III. 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 Implementierungskosten und der Art, des Umfangs und 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 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 Systeme 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 Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Jeder Verantwortliche ist somit verpflichtet, geeignete technische und organisatorische Datensicherheitsmaßnahmen zu ergreifen.

Technische und organisatorische Maßnahmen sind verpflichtend von jedem Verantwortlichen 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 Einzelfall 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 organisatorische Maßnahmen:

1. Hinsichtlich Benutzer

1.1. Technische Maßnahmen

1.1.1. Bildschirmsperre:

Der Verantwortliche stellt sicher, dass sämtliche Nutzer verpflichtet sind, beim Verlassen 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 Nichtbenutzung des Computers diesen automatisch sperrt, sodass dieser erst wieder nach Eingabe eines Kennworts verwendet werden kann.

1.1.2. Umgang mit Speichermedien:

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

1.1.3. 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.

1.1.4. 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:

Passwort, automatischer Virenscan, Sicherheitsupdates

1.1.5. Datensicherung der Clients:

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

Die Rechner werden wie folgt gesichert:

Externe Festplatten (passwortgesichert)

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).

Sofern eine private Nutzung der IT-Infrastruktur gestattet wird, stellt der Verantwortliche 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 Widerruf 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 beeinträchtigt 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 sparen. Dateien, die besonders viel Speicherkapazität in Anspruch nehmen (Grafiken, Video- und Tondateien), wird er nicht speichern.*

3. *Der Dienstnehmer ist verpflichtet, spätestens am letzten Tag des Dienstverhältnisses 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 Dienstnehmer 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 allgemeine E-Mail-System des Dienstgebers versendet und empfängt. Der Dienstnehmer 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 Attachments, insbesondere von ihm unbekannten Absendern, zu öffnen.“*

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 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 Verantwortliche, Informationen ausschließlich wie folgt zu übermitteln bzw. zu übersenden:

Klassifizierung	**Kommunikationsmedium**
Vertraulich	Persönliche Übergabe Versand per verschlüsselter elektronischer Kommunikation Versand per Post
Nicht vertraulich	Jedes Medium
Öffentlich bekannt	Jedes Medium

Der Verantwortliche klassifiziert Informationen wie folgt:

Information	Klassifizierung
Informationen, die die Sozialversicherungsnummer 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, persönlich oder per SMS (nach vorheriger schriftlicher Einwilligungserklärung des Empfängers).

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 Patienten in der Patientenakte zu dokumentieren.

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

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. 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.

1.2.6. Regelungen zu Home-Office, mobiler Arbeitsplatz:

Der Verantwortliche stellt sicher, dass Mitarbeiter, welche einen mobilen Arbeitsplatz oder das Homeoffice nutzen, sich verpflichten, ausschließlich die vom Verantwortlichen 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 umgehend mitteilen, sollten die Zugangsdaten des Mitarbeiters nicht mehr geheim sein.

1.2.7. Regelungen zu Bring your own device:

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

1.2.8. 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.

1.2.9. 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.

1.2.10. 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 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 personenbezogenen 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. Mobiltelefone:

Sofern auf mobilen Endgeräten (Mobiltelefone, Tablets oder Ähnliches) personenbezogene Daten gespeichert werden, wird der Verantwortliche Maßnahmen dahingehend ergreifen, dass der Zugriff auf die mobilen Endgeräte erst nach Eingabe eines 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 ausschließlich verschlüsselt übertragen.

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

2.1.3. Unterbrechungsfreie Stromversorgung:

Server und andere Komponenten sind mit einer unterbrechungsfreien Stromversorgung gesichert.

2.1.4. 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 Netzwerkanschlüsse (etwa Netzwerkdosen) nicht genutzt werden können.

2.1.5. 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, wobei Passwörter folgende Kriterien erfüllen müssen (Passwortrichtlinie):

Buchstaben, Zahlen, Zeichen

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

Täglich

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.

2.1.6. 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 Dienstverhält-

nisses:

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 das Aufrufen von Patienten und die Vertraulichkeit der persönlichen 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 Kommunikation erhält.

3.1.2. 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).

3.1.3. 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.

3.1.4. Serverraum:

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

3.1.5. 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

s.o.

