DATENVERARBEITUNGSVERZEICHNIS

für freiberuflich tätige Physiotherapeut*Innen
als datenschutzrechtlich Verantwortliche für die Datenverarbeitung
in Entsprechung des Art 30 Abs 1 DSGVO und § 49 DSG
(Physiotherapeut*innen sind Angehörige der im MTD-Gesetz 2024 gesetzlich geregelten, gehobenen medizinisch-therapeutisch-diagnostischen Gesundheitsberufe)

VERANTWORTLICHE:

Jeannine Gravogl BSc.

BERUFSBEZEICHNUNG:

gemäß § 1 (1) Z.6 i.V.m. § 3 (1) MTDG

Physiotherapeutin

REGISTRIERUNGSNUMMER:

gemäß § 27 (1) Z. 5 MTDG i.V.m. Gesundheitsberuferegister-Gesetz (GBRG)

18-GBR-057354

BERUFSSITZ-ADRESSE:

gemäß § 30 MTDG i.V.m. Gesundheitsberuferegister-Gesetz (GBRG)

Brunner Gasse 1-9/2/6
2380 Perchtoldsdorf

INHALTSVERZEICHNIS

I. Stammdatenblatt: Allgemeine Angaben zur Verantwortlichen

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

a) Patient*innenverwaltung (Dokumentation u. Auskunftserteilung) und Honorarabrechnung
b) Verrechnung im Rahmen der Berufsausübung (gem. Berufsbild) erbrachter Leistungen durch Physiotherapeut*innen

III. Allgemeine Beschreibung der gesetzten Datensicherheitsmaß-nahmen

a) baulich-strukturell
b) organisatorisch
c) technisch, IT-Sicherheitsstruktur

IV. Vertraglich niedergelegte organisatorische Datensicherheitsmaßnahmen

a) Schweigeklausel in Dienstverträgen, Verpflichtungserklärung zum Datengeheimnis
b) Mitarbeiter-Datenbelehrung im Zusammenhang mit dem Nachweis erfolgter Schulungen

V. Durch die Verantwortliche herangezogene Auftragsverarbeiter

a) Auflistung der eingesetzten Auftragsverarbeiter samt Nennung der jeweiligen vertraglichen Grundlage
b) Durchgeführte Datenverarbeitungen der unter a) genannten Auftragsverarbeiter i.R. der beauftragten Leistungen - Dokumentation über die durch die Auftragsverarbeiter an die/den Verantwortlichen übermittelten Aufzeichnungen der Verarbeitungstätigkeiten
c) Auftragsverarbeiter-Verträge

I. Stammdatenblatt: Allgemeine Angaben zur Verantwortlichen

1. NAME DER VERANTWORTLICHEN:

Jeannine Gravogl BSc.

2. BERUFSBEZEICHNUNG:

Physiotherapeutin

3. REGISTRIERUNGSNUMMER IM GESUNDHEITSBERUFEREGISTER:

18-GBR-057354

4. BERUFSSITZ-ADRESSE:

Brunner Gasse 1-9/2/6
2380 Pertchtoldsdorf

5. KONTAKTDATEN DER VERANTWORTLICHEN

+43 681 81645351
kontakt@physio-mitte.at

Brunner Gasse 1-9/2/6
2380 Pertchtoldsdorf

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

Die Rechtsgrundlagen der Datenverarbeitung i.R. der Berufsausübung sind insbesondere die folgenden Gesetze und Verordnungen (in der geltenden Fassung):

- Bundesgesetz über die gehobenen medizinisch-therapeutisch-diagnostischen Gesundheitsberufe (MTD-Gesetz 2024 – MTDG) StF: BGBl. I Nr. 100/2024
- Bundesgesetz über die Registrierung von Gesundheitsberufen (Gesundheitsberuferegister-Gesetz – GBRG) StF: BGBl. I Nr. 87/2016
- Datenschutz – Grundverordnung (DSGVO); Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung). Sie ist mit 01.05.2018 mit unmittelbarer Rechtswirkung in den Mitgliedsstaaten der EU in Kraft getreten.
- Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz – DSG) StF: BGBl. I Nr. 165/1999
- Gesundheitstelematikgesetz 2012 – GTelG 2012; StF: BGBl. I Nr. 111/2012

Berufsrechtliche Grundlagen - Gesetzliche Ermächtigung zur Verarbeitung besonderer Datenkategorien gem. Art. 9 DSGVO i.V.m. § 41 MTDG:

Das MTDG als Berufsgesetz der Physiotherapeut*innen enthält die gesetzliche Ermächtigung im Sinne des Art. 9 DSGVO zur Datenverarbeitung im Rahmen der Berufsausübung als Physiotherapeut/Physiotherapeutin. Der § 41 des MTDG legt die Zwecke der Datenverarbeitung im Rahmen der Berufsausübung, welche in der Erfüllung des Behandlungsvertrages und der als Nebenpflichten zu erfüllenden gesetzlichen Berufspflichten liegen, im Detail wie folgt dar. Originalauszug MTD-Gesetz 2024 – MTDG:

> „§ 41. (1) Angehörige der MTD Berufe sind *ermächtigt, die im Rahmen der Berufsausübung nach den Bestimmungen dieses Bundesgesetzes erforderlichen personenbezogenen Daten zum Zweck*
>
> *1. der Dokumentation (§ 34),*

2. *der Auskunftserteilung (§ 35),*
3. *der Honorarabrechnung (§ 36 Abs. 2 Z 3)*

unter Einhaltung der Verordnung (EU) Nr. 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (DSGVO), ABl. Nr. L 119 vom 04.05.2016 S. 1, zuletzt berichtigt durch ABl. Nr. L 74 vom 04.03.2021 S. 35, und des Datenschutzgesetzes (DSG), BGBl. I Nr. 165/1999, zu verarbeiten.“

sowie weiter:

„(3) Hinsichtlich der Verarbeitung personenbezogener Daten gemäß Abs. 1 und 2 sind die Rechte und Pflichten gemäß Art. 13, 14, 18 und 21 DSGVO ausgeschlossen.“

A) Patient*innenverwaltung (Dokumentation, Auskunftserteilung) und Honorarabrechnung über physiotherapeutische Leistungen
Zweck der Datenverarbeitung:
Wahrnehmung der Berufspflichten bei Erfüllung des Behandlungsvertrages (§§ 32ff. MTDG) namentlich der Abwicklung der sorgfaltsgemäßen Behandlung/Leistung unter Erfüllung der gesetzlich vorgesehenen interdisziplinären und interprofessionellen Zusammenarbeit (§ 33 MTDG), Führung von Patient*innen-/Klient*innenkarteien zur Dokumentation (§ 34 MTDG), Auskunftserteilung (§ 35 MTDG) sowie gesetzlicher Anzeigepflicht (§ 37 MTDG); Erstellung von Gutachten (soweit die rechtlichen Voraussetzungen für die Erstellung eines Gutachtens vorliegen) und Honorarverrechnung im Rahmen der freiberuflichen/selbständigen Berufsausübung durch Physiotherapeut*innen (§ 39 (4) i.V.m. § 36 Abs. 2 Z 3 MTDG) einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie z.B. Korrespondenz) in diesen Angelegenheiten.

Höchstdauer der zulässigen Datenaufbewahrung:
Die Daten der Patient*innen/Klient*innen sind gemäß § 34 Abs. 3 MTDG 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 je nach Erfordernis die zulässige Aufbewahrungsfrist von max. 30 Jahren.

Sonstige Hinweise:
Die Datensicherheitsmaßnahmen in diesem Verzeichnis wurden gemäß Art. 32 DSGVO gewählt und sind zu beachten. Die Verarbeitung der Gesundheitsdaten aufgrund der Berufsausübung eines gesetzlich geregelten Gesundheitsberufes erfordert die Einhaltung der gesetzlichen Anforderungen gem. Gesundheitstelematikgesetz 2012 (GtelG) an die gesicherte, verschlüsselte Übertragung von Gesundheitsdaten unter Gesundheitsdiensteanbietern (GDA) wie insbesondere Sozialversicherungsträgern, Krankenanstalten und freiberuflich tätigen Angehörige gesetzlich geregelter Gesundheitsberufe und kann nicht rechtswirksam von Patient*innenseite abbedungen werden. **Die Übermittlung der Datensätze an die Empfänger (Gesundheitsdaten als besondere Datenkategorie nach Art. 9 DSGVO) darf ausschließlich in gesicherter, verschlüsselter Form erfolgen**. Mit der Novelle des GTelG mit BGBl. I Nr. 105/2024 die im GTelG definierte Ausnahme von der verschlüsselten und gesicherten Übermittlung von Gesundheitsdaten zwischen Gesundheitsdiensteanbietern, nämlich die bis 31.12.2024 unter bestimmten Voraussetzungen zulässige Übermittlung per Fax mit 01.01.2025 endgültig ausgelaufen. Es sind geeignete professionelle Softwarelösungen für den Gesundheitsbereich zu verwenden.

Betroffene Personengruppen	Nr	Datenarten	Empfängerkreise
Patient*innen/ Klient*innen der/des Verantwortlichen sowie Patient*innen/Klient*innen von verordnenden Ärzt*innen; verordnenden Gesundheitsdienste-anbietern	01	Patient*innen-/ Klient*innennummer, Protokollnummer	1 - 5
	02	Vor- und Familienname, akad. Grad / Titel, frühere Namen (Namensteile)	1 - 6
	03	Anschrift	1 - 6
	04	Telefon,-/Mobilnummer und andere zur Kommunikation und 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
	12	Sonstige Daten zur Sozialversicherung (insbesondere der Name, das Geburtsdatum und die Sozialversicherungsnummer der/des Hauptversicherten sowie das Verwandtschaftsverhältnis zur/zum Hauptversicherten bei mitversicherten Patient*innen und Daten des Antrages auf Kostenerstattung 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 der/des Verantwortlichen (Anlass, Datum, Art u. Zahl der physiotherapeutischen Leistungen/Behandlungen/Einheiten samt Aufschlüsselung als Kassenleistung nach Rahmenvereinbarungen)	1, 2, 5, 6
	17	Daten zur Verwaltung von Terminen und Wartelisten	---
	18	Zustand der Person bei Übernahme der Behandlung, Betreuung oder Beratung	3 - 5
	19	Anamnese (Familien,- und Eigenanamnese, Berufsanamnese)	---
	20	Vorbehandlungen samt dazugehöriger (fremder) Dokumente, Informationen, welche Teil der Dokumentation werden	---
	21	Diagnosen (auch Fremddiagnosen) zu Behandlungsbeginn und bei Beendigung samt dazugehöriger (fremder) Dokumente, Informationen, welche Teil der Dokumentation werden	1, 3 - 6
	22	Besondere Risikofaktoren, z.B. Allergien, tätigkeitsbedingte Einflüsse, familiäre Disposition	3 - 5
	23	Vorgeschichte der Erkrankung, für die Physiotherapie relevante Kontraindikationen und Medikation im gesamten Verlauf samt dazugehöriger Befunde, Informationen,	3 - 5

