information an Patienten/Klienten (insbesondere über Gesundheisrisiken und Schutzfakoren in verschiedenen Lebensabschnitten bzw. -situationen) sowie erfolgte Aufklärungsschritte und allfällige Empfehlungenzur ergänzenden Abklärung | 3, 5 |
| | 26 | Angaben über Art, Umfang und Methoden (der beratenden, diagnostischen und therapeutischen Leistungen sowie der Pflege) | 1 – 3, 5, 6 |
| | 27 | Daten zur Anwendung von Arzneispezialitäten | 1 - 3, 5 |
| | 28 | Daten zur Abrechnung von Honoraren, vereinbartes Honorar und sonstige weitere Vereinbarungen im Rahmen des Behandlungsvertrages | 1 - 3, 5, 6 |
| | 29 | Daten zur Abrechnung von Gebühren oder Entgelte für Gutachtertätigkeit | 4, 5 |
| | 30 | Wert, Summe und Gesamtbetrag der Leistungen | 1, 5, 6 |
| | 31 | Konsultationen von Berufskollegen sowie von Angehörigen anderer Gesundheitsberufe oder sonstiger relevanter Berufe gemäß § 11b Abs. 2 MTD-G | 3, 4 |
| | 32 | Erfolgte Einsichtnahmen in die Dokumentation gemäß§ 11a Abs. 2 MTD-G | |
| | 33 | Begründung allfälliger Verweigerung der Einsichtnahme in die Dokumentation gemäß § 11a Abs.2 MTD-G | |
| Arbeitgeber | 34 | Name und Anschrift des Arbeitgebers des Hauptversicherten | 1 – 3, 5 |
| | 35 | Vor- und Familienname, akad. Grad / Titel | --- |
| Kontaktperson (nach Angabe des | 36 | Anschrift | --- |

| | | | |
|---|---|---|---|
| (nach Angabe des Patienten/ Klienten) oder gesetzlicher Vertreter des Patienten/Klienten | 37 | Telefon- und Faxnummer und andere zur Adressierung erforderliche Informationen, die sich durch moderne Kommunikationstechniken ergeben | --- |
| | 38 | Zustimmung des gesetzlichen Vertreters zur Behandlung | --- |

**Empfängerkreise**

1 Sozialversicherungsträger (einschließlich Betriebskrankenkassen) und sonstige Kostenträger im Rahmen ihrer rechtlichen Befugnisse auf Grund von Gesetzen oder Sozialversicherungsabkommen;

2 Privatversicherungen zum Zweck der Abwicklung des Versicherungsanspruches, mit ausdrücklicher Zustimmung des Patienten/Klienten, sofern diese gesetzlich erforderlich ist;

3 Ärzte, Vertreter von sonstigen Gesundheitsberufen und medizinische oder soziale Einrichtungen, in deren Behandlung der Patient steht, sowie Apotheken, mit ausdrücklicher Zustimmung des Patienten/Klienten;

4 Auftraggeber von Gutachten, soweit die rechtlichen Voraussetzungen für die Erstellung des Gutachtens vorliegen;

5 Mit der Rechtsdurchsetzung, Streitschlichtung und Klärung von Beschwerden der Patienten/Klienten und Abrechnungsansprüchen (des Verantwortlichen) betraute Stellen, insbesondere Rechtsanwälte, Gerichte, Schlichtungsstellen und Patientenanwälte, mit Zustimmung des Patienten, sofern diese gesetzlich erforderlich ist.

6 Vereine, Institutionen und sonstige Einrichtungen, für die der (freiberuflich tätige) Verantwortliche aufgrund eines Vertrages tätig ist, mit ausdrücklicher Zustimmung des Patienten/Klienten.

