D O K U M E N T A T I O N S P F L I C H T E N
D A T E N S C H U T Z - G R U N D V E R O R D N U N G

des gemeinnützigen Vereins

Ärzte für Menschen

Treustraße 43/4/4
1200 Wien

Datum: 1.6.2019

Soweit personenbezogene Bezeichnungen in diesem Schriftstück nur in männlicher Form angeführt sind, beziehen sie sich auf Frauen und Männer in gleicher Weise.

Inhaltsverzeichnis:

I. Allgemeine Informationen

1. Name und Anschrift der Verantwortlichen:

Vorstand des Vereins
Neuwahl alle 5 Jahre gemäß Statut
Vorstand in aktueller Fassung sowie Statut
veröffentlicht unter www.aefm.at

Treustraße 43/4/4
1200 Wien
Tel. und Fax : -

2. Kontaktinformationen des Ansprechpartners:

Treustraße 43/4/4
1200 Wien
Tel. und Fax : -

Mail: kontakt@aefm.at

3. Kontaktinformationen des Datenschutzbeauftragten:

Nicht erforderlich (unter 10 Personen, die Zugriff auf die Daten des Vereins haben)

II. Verzeichnis von Verarbeitungstätigkeiten

Hier findet sich eine Übersicht über sämtliche Datenanwendungen samt einer Definition des Zwecks, die der Verantwortliche betreibt. Zur besseren Übersicht sind die Datenanwendungen in folgende Kategorien eingeteilt:

- Verwaltung des Vereins
- Mitglieder- und Sponsorenverwaltung
- Organisation Mobile Ärzte
- Fortbildungsorganisation

Sofern nichts Anderes angegeben ist, verweist das Verzeichnis von Verarbeitungstätigkeiten auf folgende Kategorien von Übermittlungsempfängern:

1 Banken
2 Rechtsvertreter
3 Wirtschaftstreuhänder, Wirtschaftsprüfer
4 Gerichte
5 Zuständige Verwaltungsbehörden
6 Inkassounternehmen
7 Fremdfinanzierer
8 Vertrags- und Geschäftspartner
9 (private) Versicherungen
10 Statistik Österreich
11 Inspektorate
12 betriebliche und außerbetriebliche Interessenvertretungen
13 Vorsorgekassen, Abfertigungskassen, Sozialversicherungen, Pensionskassen
14 Transportunternehmen
15 Lieferanten, Druckereien
16 Ärzte, Krankenhäuser, Ambulatorien, Labore, Physiotherapeuten, Pflegeheime
17 Apotheken, Gesundheitsdiensteanbieter, nicht-ärztliche Gesundheitsberufe

A. Verwaltung des Vereins

1. Datenanwendung: Finanzbuchhaltung, Rechnungswesen und Logistik

a. **Zweck** der Verarbeitung:
Verarbeitung und Übermittlung von Daten im Rahmen einer Geschäftsbeziehung (bzw. zur Abwicklung dieser) mit Mitgliedern, Sponsoren und Lieferanten einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie z.B. Korrespondenz) in diesen Angelegenheiten.

Beinhaltet auch: Risikomanagement, Kreditoren- und Debitorenverwaltung, Budgetierung und Kostenrechnung.

b. **Rechtsgrundlage** der Verarbeitung: **Gesetzliche Verpflichtung, Erfüllung der Leistungen gemäß Mitgliedschaft und Sponsorenvereinbarung, Erfüllung des Vereinszwecks gemäß Statut.**

c. Beschreibung der **Kategorien betroffener Personen**: Arbeitnehmer, Mitglieder, Lieferanten, Sponsoren, Spender, Kooperationspartner (andere juristische Personen, zb. Vereine)

d. Verarbeitung durch **Auftragsverarbeiter:** keine

e. Allgemeine Beschreibung der **technischen und organisatorischen Maßnahmen**: **Nutzung am passwortgeschützten Computer**

Betroffene Personengruppe: Arbeitnehmer					
Nr.	**Kategorien**				
	von personenbezogenen Daten:	**an Empfänger**	**Übermittlung an ein Drittland**	**Speicherdauer**	**Anmerkung**
1	Stammdaten inkl. Kontaktinformationen (etwa Adresse, Tel., Mail, Fax, UID-Nr.)	1 - 10, 14		gemäß steuerrechtlicher und unternehmensrechtlicher Aufbewahrungspflichten: mindestens 7	
2	Bankverbindungsdaten	1 – 9			
3	Daten über Buchhaltung und Controlling	3, 5			
4	Bestell- und Vertragsdaten	14, 15			

5	Finanzierungs- und Zahlungsbedingungen	1 - 10		Jahre	
6	Bonitätsinformationen	3			
7	Gegenstand der Lieferung oder Leistung	1 - 10, 14, 15			
8	Daten über Lieferung- und Leistungsbedingungen	1 – 10			

Betroffene Personengruppe: Lieferanten					
Nr.	**Kategorien**				
	von personenbezogenen Daten:	**an Empfänger**	**Übermittlung an ein Drittland**	**Speicherdauer**	**Anmerkung**
1	Stammdaten inkl. Kontaktinformationen (etwa Adresse, Tel., Mail, Fax, UID-Nr.)	1 - 10, 14		gemäß steuerrechtlicher und unternehmensrechtlicher Aufbewahrungspflichten: 7 Jahre	
2	Leistungsdaten und -nachweise	3			
3	Daten über Buchhaltung und Controlling	3, 5			
4	Bankverbindungsdaten	1 – 9			
5	Bonitätsinformationen	3			
6	Gegenstand der Lieferung oder Leistung	1 - 10, 14			
7	Daten über Lieferungs- und Leistungsbedingungen	1 - 10			
8	Finanzierungs- und Zahlungsbedingungen	1 - 10			

