283/17-1/62/SP/48-1

**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 Arztes

**[Bitte Namen ergänzen]**

Datum: 3.4.2018

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

**Inhaltsverzeichnis:**

1. [Allgemeine Informationen 3](#_bookmark0)
2. [Verzeichnis von Verarbeitungstätigkeiten 4](#_bookmark1)
3. [Technische und organisatorische Maßnahmen 27](#_bookmark2)
4. [Auftragsverarbeiter 37](#_bookmark3)
5. [Prozessdefinitionen 40](#_bookmark4)
6. [Muster für eine Einwilligungserklärung 45](#_bookmark5)

# Allgemeine Informationen

* + 1. Name und Anschrift des Verantwortlichen:

**[Bitte ergänzen Sie den Namen, die Anschrift und die Kontaktinformatio- nen des Arztes]**

* + 1. Kontaktinformationen des Ansprechpartners:

**[Sollte der Arzt in seiner Ordination eine Ansprechperson für Daten- schutzfragen haben: Ergänzen Sie hier den Namen, die Anschrift und die Kontaktinformationen der Ansprechperson, andernfalls verweisen Sie auf die Daten des Verantwortlichen]**

* + 1. Kontaktinformationen des Datenschutzbeauftragten:

**[Sollte ein Datenschutzbeauftragter notwendig sein, ergänzen Sie hier den Namen, die Anschrift und die Kontaktinformationen des Datenschutzbe- auftragten]**

# Verzeichnis von Verarbeitungstätigkeiten

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

* Verwaltung der Ordination
* Patientenverwaltung

Sofern nichts Anderes angegeben ist, verweist das Verzeichnis von Verarbeitungstä- tigkeiten 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
16. Ärzte, Krankenhäuser, Ambulatorien, Labore, Physiotherapeuten, Pflegeheime
17. Apotheken, Gesundheitsdiensteanbieter, nicht-ärztliche Gesundheitsberufe
	1. **Verwaltung der Ordination**
18. **Datenanwendung: Kommunikation mit der Kammer**
	1. **Zweck** der Verarbeitung: Abwicklung von organisatorischen Fragen mit der jeweiligen Ärztekammer zum Betrieb der Ordination einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie z.B. Korrespondenz) in dieser Angelegen- heit.

Beinhaltet auch: Beiträge und Umlagen, die Beantragung von Fortbildungsnachweisen.

* 1. **Rechtsgrundlage** der Verarbeitung: gesetzliche Grundlage
	2. Beschreibung der **Kategorien betroffener Personen**: Arbeitnehmer, Mitglieder und Arbeitnehmer der Ärztekammer
	3. Verarbeitung durch **Auftragsverarbeiter: [Auftragsverarbeiter namentlich benennen]**
	4. Allgemeine Beschreibung der **technischen und organisatorischen Maßnahmen**: **[Sofern möglich spezifische Maßnahmen beschreiben]**

|  |  |
| --- | --- |
| **Betroffene Personengruppe: Arbeitnehmer, Mitglie-****der und Arbeitnehmer der Ärztekammer** |  |
| **Nr.** | **Kategorien** |  |
|  | **von personenbezogenen Daten:** | **an Empfänger** | **Übermittlung an ein Drittland** | **Speicherdauer** | **Anmerkung** |
| **1** | Stammdaten inkl. Kontaktinformationen (etwa Ad- resse, Tel., Mail, Fax) | 12 |  | unbegrenzt |  |
| **2** | Kommunikationsdaten (insb. Korrespondenz) | 12 |  | unbegrenzt |  |
| **3** | Bankverbindungsdaten | 12 |  | unbegrenzt |  |
| **4** | Ausbildungs- und Gerätenachweis | 12 |  | unbegrenzt |  |
| **5** | Verrechnungsdaten | 12 |  | unbegrenzt |  |

1. **Datenanwendung: Finanzbuchhaltung, Rechnungswesen und Logistik**
	1. **Zweck** der Verarbeitung:

Verarbeitung und Übermittlung von Daten im Rahmen einer Geschäftsbeziehung (bzw. zur Abwicklung dieser) mit Patienten und Lieferanten einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie z.B. Korrespondenz) in diesen Angelegenheiten.

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

* 1. **Rechtsgrundlage** der Verarbeitung: Gesetzliche Verpflichtung
	2. Beschreibung der **Kategorien betroffener Personen**: Arbeitnehmer, Patienten, Lieferanten
	3. Verarbeitung durch **Auftragsverarbeiter: [Auftragsverarbeiter namentlich benennen]**
	4. Allgemeine Beschreibung der **technischen und organisatorischen Maßnahmen**: **[Sofern möglich spezifische Maßnahmen beschreiben]**

|  |  |
| --- | --- |
| **Betroffene Personengruppe: Arbeitnehmer** |  |
| **Nr.** | **Kategorien** |  |
|  | **von personenbezogenen Daten:** | **an Empfänger** | **Übermittlung an ein Drittland** | **Speicherdauer** | **Anmerkung** |
| **1** | Stammdaten inkl. Kontaktinformationen (etwa Ad- resse, Tel., Mail, Fax, UID-Nr.) | 1 - 10, 14 |  | gemäß steuerrechtlicher und unternehmensrecht- licher Aufbewahrungs- pflichten: mindestens 7 Jahre |  |
| **2** | Bankverbindungsdaten | 1 - 9 |  |  |
| **3** | Daten über Buchhaltung und Controlling | 5 |  |  |
| **4** | Bestell- und Vertragsdaten | 14, 15 |  |  |
| **5** | Finanzierungs- und Zahlungsbedingungen | 1 - 10 |  |  |
| **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 Ad- resse, Tel., Mail, Fax, UID-Nr.) | 1 - 10, 14 |  | gemäß steuerrechtlicher und unternehmensrecht- licher Aufbewahrungs- pflichten: 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 |  |  |

1. **Datenanwendung: Personalverwaltung**
	1. **Zweck** der Verarbeitung: Verarbeitung und Übermittlung von Daten für Lohn,- Gehalts- und Entgeltverrechnung und Einhaltung von Aufzeichnungs-, Auskunfts- und Meldepflichten (inkl. Strahlenschutz), soweit dies aufgrund von Gesetzen oder Normen kol- lektiver 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

* 1. **Rechtsgrundlage** der Verarbeitung: Erfüllung eines Vertragsverhältnisses, gesetzliche Grundlage
	2. Beschreibung der **Kategorien betroffener Personen**: Arbeitnehmer
	3. Verarbeitung durch **Auftragsverarbeiter: [Auftragsverarbeiter namentlich benennen]**
	4. Allgemeine Beschreibung der **technischen und organisatorischen Maßnahmen**: **[Sofern möglich spezifische Maßnahmen beschreiben]**

|  |  |
| --- | --- |
| **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 Aus-scheiden des Mitarbei- ters) |  |
| **2** | Sozialversicherungsdaten | 2 - 5, 11 - 13 |  | 7 Jahre (nach Ausschei- den des Mitarbeiters) |  |
| **3** | Bankverbindungsdaten | 1 - 4, 11 - 13 |  | 6 Monate (nach Aus- scheiden des Mitarbei-ters) |  |
| **4** | Personalverrechnungsdaten | 1 - 5, 12 - 13 |  | 3 Jahre (nach Ausschei- den des Mitarbeiters) |  |