# B) Verrechnung ärztlich verordneter Behandlungen und diagnostischer Leistungen durch freiberuflich tätige Angehörige der gehobenen medizinisch-technischen Dienste

**Zweck der Datenanwendung:**
Verrechnung ärztlich verordneter physiotherapeutischer, logopädischer oder ergotherapeutischer Behandlungen durch freiberuflich tätige Angehörige der gehobenen medizinisch-technischen Dienste die gemäß § 7a MTD-Gesetz Bundesgesetz über die Regelung der gehobenen medizinisch-technischen Dienste, BGBl 1992/460 idgF (MTD-G) zur freiberuflichenBerufsausübung berechtigt sind (§ 135 Abs. 1 Z 1 ASVG) mit den Sozialversicherungsträgern einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie z.B. Korrespondenz) in dieser Angelegenheit.

**Rechtsgrundlagen der Anwendung sind insbesondere die folgenden Gesetze** (in der geltenden Fassung):
§ 349a Allgemeines Sozialversicherungsgesetz (ASVG), BGBl. Nr. 189/1955, (60. Novelle ASVG),
§ 193 Gewerbliches Sozialversicherungsgesetz (GSVG), BGBl. Nr. 560/1978,
§ 181 Bauern-Sozialversicherungsgesetz (BSVG), BGBl. Nr. 559/1978,
§ 3 des Bundesgesetzes über die Sozialversicherung freiberuflich selbständig Erwerbstätiger (FSVG), BGBl. Nr. 624/1978,
§ 128 Beamten- Kranken- und Unfallversicherungsgesetz (B-KUVG), BGBl. 200/1967,
Verträge abgeschlossen zwischen der beruflichen Interessensvertretung (Berufsverband) des Verantwortlichen und dem Hauptverband der österreichischen Sozialversicherungsträger bzw. dem jeweiligen Träger der Krankenversicherung gemäß §§ 338 i.V.m. § 349 Abs. 3 ASVG sowie vom Träger der Krankenversicherung abgeschlossene Einzelverträge mit freiberuflich tätigen Berufsangehörigen der im § 135 Abs. 1. Z 1 ASVG genannten gehobenen medizinisch-technischen Dienste (freiberuflich tätige PhysiotherapeutInnen, LogopädInnen, ErgotherapeutInnen).

**Höchstdauer der zulässigen Datenaufbewahrung:**
Die Daten der Patienten der verordneten Ärzte sind mindestens 7 Jahre ab Abrechnung, im Fall von Einwendungen durch die Kassen bis zum rechtskräftigen Abschluss eines entsprechenden Verfahrens aufzubewahren. Es gilt die berufsrechtliche Dokumentationspflicht i.V.m der Aufbewahrungsfrist (§ 11a) Abs. 3 MTD-Gesetz) von mindestens 10 Jahren. Darüber hinaus gelten die gesetzlichen Aufbewahrungsfristen wie insbes. die steuerrechtliche Aufbewahrungsfrist von mindestens 7 Jahren. Weiters ist es zulässig, die Daten bis zur Beendigung von allfälligen Rechtsstreitigkeiten, bei denen die Daten als Beweis benötigt werden, aufzubewahren, woraus sich die zulässsige Aufbewahrungsfrist von 30 Jahren ergibt.

**Sonstige Hinweise:**
Die Datensicherheitsmaßnahmen gemäß Art. 32 DSGVO sind zu beachten. Insbesondere hat die Übermittlung der Datensätze an den Empfänger in sicherer, verschlüsselter Form zu erfolgen.
Die Anforderungen gem. Gesundheitstelematikgesetz 2012 (GtelG) an die gesicherte, verschlüsselte Übermittlung von Gesundheitsdaten unter Gesundheitsdiensteanbietern (GDA) wie insbesondere Sozialversicherungsträgern, Krankenanstalten und niedergelassenen Gesundheitsberufen sind zu beachten.