2. Muster der abgeschlossenen Vereinbarungen

AUFTRAGSVERARBEITERVERTRAG

Abgeschlossen zwischen **Dr. Werner Kusebauch (s.o.)** als ***Verantwortlicher*** und

s.o._____

_____

_____

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

1. Allgemeine Pflichten des Auftragsverarbeiters

1.1 Der Verantwortliche hat den Auftragsverarbeiter mit der Erbringung folgender Dienstleistungen beauftragt (im Folgenden kurz: die Datenanwendung):

1.2 Die Verarbeitung erfolgt für folgende Dauer: unbefristet / befristet bis:

1.3 Im Rahmen der Datenanwendung verarbeitet der Auftragsverarbeiter folgende Datenkategorien:

1.4 Die Daten folgender Kategorien von betroffenen Personen werden im Rahmen der Datenanwendung verarbeitet:

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

2. Verarbeitungsgegenstand

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

2.1. Der Auftragsverarbeiter verpflichtet sich, sämtliche gesetzliche Vorgaben der Datenschutz-Grundverordnung (DSGVO) und des österreichischen Datenschutzgesetzes (DSG) zu beachten und Datenanwendungen (logisch und physisch) ausschließlich innerhalb der EU oder des EWR zu betreiben. Jede Form der Verlagerung der Datenanwendung (dazu zählt auch die Verlegung des Sitzes des Auftragsverarbeiters) in ein Drittland (sohin außerhalb der EU oder des EWR) bedarf der ausdrücklichen, vorherigen schriftlichen Zustimmung durch den Verantwortlichen.

2.2. Der Auftragsverarbeiter wird die Datenanwendung, wie vom Verantwortlichen gesondert in dokumentierter Weise angewiesen, verarbeiten, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet 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 verbietet.

2.3. 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 ohnedies einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

2.4. Der Auftragsverarbeiter wird unter Berücksichtigung des Stands der Technik, der Implementierungskosten 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 Schutzniveau zu gewährleisten. Die Parteien werden diese Maßnahmen im Einvernehmen festlegen und evaluieren. Der Auftragsverarbeiter verpflichtet sich, diese vereinbarten Maßnahmen umzusetzen.

2.5. 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.

2.6. 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, Widerspruch, sowie automatisierte Entscheidungsfindung im Einzelfall) fristgerecht nachzukommen. Sollte sich ein Betroffener an den Auftragsverarbeiter oder einen Subauftragnehmer anstelle des Verantwortlichen wenden, verpflichten sich diese, den Antrag dem Verantwortlichen so zukommen zu lassen, dass der Verantwortliche den Antrag fristgerecht bearbeiten kann.

2.7. 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 Datenschutzfolgenabschätzung) unterstützen.

2.8. Der Auftragsverarbeiter wird nach Abschluss der Datenanwendung alle personenbezogenen Daten nach Wahl des Verantwortlichen entweder löschen oder zurückgeben, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht.

2.9. Der Auftragsverarbeiter ist verpflichtet, dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der dem Auftragsverarbeiter in diesem Vertrag auferlegten Pflichten zur Verfügung zu stellen.

2.10. 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 unverzüglich und begründet mitzuteilen.

2.11. Der Verantwortliche ist berechtigt, die Einhaltung sämtlicher maßgeblichen datenschutzrechtlichen Vorschriften sowie die Einhaltung der vertraglichen Bestimmungen selbst oder durch Dritte beim Auftragsverarbeiter sowie allfälligen Subauftragnehmern zu kontrollieren.

2.12. Dieser Vertrag erlangt durch die Unterfertigung oder eine schriftliche Bestätigung der Parteien Geltung.

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 Verletzung.

VI. Muster für eine Einwilligungserklärung

1. Einwilligungserklärung E-Mailübermittlung für Patienten

"Ich stimme zu, dass bis auf Widerruf mein/e behandelnde/r Ärztin/Arzt sämtliche Informationen aus meiner Patientendokumentation (somit Informationen über meinen Zustand bei Übernahme der Beratung oder Behandlung, die Vorgeschichte einer Erkrankung, die Diagnose, den Krankheitsverlauf sowie über Art und Umfang der beratenden, diagnostischen oder therapeutischen Leistungen einschließlich der Anwendung von Arzneispezialitäten) an die folgende E-Mailadresse mittels unverschlüsselter E-Mail senden darf:

Ich nehme zur Kenntnis, dass durch die Übermittlung der Daten (unberechtigte) Dritte Kenntnis über die Informationen erhalten können und diese Daten verändert werden können. Mir ist bewusst, dass dies zur Offenlegung meines Gesundheitszustandes führen kann.

Diese Einwilligung kann jederzeit widerrufen werden. Die Rechtmäßigkeit der Verarbeitung meiner Daten bleibt bis zum Einlangen des Widerrufs davon unberührt.

Datum Unterschrift