Betroffene Personengruppe: Sponsoren					
Nr.	**Kategorien**				
	von personenbezogenen Daten:	**an Empfänger**	**Übermittlung an ein Drittland**	**Speicherdauer**	**Anmerkung**
1	Stammdaten inkl. Kontaktinformationen (etwa Adresse, Tel., Mail, Fax, UID-Nr.)	1 - 10, 14		gemäß steuerrechtlicher und unternehmensrechtlicher Aufbewahrungspflichten: 7 Jahre	
2	Leistungsdaten und -nachweise	3			
3	Daten über Buchhaltung und Controlling	3, 5			
4	Bankverbindungsdaten	1 – 9			
5	Bedingungen der Sponsorenleistung	3			
6	Gegenstand der Lieferung oder Leistung	1 - 10, 14			
7	Daten der Sponsorleistungen	1 - 10			
8	Finanzierungs- und Zahlungsbedingungen	1 - 10			

Betroffene Personengruppe: Spender					
Nr.	**Kategorien**				
	von personenbezogenen Daten:	**an Empfänger**	**Übermittlung an ein Drittland**	**Speicherdauer**	**Anmerkung**
1	Stammdaten inkl. Kontaktinformationen (etwa Adresse, Tel., Mail, Fax, UID-Nr.)	1 - 10, 14		gemäß steuerrechtlicher und unternehmensrechtlicher Aufbewahrungspflichten: 7 Jahre	
2	Daten der Spende	3			
3	Daten über Buchhaltung und Controlling	3, 5			
4	Bankverbindungsdaten	1 – 9			
5	Bedingungen der Spende (Widmung)	3			
6	Gegenstand der Lieferung oder Leistung	1 - 10, 14			

Betroffene Personengruppe: Kooperationenspartner					
Nr.	**Kategorien**				
	von personenbezogenen Daten:	**an Empfänger**	**Übermittlung an ein Drittland**	**Speicherdauer**	**Anmerkung**
1	Stammdaten inkl. Kontaktinformationen (etwa Adresse, Tel., Mail, Fax, UID-Nr.) des Vereins und des Ansprechpartnters	1 - 10, 14		gemäß steuerrechtlicher und unternehmensrechtlicher Aufbewahrungspflichten: 7 Jahre	
2	Leistungsdaten und -abgrenzung	3			
3	Daten über Buchhaltung und Controlling	3, 5			
4	Bankverbindungsdaten	1 – 9			
5	Bonitätsinformationen	3			
6	Gegenstand der Lieferung oder Leistung	1 - 10, 14			
7	Daten über Lieferungs- und Leistungsbedingungen	1 - 10			
8	Finanzierungs- und Zahlungsbedingungen	1 - 10			

2. Datenanwendung: Personalverwaltung

a. **Zweck** der Verarbeitung: Verarbeitung und Übermittlung von Daten für Lohn,- Gehalts- und Entgeltverrechnung und Einhaltung von Aufzeichnungs-, Auskunfts- und Meldepflichten, soweit dies aufgrund von Gesetzen oder Normen kollektiver Rechtsgestaltung oder arbeitsvertraglicher Verpflichtungen jeweils erforderlich ist einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie z.B. Korrespondenz, Zeugnisse) in diesen Angelegenheiten.

Beinhaltet auch: Verwaltung von Urlauben, Karenzierungen, Pflegefreistellungen sowie Pensionierung

b. **Rechtsgrundlage** der Verarbeitung: Erfüllung eines Vertragsverhältnisses, gesetzliche Grundlage

c. Beschreibung der **Kategorien betroffener Personen**: Arbeitnehmer (auch Ehrenamtliche)

d. Verarbeitung durch **Auftragsverarbeiter:** keine

e. Allgemeine Beschreibung der **technischen und organisatorischen Maßnahmen**: Nutzung am passwortgeschützten Computer

Betroffene Personengruppe: Arbeitnehmer (besondere Kategorien von Daten)					
Nr.	**Kategorien**				
	von personenbezogenen Daten:	**an Empfänger**	**Übermittlung an ein Drittland**	**Speicherdauer**	**Anmerkung**
1	Stammdaten über den Arbeitnehmer inkl. Kontaktinformationen (etwa Adresse, Tel, Mail, Fax)	1 - 5, 11 - 13		unbegrenzt (nach Ausscheiden des Mitarbeiters)	
2	Sozialversicherungsdaten	2 - 5, 11 - 13		7 Jahre (nach Ausscheiden des Mitarbeiters)	
3	Bankverbindungsdaten	1 - 4, 11 - 13		6 Monate (nach Ausscheiden des Mitarbeiters)	
4	Personalverrechnungsdaten	1 - 5, 12 - 13		3 Jahre (nach Ausscheiden des Mitarbeiters)	

3. Datenanwendung: Führen von Arbeitszeitaufzeichnungen

a. **Zweck** der Verarbeitung: Führen von Arbeitszeitaufzeichnungen

b. **Rechtsgrundlage** der Verarbeitung: Erfüllung eines Vertragsverhältnisses

c. Beschreibung der **Kategorien betroffener Personen**: Arbeitnehmer (auch Ehrenamtliche)

d. Verarbeitung durch **Auftragsverarbeiter:** keine

e. Allgemeine Beschreibung der **technischen und organisatorischen Maßnahmen**: Keine

