Datenverarbeitungsverzeichnis nach

Art 30 Abs 1 EU-Datenschutz- Grundverordnung (DSGVO)

Physiotherapie und Athletiktraining Medletics

Sascha Schulz Sportphysiotherapeut

mit Stand vom 26.10.2021

INHALT

Inhalt

A. Stammdatenblatt 3

B. Datenverarbeitungen/ Datenverarbeitungszwecke 3

C. Detailangaben 3

C.1. Geschäftsanbahnung und -abwicklung.....3

C.2. Buchhaltung 5

C.3. Therapiesitzung.....7

C.4. Überweisungen von Ärzten 9

C.5. Kommunikation mit Ärzten und Kollegen 10

D. Allgemeine Beschreibung der technisch-organisatorischen Maßnahmen (TOMs).....12

Vertraulichkeit

Integrität

Verfügbarkeit und Belastbarkeit

Pseudonymisierung und Verschlüsselung

Evaluierungsmaßnahmen

E. Risiko- und Folgeabschätzung 13

Risikoabschätzung

Folgenabschätzung

F. Löschungs- & Veränderungs-protokoll.....14

Datenschutzerklärung 15

A. STAMMDATENBLATT

Name und Kontaktdaten des (der) für die Verarbeitung (gemeinsam) Verantwortlichen a. **Name(n) und Anschrift(en):**

Sascha Schulz
Hasnerplatz 4, 8010 Graz Bienengasse 24b, 8501 Lieboch

office@medletics.at

+43 664 546 5654

c. **Name und Kontaktdaten (Anschrift, E-Mail und allenfalls weitere Kontaktdaten wie zB Tel.Nr.) des Datenschutzbeauftragten:** nicht nötig, da Einzelunternehmen und keine Kerntätigkeit in der Verarbeitung sensibler Daten

d. **Name und Kontaktdaten (Anschrift, E-Mail und allenfalls weitere Kontaktdaten wie zB Tel.Nr.) des Vertreters des (der) Verantwortlichen:** kein Vertreter vorhanden

B. Datenverarbeitungen/ Datenverarbeitungszwecke

1. Zwecke und Beschreibung der Datenverarbeitung:

1. **Geschäftsanbahnung und -abwicklung:** Verarbeitung von Daten im Rahmen von Geschäftsbeziehungen mit Kunden und Geschäftspartner/innen, manuell erstellte und archivierte Textdokumente (wie Korrespondenzen) in diesen Angelegenheiten. Verarbeitung im E-Mail Programm und Adressbuch.
2. **Buchhaltung: Rechnungen erstellen, Mahnungen erstellen, Buchhaltung führen und Daten an die Steuerberaterin übermitteln zur Erstellung des Jahresabschlusses**
3. **Therapiesitzung abhalten:** Verarbeitung von Gesundheitsdaten zum Zwecke einer gerichteten Therapie und Dokumentation des Therapieverlaufs.
4. **Ärztliche Überweisungen verwalten**
5. **Kommunikation mit Ärzten und Kollegen**

C. DETAILANGABEN

C.1. GESCHÄFTSANBAHNUNG UND -ABWICKLUNG Beschreibung

Wir werden von Klienten angerufen zum Zwecke der Vereinbarung eines Therapietermins. Ein Termin wird bei bestehendem Interesse fixiert. Wir speichern den Namen, das Geschlecht und die Telefonnummer damit wir bei Änderungen des Termins Kontakt aufnehmen können. Diese Daten schreiben wir händisch in unser jeweiliges analoges bzw. digitales (Handy) Telefonbuch, das wir an Arbeitstagen bei uns tragen und sonst im versperrbaren Aktenschrank lagern. Weitere Fixationen von Terminen finden zur Absicherung digital statt. Selten schreiben Patienten zum Zwecke des Erstkontaktes eine E-Mail, welche wir nach telefonischer Kontaktaufnahme löschen. Die Daten werden des Weiteren zur interdisziplinären Zusammenarbeit mit Physiotherapeut Ramin Eskandary, Carina Fuchs, Gordana Schulz und Katharina Fügerl (Mitarbeiter/innen von Sascha Schulz) ausgetauscht.