1. **Datenanwendung: Führen von Arbeitszeitaufzeichnungen**
	1. **Zweck** der Verarbeitung: Führen von Arbeitszeitaufzeichnungen
	2. **Rechtsgrundlage** der Verarbeitung: Erfüllung eines Vertragsverhältnisses
	3. Beschreibung der **Kategorien betroffener Personen**: Arbeitnehmer
	4. Verarbeitung durch **Auftragsverarbeiter: [Auftragsverarbeiter namentlich benennen]**
	5. Allgemeine Beschreibung der **technischen und organisatorischen Maßnahmen**: **[Sofern möglich spezifische Maßnahmen beschreiben]**

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

1. **Datenanwendung: Verwaltung von Zeiten der Arbeitsunfähigkeit**
	1. **Zweck** der Verarbeitung: Verwaltung von Zeiten der Arbeitsunfähigkeit der Mitarbeiter einschließlich automationsunterstützt er- stellter und archivierter Textdokumente (wie z.B. Korrespondenz) in diesen Angelegenheiten.
	2. **Rechtsgrundlage** der Verarbeitung: Gesetzliche Verpflichtung, Erfüllung eines Vertragsverhältnisses
	3. Beschreibung der **Kategorien betroffener Personen**: Arbeitnehmer
	4. Verarbeitung durch **Auftragsverarbeiter: [Auftragsverarbeiter namentlich benennen]**
	5. Allgemeine Beschreibung der **technischen und organisatorischen Maßnahmen**: **[Sofern möglich spezifische Maßnahmen beschreiben]**

|  |  |
| --- | --- |
| **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 |  |  |

1. **Datenanwendung: Bewerbungsmanagement**
	1. **Zweck** der Verarbeitung: Organisation, Verwaltung und Abwicklung sowie das Bearbeiten von Bewerbungen einschließlich au- tomationsunterstützt erstellter und archivierter Textdokumente (wie z.B. Korrespondenz) in diesen Angelegenheiten.
	2. **Rechtsgrundlage** der Verarbeitung: Einwilligungserklärung, berechtigtes Interesse, Erfüllung eines Vertragsverhältnisses
	3. Beschreibung der **Kategorien betroffener Personen**: Bewerber
	4. Verarbeitung durch **Auftragsverarbeiter: [Auftragsverarbeiter namentlich benennen]**
	5. Allgemeine Beschreibung der **technischen und organisatorischen Maßnahmen**: **[Sofern möglich spezifische Maßnahmen beschreiben]**

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

1. **Datenanwendung: Verwaltung von Benutzerkennzeichen sowie Zugangs- und Zutrittssystemen**
	1. **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 automa- tionsunterstützt erstellter und archivierter Textdokumente (z.B. Korrespondenz) in diesen Angelegenheiten.

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

* 1. **Rechtsgrundlage** der Verarbeitung: Erfüllung eines Vertragsverhältnisses
	2. Beschreibung der **Kategorien betroffener Personen**: Zugangs- und Zutrittsberechtigte
	3. Verarbeitung durch **Auftragsverarbeiter: [Auftragsverarbeiter namentlich benennen]**
	4. Allgemeine Beschreibung der **technischen und organisatorischen Maßnahmen**: **[Sofern möglich spezifische Maßnahmen beschreiben]**

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

1. **Datenanwendung: Verwaltung von Vertretungen**
	1. **Zweck** der Verarbeitung: Organisation und Abwicklung von Vertretungen in der Ordination im Verhinderungsfall (auch: Urlaubs- vertretung) einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie z.B. Korrespondenz) in diesen Angelegenheiten.
	2. **Rechtsgrundlage** der Verarbeitung: Erfüllung eines Vertragsverhältnisses
	3. Beschreibung der **Kategorien betroffener Personen**: Arbeitnehmer, Vertretungen
	4. Verarbeitung durch **Auftragsverarbeiter: [Auftragsverarbeiter namentlich benennen]**
	5. Allgemeine Beschreibung der **technischen und organisatorischen Maßnahmen**: **[Sofern möglich spezifische Maßnahmen beschreiben]**

|  |  |
| --- | --- |
| **Betroffene Personengruppe:** Arbeitnehmer, Vertretun-gen |  |
| **Nr** | **Kategorien** |  |
|  | **von personenbezogenen Daten:** | **an Empfängern** | **Übermittlung an****ein Drittland** | **Speicherdauer** | **Anmerkung** |
| **1** | Stammdaten inkl. Kontaktinformationen (etwa Ad- resse, Tel., Mail, Fax, UID-Nr., Mitgliedsnummer) | 12, 16 |  | Speicherung im Rah- men der Patientendo- kumentation |  |
| **2** | Organisationsdaten | 12, 16 |  |  |

1. **Datenanwendung: Aktenverwaltung / Büroautomation**
	1. **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.

* 1. **Rechtsgrundlage** der Verarbeitung: Erfüllung eines Vertragsverhältnisses
	2. Beschreibung der **Kategorien betroffener Personen**: Arbeitnehmer, Interessenten, Lieferanten
	3. Verarbeitung durch **Auftragsverarbeiter: [Auftragsverarbeiter namentlich benennen]**
	4. Allgemeine Beschreibung der **technischen und organisatorischen Maßnahmen**: **[Sofern möglich spezifische Maßnahmen beschreiben]**

|  |  |
| --- | --- |
| **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 Be- stell- und Vertragsdaten |  |  | gemäß steuerrechtlicher und unternehmensrecht- licher Aufbewahrungs- pflichten: zumindest 7 Jahre |  |
| **2** | Gegenstand und Referenz |  |  |  |
| **3** | Unterlagen zu den Geschäftsfällen |  |  |  |
| **4** | Liste des Inventars und Anlagevermögens | 3 |  |  |

* 1. **Patientenverwaltung**
1. **Datenanwendung: Patientenakte**
	1. **Zweck** der Verarbeitung: Erfüllung der Dokumentationspflicht gemäß § 51 Ärztegesetz sowie die Erfassung sämtlicher Leistun- gen einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie z.B. Korrespondenz) in diesen Angele- genheiten.

Beinhaltet auch: Ausstellung von Bescheinigungen, Terminmanagement (Terminvereinbarung mit Patienten), die Wahrnehmung der Anzeige- und Meldepflicht gemäß § 54 Ärztegesetz, die Wahrnehmung der Anzeige- und Meldepflicht im Missbrauchsfall sowie Meldungen an div. Gesundheitsregister und im öffentlichen Meldewesen (Meldepflichten bei ansteckenden Krankheiten); die Mitwirkung bei Verfahren bei der Patientenanwaltschaft, der Schlichtungsstelle sowie dem Beschwerdemanagement bei der Standesvertretung und Versicherungen; die Erstellung medizinischer Gutachten.

Verwaltung von Transportscheinen, Zuweisungen und Überweisungen.