Betroffene Personengruppe: Arbeitnehmer					
Nr.	**Kategorien**				
	von personenbezogenen Daten:	**an Empfänger**	**Übermittlung an ein Drittland**	**Speicherdauer**	**Anmerkung**
1	Stammdaten über den Arbeitnehmer inkl. Kontaktinformationen (etwa Adresse, Tel., Mail, Fax)	3		bis 3 Jahre nach Ende des Beschäftigungsverhältnisses	
2	Zeiterfassung (Fehlzeiten, Urlaube)	3			

4. Datenanwendung: Verwaltung von Zeiten der Arbeitsunfähigkeit

a. **Zweck** der Verarbeitung: Verwaltung von Zeiten der Arbeitsunfähigkeit der Mitarbeiter einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie z.B. Korrespondenz) in diesen Angelegenheiten.

b. **Rechtsgrundlage** der Verarbeitung: Gesetzliche Verpflichtung, Erfüllung eines Vertragsverhältnisses

c. Beschreibung der **Kategorien betroffener Personen**: Arbeitnehmer (auch Ehrenamtliche)

d. Verarbeitung durch **Auftragsverarbeiter:** keine

e. Allgemeine Beschreibung der **technischen und organisatorischen Maßnahmen**: Ablage in versperrtem Bereich

Betroffene Personengruppe: Arbeitnehmer (besondere Kategorien von Daten)					
Nr.	**Kategorien**				
	von personenbezogenen Daten:	**an Empfänger**	**Übermittlung an ein Drittland**	**Speicherdauer**	**Anmerkung**
1	Mitarbeiterdaten inkl. Kontaktinformationen (etwa Adresse, Tel., Mail, Fax)	2, 4, 11 - 13		Bis 3 Jahre nach Ende des Beschäftigungsverhältnisses	
2	Ärztliche Bestätigungen				

5. Datenanwendung: Bewerbungsmanagement

a. **Zweck** der Verarbeitung: Organisation, Verwaltung und Abwicklung sowie das Bearbeiten von Bewerbungen einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie z.B. Korrespondenz) in diesen Angelegenheiten.

b. **Rechtsgrundlage** der Verarbeitung: Einwilligungserklärung, berechtigtes Interesse, Erfüllung eines Vertragsverhältnisses

c. Beschreibung der **Kategorien betroffener Personen**: Bewerber (auch Ehrenamtliche)

d. Verarbeitung durch **Auftragsverarbeiter:** Keine

e. Allgemeine Beschreibung der **technischen und organisatorischen Maßnahmen**: Ablage in versperrtem Bereich

Betroffene Personengruppe: Bewerber					
Nr.	**Kategorien**				
	von personenbezogenen Daten:	**an Empfänger**	**Übermittlung an ein Drittland**	**Speicherdauer**	**Anmerkung**
1	Stammdaten inkl. Kontaktinformationen (etwa Adresse, Tel., Mail, Fax)			12 Monate nach Abschluss des Bewerbungsverfahrens	
2	Fähigkeiten und Kenntnisse sowie Qualifikationen (Zeugnisse, Lebenslauf, Beurteilungen, Ausbildungen)			6 Monate nach Abschluss des Bewerbungsverfahrens	
3	Informationen zum beruflichen Werdegang				

6. Datenanwendung: Verwaltung von Benutzerkennzeichen sowie Zugangs- und Zutrittssystemen

a. **Zweck** der Verarbeitung: Systemzugriffskontrolle und Verwaltung von Benutzerkennzeichen für die Datenanwendungen des Verantwortlichen sowie die Verwaltung der Zuteilung von Hard- und Software an die Systembenutzer einschließlich automationsunterstützt erstellter und archivierter Textdokumente (z.B. Korrespondenz) in diesen Angelegenheiten.

Beinhaltet auch: Zuteilung von Schlüsseln und anderen für den Zutritt notwendigen Systemen.

b. **Rechtsgrundlage** der Verarbeitung: Erfüllung eines Vertragsverhältnisses

c. Beschreibung der **Kategorien betroffener Personen**: Zugangs- und Zutrittsberechtigte

d. Verarbeitung durch **Auftragsverarbeiter:** Keine

e. Allgemeine Beschreibung der **technischen und organisatorischen Maßnahmen**: Verwaltung und Weitergabe von Zugriffsdaten nur innerhaln des Vorstandes

Betroffene Personengruppe: Zugangs- und Zutrittsberechtigte					
Nr	**Kategorien**				
	von personenbezogenen Daten:	**an Empfänger**	**Übermittlung an ein Drittland**	**Speicherdauer**	**Anmerkung**
1	Stammdaten inkl. Beziehung des Berechtigten zum Auftraggeber			10 Jahre	
2	Benutzerkennzeichen, Passwörter				
3	Zuteilung von Schlüsseln und anderen für den Zutritt notwendigen Systemen				
4	Zugriffs- und Zutrittsrechte (Gültigkeitsdauer, Bereiche, Zeiten)				

7. Datenanwendung: Aktenverwaltung / Büroautomation

a. **Zweck** der Verarbeitung: Formale Behandlung der vom Verantwortlichen zu besorgenden Geschäftsfälle (einschließlich der Aufbewahrung der bei dieser Tätigkeit anfallenden Dokumente).