Zweck

Wir brauchen die Daten, um mit den Kunden/innen kommunizieren zu können.

1. Kategorien der betroffenen Personen

1. Interessent/innenbedeutet: JemandhatInteresseangemeldet, Erstkontakt

2. Kunden/innen bedeutet: Wir haben mindestens eine Therapieeinheit abgeschlossen

3. Geschäftspartner/innen bedeutet: zuweisende Ärzte

2. Rechtsgrundlagen

- Art 6 Abs 1 lit b DSGVO (zur Vertragserfüllung erforderlich) für Name, Adresse und andere allgemeine Daten
- Art 6 Abs 1 lit f DSGVO (berechtigte Interessen des Verantwortlichen) für Notizen, die ich mir zu unseren Geschäftsbeziehungen mache

3. Verträge, Zustimmungserklärungen oder sonstige Unterlagen (z.B. Erledigung der Informationspflichten):

• E-Mail Server: medletics.at – Daten werden nach Kontaktaufnahme gelöscht

- Adressbuch: analog und digital
- Terminverwaltung: Kalender analog, digital
- Kommunikation: WhatsApp Messenger, eMail, Signal → löschen

4.a Kategorien der verarbeiteten Daten

Kategorien der betroffenen Personen (aus Punkt 1 des C-Blattes)	Lfd. Nr.	Datenkategorien	Besondere Datenkategorien iSd Art 9 DSGVO, strafrechtlich relevant iSd Art 10 DSGVO	Banken	Rechtsvertreter im Geschäftsfall	Wirtschafttreuhänder	Gerichte im Anlassfall	Verwaltungsbehörden im Anlassfall	Inkassounternehmen im Anlassfall	Fremdfinanzierer (zB Leaing)	Mitwirkende Vertrags- und Geschäftspartner	Versicherungen im Anlassfall	Provider (IT-Dienstleister)	LÖSCHUNG
Interessent/innen	1	Name	nein											*sofort*
	2	Telefonnummer	nein											*sofort*
Kund/innen und Geschäftspartner/innen	3	Name	nein											7a
	4	Telefonnummern	nein											7a

Nummer und Name der Interessenten streichen wir aus dem Kalender bzw. Telefonbuch bei Nichtzustandekommen des Termins.

4.b. Löschen und aufbewahren

Daten aus 4.a. (Lfd. Nr.)	Angabe bzw. Beschreibung der Löschungs- bzw. Aufbewahrungsfristen
1-2 (Interessenten)	Daten von Interessent/innen löschen wir sofort, falls kein Geschäft zustande gekommen ist
3-4 (Kunden)	Daten von Kunden/innen löschen wir spätestens nach 7 Jahren nach dem letzten Kontakt, sofern nichts anderes von der Person gewünscht wird.

5. Kategorien von Empfängern, an die personenbezogenen Daten offengelegt werden (inkl. Auftragsverarbeitung), speziell bei Empfängern in Drittländern Kategorien der Empfänger sowie Übermittlungsort (Drittstaat, Internationale Organisation wie zB UNO, OSZE)

Empfängerkategorien bzw. Empfänger in Drittstaaten oder Internationalen Organisationen (aus 4.a.)	Drittstaat (Angabe des Drittstaats, d.h. Staaten außerhalb der EU)	Internationale Organisation (Angabe der intern. Organisation)
WhatsApp	Irland	
Signal		
MsN		
eMail		

a. **Dokumentation der getroffenen geeigneten Garantien im Falle einer Übermittlung in Drittstaaten die nicht auf Art 45, 46, 47 oder 49 Abs 1 Unterabsatz 1 DSGVO erfolgt**

C.2. BUCHHALTUNG

Beschreibung

Rechnungen erstellen; Mahnungen erstellen, Buchhaltung führen und Daten an die Steuerberatung übermitteln zur Erstellung des Jahresabschlusses.