		Dokumente	
	24	Gutachtliche Äusserungen des Verantwortlichen (z.B. gegenüber Auftraggeber*innen von Gutachten)	4
	25	Behandlungs,-/ Beratungsverlauf, Rückfragen/Rückmeldungen an die/den verordnende/behandelnde Ärzt*in, besondere Vorkommnisse während der Behandlung wie insbesondere atypischer Heilungsverlauf, Weiterverweis an behandelnde Ärzt*in, andere Behandler*innen samt Gründen; Behandlungsabbruch samt Gründen	3 - 5
	26	Information an Patient*innen/Klient*innen (insbesondere über Gesundheitsrisiken und Schutzfaktoren in verschiedenen Lebensabschnitten bzw. -situationen) sowie erfolgte Aufklärungsschritte und allfällige Empfehlungen zur ergänzenden Abklärung, Weiterverweis an behandelnde Ärzt*in und Aufklärung über gesundheitliche Risiken und notwendige Schritte insbesondere bei Behandlungsabbruch	3, 5
	27	Angaben über Art, Umfang und Methoden der therapeutischen Leistungen	1 – 3, 5, 6
	28	Daten zur Anwendung von Arzneispezialitäten (z.B. im Rahmen der Atemtherapie angewendete, ärztlich verordnete Medikation)	1 - 3, 5

	29	Daten zur Abrechnung von Honoraren, vereinbartes Honorar und sonstige weitere Vereinbarungen im Rahmen des Behandlungsvertrages	1 - 3, 5, 6
	30	Daten zur Abrechnung von Gebühren oder Entgelte für Gutachtertätigkeit	4, 5
	31	Wert, Summe und Gesamtbetrag der Leistungen	1, 5, 6
	32	Konsultationen von verordnenden bzw. behandelnden Ärzt*innen und Berufskolleg*innen sowie von Angehörigen anderer Gesundheitsberufe oder sonstiger relevanter Berufe gemäß § 33 MTDG und § 35 MTDG	3, 4
	33	Erfolgte Einsichtnahmen in und Kopien aus der Dokumentation und erteilte Auskünfte gemäß § 35 MTDG	
	34	Begründung allfälliger Verweigerung der Einsichtnahme in die Dokumentation gemäß § 35 MTDG	
Arbeitgeber*in	35	Name und Anschrift der/des Arbeitgeber*in der/des Hauptversicherten	1 – 3, 5
Kontaktperson (nach Angabe der/s Patient*in/Klient*in) bzw. gesetzliche oder bevollmächtigte Vertretung der/des Patient*in/Klient*in	36	Vor- und Familienname, akad. Grad / Titel	---
	37	Anschrift	---
	38	Telefon- und Faxnummer und andere zur Adressierung und Kommunikation erforderliche Informationen, die sich durch moderne Kommunikationstechniken ergeben	---
	39	Zustimmung der gesetzlichen oder	---

		bevollmächtigen Vertretung zur Behandlung bzw. in die gesetzten Maßnahmen	

Empfängerkreise

1. Gesetzliche Sozialversicherungsträger und weitere gesetzlich beauftragte Kostenträger (wie insbes. die Länder, einschließlich der Krankenfürsorgeanstalten - KFA) im Rahmen ihrer rechtlichen Befugnisse auf Grund von Gesetzen oder Sozialversicherungsabkommen;
2. Privatversicherungen zum Zweck der Abwicklung des Versicherungsanspruches, mit ausdrücklicher Zustimmung der/des Patient*in/Klient*in, sofern diese gesetzlich erforderlich ist;
3. die Verordnung zur Behandlung ausstellende Ärzt*innen im Rahmen der gesetzlichen Rückmelde,-Rückfragepflicht bei Durchführung der ärztlich verordneten Maßnahmen; gesetzliche oder bevollmächtigte Vertretung selbiger; sowie mit ausdrücklicher Zustimmung der/des Patient*in/Klient*in: Angehörige anderer gesetzlich geregelter Gesundheitsberufe und medizinischer oder sozialer Einrichtungen, in deren Behandlung bzw. Betreuung der Patient/die Patientin nebst der Behandlung durch die verordnenden Ärzt*innen steht, sowie Apotheken;
4. Auftraggeber*innen von Gutachten (privat, gerichtlich, öffentlich), soweit die rechtlichen Voraussetzungen für die Erstellung des Gutachtens vorliegen und mit Zustimmung der/des Patient*in, sofern diese gesetzlich erforderlich ist;
5. mit der Rechtsdurchsetzung, Streitschlichtung und Klärung von Beschwerden der Patient*in/Klient*in bzw. der/des Verantwortlichen und Abrechnungsansprüchen (der/des Verantwortlichen) betraute Stellen, insbesondere Rechtsanwält*innen, Gerichte, Schlichtungsstellen und Patient*innenanwaltschaften, mit Zustimmung der/des Patient*in, sofern diese gesetzlich erforderlich ist;
6. Vereine, Institutionen und sonstige Einrichtungen, für welche die/der (freiberuflich tätige) Verantwortliche aufgrund eines Vertrages tätig wird jedoch nur mit ausdrücklicher Zustimmung der/des Patient*in/Klient*in.

B) Verrechnung/Honorarabrechnung (gem. § 36 Abs. 2 Z. 3 MTDG) im Rahmen der Berufsausübung (gem. § 28 MTDG) durch Physiotherapeut*innen erbrachter ärztlich verordneter Leistungen mit den Trägern der Sozialversicherung

Zweck der Datenverarbeitung:
Verrechnung/Honorarabrechnung über physiotherapeutische Leistungen, welche durch freiberuflich tätige Physiotherapeut*innen, die gem. MTDG i.V.m. GBRG zur freiberuflichen Berufsausübung berechtigt sind (Erfüllung der Kriterien des § 135 Abs. 1 Z 1 ASVG), im Rahmen der berufsrechtlich definierten Berufsausübung (§ 28 MTDG) durchgeführt wurden mit den Trägern der gesetzlichen Sozialversicherungsträgern einschließlich automations-unterstützt erstellter und archivierter Textdokumente (wie z.B. Korrespondenz) in dieser Angelegenheit.
Es handelt sich um Leistungen, welche nach ärztlicher oder zahnärztlicher Anordnung gem. § 20 Abs. 1 MTDG durchgeführt wurden und daher in Verbindung mit § 135 Abs. 1 Z. 1 ASVG Pflichtleistungen der gesetzlichen Sozialversicherung darstellen.

Rechtsgrundlagen sind insbesondere die folgenden Gesetze
(jeweils in der geltenden Fassung):
§ 36 Abs. 2 Z. 3 MTDG
§§ 135 Abs. 1 Z.1 i.V.m. 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,
sowie Verträge abgeschlossen zwischen der beruflichen Interessensvertretung (Physio Austria als Berufsverband) der/des Verantwortlichen und dem Dachverband 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 MTD-Berufe.

Rahmenvereinbarung über die Erbringung physiotherapeutischer Leistungen durch freiberuflich tätige Physiotherapeutinnen und Physiotherapeuten abgeschlossen zwischen Physio Austria einerseits und der Österreichischen Gesundheitskasse(ÖGK) andererseits) i.d.g.F. Rahmenvereinbarung über die Erbringung physiotherapeutischer Leistungen durch freiberuflich tätige Physiotherapeutinnen und Physiotherapeuten abgeschlossen zwischen Physio Austria einerseits und der Sozialversicherungsanstalt der Selbständigen (SVS) i.d.g.F. andererseits.

Rahmenvereinbarung über die Erbringung physiotherapeutischer Leistungen durch freiberuflich tätige Physiotherapeutinnen und Physiotherapeuten abgeschlossen zwischen Physio Austria einerseits und der Versicherungsanstalt öffentlich Bediensteter, Eisenbahnen und Bergbauandererseits (BVAEB) i.d.g.F. andererseits.

Rechtsgrundlage: u.a. *Originalauszug § 28 (1) MTDG – Berufsausübung:*

> *„§ 28. (1) Die Berufsausübung der MTD-Berufe besteht in der eigenverantwortlichen Ausübung der im jeweiligen Berufsbild gemäß §§ 4 bis 24 umschriebenen Tätigkeiten, unabhängig davon, ob diese Tätigkeiten freiberuflich oder im Rahmen eines Arbeitsverhältnisses ausgeführt werden.“*

Höchstdauer der zulässigen Datenaufbewahrung:
Abrechnungsdaten der Patient*innen und der verordneten Ärzte*innen 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 gem. § 34 MTDG: Die Daten der Patient*innen/Klient*innen sind gemäß § 34 Abs. 3 MTDG 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 je nach Erfordernis die zulässige Aufbewahrungsfrist von max. 30 Jahren.

Sonstige Hinweise:
Die Datensicherheitsmaßnahmen gemäß Art. 32 DSGVO sind zu beachten. **Insbesondere hat die Übermittlung der Datensätze an die Empfänger ausschließlich in gesicherter, verschlüsselter Form zu erfolgen. Bei Gesundheitsdaten als besondere Datenkategorie nach Art. 9 DSGVO ist ein besonderes Schutzniveau verpflichtend einzuhalten.** Dieses ist u.a. dadurch gekennzeichnet, dass eine Verschlüsselungspflicht für die Übermittlung von Gesundheitsdaten durch Gesundheitsdiensteanbieter (= sogenannte GDA gemäß GTelG, dies sind insbesondere freiberuflich tätige Gesundheitsberufe, Gesundheitseinrichtungen, Sozialversicherungsträger und weitere Institutionen des Gesundheitswesens) gem. GTelG gilt. **Die Anforderungen gem. Gesundheitstelematikgesetz 2012 (GtelG) an die gesicherte, verschlüsselte Übermittlung von Gesundheitsdaten unter Gesundheitsdiensteanbietern (GDA) sind einzuhalten.** Mit der Novelle des GTelG mit BGBl. I Nr. 105/2024 die im GTelG definierte Ausnahme von der verschlüsselten und gesicherten Übermittlung von Gesundheitsdaten zwischen Gesundheitsdiensteanbietern, nämlich die bis 31.12.2024 unter bestimmten Voraussetzungen gegebene Zulässigkeit einer **Übermittlung per Fax ist mit 01.01.2025 endgültig ausgelaufen**. Es sind daher für die elektronische Übermittlung ausschließlich geeignete professionelle Softwarelösungen für den Gesundheitsbereich zu verwenden, welche die DSGVO-konforme, gesicherte und verschlüsselte Übermittlung zwischen GDAs als auch an Patient*innen garantieren.