| Betroffene Personengruppen: | Nr: | Datenarten: | Empfängerkreise: |
|---|---|---|---|
| | 01 | Sozialversicherungsnummer des Patienten | 1 |
| | 02 | Sozialversicherungsnummer des Patienten Zusatzkennzeichen | 1 |

| | | | |
|---|---|---|---|
| Patienten von Ärzten, denen eine Behandlung oder diagnostische Leistunge verordnet wurde: | 03 | Sozialversicherungsnummer des Versicherten (falls der Patient Angehöriger ist) | 1 |
| | 04 | Sozialversicherungsnummer des Versicherten Zusatzkennzeichen | 1 |
| | 05 | Bezeichnung und Nummer der Krankenkasse | 1 |
| | 06 | Ordnungsgruppe (z.B. Erwerbstätig, Pensionist, Selbstversicherer, arbeitslos), Zusatzfeld | 1 |
| | 07 | Vertragspartnernummer des rezeptausstellenden / die Verordnung ausstellenden Arztes (Rezeptidentifikation) | 1 |
| | 08 | Rezeptabgabedatum / Verordnungsabgabedatum | 1 |
| | 09 | Kennzeichen neuerlicher Einreichung | 1 |
| | 10 | Angaben zum verordneten Rezept bzw. Verordnungsschein (z.B. Art der Behandlung oder diagnostischen Leistung) | 1 |
| | 11 | Chefärztliche Genehmigung | 1 |
| | 12 | Positionsnummer der verordneten Leistung / Behandlung | 1 |
| | 13 | Tarife | 1 |
| | 14 | Selbstbehaltbefreiung | 1 |
| | 15 | Selbstbehalte / Behandlungsbeiträge / Service-Entgelt | 1 |
| | 16 | Betriebs-, Lauf – und Belegnummern | 1 |
| | 17 | Mehrwertsteuersatz bzw. Hinweis auf die unechte Umsatzsteuerbefreiung | 1 |
| | 18 | Systemdatum der Eingabe, Erfassungskennzeichen | 1 |
| Krankenkassen und sonstige Rechtsträger, auf deren Rechnung ärztlich verordnete Behandlungen | 19 | Kurzbezeichnung | 1 |
| | 20 | Krankenkassennummer | 1 |
| | 21 | Versichertengruppennummer | 1 |
| | 22 | Versichertengruppenkurzbezeichnung | 1 |

| | | | |
|---|---|---|---|
| Behandlungen durchgeführt oder diagnostische Leistungen erbracht werden: | 23 | Rezeptanzahl / Verordnungsanzahl | 1 |
| | 24 | Selbstbehalt | 1 |
| | 25 | Abrechnungszeitraum | 1 |
| | 26 | Datumsangaben | 1 |

**Empfängerkreise**

1 Zuständiger Sozialversicherungsträger und sonstige Kostenträger zum Zweck der Kostenübernahme gemäß §§ 349a, 137
und 460d ASVG, §§ 93, 193 und 231a GSVG, §§ 86, 87, 181 und 219a BSVG, § 3 FSVG,
§§ 65, 128 und 159a B-KUVG.

# III. Allgemeine Angaben zu ergriffenen Datensicherheitsmaßnahmen

Der Verantwortliche hat entsprechend des § 54 DSG die geeigneten technischen und organisatorischen Maßnahmen getroffen, um das dem Risiko angemessene Schutzniveau zu gewährleisten, insbesondere im Hinblick auf die Verarbeitung von Gesundheitsdaten als besondere Kategorien personenbezogener Daten.

# a) baulich-strukturell
# b) organisatorisch
# c) technisch, IT-Sicherheitstechnisch

**a) allgemeine Angaben zu ergriffenen baulich-strukturellen Datensicherheitsmaßnahmen**
Kreuzen Sie bitte in den nachstehenden Rubriken an, welche Datensicherheitsmaßnahmen Sie für die gemeldete Datenanwendung getroffen oder nicht getroffen haben. Soferne von Ihnen vorgesehene Datensicherheitsmaßnahmen in der Auflistung nicht angeführt sind, geben Sie bitte unter „Sonstige“ an, welche Datensicherheitsmaßnahmen Sie für die gegenständliche Datenanwendung getroffen bzw. zusätzlich getroffen haben.