Ich, Sascha Schulz, schreibe meine Rechnungen am Tablet bzw. Handy über das Registrierkassen-System HelloCash.com und drucke sie doppelt aus (1 für den Klienten/ 1 für mich/Steuer). Die Rechnung gebe ich persönlich dem Klienten oder schicke sie per Post zu. Die Kopie der Rechnung lege ich in einen Aktenordner ab und schließe sie im verschließbaren Aktenschrank weg. Auf meinen Rechnungen stehen die Namen der Klienten; anfallende Kosten; die Therapietermine und meine Bankdaten.

Zum Zwecke der Einkommenssteuererklärung übermitteln wir bisher diese Kopien auch an den Steuerberater. Dem Steuerberater übermitteln wir die Akten persönlich.

Ich bekomme Zahlungsanweisungen per eMail (Webshops), postalisch oder als Kassenbeleg im Geschäft. Eingangsrechnungen überweisen wir per Internet-Banking. Dabei gehen Name und Geschäftsfall auch an die Bank. Die Kontodaten von Ausgangsrechnungen speichere ich nicht extra.

Ich bewahre diese Unterlagen 7a auf und lösche sie nach dieser Zeit!

Zweck

Nachweis meiner Einkünfte und für die Einnahmen/Ausgabenrechnung für die Finanz via Signatur.

1. Kategorien der betroffenen Personen

Kunden/innen bedeutet: Wir haben mindestens eine Therapieeinheit abgeschlossen – Ausgangsrechnung Geschäftspartner/innen bedeutet: Webshops; Verlage; Kursanbieter – Eingangsrechnungen

2. Rechtsgrundlagen

- Art 6 Abs 1 lit b DSGVO (zur Vertragserfüllung erforderlich) für Name, Adresse und andere allgemeine Daten
- Art 6 Abs 1 lit f DSGVO (berechtigte Interessen des Verantwortlichen) für Notizen, die ich mir zu unseren Geschäftsbeziehungen mache

3. Verträge, Zustimmungserklärungen oder sonstige Unterlagen (z.B. Erledigung der Informationspflichten):

- Textverarbeitung: Word
- Excel: lokal
- Registrierkasse HelloCash.com (Sascha Schulz)
- Ordner: im Aktenschrank weggesperrt
- Vertrag mit dem Steuerberater: Wilfling Wirtschafts- und Steuerberatung
- Ich erfülle die Informationspflicht durch Veröffentlichung der Datenschutz- Erklärung in meinen Praxisräumlichkeiten.

4.a Kategorien der verarbeiteten Daten

Kategorien der betroffenen Personen (aus Punkt 1 des C-Blattes)	Lfd. Nr.	Datenkategorien	Besondere Datenkategorien iSd Art 9 DSGVO, strafrechtlich relevant iSd Art 10 DSGVO	Banken	Rechtsvertreter im Geschäftsfall	Steuerberater	Gerichte im Anlassfall	Verwaltungsbehörden im Anlassfall	Inkassounternehmen im Anlassfall	Fremdfinanzierer (zB Leasing)	Mitwirkende Vertrags- und Geschäftspartner	Versicherungen im Anlassfall	Provider (IT-Dienstleister)	LÖSCHUNG
Kunden	1	Name	nein			*x*								*7a*
	2	Therapietermine	nein			*x*								*7a*

Geschäftspartner/innen	3	Name	nein			X								7a
	4	Telefonnummern	nein			X								7a
	5	Adresse	nein			X								7a
	6	Emailadresse	nein			X								7a

4.b Löschungs- und Aufbewahrungsfristen

Daten aus 4.a. (Lfd. Nr.)	Angabe bzw. Beschreibung der Löschungs- bzw. Aufbewahrungsfristen
Kunden	Rechnungsdaten von Kunden löschen wir nach spätestens 7a.
Geschäftspartner	Siehe oben

5. Kategorien von Empfängern, an die personenbezogenen Daten offengelegt werden (inkl. Auftragsverarbeitung), speziell bei Empfängern in Drittländern