Betroffene Personengruppen	Nr	Datenarten	Empfängerkreise
Patient*innen von Ärzt*innen, denen Behandlungen oder diagnostische Leistungen verordnet wurden:	01	Sozialversicherungsnummer der/des Patient*in	1
	02	Sozialversicherungsnummer der/des Patient*in Zusatzkennzeichen	1
	03	Sozialversicherungsnummer der/des Versicherten (falls die/der Patient *in mitversicherte/r Angehörige/r ist)	1
	04	Sozialversicherungsnummer der/des Versicherten, Zusatzkennzeichen	1
	05	Bezeichnung und Nummer der Krankenkasse	1
	06	Ordnungsgruppe (z.B. Erwerbstätig, Pensionist, Selbstversicherer, arbeitslos), Zusatzfeld	1
	07	Vertragspartnernummer der/des rezeptausstellenden / die Verordnung ausstellenden Ärzt*in (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 Bewilligung	1
	12	Positionsnummer der verordneten Leistung / Behandlung	1
	13	Tarife	1
	14	Selbstbehaltsbefreiung	1
	15	Selbstbehalte / Behandlungsbeiträge /	1

		Service-Entgelt	
	16	Betriebs-, Lauf – und Belegnummern	1
	17	Hinweis auf die unechte Umsatzsteuerbefreiung für berufsbildmäßige Leistungen im Rahmen der Berufsausübung gem. § 28 MTDG (bzw. Hinweis auf den Mehrwertsteuersatz)	1
	18	Systemdatum der Eingabe, Erfassungskennzeichen	1
Krankenkassen und sonstige Rechtsträger, auf deren Rechnung ärztlich verordnete Behandlungen durchgeführt oder diagnostische Leistungen erbracht werden:	19	Kurzbezeichnung	1
	20	Krankenkassennummer	1
	21	Versichertengruppennummer	1
	22	Versichertengruppenkurzbezeichnung	1
	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 gem. Art. 9 DSGVO welche ein entsprechend erhöhtes Schutzniveau erfordern.

a) baulich-strukturell
b) organisatorisch
c) technisch, IT-Sicherheitsstruktur

a) allgemeine Angaben zu ergriffenen baulich-strukturellen Datensicherheitsmaßnahmen

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

	JA	NEIN	
1.	**X**		die Räumlichkeiten der physiotherapeutischen Praxis sind durch geeignete Maßnahmen vor dem Zutritt Unbefugter geschützt. Insbesondere sind die Räumlichkeiten absperrbar.
2.	**X**		die Zutrittsberechtigung zu den Räumlichkeiten des Verantwortlichen wurde geregelt und Maßnahmen gegen den Zutritt Unbefugter ergriffen. Insbesondere erfolgt keine Schlüsselausgabe an Dritte. Ersatzschlüssel werden sicher in einem verschlossenen Kasten verwahrt.
3.	**X**		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.	**X**		Die 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 erfolgt die Datenspeicherung ausschließlich online bei einem Dienstanbieter für Praxissoftware (ein Auftragsverarbeitungsvertrag liegt vor).
5.	**X**		Die Arbeitsplätze und Geräte an denen Daten verarbeitet

			werden, sind vor der Einsichtnahme durch Unbefugte geschützt (Sichtschutz, Bildschirmplatzierung, entsprechende Aufbewahrung der Datenverarbeitungsgeräte).
6.	**X**		Die Daten werden derart verarbeitet, dass die Diskretion auch bei der mündlichen Kommunikation in der Praxis gewahrt bleibt. Der Aufruf der Patient*innen 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 und Sichtschutz, organisatorisch: Aufruf per Namen, Diskretion bei vertraulichen Inhalten und Gesundheitsdaten, Achten auf Inhalte der Kommunikation, Unterstützung der Patient*innen im diskreten Umgang mit ihren Daten). Insbesondere werden über den Namen hinausgehende Daten ausschließlich im Behandlungszimmer kommuniziert, der Schutz der Patient*innendaten ausdrücklich angesprochen und Patient*innen darin bekräftigt werden, Ihre Daten diskret zu kommunizieren.
7.	**X**		die Zugriffsberechtigung auf Daten und Programme und der Schutz der Datenträger vor der Einsicht und Verwendung durch Unbefugte wurde geregelt; Insbesondere sind die entsprechenden Datenverarbeitungsgeräte mit einem Passwort geschützt.
8.	**X**		die Berechtigung zum Betrieb der Datenverarbeitungsgeräte wurde festgelegt und jedes Gerät durch Vorkehrungen bei den eingesetzten Maschinen oder Programmen/Applikationen gegen die unbefugte Inbetriebnahme abgesichert; Insbesondere sind die entsprechenden Datenverarbeitungsgeräte mit einem Passwort geschützt.

b) allgemeine Angaben zu ergriffenen organisatorischen Datensicherheitsmaßnahmen

Folgende Datensicherheitsmaßnahmen wurden für die Datenverarbeitungen ergriffen / nicht ergriffen:

	JA	NEIN	
1.	**X**		Die Aufgabenverteilung bei der Datenverarbeitung zwischen den Organisationseinheiten und zwischen den Mitarbeiter*innen als auch deren Verantwortlichkeiten wurden ausdrücklich festgelegt;
2.	**X**		die Verwendung von Daten wurde an das Vorliegen gültiger Aufträge der anordnungsbefugten Mitarbeiter*innen bzw. Personen gebunden;
3.	**X**		die Mitarbeiter*innen kennen Ihre Aufgaben und die zum jeweiligen Zweck notwendigen Datenverarbeitungen; z.B. es gibt konkrete Handlungsanleitungen, Richtlinien und Checklisten um die Datenarten, Datenverarbeitungen dem jeweiligen Zweck und die Übermittlung an schriftliche/mündliche Freigabe durch den Verantwortlichen zu binden;
4.	**X**		jeder/m Mitarbeiter*in ist bekannt, dass personenbezogene Daten ausschließlich aufgrund eines mündlichen/schriftlichen Auftrages des Verantwortlichen auf elektronischem Wege gesichert und verschlüsselt bzw. postalisch übermittelt werden dürfen. Die dafür zur Verfügung gestellte professionelle Software ist allen Mitarbeiter*innen in allen Aspekten der sicheren Verwendung bekannt und sie sind in der sicheren Anwendung geschult;
5.	**X**		jede/r Mitarbeiter*in wurde über seine nach dem DSG und nach innerorganisatorischen Datenschutzvorschriften einschließlich der Datensicherheitsvorschriften bestehenden Pflichten belehrt;
6.	**X**		jede/r Mitarbeiter*in 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.	**X**		die Zugriffsberechtigung unter den Mitarbeiter*innen auf Daten und Programme und der Schutz der Datenträger vor der Einsicht und Verwendung durch Unbefugte wurde geregelt;
8.	**X**		die Berechtigung zum Betrieb der Datenverarbeitungsgeräte wurde festgelegt und jedes Gerät durch Vorkehrungen bei den eingesetzten Geräten und Programmen (Hard- und Software) gegen die unbefugte Inbetriebnahme abgesichert; (Passwörter und Zugriffsberechtigungen der einzelnen Personen sind entsprechend der bestehenden Aufträge gestaltet worden);

9.	**X**		die Mitarbeiter*innen 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.	**X**		die Mitarbeiter*innen wurden entsprechend im sicheren Gebrauch der Endgeräte, in der richtigen und sicheren Verwendung von Software (insbesondere Virenschutz, Firewall) und dem sicheren und Umgang als auch (Surf-) Verhalten mit dem Internet geschult: - die Installation von Programmen und die Wartung der Endgeräte bedarf der Administratorenrechte; - mitgebrachte Speichermedien dürfen nicht verwendet werden; - die Speicherung von Daten auf Speichermedien und (mobilen) Endgeräten darf nur auf den Geräten der/des Verantwortlichen erfolgen.
11.	**X**		Die Mitarbeiter*innen wurden im sorgfältigen Umgang mit risikoanfälligen Geräten, Datenträgern und Anwendungen geschult – sie können mit sämtlichen zum Einsatz kommenden Geräten und mit der verwendeten Software sicher umgehen;

Die Belegschaft besteht ausschließlich aus der Verantwortlichen.

c) allgemeine Angaben zu ergriffenen technischen Datensicherheits-maßnahmen und zur IT-Sicherheitsstruktur

Folgende Datensicherheitsmaßnahmen wurden für die Datenverarbeitungen ergriffen / nicht ergriffen:

	JA	NEIN	
1.	**X**		Die Endgeräte (Computer, PC, Laptop, Festplatten) und weiteren Geräte sind vor unbefugtem Zugriff (versperrte Aufbewahrung) und unbefugter Verwendung (Passwörter, Nutzerkennung, Bildschirmsperre) durch geeignete Maßnahmen geschützt;
2.	**X**		die Endgeräte sind durch regelmäßig aktualisierte und auf dem Stand der Technik befindlichen Virenschutz und eine Firewall 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 durch die berechtigten Personen (Administratorenrechte sind geregelt vergeben);
3.	**X**		die Verantwortliche hat sichergestellt, dass alle Geräte – sowohl Computer als auch mobile Endgeräte - derart konfiguriert sind, dass auf Bildschirmen nach kurzer Zeit (ca. 5-10min.) eine Bildschirmsperre erfolgt, die erst durch Eingabe des Passworts aufgehoben werden kann und dadurch die Daten vor der Einsichtnahme und Verwendung durch Unbefugte geschützt werden;
4.	**X**		sämtliche Geräte sind durch entsprechend sichere Passwörter geschützt – dies gilt auch für den Onlinespeicher der verwendeten Praxissoftware;
5.	**X**		Daten im Onlinespeicher der verwendeten Praxissoftware sowie die Speicher von mobilen Endgeräten sind durch Passwörter geschützt, verschlüsselt und werden versperrt aufbewahrt;
6.	**X**		die Verantwortliche hat sicher gestellt, dass zwecks Datensicherung Backups und Speicherungen (soweit möglich automatisch) in regelmäßigen Abständen erfolgen;
7.	**X**		die 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.	**X**		die Verantwortliche hat sicher gestellt, dass öffentlich/intern zugängliche Netzwerke („WLAN“), die in der Praxis betrieben werden (z.B. im Warteraum für Patient*innen) 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; Insbesondere werden aktuelle Protokolle wie WPA3 und sichere Passwörter verwendet.
9.	**X**		die Verantwortliche hat sicher gestellt, dass kein Zugriff auf und keine Nutzung durch Unbefugte auf allgemein in der Praxis zugängliche Netzwerkanschlüsse erfolgen kann; Insbesondere wird kein kabelbasiertes Netzwerk verwendet.
10.	**X**		die Verantwortliche hat Sorge dafür getragen, dass alle verwendeten Datenverarbeitungsgeräte (Computer, Laptops, Tablets, Diensthandys), Speichergeräte (Server, externe Festplatten; Cloud-Server; Plattformen) 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.	**X**		die Löschung von Daten erfolgt in einer adäquaten Form, welche sowohl in Hinblick auf physische Daten (Vernichtung der Daten bzw. Datenträger insbesondere durch sog. Schreddern) als auch in Hinblick auf elektronische Daten und verwendete Speichermedien (Löschen durch Überschreiben von Festplatten und Speichermedien) eine sichere Löschung gewährleistet ist, die eine Wiederherstellung/ein Auslesen der Daten durch Unbefugte verhindert; Insbesondere wird die DSGVO-konforme Löschung der in der Cloud gespeicherten Daten über den Auftragsverarbeitungsvertrag mit dem Betreiber gewährleistet.
12.	**X**		die Verantwortliche stellt sicher, dass insbesondere zum Zwecke der Übertragung und Speicherung von Gesundheitsdaten ausschließlich DSGVO-konforme, professionelle, für den Gesundheitsbereich entsprechend geeignete Softwareprodukte verwendet werden, die die gesetzlichen Anforderungen an eine gesicherte, verschlüsselte Übertragung von Gesundheitsdaten entsprechend dem GTelG und DSG gewährleisten. Insbesondere wird eine als Praxissoftware (Synaptos) zugelassene Software verwendet.

IV. Vertraglich niedergelegte organisatorische Datensicherheitsmaßnahmen

a) Schweigeklausel in Dienstverträgen, Verpflichtungserklärung zum Datengeheimnis

Die gesamte Belegschaft besteht ausschließlich aus der Verantwortlichen.

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

Die gesamte Belegschaft besteht ausschließlich aus der Verantwortlichen.