Beinhaltet auch: Inventarverwaltung und Verwaltung von Anlagevermögen.

b. **Rechtsgrundlage** der Verarbeitung: Erfüllung eines Vertragsverhältnisses

c. Beschreibung der **Kategorien betroffener Personen**: Arbeitnehmer (oder Ehrenamtliche), Interessenten, Lieferanten

d. Verarbeitung durch **Auftragsverarbeiter:** keine

e. Allgemeine Beschreibung der **technischen und organisatorischen Maßnahmen**: Nutzung der im (versperrten) Sekretariatsarbeitsplatz genutzten, passwortgeschützten Computer

Betroffene Personengruppe: Arbeitnehmer, Interessenten, Lieferanten					
Nr	**Kategorien**				
	von personenbezogenen Daten:	**an Empfänger**	**Übermittlung an ein Drittland**	**Speicherdauer**	**Anmerkung**
1	Stammdaten inkl. Kontaktinformationen (etwa Adresse, Tel., Mail, Fax) sowie Bestell- und Vertragsdaten			gemäß steuerrechtlicher und unternehmensrechtlicher Aufbewahrungspflichten: zumindest 7 Jahre	
2	Gegenstand und Referenz				
3	Unterlagen zu den Geschäftsfällen				
4	Liste des Inventars und Anlagevermögens	3			

8. Datenanwendung: Herausgabe eines Vereinsjournals

a. **Zweck** der Verarbeitung: Erfüllung der Vereinszwecks gemäß Statut sowie die Erfassung automationsunterstützt erstellter und archivierter Textdokumente (wie z.B. Korrespondenz) in diesen Angelegenheiten.

Beinhaltet auch: Korrespondenz mit Autoren und Rechteinhabern von Fachartikeln, Weitergabe der elektronischen Printfassung an (Online-)Druckereien, Korrespondenz im Rahmen von Werbemaßnahmen mit Firmenvertretern, postalischer namentlicher Versand der gedruckten Journale an Mitglieder, Publizierung der versendeten Journale im Internet.

b. **Rechtsgrundlage** der Verarbeitung: Wahrung berechtigter Interessen des Vereins gemäß Statut

c. Beschreibung der **Kategorien betroffener Personen**: Autoren, Firmenvertreter, Verlagsmitarbeiter

d. Verarbeitung durch **Auftragsverarbeiter:** keine

e. Allgemeine Beschreibung der **technischen und organisatorischen Maßnahmen**: Nutzung am passwortgeschützten Computer.

Betroffene Personengruppe: Autoren, Firmenvertreter, Verlagsmitarbeiter					
Nr.	**Kategorien**				
	von personenbezogenen Daten:	**an Empfänger**	**Übermittlung an ein Drittland**	**Speicherdauer**	**Anmerkung**
1	Stammdaten inkl. Kontaktinformationen (etwa Adresse, Tel, Mail, Fax)				

B. Verwaltung von Mitglieder

1. Datenanwendung: Mitgliederverwaltung

a. **Zweck** der Verarbeitung: Erfüllung der Vereinszwecks gemäß Statut sowie der Erfordernisse der Mitgliederbetreuung aufgrund von Mitgliedschaften sowie die Erfassung automationsunterstützt erstellter und archivierter Textdokumente (wie z.B. Korrespondenz) in diesen Angele- genheiten.

Beinhaltet auch: Neuaufnahme von Mitgliedern gemäß schrfltichem Antrag des Mitgliedswerbers, Löschung der Mitglieder im Falle von Austritten aus dem Verein. Korrespondenz zur Einforderung von Mitgliedsbeiträgen und zur Bekanntgabe von Vereinsnews sowie der Termine der Jahreshauptversammlungen

b. **Rechtsgrundlage** der Verarbeitung: Wahrung berechtigter Interessen des Vereins gemäß Statut

c. Beschreibung der **Kategorien betroffener Personen**: Mitglieder (ordentliche, außerordentliche und Ehrenmitglieder gemäß Statut)

d. Verarbeitung durch **Auftragsverarbeiter:** keine

e. Allgemeine Beschreibung der **technischen und organisatorischen Maßnahmen**: Nutzung am passwortgeschützten Computer.

Betroffene Personengruppe: Mitglieder					
Nr.	**Kategorien**				
	von personenbezogenen Daten:	**an Empfänger**	**Übermittlung an ein Drittland**	**Speicherdauer**	**Anmerkung**
1	Stammdaten inkl. Kontaktinformationen (etwa Adresse, Tel, Mail, Fax)			10 Jahre	
2	Mitglied seit				
3	Bezahlter Mitgliedsbeitrag				

4	Art der Mitgliedschaft				
	Bankverbindungsdaten				

C. Organisation Mobile Ärzte

1. Datenanwendung: Teilnehmerverwaltung

a. **Zweck** der Verarbeitung: Erfüllung der Vereinszwecks gemäß Statut sowie die Erfassung automationsunterstützt erstellter und archivierter Textdokumente (wie z.B. Korrespondenz) in diesen Angelegenheiten.

Beinhaltet auch: Administration der Kostenerstattung der Ärzte inklusive der Zahlung der Ausgaben, Ausgabe von Zahlungsbestätigungen

b. **Rechtsgrundlage** der Verarbeitung: Wahrung des Vereinszwecks gemäß Statut

c. Beschreibung der **Kategorien betroffener Personen**: Klienten, mitreisende Ärzte

d. Verarbeitung durch **Auftragsverarbeiter:** keine

e. Allgemeine Beschreibung der **technischen und organisatorischen Maßnahmen**: Nutzung am passwortgeschützten Computer.