Keine

C.3. THERAPIESITZUNG Beschreibung

Klienten kommen nach telefonischer (sehr selten nach Anfrage über EMail) Terminvereinbarung zu mir zur Therapie. Aufgrund der Dokumentationspflicht (siehe Standardanwendung – Physio-Austria Ausdruck) und um auch eine sichere und angepasste Therapie zu gewährleisten, sind wir verpflichtet Gesundheitsdaten aufzunehmen und die Art der Therapie(angewendete Techniken /Ratschläge usw.) zu dokumentieren und für mind. 10a aufzubewahren.
Zu diesem Zweck erheben wir bei der 1. Sitzung folgende Daten vom Klienten:
Name; Adresse; Telefonnummer,: zur Kontaktaufnahme/Rechnung schicken Familienstand; Kinder; Beruf; Hobbies: um das soziale Gefüge und alltägliche Belastungen des Patienten zu verstehen
Medikamente: um Vorerkrankungen zu erkennen/mögliche Kontraindikationen abzuschätzen
Diagnosen: aktuell und vorhergegangene
Ops/ chronische Erkrankungen; Unfälle; Frakturen: eventueller Einfluss auf momentane Problematik
Ernährung: siehe oben
Selten Fotos: zur Dokumentation des Ist – Zustands (mit dem Handy – wird ausgedruckt / am Handy gelöscht und zu den Akten gelegt)
Dokumentation über Art der Therapie/ Therapietechniken/ Ratschläge und Hausübungen
Überweisung vom Arzt: wird sofort kopiert – an den Patienten zurück gegeben und Kopie wird zu den Akten gelegt

All diese Daten nehme ich per Hand am Papier auf. Hefte sie in einen Aktenordner und lege diesen in einem versperrbaren Aktenschrank in der jeweiligen Praxis ab – Speicherdauer 10a

Des Weiteren unterschreiben unsere Patienten eine notwendige Einwilligungserklärung, welche den patientenbezogenen Akten beigefügt wird.

Zweck

Dokumentationspflicht – Rechtliche Vorlage – siehe Standardanwendungen/Ausdruck von Physio-Austria.

Therapieerfüllung.

1. Kategorien der betroffenen Personen

Kunden/innen bedeutet: Wir haben mindestens eine Therapieeinheit abgeschlossen

2. Rechtsgrundlagen

Bestimmungen über die freiberufliche/selbständige Ausübung des Berufes im Bereich des Gesundheitswesens (§§ 5 und 36 Gesundheits- und Krankenpflege- Gesetz (GuKG), BGBl. I Nr. 108/1997; §§ 9 und 19 Hebammengesetz (HebG), BGBl. Nr. 310/1994; §§ 7a und 11a MTD-Gesetz, BGBl. Nr. 460/1992; §§ 3 und 46 Medizinischer Masseur- und Heilmasseur-Gesetz(MMHmG), BGBl. I Nr. 169/2002; §§ 12 und 30 Musiktherapie-Gesetz(MuthG), BGBl. I Nr. 93/2008; §§ 1 und 11 Psychotherapiegesetz, BGBl. Nr. 361/1990; §§ 3 und 10 Psychologengesetz, BGBl. Nr. 360/1990).

3. Verträge, Zustimmungserklärungen oder sonstige Unterlagen (z.B. Erledigung der Informationspflichten):

- Zuweisung durch den Arzt: als Kopie zum Akt beigelegt. Original umgehend an den Patienten retour
- Kommunikation: sms und telefonisch
- Ich erfülle die Informationspflicht durch Veröffentlichung der Datenschutzerklärung in meinen Praxisräumlichkeiten.

4.a Kategorien der verarbeiteten Daten

Kategorien der betroffenen Personen (aus Punkt 1 des C-Blattes)	Lfd. Nr.	Datenkategorien	Besondere Datenkategorien iSd Art 9 DSGVO, strafrechtlich relevant iSd Art 10 DSGVO	Ärzte	Krankenversicgerung	Wirtschaftreuhänder	Gerichte im Anlassfall	Verwaltungsbehörden im Anlassfall	Inkassounternehmen im Anlassfall	Fremdfinanzierer (zB Leasing)	Mitwirkende Vertrags- und Geschäftspartner	Versicherungen im Anlassfall	Provider (IT-Dienstleister)	LÖSCHUNG
Kunden	1	Name	nein											*10a*
	2	Telefonnummer	nein											:-
		Adresse	nein											-:-
		Geburtsdatum	nein											-:-
		Versicherungsnummer	nein											_.-
		Personenstand	nein											-:_
		Beruf/ Hobbies	nein											-:-
		Medikamente	ja											-:-
		Ops; Unfälle; Erkrankungen	ja											-:-
		Diagnosen	ja											-:-

