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

Michaela Philipp, Kinesiologie Innsbruck
www.kinesiologie-innsbruck.com
www. yesolution.eu

Inhalt

A. Stammdatenblatt

a. Name und Anschrift:

Michaela Philipp
Kinesiologie Innsbruck
Maria-Theresien-Straße 4, A-6020 Innsbruck
www.kinesiologie-innsbruck.com
www.yesolution.at (eu, de)

b. E-Mail-Adressen (und allenfalls weitere Kontaktdaten wie zB Tel.Nr.):

michaela.philipp@kinesiologie-innsbruck.com
info@yesolution.at
+43 650 324 25 36

c. **Name und Kontaktdaten (Anschrift, E-Mail und allenfalls weitere Kontaktdaten wie zB Tel.Nr.) des Datenschutzbeauftragten[1]:**

Michaela Philipp - Kontaktdaten siehe oben

[1] Sofern ein Datenschutzbeauftragter verpflichtend oder auf freiwilliger Basis bestellt wurde.

HINWEIS: Wenn keine Verpflichtung zur Bestellung eines Datenschutzbeauftragten besteht, der Verantwortliche aber freiwillig einen bestellen möchte, müssen trotzdem alle den Datenschutzbeauftragten betreffenden Bestimmungen der DSGVO eingehalten werden; möchte man das nicht, darf die bestellte Person nicht „*Datenschutzbeauftragter*“ genannt werden, sondern sollte eine andere Bezeichnung gewählt werden (zB „*Datenschutzkoordinator*“). Dieser kann, muss aber nicht ins Verarbeitungsverzeichnis aufgenommen werden. Siehe dazu das WKO-Merkblatt „Datenschutzbeauftragter“.

B. Datenverarbeitungen/Datenverarbeitungszwecke

1. **Zwecke und Beschreibung der Datenverarbeitung[2]:**

   1. **Rechnungswesen und Geschäftsabwicklung:** Verarbeitung und Übermittlung von Daten im Rahmen von Geschäftsbeziehungen mit Kunden und Lieferanten, einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie zB Korrespondenzen oder Verträge) in diesen Angelegenheiten

   2. **Personalverwaltung:** kein Personal

   3. **Internetseiten:** kinesiologie-innsbruck.com, yesolution.at (de, eu), facebook yesolution, instagramm yesolution: Google-analytics, Newsletter yesolution.at, Newsletter Kinesiologie-Innsbruck, youtube

   4. **Führen von Kundenakten:** Vertragserfüllung

   5. **Laptop, PC, Tablet, Handy, email-Accounts: gmail, mailchimp, megamail.at, devcon.mail**

2. **Wurde eine Datenschutz-Folgenabschätzung durchgeführt?[3]**

   Ja ☐ **Nein** **x**

   Wenn Ja, wann?

   Wenn Nein, aus welchem Grund nicht?[4] Kein hohes Risiko für die Betroffenen

---

[2] Zum Begriff „Verarbeitung“ siehe das Merkblatt „Wichtige Begriffsbestimmungen“; sollten Daten auch an „Dritte“ oder an Auftragsverarbeiter übermittelt werden, sind auch die Zwecke dieser Datenübermittlungen im Verarbeitungsverzeichnis zu dokumentieren.

[3] Zur Datenschutz-Folgenabschätzung siehe das Merkblatt „Datenschutz-Folgenabschätzung“. Im Verarbeitungsverzeichnis sind zwar Angaben zur Datenschutz-Folgenabschätzung nicht zwingend vorgesehen. Aus Gründen der Rechenschaftspflicht empfehlen sich aber grundsätzliche Angaben darüber auch ins Verarbeitungsverzeichnis aufzunehmen.

[4] Eine Datenschutz-Folgenabschätzung ist nicht durchzuführen, wenn durch die Datenverarbeitung voraussichtlich kein hohes Risiko für die Rechte der Betroffenen besteht oder die Datenverarbeitungsart in der sogenannten „white list“ der Datenschutzbehörde gelistet ist (derzeit besteht noch keine „white list“); Näheres dazu siehe auch das Merkblatt „Datenschutz-Folgenabschätzung“.