* 1. **Rechtsgrundlage** der Verarbeitung: gesetzliche Grundlage
	2. Beschreibung der **Kategorien betroffener Personen**: Arbeitnehmer, Patienten
	3. Verarbeitung durch **Auftragsverarbeiter: [Auftragsverarbeiter namentlich benennen]**
	4. Allgemeine Beschreibung der **technischen und organisatorischen Maßnahmen**: **[Sofern möglich spezifische Maßnahmen beschreiben]**

|  |  |
| --- | --- |
| **Betroffene Personengruppe:** Arbeitnehmer |  |
| **Nr.** | **Kategorien** |  |
|  | **von personenbezogenen Daten:** | **an Empfänger** | **Übermittlung an****ein Drittland** | **Speicherdauer** | **Anmerkung** |
| **1** | Stammdaten inkl. Kontaktinformationen (etwa Ad- resse, Tel., Mail, Fax) | 2, 4, 5, 9, 16,17 |  | 30 Jahre |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **2** | Behandlungsinformationen |  |  |  |  |

|  |  |
| --- | --- |
| **Betroffene Personengruppe: Patienten (besondere****Kategorien von Daten)** |  |
| **Nr.** | **Kategorien** |  |
|  | **von personenbezogenen Daten:** | **an Empfänger** | **Übermittlung an****ein Drittland** | **Speicherdauer** | **Anmerkung** |
| **1** | Stammdaten inkl. Kontaktinformationen (etwa Ad- resse, Tel, Mail, Fax) | 2, 4, 5, 9, 16,17 |  | 30 Jahre |  |
| **2** | Zustand (bei Übernahme der Beratung oder Be- handlung) |  |  |
| **3** | Vorgeschichte einer Erkrankung |  |  |
| **4** | Patienteninformationen (etwa Befunde, Diagnosen) |  |  |
| **5** | Krankheitsverlauf |  |  |
| **6** | Behandlungsinformationen |  |  |
| **7** | Sozialversicherungsdaten |  |  |
| **8** | Bankverbindungsdaten |  |  |
| **9** | Leistungen |  |  |
| **10** | Daten über Aufklärungsgespräch |  |  |
| **11** | Gesetzliche Vertreter |  |  |

1. **Datenanwendung: Abrechnung (sowohl Krankenkasse / Privat)**
	1. **Zweck** der Verarbeitung: Abrechnung der erbrachten Leistungen gegenüber Versicherungen (Krankenkassen oder den Patien- ten) einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie z.B. Korrespondenz) in diesen Angele- genheiten.

Beinhaltet auch: Die Übermittlung an die Standesvertretung zur Prüfung und Evaluierung der Abrechnung.

* 1. **Rechtsgrundlage** der Verarbeitung: gesetzliche Grundlage, Erfüllung eines Vertragsverhältnisses
	2. Beschreibung der **Kategorien betroffener Personen**: Patienten
	3. Verarbeitung durch **Auftragsverarbeiter: [Auftragsverarbeiter namentlich benennen]**
	4. Allgemeine Beschreibung der **technischen und organisatorischen Maßnahmen**: **[Sofern möglich spezifische Maßnahmen beschreiben]**

|  |  |
| --- | --- |
| **Betroffene Personengruppe: Patienten** |  |
| **Nr.** | **Kategorien** |  |
|  | **von personenbezogenen Daten:** | **an Empfänger** | **Übermittlung an****ein Drittland** | **Speicherdauer** | **Anmerkung** |
| **1** | Stammdaten inkl. Kontaktinformationen (etwa Ad- |  |  | gemäß steuerrechtlicher und unternehmensrecht- licher Aufbewahrungs- pflichten: 7 Jahre |  |
| resse, Tel, Mail, Fax) | 2, 9,12, 13 |
| **2** | Bankverbindungsdaten |  |  |  |
| **3** | Abrechnungsdaten |  |  |  |
| **4** | Leistungsdaten |  |  |  |
| **5** | Sozialversicherungsdaten |  |  |  |
| **6** | Behandlungsinformationen |  |  |  |
| **7** | Patienteninformationen (etwa Befunde, Diagnosen) |  |  |  |

1. **Datenanwendung: Befundanforderung / Befundübermittlung**
	1. **Zweck** der Verarbeitung: Anforderung von Befunden von Ärztinnen und Ärzten, Krankenanstalten, Labore, sowie anderen Ge- sundheitsberufen und den Betroffenen sowie die (Rück-)Übermittlung von Befunden einschließlich automationsunterstützt er- stellter und archivierter Textdokumente (wie z.B. Korrespondenz) in diesen Angelegenheiten.

Beinhaltet auch: Rückfragen bei Überweisungen

* 1. **Rechtsgrundlage** der Verarbeitung: gesetzliche Grundlage
	2. Beschreibung der **Kategorien betroffener Personen**: Ärzte, Patienten
	3. Verarbeitung durch **Auftragsverarbeiter: [Auftragsverarbeiter namentlich benennen]**
	4. Allgemeine Beschreibung der **technischen und organisatorischen Maßnahmen**: **[Sofern möglich spezifische Maßnahmen beschreiben]**

|  |  |
| --- | --- |
| **Betroffene Personengruppe: Ärzte** |  |
| **Nr.** | **Kategorien** |  |
|  | **von personenbezogenen Daten:** | **an Empfänger** | **Übermittlung an****ein Drittland** | **Speicherdauer** | **Anmerkung** |
| **1** | Stammdaten inkl. Kontaktinformationen (etwa Ad- resse, Tel., Mail, Fax) | 16 |  | gemäß der gesetzli- chen Aufbewahrungs-pflicht (mindestens 10 Jahre) |  |

|  |  |
| --- | --- |
| **Betroffene Personengruppe: Patienten** (besondereKategorien personenbezogener Daten) |  |
| **Nr** | **Kategorien** |  |
|  | **von personenbezogenen Daten:** | **an Empfängern** | **Übermittlung an****ein Drittland** | **Speicherdauer** | **Anmerkung** |
| **1** | Stammdaten inkl. Kontaktinformationen (etwa Ad- resse, Tel, Mail, Fax) | 16 |  | gemäß der gesetzli- chen Aufbewahrungs- pflicht (mindestens 10 Jahre) |  |
| **2** | Patienteninformationen (etwa Befunde, Diagnosen) | 16 |  |  |
| **3** | Sozialversicherungsdaten | 16 |  |  |
| **4** | Behandlungsinformationen | 16 |  |  |

1. **Datenanwendung: Untersuchung von Proben**
	1. **Zweck** der Verarbeitung: Beauftragung, Organisation und Verwaltung von Probenmaterial einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie z.B. Korrespondenz) in diesen Angelegenheiten.

Beinhaltet auch: Verwaltung des Versands von Sekret-, Blut- oder Gewebsproben an Labore inkl. Pathologische Labore und Pa- thologen zur Untersuchung (samt der Abrechnung derartiger Leistungen).