Die Patienten übermitteln ihre Rechnungen selbst an die Krankenkasse. Rücksprache mit Ärzten nur nach Einwilligung/Information des betroffenen Patienten (in Zukunft schriftlich). Gutachten nur nach ausdrücklichem Wunsch/ok (ab jetzt schriftlich) an den Patienten und über diesen an die jeweilige Organisation. Von uns gehen diese Informationen ohne Absprache und Einwilligung des Patienten nicht an Dritte weiter.

Bei Zusammenarbeit mit 2. Therapeuten werden die Dokumente (nach Einverständnis des Patienten) an den 2. Kollegen weitergeleitet- (persönliche Übergabe in der Praxis)

4.b Löschungs- und Aufbewahrungsfristen

Daten aus 4.a. (Lfd. Nr.)	Angabe bzw. Beschreibung der Löschungs- bzw. Aufbewahrungsfristen
	Kunden/innen Daten werden 10 Jahre nach der letzten Behandlung gelöscht.

5. Kategorien von Empfängern, an die personenbezogene Daten offengelegt werden (inkl. Auftragsverarbeitung), speziell bei Empfängern in Drittländern

KEINE

C.4. ÜBERWEISUNGEN VON ÄRZTEN Beschreibung

Da Physiotherapie keinen Erst-Kontakt-Beruf darstellt, muss der Patient eine ärztliche Zuweisung zur Therapie mitbringen.

Diese wird von uns sofort kopiert. Das Original wird umgehend an den Patienten weitergeleitet (zum Zwecke der Rückverrechnung mit den Kassen) und die Kopie wird von mir dem Akt beigelegt und im versperrbaren Aktenschrank der jeweiligen Praxis aufbewahrt. Aufbewahrungspflicht: 10a

Zweck

Rechtliche Pflicht

1. Kategorien der betroffenen Personen

1. Klient/innen bedeutet: Wir haben mindestens eine Therapieeinheit abgeschlossen
2. zuweisende Ärzte

2. Rechtsgrundlagen

Bestimmungen über die freiberufliche/selbständige Ausübung des Berufes im Bereich des Gesundheitswesens (§§ 5 und 36 Gesundheits- und Krankenpflege-Gesetz (GuKG), BGBl. I Nr. 108/1997; §§ 9 und 19 Hebammen-Gesetz (HebG), BGBl. Nr. 310/1994; §§ 7a und 11a MTD-Gesetz, BGBl. Nr. 460/1992; §§ 3 und 46 Medizinischer Masseur- und Heilmasseur- Gesetz (MMHmG), BGBl. I Nr. 169/2002; §§ 12 und 30 Musiktherapie-Gesetz (MuthG), BGBl. I Nr. 93/2008; §§ 1 und 11 Psychotherapie-Gesetz BGBl. Nr. 361/1990; §§ 3 und 10 Psychologengesetz, BGBl. Nr. 360/1990).

3. Verträge, Zustimmungserklärungen oder sonstige Unterlagen (z.B. Erledigung der Informationspflichten):

Zuweisungsformular in Kopie im Aktenschrank
Wir erfüllen die Informationspflicht durch Veröffentlichung der Datenschutzerklärung in meinen Praxisräumlichkeiten.

4.a Kategorien der verarbeiteten Daten

Kategorien der betroffenen Personen (aus Punkt 1 des C-Blattes)	Lfd. Nr.	Datenkategorien	Besondere Datenkategorien iSd Art 9 DSGVO, strafrechtlich relevant iSd Art 10 DSGVO	Sozialversicherung	Rechtsvertreter im Geschäftsfall	Wirtschafttreuhänder	Gerichte im Anlassfall	Verwaltungsbehörden im Anlassfall	Inkassounternehmen im Anlassfall	Fremdfinanzierer (zB Leasing)	Mitwirkende Vertrags- und Geschäftspartner	Versicherungen im Anlassfall	Provider (IT-Dienstleister)	LÖSCHUNG
Kunden	1	Name	nein											*10a*
	2	Telefonnummer	nein											*10a*
		Adresse	nein											*10a*
		Geburtsdatum	nein											*10a*
		Sozialversicherungsnummer	Nein											*10a*
		Diagnose	ja											*10a*
		Arbeitsstelle	ja											*10a*
Geschäftspartner/ innen(zuweisende Ärzte)	3	Name	nein											10a
	4	Telefonnummern	nein											10a
		Adresse	nein											10a