C. Detailangaben zu (1) Rechnungswesen und Geschäftsabwicklung

1. Kategorien der betroffenen Personen

1	Kunden, Dienstleister
2	Sachbearbeiter beim Verantwortlichen
3	an der Geschäftsabwicklung mitwirkende Dritte inkl. Kontaktpersonen bei den Dritten

2. Rechtsgrundlagen[5]

Art 6 Abs 1 lit a (*Einwilligung der Betroffenen*), lit b (*zur Vertragserfüllung erforderlich*), lit c (*gesetzliche Verpflichtungen nach der BAO und dem UGB*), lit f (*berechtigte Interessen des Verantwortlichen*) DSGVO

§ 132 BAO

§§ 190, 212 UGB

3. Verträge, Zustimmungserklärungen oder sonstige Unterlagen (zB Erledigung der Informationspflichten[6]) sind abgelegt:[7] (freiwillig)

Rechnungen in Buchhaltung, Steuerberatung

---

[5] Die Rechtsgrundlagen (zB rechtliche Verpflichtung, Einwilligung, Vertragserfüllung, lebenswichtige Interessen des Betroffenen, kein überwiegendes berechtigtes Interesse des Betroffenen) sind nach der DSGVO zwar nicht verpflichtend ins Verarbeitungsverzeichnis aufzunehmen. Allerdings unterliegt der verantwortliche Verarbeiter einer sogenannten Rechenschaftspflicht. Diese besagt eine Nachweispflicht bzgl. der Einhaltung der Pflichten nach der DSGVO. Dazu gehört unter anderem auch der Nachweis, dass die Datenverarbeitung nach den in der DSGVO normierten Rechtmäßigkeitsgrundlagen erfolgt. Siehe das Merkblatt „Grundsätze und Rechtmäßigkeit der Verarbeitung“.

[6] Siehe zu den Informationspflichten das Merkblatt „Informationspflichten“.

[7] Die Angabe, wo die Unterlagen innerhalb der Organisation abgelegt wurden, ist nicht verpflichtend im Verarbeitungsverzeichnis zu dokumentieren, erleichtert aber vor allem in größeren, arbeitsteilig organisierten Organisationen das Auffinden der entscheidenden Unterlagen (dient also lediglich der innerbetrieblichen Arbeitserleichterung).

4. Kategorien der verarbeiteten Daten und Löschungs- bzw. Aufbewahrungsfristen[8]

a. Kategorien der verarbeiteten Daten und ankreuzen, ob sie an Empfänger[9] übermittelt werden

Kategorien der betroffenen Personengruppe 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	Wirtschaftstreuhänder	Gericht e im Anlassfall	Verwaltungsbehörden im Anlassfall	Inkassounternehmen im Anlassfall	Mitwirkende Vertrags- und Geschäftspart.	Provider (IT-Dienstleister)	Versicherungen im Anlassfall
1	1	Name, Firma oder sonstige Geschäftsbezeichnung	Nein	x	x	x	x	x	x	x	x	x
	2	Anschrift	Nein	x	x	x	x	x	x	x	x	x
	3	Kontaktdaten (Tel., Mail, Fax)	Nein	x	x	x	x	x	x	x	x	x
	8	UID-Nummer	Nein	x	x	x	x	x	x	x		X
	9	Namen der Kontaktpersonen	Nein	x	x	x	x	x	x	x	x	x
	11	Vertragstexte und Geschäftskorrespondenzen	Nein	x	x	x	x	x	x			x
2	12	Name	Nein	x	x	x	x	x	x	x	x	x
	13	Funktion des betroffenen Sachbearbeiters beim Verantwortlichen	Nein	x	x	x	x	x	x	x	x	x
	14	Vom betroffenen Sachbearbeiter bearbeitete Fälle	Nein	x	x	x	x	x	x	x	x	x
	15	Umfang der Vertretungsbefugnis	Nein	x	x	x	x	x	x	x	x	x
3	16	Name, Firma oder sonstige Geschäftsbezeichnung	Nein	x	x	x	x	x	x	x	x	x
	17	Anschrift	Nein	x	x	x	x	x	x	x	x	x

[8] Nach der DSGVO sind die Löschfristen bzw. Aufbewahrungsfristen nach Möglichkeit ins Verarbeitungsverzeichnis aufzunehmen. Beispielsweise kann bei unbefristeten Verträgen keine konkrete Löschfrist angegeben werden, da der konkrete Vertragsablauf unbestimmt ist. Es empfiehlt sich hier allerdings eine abstrakte Frist anzugeben (zB „nach Ablauf des Vertrages“).

[9] In der Rubrik „Empfänger“ sind nur die „Empfängerkategorien“ (zB „Gerichte“, „Banken“ oder „Sozialversicherungsträger“) einzutragen. Bei der Umschreibung der Empfängerkategorien ist darauf zu achten, dass eine Überprüfung der Rechtmäßigkeit ermöglicht wird (so wird zB die bloße Angabe von „Konzern“ als Empfänger nicht ausreichen, weil daraus nicht eruierbar sein wird, ob die Daten rechtmäßig an die Muttergesellschaft und/oder an Schwestergesellschaften übertragen werden).