**Folgende Datensicherheitsmaßnahmen wurden für die Datenverarbeitungen ergriffen / nicht ergriffen um insbesondere den Zweck zu erreichen der Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte (Zugangskontrolle) im Sinne des § 54 (2) Ziff. 1 DSG**

| | JA | NEIN | |
|---|---|---|---|
| 1. | ja | | die Räumlichkeiten der Praxis sind durch geeignete Maßnahmen vor dem Zutritt Unbefugter geschützt. (Einbruchs,- Diebstahlschutz) |
| 2. | ja | | die Zutrittsberechtigung zu den Räumlichkeiten des Verantwortlichen wurde geregelt und Maßnahmen gegen den Zutritt Unbefugter ergriffen.<br>(Vergabe von Zutrittsberechtigungen/Schlüssel entsprechend der jeweils benötigten Dateneinsicht und Aufgaben, ein Meldesystem bei Verlust von Schlüsseln/Zugangscodes besteht und ist allen bekannt) |
| 3. | ja | | Die Räumlichkeiten in denen Daten verarbeitet werden, sind innerhalb der Praxis abschließbar und vor dem Zutritt Unbefugter geschützt (z.B. Archivraum, Serverraum). Die Verarbeitung erfolgt derart, dass sie vor dem Einblick durch Unbefugte gesichert ist (Sichtschutz). Räumlichkeiten in denen Daten einsehbar/zugänglich sind, sind separat versperrbar und der Zutritt ist vor Unbefugten geschützt. |
| 4. | ja | | Der Verantwortliche hat angemessene Sicherheitsmaßnahmen getroffen, um die zur Verarbeitung genutzten Räumlichkeiten, Behältnisse und die Infrastruktur vor Untergang und Schaden insbesondere durch Brand und Überschwemmung zu schützen. Insbesondere wurden folgende Maßnahmen ergriffen …..<br>z.B. Aufbewahrung der Karteikarten in entsprechend abschließbaren als auch zum Schutz vor Brand und Wasserschaden geeigneten Karteikästen<br>z.B. Aufbewahrung der Behältnisse in entsprechenden Räumlichkeiten<br>z.B. getrennte Aufbewahrung der Daten-Sicherung (Sicherungsmedien, externe Festplatten, Server) an einem separaten Ort um das Risiko des gleichzeitigen Untergangs/ Schadens zu verhindern |
| 5. | ja | | Die Arbeitsplätze und Geräte an denen Daten verarbeitet werden, sind vor der Einsichtnahme durch Unbefugte geschützt (Sichtschutz, Bildschirmplazierung, Management des Arbeitsplatzes durch Mitarbeiter, Entsprechende Aufbewahrung der Datenverarbeitungsgeräte, Datenträger und manuellen Dateien) |

6. ja Die Daten werden derart verarbeitet, dass die Diskretion auch bei der mündlichen Kommunikation in der Praxis gewahrt bleibt. Der Aufruf der PatientInnen erfolgt lediglich mit Namen. Die weitere Kommunikation erfolgt in einer diskreten Art die gewährleistet dass Unbefugte keine Kenntnis über die Inhalte der Kommunikation erhalten. (baulich: Schalldämmung, organisatorisch: Aufruf per Namen, Diskretion bei vertraulichen Inhalten und Gesundheitsdaten, Achten auf Inhalte der Kommunikation, Unterstützung der PatientInnen im diskreten Umgang mit ihren Daten)
Hierfür wurden insbesondere durch folgende Maßnahmen ergriffen …
z.B. der Empfang gewährleistet durch den Abstand zum Wartezimmer einen akkustischen Schutz
z.B. es wurde eine baulich abgetrennte (Glasscheibe/separater Raum) Diskretionszone geschaffen
z.B. die Mitarbeiter wurden dahingehend geschult welche Informationen ausschließlich im Behandlungsraum erörtert werden und vor der Kenntnis durch Unbefugte zu schützen sind
z.B. die Mitarbeiter wurden dahingehend geschult, dass der Schutz der PatientInnendaten ausdrücklich angesprochen werden kann und PatientInnen darin bekräftigt werden, Ihre Daten diskret zu kommunizieren