Ich übermittle die Überweisung an KEINE 3. Person – sondern die Klienten geben diese selbst beim Versicherungsträger ab.

4.b Löschungs- und Aufbewahrungsfristen

Daten aus 4.a. (Lfd. Nr.)	Angabe bzw. Beschreibung der Löschungs- bzw. Aufbewahrungsfristen
Geschäftspartner(Ärzte))	10a
(Kunden)	10a

5. Kategorien von Empfängern, an die personenbezogenen Daten offengelegt werden (inkl. Auftragsverarbeitung), speziell bei Empfängern in Drittländern

KEINE

C.5. KOMMUNIKATION MIT ÄRZTEN UND KOLLEGEN/GUTACHTEN

Beschreibung

Bei schriftlicher Anfrage durch den Patienten erstelle ich ein schriftliches Gutachten, welches ich am Stand PC im Word schreibe und dann 2 mal ausdrucke (am Computer sofort lösche). Kopie bekommt der Patient persönlich . Die 2. legen wir zu seinem Krankenakt bei und bewahren diese 10 a auf.
(sehr selten!!! Daten die verwendet werden: Name; Adresse; Diagnose; therapeutische Befunde und Beschwerden; Therapieart und Ergebnisse; eventuell Empfehlungen)

Nach Rückfrage und schriftlichen „OK“ des Patienten sind Rücksprachen mit zuweisendem Arzt (zum Zwecke der Therapieoptimierung); Übergabe an behandelnden 2.Therapeuten immer persönlich!

Zweck

Optimierung der Therapie (Arztrücksprache), Absicherung und Wunsch des Klienten(„Gutachten“)

1. Kategorien der betroffenen Personen

Kund/innen bedeutet: Wir haben mindestens eine Therapieeinheit abgeschlossen
Geschäftspartner/innen bedeutet: zuweisende Ärzte/ Kollegen

2. Rechtsgrundlagen

Siehe Physio-Austria Ausdruck (wird beigelegt) über Recht zur Kommunikation mit Arzt und direktbehandelndem 2. Kollegen.

3. Verträge, Zustimmungserklärungen oder sonstige Unterlagen (z.B. Erledigung der Informationspflichten):

- „Gutachten“; im Word Dokument geschrieben – ausgedruckt und dann gelöscht am Computer
- Telefonat oder persönlicher Kontakt mit Arzt/Kollege
- Übergabe der „Krankenakte“ ausnahmslos persönlich
- Ich erfülle die Informationspflicht durch Veröffentlichung der Datenschutzerklärung in meinen Praxisräumlichkeiten.

4.a Kategorien der verarbeiteten Daten

Kategorien der betroffenen Personen (aus Punkt 1 des C-Blattes)	Lfd. Nr.	Datenkategorien	Besondere Datenkategorien iSd Art 9 DSGVO, strafrechtlich relevant iSd Art 10 DSGVO	Kunde selbst!!!!	Arzt (mit Einverständnis des Patienten)	Wirtschafttreuhänder	Gerichte im Anlassfall	Verwaltungsbehörden im Anlassfall	Inkassounternehmen im Anlassfall	Fremdfinanzierer (zB Leasing)	Mitwirkende Vertrags- und Geschäftspartner	Versicherungen im Anlassfall	Provider (IT-Dienstleister)	LÖSCHUNG
Kunden(Gutachten)	1	Name	nein	x	x									*10a*
	2	Telefonnummer	nein	x	x									*10a*
		Adresse	nein	x	x									*10a*
		Diagnose	ja	x	x									*10a*
		Therapieart	ja	x	x									*10a*
		Prognose	ja	x	x									*10a*
Ärzte und Kollegen	3	Name	nein											10a
	4	Diagnose/Anamnese	ja											10a
		Therapieart	ja											10a

Kommunikation mit dem zuweisenden Arzt ausschließlich persönlich.