* 1. **Rechtsgrundlage** der Verarbeitung: gesetzliche Grundlage
	2. Beschreibung der **Kategorien betroffener Personen**: Ärzte, Patienten
	3. Verarbeitung durch **Auftragsverarbeiter: [Auftragsverarbeiter namentlich benennen]**
	4. Allgemeine Beschreibung der **technischen und organisatorischen Maßnahmen**: **[Sofern möglich spezifische Maßnahmen beschreiben]**

|  |  |
| --- | --- |
| **Betroffene Personengruppe: Ärzte** |  |
| **Nr.** | **Kategorien** |  |
|  | **von personenbezogenen Daten:** | **an Empfänger** | **Übermittlung an ein Drittland** | **Speicherdauer** | **Anmerkung** |
| **1** | Stammdaten inkl. Kontaktinformationen (etwa Ad- resse, Tel, Mail, Fax) | 16 |  | gemäß der gesetzli- chen Aufbewahrungs- pflicht (mindestens 10Jahre) |  |

|  |  |
| --- | --- |
| **Betroffene Personengruppe: Patienten** (besondere Kategorien personenbezogener Daten) |  |
| **Nr.** | **Kategorien** |  |
|  | **von personenbezogenen Daten:** | **an Empfänger** | **Übermittlung an ein Drittland** | **Speicherdauer** | **Anmerkung** |
| **1** | Stammdaten inkl. Kontaktinformationen (etwa Ad- resse, Tel., Mail, Fax) | 16 |  | gemäß der gesetzli- chen Aufbewahrungs- pflicht (mindestens 10 Jahre) |  |
| **2** | Patienteninformationen (etwa Befunde, Diagnosen) | 16 |  |  |
| **3** | Proben von Patienten | 16 |  |  |

1. **Datenanwendung: Organisation von Konsilien**
	1. **Zweck** der Verarbeitung: Organisation, Abwicklung und Abrechnung von Konsilien einschließlich automationsunterstützt erstell- ter und archivierter Textdokumente (wie z.B. Korrespondenz) in diesen Angelegenheiten.
	2. **Rechtsgrundlage** der Verarbeitung: gesetzliche Grundlage
	3. Beschreibung der **Kategorien betroffener Personen**: Patienten
	4. Verarbeitung durch **Auftragsverarbeiter: [Auftragsverarbeiter namentlich benennen]**
	5. Allgemeine Beschreibung der **technischen und organisatorischen Maßnahmen**: **[Sofern möglich spezifische Maßnahmen beschreiben]**

|  |  |
| --- | --- |
| **Betroffene Personengruppe: Patienten** (besondere Kategorien personenbezogener Daten) |  |
| **Nr.** | **Kategorien** |  |
|  | **von personenbezogenen Daten:** | **an Empfänger** | **Übermittlung an****ein Drittland** | **Speicherdauer** | **Anmerkung** |
| **1** | Stammdaten inkl. Kontaktinformationen (etwa Ad- resse, Tel., Mail, Fax) | 16 |  | gemäß der gesetzli- chen Aufbewahrungs- pflicht (mindestens 10 Jahre) |  |
| **2** | Patienteninformationen (etwa Befunde, Diagnosen) | 16 |  |  |
| **3** | Bankverbindungsdaten | 16 |  |  |
| **4** | Abrechnungsdaten | 16 |  |  |
| **5** | Leistungsdaten | 16 |  |  |
| **6** | Sozialversicherungsdaten | 16 |  |  |

1. **Datenanwendung: Verwaltung von Rezepten**
	1. **Zweck** der Verarbeitung: Ausgabe, Verwaltung und Organisation von Rezepten und Verordnungen von Heilbehelfen.

Beinhaltet auch: Einholung von Chefarztbewilligungen

* 1. **Rechtsgrundlage** der Verarbeitung: gesetzliche Grundlage
	2. Beschreibung der **Kategorien betroffener Personen**: Patienten
	3. Verarbeitung durch **Auftragsverarbeiter: [Auftragsverarbeiter namentlich benennen]**
	4. Allgemeine Beschreibung der **technischen und organisatorischen Maßnahmen**: **[Sofern möglich spezifische Maßnahmen beschreiben]**

|  |  |
| --- | --- |
| **Betroffene Personengruppe: Patienten** (besondereKategorien personenbezogener Daten) |  |
| **Nr.** | **Kategorien** |  |
|  | **von personenbezogenen Daten:** | **an Empfänger** | **Übermittlung an****ein Drittland** | **Speicherdauer** | **Anmerkung** |
| **1** | Stammdaten inkl. Kontaktinformationen (etwa Ad- resse, Tel., Mail, Fax) | 13, 16, 17 |  | gemäß der gesetzli- chen Aufbewahrungs- pflicht (mindestens 10 Jahre) |  |
| **2** | Rezeptdaten | 13, 16, 17 |  |  |
| **3** | Verordnungsdaten | 13, 16, 17 |  |  |

1. **Datenanwendung: Hausapotheke**
	1. **Zweck** der Verarbeitung: Betrieb, Verwaltung, Abrechnung und Organisation einer Hausapotheke einschließlich automationsun- terstützt erstellter und archivierter Textdokumente (wie z.B. Korrespondenz) in diesen Angelegenheiten.
	2. **Rechtsgrundlage** der Verarbeitung: gesetzliche Grundlage
	3. Beschreibung der **Kategorien betroffener Personen**: Patienten
	4. Verarbeitung durch **Auftragsverarbeiter: [Auftragsverarbeiter namentlich benennen]**
	5. Allgemeine Beschreibung der **technischen und organisatorischen Maßnahmen**: **[Sofern möglich spezifische Maßnahmen beschreiben]**

|  |  |
| --- | --- |
| **Betroffene Personengruppe: Patienten** (besondere Kategorien personenbezogener Daten) |  |
| **Nr.** | **Kategorien** |  |
|  | **von personenbezogenen Daten:** | **an Empfänger** | **Übermittlung an****ein Drittland** | **Speicherdauer** | **Anmerkung** |
| **1** | Stammdaten inkl. Kontaktinformationen (etwa Ad- resse, Tel, Mail, Fax) | 9, 13, 16 |  | gemäß der gesetzli- chen Aufbewahrungs- pflicht (mindestens 10Jahre) |  |
| **2** | Rezeptdaten | 9, 13, 16 |  |  |

1. **Datenanwendung: ELGA**
	1. **Zweck** der Verarbeitung: Speicherung von Gesundheitsdaten im Rahmen von ELGA als ELGA-Gesundheitsdiensteanbieter (im Sinne des § 2 Z 10 Gesundheitstelematikgesetz 2012) einschließlich automationsunterstützt erstellter und archivierter Textdo- kumente (wie z.B. Korrespondenz) in diesen Angelegenheiten.
	2. **Rechtsgrundlage** der Verarbeitung: gesetzliche Grundlage
	3. Beschreibung der **Kategorien betroffener Personen**: Patienten
	4. Verarbeitung**: [Auftragsverarbeiter namentlich benennen]**
	5. Allgemeine Beschreibung der **technischen und organisatorischen Maßnahmen**: **[Sofern möglich spezifische Maßnahmen beschreiben]**

|  |  |
| --- | --- |
| **Betroffene Personengruppe: Patienten** (besondereKategorien personenbezogener Daten) |  |
| **Nr.** | **Kategorien** |  |
|  | **von personenbezogenen Daten:** | **an Empfänger** | **Übermittlung an****ein Drittland** | **Speicherdauer** | **Anmerkung** |
| **1** | Stammdaten inkl. Kontaktinformationen (etwa Ad- resse, Tel., Mail, Fax) | Elektronische Gesundheitsakte („ELGA“) gemäß§ 2 Z 6 GTelG |  | 10 Jahre |  |
| **2** | Laborbefunde |  |  |
| **3** | Befunde der bildgebenden Diagnostik |  |  |
| **4** | Medikationsdaten |  |  |
| **5** | weitere Befunde |  |  |