Betroffene Personengruppe: Klienten					
Nr.	**Kategorien**				
	von personenbezogenen Daten:	**an Empfänger**	**Übermittlung an ein Drittland**	**Speicherdauer**	**Anmerkung**

1	Stammdaten inkl. Kontaktinformationen (etwa Ad- resse, Tel, Mail, Fax)	16		30 Jahre	
2	Gesundheitsdaten im minimalen zur Bewertung der Reisefähigkeit und des Betreuungsaufwandes wärhend der Reise	16			
3	Reise- Ausflugsdaten				
4	Daten etwaiger Angehöriger (Kontaktdaten)				

Betroffene Personengruppe: Mitreisende Ärzte

Nr.	**Kategorien**				
	von personenbezogenen Daten:	**an Empfänger**	**Übermittlung an ein Drittland**	**Speicherdauer**	**Anmerkung**
1	Stammdaten inkl. Kontaktinformationen (etwa Ad- resse, Tel, Mail, Fax)			10 Jahre	
2	Reise- Ausflugsdaten				

III. Technische und organisatorische Maßnahmen

In Entsprechung des Art 32 DSGVO trifft der Verantwortliche folgende technische und organisatorische Maßnahmen

1. Hinsichtlich Benutzer

1.1. Technische Maßnahmen

1.1.1. Sichere Nutzung des Internets:

Der Verantwortliche stellt sicher, dass Benutzer eine Schulung zum sicheren Umgang mit dem Internet erhalten. Die Schulung der Mitarbeiter erfolgt einmal im Jahr.

1.1.2. Technische Maßnahmen zum Sichern von Arbeitsplatzrechnern:

Der Verantwortliche stellt sicher, dass sämtliche Arbeitsplatzrechner so gesichert sind, dass Rechnermikrofone und Kameras gegen unberechtigten Zugriff gesperrt sind. Sämtliche Arbeitsplatzrechner erhalten regelmäßig Sicherheitsupdates und werden regelmäßig auf Viren untersucht. Die Grundkonfiguration der Rechner sieht vor, dass die Rechner vor unberechtigtem Zugang geschützt sind (die Nutzung des Rechners ist nur nach Eingabe eines Passworts möglich).

1.1.3. Datensicherung der Clients:

Der Verantwortliche stellt sicher, dass sämtliche lokal auf den Arbeitsplatzrechnern gespeicherten Daten regelmäßig gesichert werden.

Die Rechner werden wie folgt gesichert:
Die Daten werden täglich regelmäßig auf externe Datenträger gesichert.

1.2. Organisatorische Maßnahmen

1.2.1. Mitarbeiterschulung:

Der Verantwortliche stellt sicher, dass sämtliche Mitarbeiter regelmäßig geschult werden. Im Rahmen der Schulung werden die Mitarbeiter aufgeklärt, auf welche Art und Weise personenbezogene Daten verarbeitet werden dürfen und welche Datensicherheitsmaßnahmen zu ergreifen sind. Der Verantwortliche stellt sicher, dass ein entsprechender Nachweis der Schulung im Personalakt des jeweiligen Mitarbeiters abgelegt wird.

Im Rahmen der Schulung werden die Mitarbeiter auch über die sichere Nutzung von Browsern, die sichere Nutzung von sozialen Netzwerken sowie über die Zulässigkeit der Nutzung von Kommunikationsmedien informiert.

Der Verantwortliche hat seine Mitarbeiter darüber aufgeklärt, dass die Nutzung von Onlinespeichern („Cloud-Dienste“) – ohne ausdrückliche Genehmigung des Verantwortlichen – nicht zulässig ist.

Die Mitarbeiter werden dahingehend geschult, dass diese umgehend bekannt geben müssen, sollte ein genutztes Endgerät – egal aus welchem Grund – nicht mehr nutzbar sein (Defekt, Verlust, Diebstahl).

1.2.2. Nutzung von Kommunikationsmitteln:

Der Verantwortliche klassifiziert Dokumente wie folgt:

1. Vertraulich
2. Nicht vertraulich
3. Öffentlich bekannt

Der Verantwortliche nutzt folgende Kommunikationsmedien:

1. Persönliche Übergabe
2. Versand per eingeschriebenem Brief
3. Versand per Post
4. Versand per Fax
5. Versand per E-Mail
6. Telefonische Mitteilung

Zur Einhaltung eines angemessenen Sicherheitsniveaus verpflichtet sich der Verantwortliche, Informationen ausschließlich wie folgt zu übermitteln bzw. zu übersenden:

Klassifizierung	Kommunikationsmedium
Vertraulich	Persönliche Übergabe Versand per Post
Nicht vertraulich	Jedes Medium
Öffentlich bekannt	Jedes Medium

Der Verantwortliche klassifiziert Informationen wie folgt:

Information	Klassifizierung
Informationen, die Gesundheitsdaten oder Sozialversicherungsnummer enthalten	Vertraulich
Adressinformationen	Nicht vertraulich
Kontaktinformationen	Nicht vertraulich

Die Weitergabe von Zugangsdaten und Passwörtern im Zusammenhang mittels verschlüsselter elektronischer Kommunikation erfolgt ausschließlich per Post, persönlich oder per SMS (nach vorheriger schriftlicher Einwilligungserklärung des Empfängers).

1.2.3. Verpflichtung der Benutzer zum Abmelden nach Aufgabenerfüllung:

Der Verantwortliche stellt sicher, dass sämtliche Nutzer sich verpflichten, sich nach dem Erfüllen einer Aufgabe vom jeweiligen Arbeitsplatzrechner abzumelden.