4.b Löschungs- und Aufbewahrungsfristen

Daten aus 4.a. (Lfd. Nr.)	Angabe bzw. Beschreibung der Löschungs- bzw. Aufbewahrungsfristen
Kunden	WhatsApp
Ärzte	Persönliches Gespräch/ Dokumentation über Verlauf der Therapie - schriftlich 10a
Kollegen(die Patient auch behandeln)	Krankenakt - 10a

5. Kategorien von Empfängern, an die personenbezogenen Daten offengelegt werden (inkl. Auftragsverarbeitung), speziell bei Empfängern in Drittländern

Keine

D. ALLGEMEINE BESCHREIBUNG DER TECHNISCH-ORGANISATORISCHEN MAßNAHMEN (TOMS)VERTRAULICHKEIT

So verhindern wir die (unbeabsichtigte) Offenlegung und den unbefugten Zugang zu den personenbezogenen Daten: (Zugangskontrolle, ...)

Räumlich/ baulich:
o Wir lassen keine personenbezogenen Informationen (Visitenkarten, Notizzettel, Protokolle, Texte, Listen,...) offen auf meinem

Schreibtisch liegen, vor allem dann nicht, wenn ein Kunde zu mir kommt. (Clear Desk Policy)
o Am Ende des Arbeitstages räume ich alle Unterlagen mit personenbezogen Informationen vom Schreibtisch weg (und versperre sie z.B. in

einer Schublade).
o Wenn ich das Haus verlasse, **versperre ich das Büro**, sodass niemand zu den Akten und Ordnern Zugang hat.
o Wenn ich das Haus verlasse, sperre ich meinen **Laptop im Schreibtisch** ein.
o Weil ich **sensible Daten** verarbeite (gesundheitsbezogen, etc.), sind meine Unterlagen (Ordner, Register, Notizen) in einem Schrank

eingesperrt. Den Schlüssel verwahre ich sicher.
o Vertrauliche Daten speichere ich ausschließlich digital auf verschlüsselten Medien (Laptop, externe Festplatte, USB-Sticks,...) oder in

Cloud-Speichern mit entsprechenden Zugangsbeschränkungen.
o Ich habe die Daten auf einem externen Server gespeichert Dropbox). Mein Notebook startet erst nach Eingabe eines „starken“

Passworts. ODER
o Ich lege wichtige Daten in einem **verschlüsselten Verzeichnis** ab, das ich erst nach Eingabe eines eigenen „starken“ Passworts öffnen

kann.
o Ich habe meine **externen Festplatten** (zur Datensicherung, zum Datentransport) verschlüsselt .
o Ich habe meine **USB-Sticks** (zur Datensicherung, zum Datentransport) verschlüsselt.
o (Wenn am Handy Kundendaten sind.) Ich habe **mein Handy verschlüsselt** und es FingerPrint geschützt. Zusätzlich kann ich bei Verlust

oder Diebstahl die gespeicherten Daten „fernlöschen".
o Andere Personen und Kinder lasse ich meine Geräte ausschließlich mit einem **Gast-Account** benutzen.
o Ich erlaube keinen Apps Zugriff auf meine Kontakte, wenn diese meine Kontakte auf fremde Server herunterladen.
o Ich verwende WhatsApp auf einem eigenen Gerät (Inselbetrieb), auf dem ich keine beruflichen Kontakte speichere, sodass keine

Kontakte auf fremde Server geladen werden. (sicherste Variante) ODER:
o Ich gewähre WhatsApp und anderen Messenger-Apps **keinen Zugriff auf meine Kontakte** am Handy.
o Sensible Daten verschicke ich nicht per E-Mail sondern **nur per Post**.
o Sensible Daten verschicke ich nur in **verschlüsselten, passwortgesicherten PDFs** per E-Mail. Das Passwort verschicke ich in einem extra

E-Mail.
o Ich verwende ein starkes Passwort für die Anmeldung an meinem Computer: eine sehr lange selbst abgewandelte Passphrase, mindestens

12 Zeichen, kein sinnvolles Wort

o Ich verwende **für jeden Dienst ein anderes „starkes" Passwort**.
o Ich habe die Passwörter in einem Passwort-Safe gespeichert, um sie nicht zu vergessen.
o Sämtliche Kommunikations-Apps habe ich so eingestellt, dass sie KEINEN Zugriff auf meine Kontakte haben.