7. ja die Zugriffsberechtigung auf Daten und Programme und der Schutz der Datenträger vor der Einsicht und Verwendung durch Unbefugte wurde geregelt;

8. ja die Berechtigung zum Betrieb der Datenverarbeitungsgeräte wurde festgelegt und jedes Gerät durch Vorkehrungen bei den eingesetzten Maschinen oder Programmen gegen die unbefugte Inbetriebnahme abgesichert;

9. ___ Sonstige Datensicherheitsmaßnahmen:

**b) allgemeine Angaben zu ergriffenen organisatorischen Datensicherheitsmaßnahmen**
Kreuzen Sie bitte in den nachstehenden Rubriken an, welche Datensicherheitsmaßnahmen Sie für die gemeldete Datenanwendung getroffen oder nicht getroffen haben. Soferne von Ihnen vorgesehene Datensicherheitsmaßnahmen in der Auflistung nicht angeführt sind, geben Sie bitte unter „Sonstige“ an, welche Datensicherheitsmaßnahmen Sie für die gegenständliche Datenanwendung getroffen bzw. zusätzlich getroffen haben.

**Folgende Datensicherheitsmaßnahmen wurden für die Datenverarbeitungen ergriffen / nicht ergriffen:**

___ ~~JA~~ ~~NEIN~~ _____

1 ja Die Aufgabenverteilung bei der Datenverwendung zwischen den Organisationseinheiten und zwischen den Mitarbeitern wurde ausdrücklich festgelegt;
(… das Wer, Was, Wann und Warum wurde klar festgelegt)

2. ja die Verwendung von Daten wurde an das Vorliegen gültiger Aufträge der anordnungsbefugten Organisationseinheiten und Mitarbeiter gebunden;

3. ja Die Mitarbeiter kennen Ihre Aufgaben und die zum jeweiligen Zweck notwendigen Datenverarbeitungen;
z.B. es gibt konkrete Handlungsanleitungen, Richtlinien und Checklisten um die Datenarten, Datenverwendungen dem jeweiligen Zweck und die Übermittlung an schriftliche/mündliche Freigabe durch den Verantwortlichen zu binden

4. ja Jedem Mitarbeiter ist bekannt, dass personenbezogene Daten ausschließlich aufgrund eines mündlichen/schriftlichen Auftrages des Verantwortlichen auf gesichertem Wege verschlüsselt bzw. postalisch oder per Fax (GTelG § 27) übermittelt werden dürfen;

5. ja jeder Mitarbeiter wurde über seine nach dem DSG und nach innerorganisatorischen Datenschutzvorschriften einschließlich der Datensicherheitsvorschriften bestehenden Pflichten belehrt;

6. ja Jedem Mitarbeiter ist bekannt, welche wesentlichen Verarbeitungstätigkeiten zu dokumentieren sind, insbesondere dass die Gewährung der Einsichtnahme, die Aushändigung von Kopien und die Übermittlung von Daten zu dokumentieren sind;

7. ja die Zugriffsberechtigung innerhalb der Mitarbeiter auf Daten und Programme und der Schutz der Datenträger vor der Einsicht und Verwendung durch Unbefugte wurde geregelt;