18	Kontaktdaten (Tel., Mail, Fax)	Nein	x	x	x	x	x	x	x	x	x
20	Namen der Kontaktpersonen	Nein	x	x	x	x	x	x	x	x	X
21	Kontaktdaten der Kontaktpersonen (Tel., Mail, Fax, Anschrift)	Nein	x	x	x	x	x	x	x	x	x
22	UID-Nummer	Nein	x	x	x	x	x	x	x	x	x

b. Löschungs- und Aufbewahrungsfristen (wenn möglich)

Daten aus 4.a. (Lfd. Nr.)	Angabe bzw. Beschreibung der Löschungs- bzw. Aufbewahrungsfristen
1-4, 6-25	Aufgrund der gesetzlichen Aufbewahrungsfristen auf jeden Fall 7 Jahre; darüberhinausgehend bis zur Beendigung eines allfälligen Rechtsstreits, fortlaufender Gewährleistungs- oder Garantiefristen
5, 25	Bis zur Beendigung der Geschäftsbeziehungen

5. Kategorien von Empfängern[10], an die personenbezogene Daten offengelegt werden (inkl. Auftragsverarbeitung), speziell bei Empfängern in Drittländern[11]

a. 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)
Banken	
Rechtsvertreter im Geschäftsfall	
Wirtschaftstreuhänder	
Gerichte	
Verwaltungsbehörden	
Inkassounternehmen	
Fremdfinanzierer zB Leasing	

[10] Es sind vor allem Übermittlungsempfänger („Dritte“) als auch Auftragsverarbeiter hier zu dokumentieren. Bei der Umschreibung der Empfängerkategorien ist darauf zu achten, dass eine Überprüfung der Rechtmäßigkeit ermöglicht wird (so wird zB die bloße Angabe von „Konzern“ als Empfänger nicht ausreichen, weil daraus nicht eruierbar sein wird, ob die Daten rechtmäßig an die Muttergesellschaft und/oder an Schwestergesellschaften übertragen werden).

[11] Siehe dazu das Merkblatt „Internationaler Datenverkehr“. Bei Empfängern in Drittstaaten (speziell in den USA wegen dem „Privacy Shield“-System) empfiehlt sich eine namentliche Nennung des Empfängers.

Mitwirkende Vertrags- und Geschäftspartner:	
Versicherungen im Anlassfall	
Provider (IT-Dienstleister): Devcon, Mailchimp, Offisys	

b. **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** (vor allem wenn kein Angemessenheitsbeschluss der Europäischen Kommission vorliegt, keine Standardvertragsklauseln der Europäischen Kommission oder der nationalen Datenschutzbehörde verwendet werden oder genehmigte Zertifizierungsmechanismen in Anspruch genommen werden, keine Corporate binding rules zur Anwendung kommen (genehmigte verbindliche konzerninterne Datenschutzvorschriften), die Übermittlung nicht für Vertragserfüllungszwecke erforderlich ist oder keine ausdrückliche Einwilligung vorliegt)**:**

D. Datensicherungsmaßnahmen

Zutrittskontrolle in die Räumlichkeiten Maria-Theresien-Straße 4, 6020 Innsbruck: Türschloss, kein elektrischer Türöffner – Tür fällt immer ins Schloss

Zugangskontrolle: Schutz vor unbefugter Systembenutzung mit Kennwörtern Verschlüsselung von Datenträgern

Double Opt-In für Newsletter und Registrierungen auf den Internetseiten

Google-Analytics Daten werden mit Cookies erfasst - Besucher der web-sites können der Verwendung von Cookies widersprechen, Google-Analytics Daten werden lt. Google als vertraulich eingestuft

Regelmässiges Backup der Daten der Laptops auf einem gesonderten Server in einem abgesperrten Kasten

Klientenprotokolle werden in abgesperrten Schränken aufbewahrt, passwortgeschützt digitalisiert abgelegt (Google-Drive)

Mitarbeiter sind dazu verpflichtet worden, das Datengeheimnis zu wahren

Emails von Klienten werden nach 3-6 Monaten gelöscht, bei relevanten Inhalten wird die Löschung nach 3 Jahren vorgenommen

Das Geburtsdatum wird abgefragt: bei Minderjährigen ist die Zustimmung des Erziehungsberechtigten für eine Begleitung notwendig

Beim Kauf von e-learnings wird das Geburtsdatum abgefragt, damit erst ab einem Alter von 14 Jahren ein Kauf getätigt werden kann