V. Auftragsverarbeiter*in

Rechtsgrundlagen: Auftragsverarbeiter*in
DSG § 48 Abs. 1:

> *„Auftragsverarbeiter*in und Aufsicht über die Verarbeitung § 48. (1) Erfolgt eine Verarbeitung im Auftrag einer/eines Verantwortlichen, so arbeitet diese/r nur mit Auftragsverarbeiter*innen, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieses Bundesgesetzes erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.“*

DGS § 48 Abs. 3:

> *„§ 48 Auftragsverarbeiter*in und Aufsicht über die Verarbeitung Abs. (3) Die Verarbeitung durch eine/einen Auftragsverarbeiter*in erfolgt auf der Grundlage eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder aufgrund ausdrücklicher gesetzlicher Ermächtigung, der oder das die/den Auftragsverarbeiter*in in Bezug auf den Verantwortlichen bindet und in dem Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte der/des Verantwortlichen festgelegt sind. Dieser Vertrag oder dieses andere Rechtsinstrument sieht insbesondere vor, dass die/der Auftragsverarbeiter*in (…).“*

DGS § 48 Abs. 5:

> *„Der Vertrag oder das andere Rechtsinstrument im Sinne der Abs. 3 und 4 ist schriftlich abzufassen, was auch in einem elektronischen Format erfolgen kann.“*

a) Auflistung der eingesetzten Auftragsverarbeiter*in samt Nennung der jeweiligen vertraglichen Grundlage

Patient*innen-Verwaltung

Synaptos GmbH
St. Veiter Straße 188/1 EG
9020 Klagenfurt am Wörthersee
Österreich

https://synaptos.at

Homepage und Mail-Server

World4You Internet Services GmbH
Hafenstrasse 47-51
4020 Linz
Österreich

https://www.world4you.com

Steuerberatung und Buchhaltung

Mag. Rainer Tiefenböck
Steuerberatung | Unternehmerberatung
Vienna Twin Tower Turm A
Wienerbergstraße 11
1100 Wien

https://www.tiefenboeck.at

b) Verzeichnisse der Daten-Verarbeitungstätigkeiten der unter a) genannten Auftragsverarbeiter*in welche im Rahmen der Erfüllung des vertraglichen Auftrages an die/den Verantwortlichen (gem. § 48 DSG) durchgeführt werden.

Dies stellt eine Dokumentation dar über die durch die/den Auftragsverarbeiter*in an die Verantwortliche mit erfolgten Aufträgen verbundenen, übermittelten Verarbeitungstätigkeiten welche aus dem jeweiligen Auftragsverarbeiter-Vertrag resultieren und gem. § 48 Abs. 3) DSG schriftlich abzufassen sind.

Rechtsgrundlage: insbes. Originalauszug aus der DSGVO Art. 30 (sowie s. obig § 48 DSG):

DSGVO Art 30 Abs. 2:

> *„(2) Jede/r Auftragsverarbeiter*in und gegebenenfalls sein/e Vertreter*in führen ein Verzeichnis zu allen Kategorien von im Auftrag einer/eines Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung, die Folgendes enthält:…“*

DSGVO Art 30 Abs. 4:

> *„(4) Die/der Verantwortliche oder die/der Auftragsverarbeiter*in sowie gegebenenfalls die/der Vertreter*in der/des Verantwortlichen oder der/des Auftragsverarbeiter*in/s stellen der Aufsichtsbehörde das Verzeichnis auf Anfrage zur Verfügung.“*

Die von unseren Auftragsverarbeitern erstellten Verarbeitungsverzeichnisse finden Sie am Ende dieses Dokuments bzw. können von unserer Webseite im Bereich Datenschutz (https://www.physio-mitte.at/datenschutz/) heruntergeladen werden.

c) Auftragsverarbeiter*innen-Verträge

Rechtsgrundlage:
u.a. Originalauszug aus dem DSG

DSG § 48 Abs. 3:

> *„§ 48 Auftragsverarbeiter*in und Aufsicht über die Verarbeitung Abs. (3) Die Verarbeitung durch eine/n Auftragsverarbeiter*in erfolgt auf der Grundlage eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder aufgrund ausdrücklicher gesetzlicher Ermächtigung, der oder das die/den Auftragsverarbeiter*in in Bezug auf die/den Verantwortliche/n bindet und in dem Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte der/des Verantwortlichen festgelegt sind. Dieser Vertrag oder dieses andere Rechtsinstrument sieht insbesondere vor, dass die/der Auftragsverarbeiter*in (...).“*

DGS § 48 Abs. 5:

> *„§ 48 Auftragsverarbeiter*in und Aufsicht über die Verarbeitung Abs. (5) Der Vertrag oder das andere Rechtsinstrument im Sinne der Abs. 3 und 4 ist schriftlich abzufassen, was auch in einem elektronischen Format erfolgen kann.“*

Die von uns mit den Auftragsverarbeitern abgeschlossenen Auftragsverarbeitungsverträge finden Sie am Ende dieses Dokuments bzw. können auf unserer Webseite im Bereich Datenschutz (https://www.physio-mitte.at/datenschutz/) heruntergeladen werden.

Vertrag
über eine
Auftragsverarbeitung nach Art. 28 DSGVO

zwischen
Synaptos GmbH
St. Veiter Straße 188/1 EG
9020 Klagenfurt am Wörthersee
Österreich

– im Folgenden „Synaptos" genannt –
als „Auftragsverarbeiter" gemäß DSGVO

und

Vorname:	JEANNINE
Nachname:	GRAVOGL
Adresse:	BRUNNERGASSE 1-9/2/6
PLZ:	2380
Ort:	PERCHTOLDSDORF

- im Folgenden „Auftraggeber" genannt –
als „Verantwortlicher" gemäß DSGVO

Stand: November 2025

Präambel

1. Dieser Vertrag konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Vertragsparteien im Rahmen einer Verarbeitung von personen- und gesundheitsbezogenen Daten im Auftrag, die sich aus der am [Datum] abgeschlossenen Nutzungsvereinbarung ergeben und nach der Synaptos, eine Spezialsoftware für Selbstständige im Gesundheitswesen und die für den Betrieb erforderliche IT-Infrastruktur als Dienstleister dem Auftraggeber zur Verfügung stellt.
2. Dieser Vertrag findet auf alle Tätigkeiten Anwendung, bei denen Mitarbeiter von Synaptos oder durch Synaptos beauftragte Unterauftragnehmer (Subunternehmer) personen- und gesundheitsbezogenen Daten des Auftraggebers in dessen Auftrag verarbeiten.
3. In diesem Vertrag verwendete Begriffe sind entsprechend ihrer Definition in der EU-Datenschutz-Grundverordnung zu verstehen und auszulegen. In diesem Sinne ist der Auftraggeber der Verantwortliche und Synaptos der Auftragsverarbeiter.

Gegenstand des Vertrages

Art der Daten	Zweck der Verarbeitung	Art der Verarbeitung	Kategorien der betroffenen Personen
Stammdaten (Anrede, Vorname, Nachname, Anschrift, Telefonnummer, E- Mail-Adresse, Geburtsdatum, Sprache, Geschlecht, Sozialversicherungsnummer, Adresse, PLZ, Stadt, Land, Einwilligung zur DSGVO und Bankverbindung)	Stammdaten-verwaltung	Erfassen, Verändern, Speichern, Lesen, Löschen der Daten	Patienten des Auftraggebers
Stammdaten (Titel, Vorname, Nachname, Straße, PLZ, Stadt, Land, E- Mail-Adresse, Telefonnummer, Fachgebiet)	Stammdaten-verwaltung	Erfassen, Verändern, Speichern, Lesen, Löschen der Daten	Ärzte des Auftraggebers
Kalendereinträge	Terminmanagement	Erfassen, Verändern, Speichern, Lesen, Absagen, Löschen der Daten	Patienten des Auftraggebers
Anamnese	Behandlungsdoku-mentation	Erfassen, Verändern, Speichern, Lesen, Löschen der Daten, Hochladen	Patienten des Auftraggebers
Befunderhebung	Behandlungsdoku-mentation	Erfassen, Verändern, Speichern, Lesen, Löschen der Daten	Patienten des Auftraggebers
Patienteninformationen (z.B. Befunde, Diagnosen, ...)	Behandlungsdoku-mentation	Erfassen, Verändern, Speichern, Lesen, Löschen der Daten, Hochladen	Patienten des Auftraggebers
Erbrachte Leistung	Behandlungsdoku-mentation	Erfassen, Verändern, Speichern, Lesen, Löschen der Daten	Patienten des Auftraggebers
Abrechnungsdaten	Leistungsverrech-nung	Erfassen, Verändern, Speichern, Lesen, Löschen der Daten	Patienten des Auftraggebers
Belegverwaltung	Einnahmen- & Aus-gabenverwaltung	Erfassen, Speichern, Lesen, Hochladen, Löschen der Daten	Patienten des Auftraggebers, Krankenkassen, Lief-eranten

1. Gegenstand dieses Auftrages ist die Durchführung folgender Aufgaben, deren Aufgaben Synaptos übernimmt: Die Therapiesoftware umfasst Funktionen der Stammdatenverwaltung, des Terminmanagements, der Behandlungsdokumentation, der Behandlungsverrechnung sowie der Einnahmen und Ausgabenverwaltung. Abhängig vom gewählten Paket stehen dem Auftraggeber eine definierte Auswahl von Funktionen zur Verfügung.

2. Die folgenden Daten sind Bestandteil der Datenverarbeitung:

a. Dauer des Vertrages

- Der Vertrag ist auf unbestimmte Zeit geschlossen und kann vom Auftraggeber jederzeit gekündigt werden. Mit Beendigung des dieses Vertrages zu Grunde liegenden Nutzungsvertrages gilt auch dieser Vertrag als gekündigt. Mit der Kündigung des Vertrages geht die Verantwortung zur gesetzlichen Aufbewahrung der gespeicherten Daten an den Auftraggeber über. Während der Vertragslaufzeit stehen dem Auftraggeber entsprechende Downloadfunktionen zur Verfügung. Die Möglichkeit zur außerordentlichen Kündigung aus wichtigem Grund seitens des Auftragnehmers bleibt unberührt und ist im §9 der AGBs geregelt.

b. Anwendungsbereich und Verantwortlichkeit

- Synaptos verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Der Auftraggeber ist für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an Synaptos in Form der Eingabe personen- und gesundheitsbezogener Daten Dritter in die zur Verfügung gestellte Software für Therapeuten, sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich (»Verantwortlicher« im Sinne des Art. 4 Nr. 7 DSGVO).

c. Pflichten des Auftragnehmers

- Synaptos bestätigt, das Bekanntsein der einschlägigen, allgemeinen datenschutzrechtlichen Vorschriften und beachtet die Grundsätze ordnungsgemäßer Datenverarbeitung.
- Synaptos sichert zu, dass die zur Verarbeitung eingesetzten Personen vor Beginn der Verarbeitung mit den relevanten Bestimmungen des Datenschutzes und dieses Vertrags vertraut gemacht wurden. Synaptos führt mit diesen Personen regelmäßig angemessene Schulungs- und Sensibilisierungsmaßnahmen im Hinblick auf Datenschutz durch und trägt dafür Sorge, dass zur Auftragsverarbeitung eingesetzte Personen hinsichtlich der Erfüllung der Datenschutzanforderungen laufend angemessen angeleitet und überwacht werden.
- Auskünfte an Dritte oder Betroffene wird Synaptos nur nach vorheriger Zustimmung durch den Auftraggeber erteilen. Direkt an Synaptos gerichtete Anfragen wird Synaptos unverzüglich an den Auftraggeber weiterleiten.
- Soweit gesetzlich verpflichtet, bestellt Synaptos eine fachkundige und zuverlässige Person als Datenschutzbeauftragten und stellt dabei sicher, dass für den Beauftragten keine Interessenskonflikte bestehen. In Zweifelsfällen kann sich der Auftraggeber direkt an den Datenschutzbeauftragten wenden. Synaptos teilt dem Auftraggeber unverzüglich die Kontaktdaten des Datenschutzbeauftragten mit oder begründet, weshalb kein Beauftragter bestellt wurde. Änderungen in der Person oder den innerbetrieblichen Aufgaben des Beauftragten teilt Synaptos dem Auftraggeber unverzüglich mit.