1. **Datenanwendung: Information an eigene Patienten**
	1. **Zweck** der Verarbeitung: Übersendung von Informationen und Erinnerungen an eigene Patienten, um Vorsorge und Kontrollun- tersuchungen wahrzunehmen, Impftermine einzuhalten, Befundbesprechungen etc. einschließlich automationsunterstützt erstell- ter und archivierter Textdokumente (wie z.B. Korrespondenz) in diesen Angelegenheiten.
	2. **Rechtsgrundlage** der Verarbeitung: gesetzliche Grundlage, Erfüllung eines Vertragsverhältnisses
	3. Beschreibung der **Kategorien betroffener Personen**: Patienten (besondere Kategorien personenbezogener Daten)
	4. Verarbeitung durch **Auftragsverarbeiter: [Auftragsverarbeiter namentlich benennen]**
	5. Allgemeine Beschreibung der **technischen und organisatorischen Maßnahmen**: **[Sofern möglich spezifische Maßnahmen beschreiben]**

|  |  |
| --- | --- |
| **Betroffene Personengruppe: Patienten** (besondereKategorien personenbezogener Daten) |  |
| **Nr.** | **Kategorien** |  |
|  | **von personenbezogenen Daten:** | **an Empfänger** | **Übermittlung an****ein Drittland** | **Speicherdauer** | **Anmerkung** |
| **1** | Stammdaten inkl. Kontaktinformationen (etwa Ad- resse, Tel., Mail, Fax) |  |  | 2 Jahre |  |
| **2** | Patienteninformationen (etwa Befunde, Diagnosen) |  |  |  |
| **3** | Impfdaten |  |  |  |
| **4** | Informationen über Vorsorge und Kontrolluntersu- chungen |  |  |  |

# Technische und organisatorische Maßnahmen

**HINWEIS: DIE HIER VORGESCHLAGENEN MASSNAHMEN SIND UNVERBINDLICH UND MÜSSEN MIT DEM ZUSTÄNDIGEN SYSTEMADMINISTRATOR ABGESTIMMT WERDEN!**

Gemäß Art 32 DSGVO sind unter Berücksichtigung des Stands der Technik, der Implemen- tierungskosten und der Art, des Umfangs und der Umstände und der Zwecke der Verarbei- tung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen, geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

Diese Maßnahmen schließen unter anderem Folgendes ein:

* die Pseudonymisierung und Verschlüsselung personenbezogener Daten;
* die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Sys- teme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
* die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu

ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;

* ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirk- samkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Jeder Verantwortliche ist somit verpflichtet, geeignete technische und organisatorische Da- tensicherheitsmaßnahmen zu ergreifen.

Technische und organisatorische Maßnahmen sind verpflichtend von jedem Verantwortli- chen umzusetzen, um den unberechtigten Zugriff durch Dritte auf personenbezogene Daten zu verhindern.

Die vorliegenden technischen und organisatorischen Maßnahmen (TOM) sind ein Beispiel für einen Mindestschutz, um die Wiederherstellbarkeit von personenbezogenen Daten zu gewährleisten. Bitte beachten Sie, dass es sich hierbei um ein Beispiel handelt und im Ein- zelfall weitere Maßnahmen notwendig sein können.

Die technische Umsetzung kann dabei durch beauftragte Unternehmen (etwa einen IT- Dienstleister) erfolgen.

In Entsprechung des Art 32 DSGVO trifft der Verantwortliche folgende technische und orga- nisatorische Maßnahmen:

1. **Hinsichtlich Benutzer**
	1. **Technische Maßnahmen**
		1. Bildschirmsperre:

Der Verantwortliche stellt sicher, dass sämtliche Nutzer verpflichtet sind, beim Ver- lassen des Arbeitsplatzes den Computer so zu sperren, dass er durch Dritte nicht genutzt werden kann (Stichwort: Bildschirmsperre). Es sind sämtliche Geräte so einzustellen, dass eine Bildschirmsperre nach spätestens 10 Minuten Nichtbenut- zung des Computers diesen automatisch sperrt, sodass dieser erst wieder nach Eingabe eines Kennworts verwendet werden kann.

* + 1. Umgang mit Speichermedien:

Der Verantwortliche stellt sicher, dass sämtliche Computer so gesperrt sind, dass Speichermedien nur nach Eingabe eines Passworts verwendet werden können.

* + 1. Sichere Nutzung des Internets:

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

* + 1. 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).

Folgende technische Maßnahmen werden je Arbeitsplatzrechner ergriffen:

**[bitte ergänzen]**

* + 1. Datensicherung der Clients:

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

Die Rechner werden wie folgt gesichert:

**[bitte ergänzen]**

* 1. **Organisatorische Maßnahmen**
		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 Daten- sicherheitsmaßnahmen 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 Verant- wortlichen – 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).

Sofern eine private Nutzung der IT-Infrastruktur gestattet wird, stellt der Verantwort- liche sicher, dass mit den Mitarbeitern eine Vereinbarung hinsichtlich der privaten Nutzung der IT-Infrastruktur mit folgendem Inhalt geschlossen wird:

„*Dem Dienstnehmer ist das Benutzen der IT-Anlage für private Zwecke bis auf Wi- derruf nach Maßgabe der folgenden Bestimmungen gestattet:*

* + - 1. *Der Dienstnehmer darf die IT-Systeme nur in einem solchen Maße in Anspruch nehmen, dass dadurch die betriebliche Nutzung der IT-Systeme nicht beeinträch- tigt wird; dies betrifft insbesondere die Menge der abgelegten Daten.*
			2. *Der Dienstnehmer ist verpflichtet, die für private Zwecke eingerichteten Ordner ständig von nicht mehr benötigten Daten zu räumen, um Speicherplatz zu spa- ren. Dateien, die besonders viel Speicherkapazität in Anspruch nehmen (Grafi- ken, Video- und Tondateien), wird er nicht speichern.*
			3. *Der Dienstnehmer ist verpflichtet, spätestens am letzten Tag des Dienstverhält- nisses sämtliche seiner privaten Dateien von den Speichern der Dienstgeberin zu entfernen. Sollte er für die von ihm angelegten Dateien ein Kennwort oder eine sonstige Zugangssperre verwendet und nicht alle Dateien entfernt haben, so setzt er die Dienstgeberin durch Bekanntgabe dieses Kennworts in die Lage, die Dateien selbst zu entfernen.*
			4. *Nach Beendigung des Dienstverhältnisses muss die Dienstgeberin dem Dienst- nehmer nicht mehr Gelegenheit geben, seine Dateien selbst zu entfernen; sie muss ihm auch keinen Zugang mehr zu seinen privaten Dateien ermöglichen.*
			5. *Der Dienstnehmer nimmt zur Kenntnis, dass es möglich ist, dass seine privaten E-Mails von anderen Mitarbeitern gelesen werden, wenn er diese über das all- gemeine E-Mail-System des Dienstgebers versendet und empfängt. Der Dienst- nehmer darf die E-Mail-Funktion nur in einem solchen Maß in Anspruch nehmen, dass dadurch die betriebliche Nutzung der IT-Anlage sowie der Leitungen der Dienstgeberin nicht beeinträchtigt wird; dies betrifft insbesondere die Menge des Datentransfers.*
			6. *Der Dienstnehmer wird genau darauf achten, keine verdächtigen Mails oder Atta- chments, insbesondere von ihm unbekannten Absendern, zu öffnen.“*
		1. 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 verschlüsselter elektronischer Kommunikation
3. Versand per eingeschriebenem Brief
4. Versand per Post
5. Versand per Fax
6. Versand per E-Mail
7. Telefonische Mitteilung
8. Versand per SMS
9. Versand per Messenger Dienst (etwa: Whatsapp)