8. ja die Berechtigung zum Betrieb der Datenverarbeitungsgeräte wurde festgelegt und jedes Gerät durch Vorkehrungen bei den eingesetzten Maschinen oder Programmen gegen die unbefugte Inbetriebnahme abgesichert; (Passwörter und Zugriffsberechtigungen der einzelnen Personen sind entsprechend der bestehenden Aufträge gestaltet worden);

9. ja Die Mitarbeiter wurden dahingehend geschult, sowohl die Datenträger/-geräte und manuell geführten Aufzeichnungen, die Arbeitsplätze, die abschließbaren Aufbewahrungen der Daten als auch die Räumlichkeiten nach Abschluss der Tätigkeit versperrt und entsprechend vor Zugriff Unbefugter als auch vor Schäden/ Untergang (Wasser, Brand) gesichert zu verlassen;

10. ja — Die Mitarbeiter wurden entsprechend im sicheren Gebrauch der Endgeräte, in der richtigen Verwendung von Software (insbesondere Virenschutz, Firewall) und dem sicheren Umgang mit dem Internet geschult
- z.B. die Installation von Programmen und die Wartung der Endgeräte bedarf der Administratorenrechte
- z.B. mitgebrachte Speichermedien dürfen nur beschränkt verwendet werden
- z.B. die Speicherung von Daten auf Speichermedien und (mobilen) Endgeräten darf nur auf den Geräten (Inventarliste!) des Verantwortlichen erfolgen;

11. ja — Die Mitarbeiter wurden geschult im sorgfältigen Umgang mit risikoanfälligen Geräten, Datenträgern und Anwendungen – sie können mit sämtlichen zum Einsatz kommenden Geräten und Software sicher umgehen;

12. — Sonstige Datensicherheitsmaßnahmen:

**c) allgemeine Angaben zu ergriffenen technischen, it-technischen Datensicherheitsmaßnahmen**

Kreuzen Sie bitte in den nachstehenden Rubriken an, welche Datensicherheitsmaßnahmen Sie für die gemeldete Datenanwendung getroffen oder nicht getroffen haben. Soferne von Ihnen vorgesehene Datensicherheitsmaßnahmen in der Auflistung nicht angeführt sind, geben Sie bitte unter „Sonstige“ an, welche Datensicherheitsmaßnahmen Sie für die gegenständliche Datenanwendung getroffen bzw. zusätzlich getroffen haben.

**Folgende Datensicherheitsmaßnahmen wurden für die Datenverarbeitungen ergriffen / nicht ergriffen:**

| | **JA** | **NEIN** | |
|---|---|---|---|
| 1. | ja | | Die Computer, Festplatten und weiteren Geräte sind vor unbefugtem Zugriff (Verankerung, versperrte Aufbewahrung) und unbefugter Verwendung (Passwörter, Nutzerkennung, Bildschirmsperre) durch geeignete Maßnahmen geschützt; |
| 2. | ja | | die Computer sind durch regelmäßig aktualisierte und auf dem Stand der Technik befindlichen Virenschutz und eine Firewall (Spamfilter) geschützt. Die Aktualisierung der hierfür notwendigen Software im Wege von Updates, Servicepatches und Aktualisierungen verläuft so weit als möglich automatisch bzw. erfolgt manuell in den erforderlichen, regelmäßigen Abständen; |

3. ja der Verantwortliche hat sichergestellt, alle Geräte – sowohl Computer als auch mobile Endgeräte derart konfiguriert sind, dass auf Bildschirmen nach kurzer Zeit (ca. 5-10min.) eine Bildschirmsperre erfolgt, erst durch Eingabe des Passworts aufgehoben werden kann und dadurch die Daten vor der Einsichtnahme und Verwendung durch Unbefugte geschützt werden;

4. ja Sämtliche Geräte sind nur durch entsprechend sichere Passwörter geschützt – dies gilt auch für Speichermedien wie u.a. externe Festplatten;