- Synaptos verarbeitet personenbezogene Daten ausschließlich wie vertraglich vereinbart oder wie vom Auftraggeber angewiesen, es sei denn, Synaptos ist gesetzlich zu einer bestimmten Verarbeitung verpflichtet. Sofern solche Verpflichtungen für Synaptos bestehen, teilt Synaptos diese dem Auftraggeber vor der Verarbeitung mit, es sei denn, die Mitteilung ist gesetzlich verboten. Synaptos verwendet darüber hinaus die zur Verarbeitung überlassenen Daten für keine anderen, insbesondere nicht für eigene Zwecke.
- Synaptos erklärt rechtsverbindlich, dass alle mit der Datenverarbeitung beauftragten Personen vor Aufnahme der Tätigkeit zur Vertraulichkeit verpflichtet werden oder diese einer der Art der verarbeiteten Daten angemessenen gesetzlichen Verschwiegenheitsverpflichtung unterliegen. Insbesondere bleibt die Verschwiegenheitsverpflichtung der mit der Datenverarbeitung beauftragten Personen auch nach Beendigung ihrer Tätigkeit und Ausscheiden bei Synaptos aufrecht.
- Synaptos erklärt rechtsverbindlich, dass alle erforderlichen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung nach Art 32 DSGVO ergriffen werden (Einzelheiten sind der Anlage 1 zu entnehmen).
- Synaptos ergreift die technischen und organisatorischen Maßnahmen, damit der Auftraggeber die Rechte der betroffenen Person nach Kapitel III der DSGVO (Information, Auskunft, Berichtigung und Löschung, Datenübertragbarkeit, Widerspruch, sowie automatisierte Entscheidungsfindung im Einzelfall) innerhalb der gesetzlichen Fristen jederzeit erfüllen kann und überlässt dem Auftraggeber alle dafür notwendigen Informationen. Wird ein entsprechender Antrag an
- Synaptos gerichtet und lässt dieser erkennen, dass der Antragsteller ihn irrtümlich für den Auftraggeber der von ihm betriebenen Datenanwendung hält, hat Synaptos den Antrag unverzüglich an den Auftraggeber weiterzuleiten und dies dem Antragsteller mitzuteilen.
- Synaptos unterstützt den Auftraggeber bei der Einhaltung der in den Art 32 bis 36 DSGVO genannten Pflichten (Datensicherheitsmaßnahmen, Meldungen von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde, Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person, Datenschutz-Folgeabschätzung, vorherige Konsultation).
- Synaptos erstellt ein Verarbeitungsverzeichnis zu allen Kategorien der im Auftrag durchgeführten Tätigkeiten nach Art 30 DSGVO und stellt diese dem Auftraggeber zur Verfügung.
- Dem Auftraggeber wird hinsichtlich der Verarbeitung der von ihm überlassenen Daten das Recht jederzeitiger Einsichtnahme und Kontrolle, sei es auch durch ihn beauftragte Dritte, der Datenverarbeitungseinrichtungen eingeräumt. Synaptos verpflichtet sich, dem Auftraggeber jene Informationen zur Verfügung zu stellen, die zur Kontrolle der Einhaltung der in diesem Vertrag genannten Verpflichtungen notwendig sind.
- Möchte der Auftraggeber die Dienstleistung im klassischen Sinne von Synaptos nicht mehr nutzen, so kann er die vollständige Datenübergabe verlangen oder Synaptos mit der Speicherung der Daten über die gesetzliche Aufbewahrungsfrist beauftragen. Im Falle der Speicherung über die gesetzliche Aufbewahrungsfrist läuft der Vertrag eingeschränkt weiter und es gilt nach wie vor der vorhandene Vertrag.

- Sonst gilt der Vertrag als beendet und Synaptos ist verpflichtet, alle Verarbeitungsergebnisse und Unterlagen, die Daten enthalten, dem Auftraggeber zu übergeben und nach vollständiger Übergabe auf den eigenen Systemen zu löschen. Wenn Synaptos die Daten in einem speziellen technischen Format verarbeitet, sind wir verpflichtet, die Daten nach Beendigung dieses Vertrages entweder in diesem Format oder nach Wunsch des Auftraggebers in dem Format, in dem er die Daten vom Auftraggeber erhalten hat oder in einem anderen, gängigen Format herauszugeben.
- Synaptos hat den Auftraggeber unverzüglich zu informieren, falls er der Ansicht ist, eine Weisung des Auftraggebers verstößt gegen Datenschutzbestimmungen der Union oder der Mitgliedstaaten.

d. Pflichten des AUFTRAGGEBERS

- Für die Beurteilung der Zulässigkeit der beauftragten Verarbeitung sowie für die Wahrung der Rechte von Betroffenen ist allein der Auftraggeber verantwortlich.
- Der Auftraggeber erteilt alle Aufträge, Teilaufträge oder Weisungen dokumentiert. In Eilfällen können Weisungen mündlich erteilt werden. Solche Weisungen wird der Auftraggeber unverzüglich dokumentiert bestätigen.
- Der Auftraggeber informiert Synaptos unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

e. Ort der Durchführung der Datenverarbeitung

- Alle Datenverarbeitungstätigkeiten werden ausschließlich innerhalb der EU bzw. des EWR durchgeführt.

f. Sub-Auftragsverarbeiter

- Synaptos ist befugt folgende Unternehmen als Sub-Auftragsverarbeiter hinzuziehen:

Name & Anschrift des Subunternehmers	Beschreibung der Teilleistungen
MEDIALINE	Technischer Betrieb der Server
iBasis	SMS-Versand

- Beabsichtigte Änderungen von Sub-Auftragsverarbeitern werden dem Auftraggeber schriftlich bekanntgegeben. Synaptos schließt den Vertrag im Sinne des Art 28 Abs. 4 DSGVO mit dem Sub-Auftragsverarbeiter ab. Dabei wird sichergestellt, dass der Sub- Auftragsverarbeiter dieselben Verpflichtungen eingeht, die Synaptos auf Grund dieses Vertrages obliegen. Kommt der Sub-Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet Synaptos gegenüber dem Auftraggeber für die Einhaltung der Pflichten des Sub-Auftragsverarbeiters.
- Die Verantwortlichkeiten von Synaptos und des Subunternehmers sind eindeutig voneinander abzugrenzen.
- Synaptos wählt Subunternehmer unter besonderer Berücksichtigung der Eignung

der vom Subunternehmer getroffenen technischen und organisatorischen Maßnahmen sorgfältig aus.

g. Sicherheit der Verarbeitung

- Die in Anlage 1 beschriebenen Datensicherheitsmaßnahmen werden als verbindlich festgelegt. Sie definieren das von Synaptos geschuldete Minimum.
- Die Datensicherheitsmaßnahmen können der technischen und organisatorischen Weiterentwicklung entsprechend angepasst werden, solange das hier vereinbarte Niveau nicht unterschritten wird. Zur Aufrechterhaltung der Informationssicherheit erforderliche Änderungen hat Synaptos unverzüglich umzusetzen. Änderungen werden dem Auftraggeber unverzüglich mitgeteilt.
- Soweit die getroffenen Sicherheitsmaßnahmen den Anforderungen des Auftraggebers nicht oder nicht mehr genügen, benachrichtigt Synaptos den Auftraggeber hierüber.
- Synaptos sichert zu, dass die im Auftrag verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.
- Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Ausgenommen sind technisch notwendige, temporäre Vervielfältigungen, soweit eine Beeinträchtigung des hier vereinbarten Datenschutzniveaus ausgeschlossen ist.

h. Regelungen zur Berichtigung, Löschung und Sperrung von Daten

- Im Rahmen des Auftrags verarbeitete Daten wird Synaptos nur entsprechend der getroffenen vertraglichen Vereinbarung oder nach Weisung des Auftraggebers berichtigen, löschen oder sperren.
- Den entsprechenden Weisungen des Auftraggebers zur Löschung, Sperrung oder Berichtigung wird Synaptos auch über die Beendigung dieses Vertrages hinaus Folge leisten.

i. Vergütung

- Die Vergütung von Synaptos ist abschließend im Nutzungsvertrag mit dem Auftraggeber geregelt. Eine gesonderte Vergütung oder Kostenerstattung im Rahmen dieses Vertrages erfolgt nicht.

j. Haftung

- Synaptos ist im Rahmen der Auftragsverarbeitung darauf angewiesen, dass die vom Auftraggeber weitergegebenen Daten rechtskonform verarbeitet werden dürfen. Wird Synaptos von Dritten, insbesondere Patienten oder Kunden des Auftraggebers diesbezüglich in Anspruch genommen, hält der Auftraggeber Synaptos klag- und schadlos.
- Synaptos haftet dem Auftraggeber für Schäden, die Synaptos, die Mitarbeiter von Synaptos bzw. die von Synaptos mit der Vertragsdurchführung Beauftragten oder die von eingesetzten Subdienstleister im Zusammenhang mit der Erbringung der beauftragten vertraglichen Leistung schuldhaft verursachen.
- Absatz (2) gilt nicht, soweit der Schaden durch die korrekte Umsetzung der beauftragten Dienstleistung oder einer vom Auftraggeber erteilten Weisung entstanden ist.

k. Sonstiges

- Beide Parteien sind verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen der jeweils anderen Partei auch über die Beendigung des Vertrages vertraulich zu behandeln. Bestehen Zweifel, ob eine Information der Geheimhaltungspflicht unterliegt, ist sie bis

zur schriftlichen Freigabe durch die andere Partei als vertraulich zu behandeln.

- Für Nebenabreden ist die Schriftform und die ausdrückliche Bezugnahme auf diese Vereinbarung erforderlich. Das Schriftformgebot gilt auch für ein Abgehen vom Schriftformgebot.
- Sollten einzelne Teile dieses Vertrages unwirksam sein, so berührt dies die Wirksamkeit des Vertrages im Übrigen nicht.

Ort/Datum Perchtoldsdorf, 17.9.2026

Für den Auftraggeber:

Name

Klagenfurt, November 2025

Für synaptos:

Alexander Doboczky (Geschäftsführung)

ANLAGE 1
TECHNISCH-ORGANISATORISCHE MASSNAHMEN

1. Vertraulichkeit

• Zutrittskontrolle:
Maßnahmen, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen die personenbezogenen Daten verarbeitet und genutzt werden, zu verwehren:

o Die Büroräumlichkeiten von Synaptos sind mit einem elektronischen Schließsystem gesichert. Die Daten selbst werden bei der Firma Medialine gespeichert.
o Medialine betreibt ein mehrschichtiges Zutrittssystem zu den Datenverarbeitungsanlagen. Sämtliche Mitarbeiter erhalten angepasste Zutrittskarten, die nur für den jeweiligen Bereich gültig sind. Zutritt zu den Schrankanlagen bzw. Zutrittstüren sind nur mittels eigener Schlüssel bzw. Telefonnummern mit Absenderkennung möglich. Die gesamten Räumlichkeiten des Ortes der Datenverarbeitung (Rechenzentrum) sind flächendeckend durch Überwachungskameras geschützt.