1.2.4. Geeigneter Umgang mit Laufwerken für Wechselmedien und externe Datenträger (Handhabung, Entsorgung, Transport):

Den Mitarbeitern ist es ohne explizite Erlaubnis nicht gestattet, personenbezogene Daten, die der Verantwortliche verarbeitet, auf Datenträger zu speichern. Eine solche Speicherung wird der jeweilige Verantwortliche explizit anordnen und – für den Einzelfall – geeignete Sicherheitsmaßnahmen anordnen.

1.2.5. Regeln zum Verlassen der Räumlichkeiten:

Der Verantwortliche stellt sicher, dass die Mitarbeiter dahingehend geschult werden, dass sämtliche Fenster und Türen bei Verlassen der Räumlichkeiten geschlossen bzw. abgeschlossen werden, sodass ein unbefugter Dritter keinen Zugang zu den Räumlichkeiten des Verantwortlichen bzw. zu personenbezogenen Daten hat.

1.2.6. Sicherung von physischen Dokumenten:

Der Verantwortliche stellt sicher, dass sämtliche Mitarbeiter dahingehend geschult werden, dass Dokumente der Kategorie „vertraulich“ in einem verschlossenen Aktenordner oder Aktenschrank verwahrt und unmittelbar nach dem Gebrauch wieder eingeschlossen werden müssen.

Der Verantwortliche hat mit den Mitarbeitern geeignete Maßnahmen zur Sicherung des Schlüssels getroffen.

1.2.7. Geheimhaltungsvereinbarung:

Der Verantwortliche stellt sicher, dass mit sämtlichen Mitarbeitern eine Geheimhaltungsvereinbarung mit folgendem Inhalt geschlossen worden ist:

„*Der Dienstnehmer ist verpflichtet, personenbezogene Daten aus Datenverarbeitungen, die ihm ausschließlich auf Grund seiner berufsmäßigen Beschäftigung anvertraut wurden oder zugänglich geworden sind, unbeschadet sonstiger gesetzlicher Verschwiegenheitspflichten, geheim zu halten, soweit kein rechtlich zulässiger Grund für eine Übermittlung der anvertrauten oder zugänglich gewordenen perso- nenbezogenen Daten besteht (kurz: das Datengeheimnis).*
Dienstnehmer dürfen personenbezogene Daten nur auf Grund einer ausdrücklichen Anordnung des Dienstgebers übermitteln.
Das Datengeheimnis besteht auch über das Ende des Dienstverhältnisses hinaus unbefristet fort.“

2. Hinsichtlich IT-Infrastruktur:

2.1. Technische Maßnahmen

2.1.1. Arbeitsplatzrechner:

Der Verantwortliche stellt sicher, dass Computer vor unbefugtem Zugriff und unbefugter Nutzung geschützt sind. Darüber hinaus sind sämtliche Arbeitsplatzrechner so konfiguriert, dass sich Updates und Softwarekorrekturen, die Sicherheitslücken schließen, automatisch installieren. Bei Arbeitsplatzrechnern, auf denen besondere Kategorien von Daten gespeichert sind, sind die genutzten Speichermedien verschlüsselt.

2.1.2. Softwaresicherheitsmaßnahmen:

Der Verantwortliche stellt sicher, dass sämtliche Endgeräte regelmäßig mit Updates versorgt werden und Softwarepakete, welche Sicherheitslücken schließen, automatisch und regelmäßig in die entsprechenden Systeme eingespielt werden. Er stellt darüber hinaus sicher, dass regelmäßig geprüft wird, ob das Einspielen ordnungsgemäß funktioniert hat.

Der Verantwortliche stellt sicher, dass der Zugriff auf Systeme nur nach Eingabe eines Passworts möglich ist.

Der Verantwortliche stellt sicher, dass Benutzer gelöscht oder gesperrt werden, sobald diese keinen Zugriff mehr auf das System benötigen (etwa: Löschen von Benutzer-Konten von ehemaligen Mitarbeitern).

Der Verantwortliche stellt sicher, dass sämtliche Systeme durch eine Firewall geschützt werden, um einen unberechtigten externen Zugriff zu verhindern. Der Verantwortliche stellt sicher, dass ein aktueller Viren- und Spamfilter installiert ist und gewartet wird.

2.1.3. Sicherung von Telekommunikationseinrichtungen:

Der Verantwortliche stellt sicher, dass sämtliche Telekommunikationseinrichtungen (etwa Telefonanlage, Fax, VPN, W-LAN, E-Mailserver, Firewalls) vor unberechtigtem Zugriff geschützt sind.

2.2. Organisatorische Maßnahmen

2.2.1. Maßnahmen bei Außerbetriebnahme eines Clients / Beendigung des Dienstverhältnisses:

Der Verantwortliche stellt sicher, dass sämtliche Rechner, welche nicht mehr genutzt werden sollen, ordnungsgemäß entsorgt werden und personenbezogene Daten auf den Rechnern vor unberechtigtem Zugriff geschützt werden.

2.2.2. Dokumentation der technischen Infrastruktur:

Der Verantwortliche stellt sicher, dass die gesamte technische Infrastruktur ausreichend dokumentiert ist. Dies beinhaltet auch die Dokumentation und Kennzeichnung der Verkabelung sowie relevanter baulicher Maßnahmen.

3. Bauseitig:

3.1. Organisatorische Maßnahmen:

3.1.1. Regelungen über den Zutritt zu Räumlichkeiten:

Der Verantwortliche stellt sicher, dass der Zutritt zu den Räumlichkeiten nur berechtigten Personen möglich ist. Mitarbeiter, welche Schlüssel oder Zutrittsberechtigungen zu den Räumlichkeiten erhalten haben, sind entsprechend geschult, dass diese den Verantwortlichen umgehend informieren müssen, sollte der Schlüssel abhandenkommen (Verlust, Diebstahl oder ähnliches).