INTEGRITÄT

So verhindere ich die (unbeabsichtigte) Zerstörung/Vernichtung, die (unbeabsichtigte) Schädigung, den (unbeabsichtigten) Verlust, die (unbeabsichtigter) Veränderung von personenbezogenen Daten.

o Wichtige Geschäftsunterlagen, die ich ausschließlich als Dateien besitze und später noch als Nachweis brauchen könnte, brenne ich (zusätzlich zur normalen Datensicherung) **regelmäßig auf CD oder DVD**. Diese Datenträger bewahre ich an einem sicheren Ort (Bankschließfach) auf. ODER

o Wichtige Geschäftsunterlagen, die ich ausschließlich als Dateien besitze und später noch als Nachweis brauchen könnte, speichere ich (zusätzlich zur normalen Datensicherung) auf Google-Drive (G-Suite).

o Auf allen meinen Computern und Mobilgeräten laufen aktuelle **Virenscanner**.
o **Software-Aktualisierungen** führe ich durch, sobald sie mir vom Programm oder Betriebssystem gemeldet werden.
o Ich betreibe nur Software, für die noch Sicherheitsupdates zur Verfügung gestellt werden (Am aktuellen Stand der Technik)

VERFÜGBARKEIT UND BELASTBARKEIT

So stelle ich sicher, dass die Daten immer verfügbar sind und meine Systeme belastbar sind. Wenn ich meinen Computer nicht mehr verwenden kann (von Viren befallen, gestohlen, technischer Defekt), bin ich in kurzer Zeit – eventuell auf einem anderen Gerät – wieder einsatzbereit.

o Wir sichern täglich unsere Daten via Apple TimeMaschin-Mails und Datenbanken sowie das Betriebssystem meines Computers auf eine externe Festplatte / mit einem Online-Dienst (Cloud-Dienst).

o Ich **teste regelmäßig**, ob die Sicherung wiederherstellen kann.
o (Wenn der Internetzugang für die Geschäftstätigkeit wichtig ist:) Ich habe ein **zweites USB-Modem** (Internet-Stick), um meinen

Internetzugang zu gewährleisten, auch wenn mein hauptsächlicher Internetzugang ausfällt.
o Ich habe zusätzlich zu meinem kabelgebundenen Internetzugang einen weiteren Zugang über einen LTE Router, um meinen

Internetzugang zu gewährleisten.

PSEUDONYMISIERUNG UND VERSCHLÜSSELUNG

So pseudonymisieren und verschlüsseln wir die Daten:

o Weil ich sensible Daten verarbeite (gesundheitsbezogen, etc.), pseudonymisieren wir alle Notizen und Protokolle. o Die Liste der Personennamen & zugeordneten Nummern verwahre ich in einem Safe.
o Ich habe die Festplatte meines Computers verschlüsselt und mit einem starken Passwort gesichert.

EVALUIERUNGSMAßNAHMEN

Ich überprüfe regelmäßig, ob meine Maßnahmen am aktuellen Stand und ausreichend sind, indem ich...

Ich überprüfe regelmäßig, ob meine Maßnahmen am aktuellen Stand und ausreichend sind, indem ich dieses Dokument regelmäßig überarbeite. Bei Bedarf setze ich entsprechende Korrekturmaßnahmen.

E. RISIKO- UND FOLGEABSCHÄTZUNG

RISIKOABSCHÄTZUNG

Bedrohung: Verlust der Vertraulichkeit	Eintritt x	
	Auswirkungen =	
	Risikowert	
Bedrohung: Verlust der Integrität	Eintritt x	
	Auswirkungen =	
	Risikowert	
Bedrohung: Verlust der Verfügbarkeit	Eintritt x	
	Auswirkungen =	