• Zugangskontrolle:
Maßnahmen, um zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können:

o Der Auftraggeber erhält Zugriff auf einem sicheren und verschlüsselten Weg. Der Auftraggeber verwaltet seine Zugriffe selbständig.
o Die Zugangskontrolle erfolgt mittels Benutzername (E-Mail-Adresse) und Passwort. Das Passwort muss mindestens 9 Zeichen lang, Groß-, Kleinbuchstaben, Ziffern und Sonderzeichen beinhalten. Für die Verwaltung des Passwortes ist der Auftraggeber selbst verantwortlich.
o Sämtliche Zugriffe auf die Systeme werden protokolliert.
o Nach 5 erfolglosen Login-Versuchen, wird das Benutzerkonto für 10 Minuten gesperrt.

• Zugriffskontrolle:
Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können:

o Sämtliche Zugriffe auf die Systeme erfolgen auf Web-Basis und werden mittels Sicherheitszertifikat mit 256 Bit verschlüsselt.
o Die Verwaltung der Daten erfolgt mittels Datenbank-Mandantenkonzept. Jeder Auftraggeber besitzt seinen eigenen Mandanten. Grundsätzlich besitzt der Auftraggeber exklusive Zugriffsrechte (Erstellen, Lesen, Verändern und Löschen von Daten).
o Im Zuge der Zusammenarbeit in Gruppenpraxen, besteht die Möglichkeit, dass der Auftraggeber definierten Personen spezifische Rechte auf Funktionen gewähren kann. (z.B. im Terminmanagement: Anlegen, Ändern, Lesen und Löschen von Kalendereinträgen).

o Die Berechtigungsvergabe mit Hinblick auf den zur Verfügung stehenden Funktionsumfang, ist in Form von Standard-Berechtigungsprofilen organisiert. Abhängig vom gewählten Paket, wird dem Auftraggeber automatisch ein Berechtigungsprofil zugeordnet. Ändert der Auftraggeber das Paket, so ändert sich das Berechtigungsprofil automatisch mit.
o Sämtliche Zugriffe auf Netzwerk- und Systemebene (z.B. Firewall, Router, Webserver, Applikationsserver, ...) werden von der Firma Medialine protokolliert. Die ist erforderlich, um die Datensicherheit sicherzustellen.
o Alle Zugriffe auf Applikationsebene werden seitens Synaptos protokolliert (z.B. Homepage, Portal, Applikations- und Dantebankadministration sowie Kalendersynchronisierung).

2. Integrität

• Weitergabekontrolle:
Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transportes oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist:

o Grundsätzlich verläuft der Datenaustausch über eine state-of-the-art Punkt-zu-Punkt Verschlüsselung zwischen Server und Endgerät.
o Bei einzelnen Funktionen (z.B. SMS-Versand, Kalendersynchronisierung, E-Mail-Versand) obliegt dem Auftraggeber die Kontrolle der Weitergabe bzw. Nutzung der Funktion. In diesen Fällen hat der Auftraggeber selbst zu entscheiden, ob eine Zustimmung der Betroffenen erforderlich ist.
o Seitens Synaptos erfolgt eine Protokollierung aller Übertragungsvorgänge.

• Eingabekontrolle:
Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt wurden.

o Es erfolgt eine Protokollierung/Dokumentation der Eingabe, letzten Änderung, Entfernung und Löschung von Daten.
o Es erfolgt die Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts.

3. Verfügbarkeit und Belastbarkeit

• Verfügbarkeitskontrolle:
Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind und bei Zwischenfällen rasch wiederhergestellt werden können.

Medialine ergreift folgende Maßnahmen zur Sicherung der Verfügbarkeit:
o ISO 9001 und ISO 27001 Zertifizierungen garantieren höchste Standards in Qualitätsmanagement und IT-Sicherheit.
o Die Medialine Datacenter sind mit modernster Infrastruktur sowie Hard- und Software ausgestattet und werden rund um die Uhr überwacht.
o Die Wiederherstellbarkeit kann innerhalb von 24 Stunden während der Werktage erfolgen.

o Medialine setzt ebenso auf Nachhaltigkeit und Energieeffizienz, indem sie die Server-Racks optimal klimatisieren, hocheffiziente Netzteile einsetzen oder den Energiebedarf anhand der Betriebstemperatur bedarfsgerecht anpassen.

Die Löschung einer Datenbank erfolgt ausschließlich nach schriftlicher Aufforderung durch den Auftraggeber. Im Falle einer Vertragsauflösung kann die Datenbank per Datenträger zur Verfügung gestellt werden oder eine Beauftragung zur Fortführung der Datenspeicherung über die gesetzliche Aufbewahrungsfrist erfolgen.

• Trennungskonzept
Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind und bei Zwischenfällen rasch wiederhergestellt werden können.

o Es kommt ein Mandantenkonzept zum Einsatz, bei der jeder Auftraggeber über eine physikalisch getrennte Datenbank (Schema) verfügt.
o Weiters werden die vom Auftraggeber hochgeladenen Dokumente in einer separaten Verzeichnisstruktur abgelegt.

World4You Internet Services GmbH
Wolfgang-Pauli-Straße 2, BT3
4020 Linz

Tel.: +43 50 5859
E-Mail: office@world4you.com
www.world4you.com

World4You Auftragsverarbeitungsvertrag (AVV - nach Art. 28 Abs. 3 Datenschutz-Grundverordnung)

1. Gegenstand und Dauer der Verarbeitung

1.1 Gegenstand der Vereinbarung sind die Rechte und Pflichten der Parteien im Rahmen der Leistungserbringung gemäß Leistungsbeschreibung und AGB (nachfolgend Hauptvertrag), soweit eine Verarbeitung von personenbezogenen Daten durch World4You (nachfolgend Auftragnehmer) als Auftragsverarbeiter für den Kunden als Verantwortlicher (nachfolgend Auftraggeber) gemäß Art. 28 DSGVO erfolgt. Dies umfasst alle Tätigkeiten, die der Auftragnehmer zur Erfüllung des Auftrags erbringt und die eine Auftragsverarbeitung darstellen. Dies gilt auch, sofern der Auftrag nicht ausdrücklich auf diese Vereinbarung zur Auftragsverarbeitung verweist.

1.2 Die Dauer der Verarbeitung entspricht der im Vertrag vereinbarten Laufzeit.

2. Art und Zweck der Verarbeitung

2.1 Die Art der Verarbeitung umfasst alle Arten von Verarbeitungen im Sinne der DSGVO zur Erfüllung des Auftrags.

2.2 Zwecke der Verarbeitung sind alle zur Erbringung der vertraglich vereinbarten Leistung (siehe hierzu auch Anhang 1 Leistungsbeschreibung), insbesondere im Bereich Cloud-Dienstleistungen, Hosting, Software as a Service (SaaS) und IT-Support, erforderlichen Zwecke.

3. Art der personenbezogenen Daten und Kategorien von Betroffenen

3.1 Die Art der verarbeiteten Daten bestimmt der Auftraggeber durch die Produktwahl, die Konfiguration, die Nutzung der Dienste und die Übermittlung von Daten. Siehe hierzu auch die Leistungsbeschreibung Anhang 1.

3.2 Die Kategorien von Betroffenen bestimmt der Auftraggeber durch die Produktwahl, die Konfiguration, die Nutzung der Dienste und die Übermittlung von Daten. Siehe hierzu auch die Leistungsbeschreibung Anhang 1.

4. Verantwortlichkeit und Verarbeitung auf dokumentierte Weisungen

4.1 Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung

allein verantwortlich (»Verantwortlicher« im Sinne des Art. 4 Nr. 7 DSGVO). Dies gilt auch im Hinblick auf die in dieser Vereinbarung geregelten Zwecke und Mittel der Verarbeitung.

4.2 Die Weisungen werden anfänglich durch den Hauptvertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in einem elektronischen Format (Textform) durch einzelne Weisungen geändert werden (Einzelweisung). Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen. Bei Änderungsvorschlägen teilt der Auftragnehmer dem Auftraggeber mit, welche Auswirkungen sich auf die vereinbarten Leistungen, insbesondere die Möglichkeit der Leistungserbringung, Termine und Vergütung ergeben. Ist dem Auftragnehmer die Umsetzung der Weisung nicht zumutbar, so ist der Auftragnehmer berechtigt, die Verarbeitung zu beenden. Eine Unzumutbarkeit liegt insbesondere vor, wenn die Leistungen in einer Infrastruktur erbracht werden, die von mehreren Auftraggebern / Kunden des Auftragnehmers genutzt wird (Shared Services), und eine Änderung der Verarbeitung für einzelne Auftraggeber nicht möglich oder nicht zumutbar ist.

4.3 Die vertraglich vereinbarte Datenverarbeitung findet in der Regel überwiegend in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt, sofern nicht zur Erbringung der Leistung der Datentransfer in Drittstaaten erforderlich wird. Für den Fall, dass eine Übermittlung in einen Drittstaat erfolgt, stellt der Auftragnehmer sicher, dass die Voraussetzungen nach Art. 44 ff. DSGVO erfüllt sind.

5. Rechte des Auftraggebers, Pflichten des Auftragnehmers

5.1 Der Auftragnehmer darf Daten von betroffenen Personen nur im Rahmen des Auftrages und der dokumentierten Weisungen des Auftraggebers verarbeiten, außer es liegt ein Ausnahmefall im Sinne des Artikel 28 Abs. 3 a) DSGVO vor (Verpflichtung nach dem Recht der Europäischen Union oder eines Mitgliedstaates). Dies bezieht sich auch auf Übermittlungen von personenbezogenen Daten an Drittländer oder internationale Organisationen. Besteht eine Verarbeitungspflicht entgegen einer Weisung, so informiert der Auftragnehmer vor der Verarbeitung den Auftraggeber über die entsprechende rechtliche Anforderung, es sei denn, das betreffende Recht verbietet eine solche Information wegen eines wichtigen öffentlichen Interesses. Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Der Auftragnehmer darf die Umsetzung der Weisung solange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde. Die Weisungen sind durch den Auftraggeber zu dokumentieren und mindestens für die Dauer des Auftragsverhältnisses aufzubewahren.

5.2 Der Auftragnehmer unterstützt den Auftraggeber angesichts der Art der Verarbeitung nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung der Ansprüche der betroffenen Personen nach Kapitel III der DSGVO. Der Auftragnehmer ist berechtigt, für diese Leistungen eine angemessene Vergütung vom Auftraggeber zu verlangen, soweit die Unterstützung nicht aufgrund eines Gesetzes- oder Vertragsverstoßes durch den

Auftragnehmer erforderlich wurde. Der Auftragnehmer wird dem Auftraggeber vorab eine Kosteninformation zukommen lassen.

5.3 Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in den Artikeln 32 bis 36 DSGVO genannten Pflichten. Der Auftragnehmer ist berechtigt, für diese Leistungen eine angemessene Vergütung vom Auftraggeber zu verlangen, soweit die Unterstützung nicht aufgrund eines Gesetzes- oder Vertragsverstoßes durch den Auftragnehmer erforderlich wurde. Der Auftragnehmer wird dem Auftraggeber vorab eine Kosteninformation zukommen lassen.