5. ja Daten auf Speichermedien (z.B. externe Festplatten) sowie die Speicher von mobilen Endgeräte sind durch Passwörter geschützt , verschlüsselt und die Speichermedien werden räumlich getrennt von den Arbeitsplatzgeräten (für deren Daten sie eine Sicherung enthalten) und versperrt aufbewahrt;

6. ja Der Verantwortliche hat sicher gestellt dass Backups und Speicherungen (soweit möglich automatisch) in regelmässigen Abständen erfolgen;

7. ja Der Verantwortliche hat sicher gestellt dass in regelmäßigen Abständen die Funktionsfähigkeit der Geräte und Speichermedien als auch die einwandfreie Funktionsfähigkeit der Wiederherstellung der gespeicherten Daten überprüft wird;

8. ja Der Verantwortliche hat sicher gestellt, dass öffentlich zugängliche Netzwerke („WLAN“) die in der Praxis betrieben werden (z.B. im Warteraum für PatientInnen) gesichert betrieben werden, sodass über diesen Zugang kein Zugriff auf nicht öffentlich betriebene Systeme des Verantwortlichen möglich ist als auch kein Zugriff durch Unbefugte auf die Netzwerke möglich ist;

9. ja Der Verantwortliche hat sicher gestellt, dass kein Zugriff auf und keine Nutzung durch Unbefugte auf öffentlich zugänglichen Netzwerkanschlüsse (z.B. Steckdosen, Anschlüsse) erfolgen kann;

10. ja Der Verantwortliche hat Sorge dafür getragen, dass alle verwendeten Datenverarbeitungsgeräte (Computer, Laptops, Tablets, Diensthandys), Speichergeräte (Server, externe Festplatten) und Speichermedien (USB-Sticks, wesentliche DVD/ CD-Speicherungen) vollständig inventarisiert sind und bei ihrem Verlust sowohl benannt werden kann welche Daten untergegangen/ entwendet wurden als auch durch welche Speicherung sie wiederhergestellt werden können;

11. ja — Die Lösung von Daten erfolgt in einer adäquaten Form, welche sowohl in Hinblick auf physische Daten (Schreddern) als auch in Hinblick auf elektronische Daten und verwendete Speichermedien (Löschen durch Überschreiben von Festplatten und Speichermedien) eine sichere Löschung die eine Wiederherstellung/ein Auslesen der Daten durch Unbefugte verhindert gewährleistet ist;

12. ja — Der Verantwortliche stellt sicher, dass insbesondere zum Zwecke der Übertragung und Speicherung von Gesundheitsdaten ausschließlich entsprechend zertifizierte Softwareprodukte (Zertifizierung durch HVB) verwendet werden die die gesetzlichen Anforderungen an eine gesicherte, verschlüsselte Übertragungsart entsprechend dem GTelG und DSG gewährleisten;

13. = Sonstige Datensicherheitsmaßnahmen:

## IV. Vertraglich niedergelegte organisatorische Datensicherheitsmaßnahmen

## a) Schweigeklausel in Dienstverträgen, Verpflichtungserklärung zum Datengeheimnis

## b) Mitarbeiter-Datenbelehrung im Zusammenhang mit dem Nachweis erfolgter Schulungen

## V. Auftragsverarbeiter

## a) Auflistung der eingesetzten Auftragsverarbeiter samt Nennung der jeweiligen vertraglichen Grundlage

## b) Datenverarbeitungsverzeichnisse der unter a) genannten Auftragsverarbeiter - Dokumentation über die durch die Auftragsverarbeiter an die/den Verantwortlichen übermittelten Datenverarbeitungsverzeichnisse

Gemäß § 49 Abs. 3 DSG hat jeder Auftragsverarbeiter ein Verzeichnis zu allen Kategorien von im Auftrag eines Verantwortlichen durchgeführten Verarbeitungstätigkeiten zu führen.
Diese Verarbeitungsverzeichnisse sind an den jeweiligen Verantwortlichen zu übermitteln.

## c) Auftragsverarbeiter-Verträge