Zur Einhaltung eines angemessenen Sicherheitsniveaus verpflichtet sich der Ver- antwortliche, Informationen ausschließlich wie folgt zu übermitteln bzw. zu übersen- den:

|  |  |
| --- | --- |
| **Klassifizierung** | **Kommunikationsmedium** |
| Vertraulich | Persönliche ÜbergabeVersand per verschlüsselter elektronischer KommunikationVersand per Post |
| Nicht vertraulich | Jedes Medium |
| Öffentlich bekannt | Jedes Medium |

Der Verantwortliche klassifiziert Informationen wie folgt:

|  |  |
| --- | --- |
| **Information** | **Klassifizierung** |
| Informationen, die die Sozialversi- cherungsnummer enthalten | Vertraulich |
| Gesundheitsdaten | Vertraulich |
| Adressinformationen | Vertraulich |
| Kontaktinformationen | Vertraulich |
| Informationen über Patienten | Vertraulich |
| Befunde | Vertraulich |

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

**Zulässige Kommunikationsmedien**

Der Arzt als datenschutzrechtlicher Verantwortlicher wird vertrauliche Informationen (etwa Gesundheitsdaten und Befunde) an Patienten mittels unverschlüsselter E-Mail nur senden, wenn der jeweilige Patient vorab in die unverschlüsselte Zusendung eingewilligt hat. Sollte keine schriftliche Einwilligung des Patienten vorliegen, hat der Arzt als datenschutzrechtlicher Verantwortliche die mündliche Einwilligung des Pati- enten in der Patientenakte zu dokumentieren.

Der Verantwortliche verpflichtet sich, vertrauliche Informationen (etwa Gesundheits- daten) an zulässige Übermittlungsempfänger (etwa: Apotheken, Ärzte, Krankenhäu- ser, Pflegeheime, Krankenversicherungen) ausschließlich mittels verschlüsselter elektronischer Kommunikation oder mittels Fax zu senden.

* + 1. 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. 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 sol- che Speicherung wird der jeweilige Verantwortliche explizit anordnen und – für den Einzelfall – geeignete Sicherheitsmaßnahmen anordnen.

* + 1. Clean Desk Policy:

Der Verantwortliche stellt sicher, dass jeder Mitarbeiter sich verpflichtet, Dokumente und Unterlagen vor Verlassen des Arbeitsplatzes entsprechend zu verstauen und einzuschließen, sodass ein unbefugter Dritter keinerlei Kenntnis über deren Inhalt erhalten kann. Das „Aufräumen und Abschließen“ beinhaltet sämtliche Unterlagen, Datenträger und sonstige Informationsmedien.

* + 1. Regelungen zu Home-Office, mobiler Arbeitsplatz:

Der Verantwortliche stellt sicher, dass Mitarbeiter, welche einen mobilen Arbeits- platz oder das Homeoffice nutzen, sich verpflichten, ausschließlich die vom Verant- wortlichen bereit gestellten Systeme zu nutzen und sämtliche Zugangsdaten geheim zu halten. Das schriftliche Festhalten der Zugangsdaten ist nicht zulässig.

Der Verantwortliche stellt sicher, dass die Mitarbeiter dem Verantwortlichen umge- hend mitteilen, sollten die Zugangsdaten des Mitarbeiters nicht mehr geheim sein.

* + 1. Regelungen zu Bring your own device:

Sollte der Verantwortliche den Mitarbeitern gestatten, eigene Endgeräte (Smartpho- nes, Tablets, Laptops) zu nutzen, wird der Verantwortliche eine entsprechende Richtlinie erlassen und den Mitarbeitern zur Kenntnis bringen.

* + 1. 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. Sicherung von physischen Dokumenten:

Der Verantwortliche stellt sicher, dass sämtliche Mitarbeiter dahingehend geschult werden, dass Dokumente der Kategorie „vertraulich“ in einem verschlossenen Ak- tenordner 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. Geheimhaltungsvereinbarung:

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

„*Der Dienstnehmer ist verpflichtet, personenbezogene Daten aus Datenverarbeitun- gen, die ihm ausschließlich auf Grund seiner berufsmäßigen Beschäftigung anver-*

*traut 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.*“

1. **Hinsichtlich IT-Infrastruktur:**
	1. **Technische Maßnahmen**
		1. Arbeitsplatzrechner:

Der Verantwortliche stellt sicher, dass Computer vor unbefugtem Zugriff und unbe- fugter 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 ver- schlüsselt.

* + 1. Mobiltelefone:

Sofern auf mobilen Endgeräten (Mobiltelefone, Tablets oder Ähnliches) personen- bezogene Daten gespeichert werden, wird der Verantwortliche Maßnahmen dahin- gehend ergreifen, dass der Zugriff auf die mobilen Endgeräte erst nach Eingabe ei- nes Kennworts möglich ist. Mobile Endgeräte sind darüber hinaus so konfiguriert, dass sich der Bildschirm des mobilen Endgeräts nach spätestens 30 Sekunden sperrt, sodass das Endgerät erst nach Eingabe eines Kennworts wiederverwendet werden kann.

Darüber hinaus stellt der Verantwortliche sicher, dass der Speicher der mobilen Endgeräte verschlüsselt ist. Daten von und zu mobilen Endgeräten werden aus- schließlich verschlüsselt übertragen.

Der Verantwortliche stellt sicher, dass die Daten auf Mobiltelefonen aus der Ferne („Remote“) gelöscht werden können, wenn diese verloren gegangen sind.

* + 1. Unterbrechungsfreie Stromversorgung:

Server und andere Komponenten sind mit einer unterbrechungsfreien Stromversor- gung gesichert.

* + 1. Sicherung von öffentlich zugänglichen Bereichen:

Sofern der Verantwortliche öffentlich zugängliche Netzwerke („WLAN“) betreibt, wird er diese so sichern, dass ein Zugriff auf nicht öffentlich zugängliche Systeme des Verantwortlichen nicht möglich ist.

Der Verantwortliche stellt ferner sicher, dass öffentlich zugängliche Netzwerkan- schlüsse (etwa Netzwerkdosen) nicht genutzt werden können.

* + 1. Softwaresicherheitsmaßnahmen:

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

Der Verantwortliche stellt sicher, dass der Zugriff auf Systeme nur nach Eingabe eines Passworts möglich ist, wobei Passwörter folgende Kriterien erfüllen müssen (Passwortrichtlinie):

**[bitte ergänzen]**

Der Verantwortliche stellt sicher, dass Backups der Datenbestände in folgenden Abständen erstellt werden:

**[bitte ergänzen]**

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

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

* + 1. Sicherung von Telekommunikationseinrichtungen:

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

* 1. **Organisatorische Maßnahmen**
		1. Maßnahmen bei Außerbetriebnahme eines Clients / Beendigung des Dienstverhält-

nisses:

Der Verantwortliche stellt sicher, dass sämtliche Rechner, welche nicht mehr ge- nutzt werden sollen, ordnungsgemäß entsorgt werden und personenbezogene Da- ten auf den Rechnern vor unberechtigtem Zugriff geschützt werden.