5.4 Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeitern und anderen für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits-/ Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.

5.5 Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden. Der Auftragnehmer trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen für die betroffenen Personen.

5.6 Der Auftragnehmer gewährleistet die schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DSGVO ausübt. Eine Kontaktmöglichkeit wird auf der Webseite des Auftragnehmers veröffentlicht.

5.7 Nach Abschluss der Erbringung der Verarbeitungsleistungen löscht der Auftragnehmer nach Wahl des Auftraggebers entweder alle personenbezogenen Daten oder gibt sie dem Auftraggeber zurück, sofern nicht nach dem Unionsrecht oder nach dem anwendbaren Recht eines Mitgliedstaates eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht oder sich aus jeweiligen vertraglichen Vereinbarungen etwas anderes ergibt. Macht der Auftraggeber von diesem Wahlrecht keinen Gebrauch, gilt die Löschung als vereinbart. Wählt der Auftraggeber die Rückgabe, kann der Auftragnehmer eine angemessene Vergütung verlangen. Der Auftragnehmer wird dem Auftraggeber vorab eine Kosteninformation zukommen lassen.

5.8 Machen betroffene Personen Schadensersatzansprüche nach Art. 82 DSGVO geltend, unterstützt der Auftragnehmer den Auftraggeber bei der Abwehr der Ansprüche im Rahmen seiner Möglichkeiten. Der Auftragnehmer kann hierfür eine angemessene Vergütung verlangen.

6. Pflichten des Auftraggebers

6.1 Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Durchführung des Auftrags Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

6.2 Im Falle der Beendigung verpflichtet sich der Auftraggeber, diejenigen personenbezogenen Daten vor Vertragsbeendigung zu löschen, die er in den Diensten gespeichert hat.

6.3 Auf Anforderung des Auftragnehmers benennt der Auftraggeber einen Ansprechpartner in Datenschutzangelegenheiten.

7. Anfragen betroffener Personen

Wendet sich eine betroffene Person mit Forderungen zur Berichtigung, Löschung oder Auskunft an den Auftragnehmer, wird der Auftragnehmer die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber nach Angaben der betroffenen Person möglich ist. Der Auftragnehmer leitet den Antrag der betroffenen Person unverzüglich an den Auftraggeber weiter. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten. Der Auftragnehmer haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

8. Maßnahmen zur Sicherheit der Verarbeitung gemäß Art. 32 DSGVO

8.1 Der Auftragnehmer ergreift in seinem Verantwortungsbereich geeignete technische und organisatorische Maßnahmen, um sicherzustellen, dass die Verarbeitung gemäß den Anforderungen der DSGVO erfolgt und den Schutz für die Rechte und Freiheiten der betroffenen Person gewährleistet. Der Auftraggeber ergreift in seinem Verantwortungsbereich gemäß Art. 32 DSGVO geeignete technische und organisatorische Maßnahmen, um die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen.

8.2 Die aktuellen technischen und organisatorischen Maßnahmen des Auftragnehmers sind unter diesem Link einsehbar. Der Auftragnehmer stellt klar, dass es sich bei den unter dem Link aufgeführten technischen und organisatorischen Maßnahmen lediglich um Beschreibungen technischer Art handelt, welche nicht als Bestandteil dieser Vereinbarung anzusehen sind.

8.3 Der Auftragnehmer betreibt ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung gemäß Art. 32 Abs. 1 lit. d) DSGVO.

8.4 Der Auftragnehmer passt die getroffenen Maßnahmen im Laufe der Zeit an die Entwicklungen beim Stand der Technik und die Risikolage an. Eine Änderung der getroffenen technischen und organisatorischen Maßnahmen bleibt dem Auftragnehmer vorbehalten, sofern das Schutzniveau nach Art 32 DSGVO nicht unterschritten wird.

9. Nachweis und Überprüfung

9.1 Der Auftragnehmer stellt dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten zur Verfügung. Sollte im Einzelfall

eine Inspektion beim Auftragnehmer erforderlich sein sollte, wird diese auf Kosten des Auftraggebers durch einen unabhängigen externen Prüfer durchgeführt, den der Auftragnehmer benennt. Der Auftragnehmer darf nur solche Prüfer benennen, die gegenüber dem Auftraggeber ihre Unabhängigkeit vom Auftragnehmer versichert und sich zur Verschwiegenheit verpflichtet haben.

9.4 Für Informationen und Unterstützungshandlungen kann der Auftragnehmer eine angemessene Vergütung verlangen, soweit die Kontrolle nicht wegen eines Gesetzes- oder Vertragsverstoßes durch den Auftragnehmer erforderlich wurde. Der Auftragnehmer wird dem Auftraggeber vorab eine Kosteninformation zukommen lassen.

10. Subunternehmer (weitere Auftragsverarbeiter)

10.1 Der Auftraggeber erteilt dem Auftragnehmer die allgemeine Genehmigung, weitere Auftragsverarbeiter im Sinne des Art. 28 DSGVO zur Vertragserfüllung einzusetzen.

10.2 Die aktuell eingesetzten weiteren Auftragsverarbeiter sind in Anhang 2 aufgeführt. Der Auftraggeber erklärt sich mit deren Einsatz einverstanden.

10.3 Der Auftragnehmer stellt die jeweils aktuellen Auftragsverarbeiter auf folgender Website dar: **Auftragsverarbeiter**. Der Auftraggeber hat somit die Möglichkeit, sich durch Abruf der Website über jeweils weitere Auftragsverarbeiter zu informieren.

10.4 Der Einspruch gegen die beabsichtigte Änderung kann nur aus einem sachlichen Grund innerhalb von 14 Tagen nach Zugang der Information über die Änderung gegenüber dem Auftragnehmer erhoben werden. Im Fall des Einspruchs kann der Auftragnehmer nach eigener Wahl die Leistung ohne die beabsichtigte Änderung erbringen oder - sofern die Erbringung der Leistung ohne die beabsichtigte Änderung für den Auftragnehmer nicht zumutbar ist - die von der Änderung betroffene Leistung gegenüber dem Auftraggeber innerhalb einer angemessenen Frist (mindestens 14 Tage) nach Zugang des Einspruchs einstellen.

10.5 Erteilt der Auftragnehmer Aufträge an weitere Auftragsverarbeiter, so obliegt es dem Auftragnehmer, seine datenschutzrechtlichen Pflichten aus diesem Vertrag auf den weiteren Auftragsverarbeiter zu übertragen. Der Auftragnehmer stellt insbesondere durch regelmäßige Überprüfungen sicher, dass die weiteren Auftragsverarbeiter die technischen und organisatorischen Maßnahmen einhalten.

11. Haftung und Schadensersatz

11.1. Im Fall der Geltendmachung eines Schadensersatzanspruches durch eine betroffene Person nach Art. 82 DSGVO verpflichten sich die Parteien, sich gegenseitig zu unterstützen und zur Aufklärung des zugrundeliegenden Sachverhalts beizutragen.

11.2. Die zwischen den Parteien im Hauptvertrag zur Leistungserbringung vereinbarte Haftungsregelung gilt auch für Ansprüche aus dieser Vereinbarung zur Auftragsverarbeitung und im Innenverhältnis zwischen den Parteien für Ansprüche Dritter nach Art 82 DSGVO, außer soweit ausdrücklich etwas anderes vereinbart ist.

World4You Internet Services GmbH
Wolfgang-Pauli-Straße 2, BT3
4020 Linz

Tel.: +43 50 5859
E-Mail: office@world4you.com
www.world4you.com

12. Vertragslaufzeit, Sonstiges

12.1 Die Vereinbarung beginnt mit dem Abschluss durch den Auftraggeber. Sie endet mit Ende des letzten Vertrages unter der jeweiligen Kundennummer. Sollte eine Auftragsverarbeitung noch nach Beendigung dieses Vertrages stattfinden, gelten die Regelungen dieser Vereinbarungen bis zum tatsächlichen Ende der Verarbeitung.

12.2 Der Auftragnehmer kann die Vereinbarung nach billigem Ermessen mit angemessener Ankündigungsfrist ändern. Insbesondere behält er sich ausdrücklich vor, die vorliegende Vereinbarung einseitig zu ändern, sofern sich wesentliche rechtliche Änderungen im Bezug auf diese Vereinbarung ergeben. Der Auftragnehmer wird den Auftraggeber über die Bedeutung der geplanten Änderung gesondert hinweisen und darüber hinaus dem Auftraggeber eine angemessene Frist zur Erklärung eines Widerspruchs einräumen. Der Auftragnehmer weist den Auftraggeber in der Änderungs-Ankündigung darauf hin, dass die Änderung wirksam wird, wenn er nicht binnen der gesetzten Frist widerspricht. Im Falle eines Widerspruchs durch den Auftraggeber steht dem Auftragnehmer ein außerordentliches Kündigungsrecht zu.

12.3 Der Auftraggeber erkennt diese Vereinbarung als Teil der AGB über die/das von ihm gebuchte/n Produkt/e an. Bei etwaigen Widersprüchen gehen Regelungen dieser Vereinbarung zur Auftragsverarbeitung den Regelungen des Hauptvertrages vor. Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarungen im Übrigen nicht.

12.4 Ausschließlicher Gerichtsstand für alle Streitigkeiten aus und im Zusammenhang mit diesem Vertrag ist der Sitz des Auftragnehmers. Dieser gilt vorbehaltlich eines etwaigen ausschließlich gesetzlichen Gerichtsstandes. Dieser Vertrag unterliegt den gesetzlichen Bestimmungen der Bundesrepublik Österreich.

12.5 Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als Verantwortlicher im Sinne der DSGVO liegen.

Linz, den 30.09.2026
Ort Datum

30.09.2026 18:18:53
Digital unterzeichnet auf
my.world4you.com mit Login 50385533
- Auftraggeber -

- Auftragnehmer -

World4You Internet Services GmbH
Wolfgang-Pauli-Straße 2, BT3
4020 Linz

Tel.: +43 732 93035
E-Mail: office@world4you.com
www.world4you.com

Anhang 1 zum World4You Auftragsverarbeitungsvertrag - Leistungsbeschreibung

Domain Leistungsbeschreibung:

Wenn Sie bei uns eine Domain bestellen, kümmern wir uns um die Konnektierung und die Registrierung Ihrer Domain bei der zuständigen Registry. Zudem ist die Aufrechterhaltung der Registrierung, Domainumzüge und Abmeldung Vertragsbestandteil. Gleiches gilt für auf ihren Domains basierenden SSL Zertifikaten.

Art der personenbezogenen Daten: Domain, Stammdaten (Name, Adresse, E-Mail, Telefonnummer)
Kategorien betroffener Personen: Kunden

Mail Leistungsbeschreibung:

Wenn Sie bei uns ein Mailprodukt bestellen, erhalten Sie eine oder mehrere E-Mail-Adressen. Wir legen für Sie die entsprechenden Postfächer an, auf die Sie mittels Web zugreifen oder die Sie in verschiedene Clients einbinden können. Des Weiteren können Sie im Web-Client entsprechend der gebuchten Leistung Termine und Aufgaben erstellen und Kontakte verwalten. Zudem gehört auch ein konfigurierbarer Spamfilter zum Produkt.
Art der personenbezogenen Daten: Mails, Kontakte, Termine, Domain
Kategorien betroffener Personen: Mitarbeiter

Cloud Speicher Leistungsbeschreibung:

Unser Cloud-Speicher World4You-Cloud ermöglicht die Speicherung Ihrer Daten in unserem Rechenzentrum, sodass Sie von überall und jederzeit auf die Daten zugreifen können. Sie können Freigaben auf bestimmte Ordner erteilen und diese verwalten.