3.1.2. Maßnahmen zum Schutz der Infrastruktur:

Der Verantwortliche stellt sicher, dass die Infrastruktur vor unberechtigtem Zutritt geschützt ist. Ferner hat der Verantwortliche Maßnahmen ergriffen, die Infrastruktur vor Zerstörung (etwa durch Feuer) zu schützen.

3.1.3. Archiv:

Der Verantwortliche hat Maßnahmen dahingehend ergriffen, dass der Zutritt zum Archiv nur berechtigten Personen möglich ist.

4. Administrativ:

4.1. Definition von Prozessen:

Der Verantwortliche hat in Punkt V dieses Dokuments Prozesse zur Auskunft, Löschung und Richtigstellung von Daten definiert.

4.2. Behandlung von Sicherheitsvorfällen:

Der Verantwortliche hat Prozesse definiert, was im Fall eines Sicherheitsvorfalles passieren soll.

4.3. Überprüfung der Einhaltung:

Der Verantwortliche wird regelmäßig die hier beschriebenen technischen und organisatorischen Maßnahmen evaluieren und prüfen.

IV. Auftragsverarbeiter[1]

1. Liste der Auftragsverarbeiter

Siehe oben

2. Muster der abgeschlossenen Vereinbarungen

Siehe Beilage

V. Prozessdefinitionen

1. Recht auf Auskunft

Gemäß Art 15 hat die betroffene Person das Recht, von den Verantwortlichen eine Bestätigung darüber zu verlangen, ob personenbezogene Daten über sie vom Verantwortlichen verarbeitet werden. Sollte dies der Fall sein, hat die betroffene Person ein Recht auf Auskunft über diese personenbezogenen Daten und darüber hinaus auf folgende Informationen:

a) die Verarbeitungszwecke;
b) die Kategorien personenbezogener Daten, die verarbeitet werden;
c) die Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, insbesondere bei Empfängern in Drittländern oder bei internationalen Organisationen;
d) falls möglich die geplante Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;
e) das Bestehen eines Rechts auf Berichtigung oder Löschung der sie betreffenden personenbezogenen Daten oder auf Einschränkung der Verarbeitung durch den Verantwortlichen oder eines Widerspruchsrechts gegen diese Verarbeitung;
f) das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;
g) wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden, alle verfügbaren Informationen über die Herkunft der Daten;
h) das Bestehen einer automatisierten Entscheidungsfindung (Hinweis: bei Ärzten nicht einschlägig) einschließlich Profiling und in diesen Fällen aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

Sollten personenbezogene Daten an ein Drittland oder an eine internationale Organisation übermittelt werden, so hat die betroffene Person darüber hinaus das Recht, über die geeigneten Garantien gemäß Art 46 DSGVO im Zusammenhang mit der Übermittlung unterrichtet zu werden. Sollte die betroffene Person dies wünschen, stellt der Verantwortliche eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, dem Betroffenen zur Verfügung.

Für jede weitere Kopie, die die betroffene Person beantragt, kann der Verantwortliche ein angemessenes Entgelt auf Grundlage der Verwaltungskosten verlangen. Dieses Recht hat der Betroffene allerdings nur aufgrund unbegründeter oder exzessiver Ausübung des Rechts auf Auskunft.

Die betroffene Person hat das Recht den Antrag elektronisch zu stellen. In diesem Fall

sind die Informationen in einem gängigen elektronischen Format (gesichert) zur Verfügung zu stellen, sofern die betroffene Person nichts Anderes angibt.

In Entsprechung dieser Verpflichtungen wird der Verantwortliche das Auskunftsrecht der betroffenen Person wie folgt handhaben:

Sobald der Betroffene einen Antrag auf Auskunft an den Verantwortlichen stellt, wird der Ansprechpartner des Verantwortlichen alle vertretbaren Mittel nutzen, um die Identität der betroffenen Person zu überprüfen. Der Antrag der betroffenen Person bedarf keiner besonderen Form und darf auch elektronisch erfolgen.

Der Antrag muss dem Verantwortlichen aber ermöglichen, die Informationen herauszufinden, die er beauskunften soll. Für die Beauskunftung ist beim Verantwortlichen **der Ansprechpartner** zuständig.

Sollte der Betroffene eine **mündliche Auskunft** verlangen, so wird der Zuständige die Identität des Betroffenen in geeigneter Weise feststellen und die Auskunft ebenso mündlich erteilen. Der Zuständige wird sämtliche Datenbestände nach Informationen, die die betroffene Person betreffen, durchsuchen und diese Informationen zusammenstellen.

Der Ansprechpartner wird sämtliche Datenbestände, in denen personenbezogene Daten über den Betroffenen zu finden sind, zusammenstellen und – sofern diese inhaltlich unübersichtlich sind – kurz erläutern.

Die Auskunft wird folgende Informationen umfassen:

- **Verarbeitete Daten:** Der Verantwortliche wird die betroffene Person darüber informieren, welche Informationen er über die Person verarbeitet.