* + 1. Dokumentation der technischen Infrastruktur:

Der Verantwortliche stellt sicher, dass die gesamte technische Infrastruktur ausrei- chend dokumentiert ist. Dies beinhaltet auch die Dokumentation und Kennzeich- nung der Verkabelung sowie relevanter baulicher Maßnahmen.

1. **Bauseitig:**
	1. **Organisatorische Maßnahmen:**
		1. Regelungen über das Aufrufen von Patienten und die Vertraulichkeit der persönli- chen Kommunikation:

Der Verantwortliche stellt sicher, dass Patienten diskret aufgerufen werden. Dazu werden der Verantwortliche oder dessen Mitarbeiter lediglich den Nachnamen des Patienten aufrufen. Der Verantwortliche und dessen Mitarbeiter werden so mit dem Patienten kommunizieren, dass ein Dritter keine Kenntnis über den Inhalt der Kom- munikation erhält.

* + 1. Regelungen über den Zutritt zu Räumlichkeiten:

Der Verantwortliche stellt sicher, dass der Zutritt zu den Räumlichkeiten nur berech- tigten Personen möglich ist. Mitarbeiter, welche Schlüssel oder Zutrittsberechtigun- gen zu den Räumlichkeiten erhalten haben, sind entsprechend geschult, dass diese den Verantwortlichen umgehend informieren müssen, sollte der Schlüssel abhan- denkommen (Verlust, Diebstahl oder ähnliches).

* + 1. 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.

* + 1. Serverraum:

Der Verantwortliche stellt sicher, dass Server vor unberechtigtem Zugriff geschützt (etwa versperrt) sind und eine Verfügbarkeit des Servers in ausreichendem Ausmaß sichergestellt ist.

* + 1. Archiv:

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

1. **Administrativ:**
	1. Definition von Prozessen:

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

* 1. Behandlung von Sicherheitsvorfällen:

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

* 1. Überprüfung der Einhaltung:

Der Verantwortliche wird regelmäßig die hier beschriebenen technischen und orga- nisatorischen Maßnahmen evaluieren und prüfen.

1. **Auftragsverarbeiter**1
	1. **Liste der Auftragsverarbeiter**

**[Zur besseren Übersicht kann hier eine Liste sämtlicher Auftragsverarbeiter er- gänzt werden. Dieser Punkt kann auch gestrichen werden.]**

* 1. **Muster der abgeschlossenen Vereinbarungen**

**AUFTRAGSVERARBEITERVERTRAG**

Abgeschlossen zwischen **[Bitte Namen und Adresse ergänzen]** als ***Verantwortlicher*** und

als ***Auftragsverarbeiter***, gemeinsam kurz: die ***Parteien***

1. **Allgemeine Pflichten des Auftragsverarbeiters**
	1. Der Verantwortliche hat den Auftragsverarbeiter mit der Erbringung folgender Dienst- leistungen beauftragt (im Folgenden kurz: die Datenanwendung):
	2. Die Verarbeitung erfolgt für folgende Dauer: unbefristet / befristet bis:
	3. Im Rahmen der Datenanwendung verarbeitet der Auftragsverarbeiter folgende Daten- kategorien:
	4. Die Daten folgender Kategorien von betroffenen Personen werden im Rahmen der Datenanwendung verarbeitet:

1 Nicht zwingend notwendig, jedoch aus Gründen der Übersichtlichkeit sinnvoll.

1. **Verarbeitungsgegenstand**

Solange der Auftragsverarbeiter die Datenanwendung betreibt und personenbezogene Daten für den Verantwortlichen verarbeitet, gelten in Entsprechung des Art 28 DSGVO folgende Bedingungen:

* 1. Der Auftragsverarbeiter verpflichtet sich, sämtliche gesetzliche Vorgaben der Daten- schutz-Grundverordnung (DSGVO) und des österreichischen Datenschutzgesetzes (DSG) zu beachten und Datenanwendungen (logisch und physisch) ausschließlich in- nerhalb der EU oder des EWR zu betreiben. Jede Form der Verlagerung der Datenan- wendung (dazu zählt auch die Verlegung des Sitzes des Auftragsverarbeiters) in ein Drittland (sohin außerhalb der EU oder des EWR) bedarf der ausdrücklichen, vorheri- gen schriftlichen Zustimmung durch den Verantwortlichen.
	2. Der Auftragsverarbeiter wird die Datenanwendung, wie vom Verantwortlichen geson- dert in dokumentierter Weise angewiesen, verarbeiten, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu ver- pflichtet ist; in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses ver- bietet.
	3. Der Auftragsverarbeiter gewährleistet, dass sich Personen, die Kenntnis von den im Auftrag verarbeiteten Daten haben oder erhalten können, vor Verarbeitung bzw. Kenntnis dieser Daten schriftlich zur Vertraulichkeit verpflichten, sofern diese nicht oh- nedies einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.
	4. Der Auftragsverarbeiter wird unter Berücksichtigung des Stands der Technik, der Im- plementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen ergreifen, um ein dem Risiko angemessenes Schutzni- veau zu gewährleisten. Die Parteien werden diese Maßnahmen im Einvernehmen fest- legen und evaluieren. Der Auftragsverarbeiter verpflichtet sich, diese vereinbarten Maßnahmen umzusetzen.
	5. Die Beauftragung bzw. Inanspruchnahme von Subauftragsverarbeitern (im Folgenden kurz Subauftragnehmer) ist dem Auftragsverarbeiter prinzipiell gestattet, sofern er den Verantwortlichen vorab über jede beabsichtigte Beauftragung bzw. Inanspruchnahme von Subauftragnehmern schriftlich informiert und es dem Verantwortlichen freisteht, dieser Beauftragung bzw. Inanspruchnahme begründungslos zu widersprechen. Im Fall eines solchen Widerspruchs wird der Auftragsverarbeiter den Subauftragnehmer nicht beauftragen bzw. in Anspruch nehmen. Der Auftragsverarbeiter ist verpflichtet, sämtliche Subauftragnehmer im Sinne des Art 28 Abs 4 DSGVO schriftlich im Sinne

dieses Vertrags zu verpflichten und sämtliche Pflichten, die den Auftragsverarbeiter treffen, an den Subauftragnehmer zu überbinden. Sollte der Subauftragnehmer seine Pflichten verletzen, haftet der Auftragsverarbeiter. Der Subauftragnehmer muss seine Niederlassung innerhalb der EU oder des EWR haben. Der Subauftragnehmer darf die Datenanwendung ausschließlich innerhalb der EU oder des EWR betreiben.