Art der personenbezogene Daten: Daten, die Sie in der Cloud speichern
Kategorien betroffener Personen: Mitarbeiter

Hosting Leistungsbeschreibung:

Wenn Sie bei uns ein Hosting Paket bestellen, gehören zu unserer Leistung die Registrierung und Konnektierung der Domain sowie die Zurverfügungstellung des Webspaces und der Datenbanken. Inbegriffene Leistungen sind SSL-Zertifikate und Mail. Mittels SSL-Zertifikat werden die Daten zwischen Ihrer Webseite und dem Webserver verschlüsselt übertragen. Mit den Easy.Install Apps können Sie verschiedene Applikationen zum Aufbau und zur Verwaltung von Websites verwenden. Zusätzlich erhalten Sie Zugriff auf das Tool marketingRadar, mit dem Sie die Sichtbarkeit und das Ranking Ihrer Website bei Suchmaschinen prüfen und optimieren können.

World4You Internet Services GmbH
Wolfgang-Pauli-Straße 2, BT3
4020 Linz

Tel.: +43 732 93035
E-Mail: office@world4you.com
www.world4you.com

Art der personenbezogenen Daten: Inhaltsdaten der Webseite, Domain, Daten E-Mail (siehe unter Mailprodukt), Daten Ihrer Websitebesucher
Kategorien betroffener Personen: Mitarbeiter, Besucher der Webseite

WordPress- & WooCommerce Hosting

Wenn Sie eines unserer Webhosting Pakete, die speziell auf die Verwendung für das CMS WordPress bzw WordPress mit dem WooCommerce Plug-In ausgerichtet sind, bestellen, erhalten Sie die Registrierung und Konnektierung der Domain, sowie die Zurverfügungstellung des Webspace mit direkt installierten Datenbanken für WordPress bzw WordPress inklusive WooCommerce. Zusätzlich enthalten sind SSL-Zertifikate, die Daten zwischen Ihrer Website und dem Webserver verschlüsselt übertragen, das Online-Marketing-Tool marketingRadar, mehrere E-Mail-Adressen mit entsprechenden Postfächern und Zugriff auf die World4You Cloud.

Art der personenbezogenen Daten: Inhaltsdaten der Webseite, Domain, Daten E-Mail (siehe unter Mailprodukt), Daten Ihrer Websitebesucher
Kategorien betroffener Personen: Mitarbeiter, Besucher der Webseite

Server Leistungsbeschreibung:

Sie können virtuelle Server bei uns bestellen. Wir stellen Ihnen hierfür einen geteilten Speicherplatz auf einem Server zur Verfügung.

Art der verarbeiteten Daten: Daten, die Sie auf dem Server speichern
Kategorien betroffener Personen: Mitarbeiter, Besucher der Webseite

weitere SaaS Produkte:

Wir bieten zudem noch weitere Software-as-a-Service Produkte an. Hierzu gehören z.B. - aber nicht abschließend - Online Marketing Tools, die Möglichkeit, sich eine Webseite mittels Homepage-Baukastens zu erstellen oder auch der Vertrieb von Office Anwendungen.

Art der verarbeiteten Daten: Daten, die Sie in den Diensten speichern Kategorien betroffener Personen: Mitarbeiter, Kunden, Besucher der Webseite

World4You Internet Services GmbH
Wolfgang-Pauli-Straße 2, BT3
4020 Linz

Tel.: +43 732 93035
E-Mail: office@world4you.com
www.world4you.com

Anhang 2 zum World4You Auftragsverarbeitungsvertrag - genehmigte Subunternehmen

World4You setzt folgende Subunternehmen ein:

Nr.	Name, vollständige Anschrift	Produkt / Beschreibung der Leistung
1	rankingCoachGmbH, im Mediapark 6b 50670 Köln, Deutschland	Suchmaschinenoptimierung rankingCoach Optimierung der Suchergebnisse Ihrer Website bei Google
2	IONOS SE Elgendorfer Str. 57 56410 Montabaur Deutschland	vServer, Security Dienstleistungen AD-Server, Webhosting (Stretch), KI-Telefonassistent
3	Google Cloud EMEA Limited Velasco Clanwilliam Place Dublin 2 Ireland	World4You Kollaborations Tools
4	Microsoft Ireland Operations Ltd One Microsoft Place South County Business Park Leopardstown Dublin 18, D18 P521 Ireland	Security Dienstleistungen, Office Software
5	CM4all GmbH Im Mediapark 6a 50670 Köln Deutschland	Baukastensystem
6	Dixa ApS Vimmelskaftet 41 A, 1st floor 1161 Copenhagen K Dänemark	Kundenservice-Dienstleister im Bereich Telefonie, E-Mail/Ticket, Chatbot und Livechat
7	united-domains GmbH Gautinger Straße 10 82319 Starnberg Deutschland	Produktmanagement-Dienstleister (Entwicklung, Verbesserung und Verwaltung des Produktportfolios der World4You)

World4You Internet Services GmbH
Wolfgang-Pauli-Straße 2, BT3
4020 Linz

Tel.: +43 732 93035
E-Mail: office@world4you.com
www.world4you.com

8	Arsys Internet S.L.U. C. Madre de Dios, 21 26004 Logroño La Rioja, Spanien	Technical Operations-Dienstleister (Setup und Wartung von Kundenservices & internen Service-Landschaften)
9	Strato AG Otto-Ostrowski-Straße 7 10249 Berlin Deutschland	E-Mail-Archivierung

World4You Internet Services GmbH
Wolfgang-Pauli-Straße 2, BT3
4020 Linz

Tel.: +43 732 93035
E-Mail: office@world4you.com
www.world4you.com

Technisch organisatorische Maßnahmen

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

1.1 Zutrittskontrolle

Unbefugten ist der Zutritt zu Räumen zu verwehren, in denen Datenverarbeitungsanlagen untergebracht sind. Festlegung von Sicherheitsbereichen

- Realisierung eines wirksamen Zutrittsschutzes
- Protokollierung des Zutritts
- Festlegung zutrittsberechtigter Personen
- Verwaltung von personengebundenen Zutrittsberechtigungen
- Begleitung von Fremdpersonal
- Überwachung der Räume

1.2 Zugangskontrolle

Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden.

- Festlegung des Schutzbedarfs
- Zugangsschutz
- Umsetzung sicherer Zugangsverfahren, starke Authentisierung
- Umsetzung einfacher Authentisierung per Username/Passwort
- Protokollierung des Zugangs
- Monitoring bei kritischen IT-Systemen
- Gesicherte (verschlüsselte) Übertragung von Authentisierungsgeheimnissen
- Sperrung bei Fehlversuchen/Inaktivität und Prozess zur Rücksetzung gesperrter
- Zugangskennungen
- Verbot Speicherfunktion für Passwörter und/oder Formulareingaben (Server/Clients)
- Festlegung befugter Personen
- Verwaltung und Dokumentation von personengebundenen Authentifizierungsmedien und
- Zugangsberechtigungen
- Automatische Zugangssperre und Manuelle Zugangssperre

1.3 Zugriffskontrolle

Es kann nur auf die Daten zugegriffen werden, für die eine Zugriffsberechtigung besteht. Daten können bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden.

World4You Internet Services GmbH
Wolfgang-Pauli-Straße 2, BT3
4020 Linz

Tel.: +43 732 93035
E-Mail: office@world4you.com
www.world4you.com

- Erstellen eines Berechtigungskonzepts
- Umsetzung von Zugriffsbeschränkungen
- Vergabe minimaler Berechtigungen
- Verwaltung und Dokumentation von personengebundenen Zugriffsberechtigungen
- Vermeidung der Konzentration von Funktionen

1.4 Verwendungszweckkontrolle

Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

- Datensparsamkeit im Umgang mit personenbezogenen Daten
- Getrennte Verarbeitung verschiedener Datensätze
- Regelmäßige Verwendungszweckkontrolle und Löschung
- Trennung von Live-/Test- und Entwicklungsumgebung

1.5 Datenschutzfreundliche Voreinstellungen

Sofern Daten zur Erreichung des Verwendungszwecks nicht erforderlich sind, werden die technischen Voreinstellungen so festgelegt, dass Daten nur durch eine Aktion der betroffenen Person erhoben, verarbeitet, weitergegeben oder veröffentlicht werden.

2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

2.1 Weitergabekontrolle

Ziel der Weitergabekontrolle ist es, zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

- Festlegung empfangs-/weitergabeberechtigter Instanzen/Personen
- Prüfung der Rechtmäßigkeit der Übermittlung ins Ausland
- Protokollierung von Übermittlungen gemäß Protokollierungskonzept
- Sichere Datenübertragung zwischen Server und Client
- Sicherung der Übertragung im Backend
- Sichere Übertragung zu externen Systemen
- Risikominimierung durch Netzseparierung
- Implementation von Sicherheitsgateways an den Netzübergabepunkten
- Härtung der Backendsysteme
- Beschreibung der Schnittstellen

World4You Internet Services GmbH
Wolfgang-Pauli-Straße 2, BT3
4020 Linz

Tel.: +43 732 93035
E-Mail: office@world4you.com
www.world4you.com

- Umsetzung einer Maschine-Maschine-Authentisierung
- Sichere Ablage von Daten, inkl. Backups
- Gesicherte Speicherung auf mobilen Datenträgern
- Einführung eines Prozesses zur Datenträgerverwaltungen
- Prozess zur Sammlung und Entsorgung
- Datenschutzgerechter Lösch- und Zerstörungsverfahren
- Führung von Löschprotokollen

2.2 Eingabekontrolle

Zweck der Eingabekontrolle ist es, zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

- Protokollierung der Eingaben
- Dokumentation der Eingabeberechtigungen

3. Verfügbarkeit, Belastbarkeit, Disaster Recovery

3.1 Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

- Brandschutz
- Redundanz der Primärtechnik
- Redundanz der Stromversorgung
- Redundanz der Kommunikationsverbindungen
- Monitoring
- Ressourcenplanung und Bereitstellung
- Abwehr von systembelastendem Missbrauch
- Datensicherungskonzepte und Umsetzung
- Regelmäßige Prüfung der Notfalleinrichtungen

3.2 Disaster Recovery – rasche Wiederherstellung nach Zwischenfall (Art. 32 Abs. 1 lit. c DSGVO)

- Notfallplan
- Datensicherungskonzepte und Umsetzung

4. Datenschutzorganisation

- Festlegung von Verantwortlichkeiten
- Umsetzung und Kontrolle geeigneter Prozesse
- Melde- und Freigabeprozess

- Umsetzung von Schulungsmaßnahmen
- Verpflichtung auf Vertraulichkeit
- Regelungen zur internen Aufgabenverteilung
- Einführung einer geeigneten Vertreterregelung

5. Auftragskontrolle

Ziel der Auftragskontrolle ist es, zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

- Auswahl weiterer Auftragnehmer nach geeigneten Garantien
- Abschluss einer Vereinbarung zur Auftragsverarbeitung mit weiteren Auftragnehmern

6. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

- Informationssicherheitsmanagement
- Prozess zur Evaluation der technischen und organisatorischen Maßnahmen
- Prozess Sicherheitsvorfall-Management
- Durchführung von technischen Überprüfungen