- **Informationen:** Darüber hinaus wird der Verantwortliche der betroffenen Person folgende Informationen über die Datenverarbeitung zur Verfügung stellen:
  - die Zwecke der Verarbeitung
  - Datenkategorien
  - Empfänger und Kategorien von Empfängern
  - Dauer der Datenspeicherung
  - Herkunft der Daten
  - Sollte eine automatisierte Entscheidungsfindung und Profiling erfolgt sein, die Methoden und Kriterien sowie die Tragweite und Auswirkungen der Datenverarbeitung

- **Betroffene Rechte:** Der Verantwortliche wird die betroffene Person über Folgendes informieren:

  „Die betroffene Person hat das Recht auf Auskunft über die gespeicherten Daten gemäß Art 15 DSGVO, auf Berichtigung unzutreffender Daten gemäß Art 16 DSGVO, auf Löschung von Daten gemäß Art 17 DSGVO, auf Einschränkung der Verarbeitung von Daten gemäß Art 18 DSGVO, auf Widerspruch gegen die unzumutbare Datenverarbeitung gemäß Art 21 DSGVO sowie auf Datenübertragbarkeit gemäß Art 20 DSGVO.

  Der Betroffene hat das Recht, sich bei der Aufsichtsbehörde zu beschweren – zuständig ist in Österreich die Datenschutzbehörde.“

Der Verantwortliche wird – sofern der Betroffene dies wünscht – die personenbezogenen Daten, die die betroffene Person betreffen, dieser so zur Verfügung stellen, dass diese in einem strukturierten, gängigen und maschinenlesbaren Format vorliegen.

Der Betroffene soll so die Möglichkeit haben, die Daten einem anderen Verantwortlichen ohne Behinderung zu übermitteln.

Frist:

Der Verantwortliche wird die Auskunft unverzüglich erteilen, jedenfalls binnen eines Monats ab Eingang beim Verantwortlichen. Sollte es sich um eine umfangreiche und komplexe Auskunft handeln, kann der Verantwortliche im Einzelfall die Frist zur Beauskunftung einmalig um weitere zwei Monate verlängern, der Verantwortliche wird dies unter Nennung der Gründe dem Betroffenen binnen eines Monats mitteilen.

Negativauskunft:

Sollte der Verantwortliche die Beauskunftung nicht erteilen, wird er dies ebenso binnen eines Monats unter Angabe von Gründen dem Betroffenen mitteilen.

Sollte der Verantwortliche keine Daten über die betroffene Person verarbeiten, wird der Verantwortliche eine Negativauskunft (eine Bestätigung, dass er keine Daten über den Betroffenen verarbeitet) dem Betroffenen übermitteln.

2. Recht auf Berichtigung

Sollte der Betroffene den Verantwortlichen darüber informieren, dass dieser unrichtige oder (für den Zweck der Datenverarbeitung) unvollständige Daten verarbeitet, hat der Betroffene das Recht, sich an den **Ansprechpartner** beim Verantwortlichen zu melden. Dieser wird die von der betroffenen Person bekanntgegeben Daten unverzüglich inhaltlich prüfen und gegebenenfalls vervollständigen bzw. richtigstellen.

Sollte die Korrektheit der Daten strittig sein, wird der Verantwortliche die Verarbeitung einschränken (siehe dazu unten).

Weiters wird der Verantwortliche etwaige Empfänger der (unrichtigen) Daten über die berichtigten Daten informieren.

3. Das Recht auf Löschung

Die betroffene Person hat das Recht, von dem Verantwortlichen zu verlangen, dass betreffende personenbezogene Daten unverzüglich gelöscht werden. Der Verantwortliche ist verpflichtet, personenbezogene Daten unverzüglich zu löschen, sofern einer der folgenden Gründe zutrifft:

- Die personenbezogenen Daten sind für die Zwecke, für die sie erhoben wurden, nicht mehr notwendig;
- Die betroffene Person widerruft ihre Einwilligung, auf die sich die Verarbeitung stützt und es fehlt an einer anderweitigen Rechtsgrundlage für die Verarbeitung;

- Die betroffene Person legt Widerspruch gegen die Verarbeitung ein und es liegen keine vorrangigen berechtigten Gründe für die Verarbeitung vor;
- Die personenbezogenen Daten wurden unrechtmäßig verarbeitet;
- Die Löschung der personenbezogenen Daten ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich;
- Bei den personenbezogenen Daten handelt es sich um die Daten eines Kindes in Bezug auf angebotene Internetdienste.

Der Verantwortliche wird jedes Löschungsbegehren umgehend prüfen und mit zumutbarem Aufwand die Voraussetzungen des Anspruchs prüfen.

Der Verantwortliche wird die betroffene Person jedenfalls innerhalb eines Monats nach Eingang des Antrags über die ergriffenen Maßnahmen bzw. über die Gründe der Ablehnung informieren. Gegebenenfalls wird der Verantwortliche den Betroffenen – sofern es sich um ein komplexes Begehren handelt – über die Verlängerung der Prüfung des Löschungsbegehrens um zwei Monate ebenso binnen eines Monats informieren.

Sollte die betroffene Person einen Widerspruch erhoben haben, und hat die betroffene Person vom Verantwortlichen die Einschränkung der Verarbeitung verlangt, wird der Verantwortliche die Verarbeitung einschränken (siehe dazu unten).

6. Meldung an die Behörde

Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet der Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der österreichischen Datenschutzbehörde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Erfolgt die Meldung an die Aufsichtsbehörde nicht binnen 72 Stunden, so ist ihr eine Begründung für die Verzögerung beizufügen.

Die Meldung an die Behörde enthält zumindest folgende Informationen:
a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
b) den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;
c) eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
d) eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Meldung an den Betroffenen

Hat die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge, so benachrichtigt der Verantwortliche die betroffene Person unverzüglich von der Verlet-

zung