* 1. Der Auftragsverarbeiter wird den Verantwortlichen mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützen, dessen Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III genannten Rechte der betroffenen Person (Auskunft, Berichtigung und Löschung, Information, Datenübertragbarkeit, Wi- derspruch, sowie automatisierte Entscheidungsfindung im Einzelfall) fristgerecht nach- zukommen. Sollte sich ein Betroffener an den Auftragsverarbeiter oder einen Subauf- tragnehmer anstelle des Verantwortlichen wenden, verpflichten sich diese, den Antrag dem Verantwortlichen so zukommen zu lassen, dass der Verantwortliche den Antrag fristgerecht bearbeiten kann.
	2. Der Auftragsverarbeiter wird den Verantwortlichen bei der Einhaltung der in den Art 32 bis 36 DSGVO genannten Pflichten (Ergreifung technischer und organisatorischer Maßnahmen, Security Breach Notification, Erstellung einer Datenschutzfolgenabschät- zung) unterstützen.
	3. Der Auftragsverarbeiter wird nach Abschluss der Datenanwendung alle personenbezo- genen Daten nach Wahl des Verantwortlichen entweder löschen oder zurückgeben, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflich- tung zur Speicherung der personenbezogenen Daten besteht.
	4. Der Auftragsverarbeiter ist verpflichtet, dem Verantwortlichen alle erforderlichen Infor- mationen zum Nachweis der Einhaltung der dem Auftragsverarbeiter in diesem Vertrag auferlegten Pflichten zur Verfügung zu stellen.
	5. Sollte der Auftragsverarbeiter der Auffassung sein, dass eine vom Verantwortlichen erteilte Weisung gegen die DSGVO oder gegen andere Datenschutzbestimmungen der EU oder deren Mitgliedstaaten verstößt, so hat er dies dem Verantwortlichen unverzüg- lich und begründet mitzuteilen.
	6. Der Verantwortliche ist berechtigt, die Einhaltung sämtlicher maßgeblichen daten- schutzrechtlichen Vorschriften sowie die Einhaltung der vertraglichen Bestimmungen selbst oder durch Dritte beim Auftragsverarbeiter sowie allfälligen Subauftragnehmern zu kontrollieren.
	7. Dieser Vertrag erlangt durch die Unterfertigung oder eine schriftliche Bestätigung der Parteien Geltung.

# Prozessdefinitionen

1. **Recht auf Auskunft**

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

* 1. die Verarbeitungszwecke;
	2. die Kategorien personenbezogener Daten, die verarbeitet werden;
	3. die Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbe- zogenen Daten offengelegt worden sind oder noch offengelegt werden, insbesondere bei Empfängern in Drittländern oder bei internationalen Organisationen;
	4. 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;
	5. das Bestehen eines Rechts auf Berichtigung oder Löschung der sie betreffenden per- sonenbezogenen Daten oder auf Einschränkung der Verarbeitung durch den Verant- wortlichen oder eines Widerspruchsrechts gegen diese Verarbeitung;
	6. das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;
	7. wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wer- den, alle verfügbaren Informationen über die Herkunft der Daten;
	8. 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 Organisa- tion 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 Verant- wortliche 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 Aus- übung 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 Verfü- gung zu stellen, sofern die betroffene Person nichts Anderes angibt.

**In Entsprechung dieser Verpflichtungen wird der Verantwortliche das Auskunfts- recht 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 herauszu- finden, 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 münd- lich 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 un- übersichtlich sind – kurz erläutern.

**Die Auskunft wird folgende Informationen umfassen:**

* **Verarbeitete Daten:** Der Verantwortliche wird die betroffene Person darüber infor- mieren, welche Informationen er über die Person verarbeitet.
* **Informationen:** Darüber hinaus wird der Verantwortliche der betroffenen Person fol- gende 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 Datenverar- beitung
* **Betroffene Rechte:** Der Verantwortliche wird die betroffene Person über Folgendes informieren:

*„Die betroffene Person hat das Recht auf Auskunft über die gespeicherten Daten ge- mäß 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 Daten- verarbeitung gemäß Art 21 DSGVO sowie auf Datenübertragbarkeit gemäß Art 20 DSGVO.*

*Der Betroffene hat das Recht, sich bei der Aufsichtsbehörde zu beschweren – zu- ständig 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 Mo- nats ab Eingang beim Verantwortlichen. Sollte es sich um eine umfangreiche und kom- plexe Auskunft handeln, kann der Verantwortliche im Einzelfall die Frist zur Beauskunf- tung 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.

1. **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 inhalt- lich 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.

1. **Das Recht auf Löschung**

Die betroffene Person hat das Recht, von dem Verantwortlichen zu verlangen, dass be- treffende personenbezogene Daten unverzüglich gelöscht werden. Der Verantwortliche ist verpflichtet, personenbezogene Daten unverzüglich zu löschen, sofern einer der fol- genden 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 Ver- pflichtung erforderlich;
* Bei den personenbezogenen Daten handelt es sich um die Daten eines Kindes in Be- zug auf angebotene Internetdienste.

Der Verantwortliche wird jedes Löschungsbegehren umgehend prüfen und mit zumutba- rem 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 Ableh- nung informieren. Gegebenenfalls wird der Verantwortliche den Betroffenen – sofern es sich um ein komplexes Begehren handelt – über die Verlängerung der Prüfung des Lö- schungsbegehrens 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).

**4. Recht auf Einschränkung**

Der Verantwortliche wird die personenbezogenen Daten eines Betroffenen nur eingeschränkt verarbeiten, sofern:

 - die betroffene Person die Richtigkeit der personenbezogenen Daten bestritten hat (für die Dauer der Prüfung der Richtigkeit der personenbezogenen Daten durch den Verantwortlichen);

 - die Verarbeitung unrechtmäßig erfolgt und die betroffene Person die Löschung der personenbezogenen Daten ablehnt und stattdessen die Einschränkung der Nutzung der personenbezogenen Daten verlangt;

 - der Verantwortliche die personenbezogenen Daten für die Zwecke der Verarbeitung nicht länger benötigt, die betroffene Person sie jedoch zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt;

 - die betroffene Person Widerspruch gegen die Verarbeitung eingelegt hat, solange noch nicht feststeht, ob die berechtigten Gründe des Verantwortlichen gegenüber denen der betroffenen Person überwiegen.

Sollte die Verarbeitung eingeschränkt worden sein, so dürfen diese personenbezogenen Daten – von ihrer Speicherung abgesehen – nur mit Einwilligung der betroffenen Personen oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder zum Schutz der Rechte einer anderen natürlichen Personen oder aus Gründen eines wichtigen öffentlichen Interesses – verarbeitet werden.

Der Verantwortliche wird die betroffene Person jeweils schriftlich über die ergriffenen Maßnahmen informieren.

Der Verantwortliche wird allen Empfängern, denen personenbezogene Daten offengelegt wurden, die Einschränkung der Verarbeitung mitteilen, es sei denn, dies erweist sich als unmöglich oder ist mit einem unverhältnismäßigen Aufwand verbunden.

Sofern die betroffene Person dies wünscht, wird der Verantwortliche die betroffene Person über die Empfänger dieser Mitteilung informieren.

**5. Widerspruchsrecht**

Die betroffene Person hat das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung sie betreffender personenbezogener Daten Widerspruch einzulegen, sofern die Verarbeitung für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde oder aber die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist.

Der Verantwortliche wird die Identität der betroffenen Person und anschließend – sollte die Identität einwandfrei nachgewiesen worden sein – den Widerspruch inhaltlich prüfen.

Im Anschluss wird der Verantwortliche die betroffene Person über die Entscheidung informieren.

1. **Meldung an die Behörde**

Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet der Verant- wortliche 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 Risi- ko 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 Verzöge- rung beizufügen.

Die Meldung an die Behörde enthält zumindest folgende Informationen:

* 1. 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 perso- nenbezogenen Datensätze;
	2. den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;
	3. eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes perso- nenbezogener Daten;
	4. 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 Auswirkun- gen.

**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