UNIKLINIK KÖLN

Auftragnehmer, zuständiger Bereich:

Auftraggeber, zuständiger Bereich:

Anlage 1 zum Rahmen-AV-Vertrag: Datenkategorien und Betroffene

1) Art der Daten

Der Auftragnehmer erhält Zugriff auf personenbezogene Daten (dadurch, dass der Auftraggeber ihm die Daten bereitstellt oder ihm einen Zugriff auf die Daten ermöglicht) bzw. der Auftraggeber erlaubt dem Auftragnehmer folgende personenbezogene Daten zu verarbeiten:

☐	Personenstammdaten (z. B. Mitarbeiter, Kooperationspartner, nicht med. Patientendaten)
☐	Medizinische Patientendaten (Befunde, Diagnosen, Krankengeschichte, etc.) Patientenverfügungen/-vollmachten
☐	Meldepflichtige Erkrankungen
☐	Daten zur Organspende
☐	Medikation und Verschreibung von Heilmitteln
☐	Daten zum Tod des Patienten
☐	Kontaktdaten/Kommunikationsdaten (z. B. IP-Adressen, Telefon, E-Mail)
☐	Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
☐	Vertragsabrechnungs- und Zahlungsdaten
☐	Auskunftsangaben (von Dritten, z. B. Auskunfteien, oder aus öffentlichen Verzeichnissen)
☐	Versicherungsdaten (Sozialversicherung, Krankenversicherung, etc.)
☐	Kundenhistorie
☐	Planungs- und Steuerungsdaten
☐	Beschäftigtendaten inkl. Gehaltsdaten
☐	Bilddaten/Fotos
☐	
☐	
☐	

2) Betroffene

Der Kreis der durch den Umgang mit ihren personenbezogenen Daten im Rahmen des Auftrags Betroffenen umfasst:

☐	Stationäre und ambulante Patienten des Auftraggebers sowie ggf. deren gesetzliche Vertreter
☐	Angehörige und Kontaktpersonen von Patienten und Begleitpersonen
☐	Beschäftigte des Auftraggebers (aktuelle/ehemalige)
☐	Einweisende, behandelnde und nachbehandelnde Ärzte sowie andere Fachkräfte, deren Dokumentation in Patientenakten enthalten sein kann
☐	Lieferanten/Handelsvertreter
☐	Kunden
☐	Bewerber
☐	
☐	

P2002113 - Stand: 21.07.2021

Auftragnehmer, zuständiger Bereich:

Auftraggeber, zuständiger Bereich:

Anlage 2 zum Rahmen-AV-Vertrag:
Weitere Angaben des Auftragnehmers

1) Ansprechpartner für den Datenschutz beim Auftragnehmer

Name, Vorname:	
Anschrift:	
Telefon:	
E-Mail:	

2) Verarbeitungsort/e (§ 6 Abs. 1)

Anschrift:	

3) Unterauftragsverhältnis des Auftragnehmers (§ 12 Abs. 5)

Name und Anschrift des Unterauftragnehmers	Beschreibung der Teilleistungen	Ort der Leistungserbringung

Auftragnehmer, zuständiger Bereich:

Auftraggeber, zuständiger Bereich:

Anlage 3 zum Rahmen-AV-Vertrag: Nachweis der technischen und organisatorischen Maßnahmen

1. Vertraulichkeit

1.1. Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren. Als Maßnahmen zur Zutrittskontrolle können zur Gebäude- und Raumsicherung unter anderem automatische Zutrittskontrollsysteme, Einsatz von Chipkarten und Transponder, Kontrolle des Zutritts durch Pförtnerdienste und Alarmanlagen eingesetzt werden. Server, Telekommunikationsanlagen, Netzwerktechnik und ähnliche Anlagen sind in verschließbaren Serverschränken zu schützen. Darüber hinaus ist es sinnvoll, die Zutrittskontrolle auch durch organisatorische Maßnahmen (z.B. Dienstanweisung, die das Verschließen der Diensträume bei Abwesenheit vorsieht) zu stützen.

Technische Maßnahmen		**Organisatorische Maßnahmen**	
☐	Alarmanlage	☐	Schlüsselregelung / Liste (Pflicht)
☐	Automatisches Zugangskontrollsystem	☐	Empfang / Rezeption / Pförtner
☐	Biometrische Zugangssperren	☐	Besucherbuch / Protokoll der Besucher (Pflicht)
☐	Chipkarten / Transpondersysteme	☐	Mitarbeiter- / Besucherausweise (Pflicht)
☐	Manuelles Schließsystem	☐	Besucher in Begleitung durch Mitarbeiter (Pflicht)
☐	Sicherheitsschlösser (Pflicht)	☐	
☐	Schließsystem mit Codesperre	☐	
☐	Absicherung der Gebäudeschächte	☐	
☐	Türen mit Knauf Außenseite	☐	
☐	Klingelanlage mit Kamera	☐	
☐	Videoüberwachung der Eingänge	☐	
☐		☐	
☐		☐	

1.2. Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme (Computer) von Unbefugten genutzt werden können.

Mit Zugangskontrolle ist die unbefugte Verhinderung der Nutzung von Anlagen gemeint. Möglichkeiten sind beispielsweise Bootpasswort, Benutzerkennung mit Passwort für Betriebssysteme und eingesetzte Softwareprodukte, Bildschirmschoner mit Passwort, der Einsatz von Chipkarten zur Anmeldung wie auch der Einsatz von CallBack-Verfahren. Darüber hinaus können auch organisatorische Maßnahmen notwendig sein, um beispielsweise eine unbefugte Einsichtnahme zu verhindern (z.B. Vorgaben zur Aufstellung von Bildschirmen, Herausgabe von Orientierungshilfen für die Anwender zur Wahl eines „guten" Passworts).

Technische Maßnahmen		**Organisatorische Maßnahmen**	
☐	Login mit Benutzername + Passwort (Pflicht)	☐	Verwalten von Benutzerberechtigungen (Pflicht)
☐	Login mit biometrischen Daten	☐	Erstellen von Benutzerprofilen (Pflicht)
☐	Anti-Viren-Software	☐	Zentrale Passwortvergabe (Pflicht)
☐	Anti-Virus-Software Clients (Pflicht)	☐	Richtlinie „Sicheres Passwort"
☐	Anti-Virus-Software mobile Geräte	☐	Richtlinie „Löschen / Vernichten"
☐	Firewall (Pflicht)	☐	Richtlinie „Clean desk"
☐	Intrusion Detection Systeme	☐	Allg. Richtlinie Datenschutz und / oder Sicherheit (Pficht)
☐	Mobile Device Management	☐	Mobile Device Policy
☐	Einsatz VPN bei Remote-Zugriffen (Pflicht)	☐	Anleitung „Manuelle Desktopsperre"
☐	Verschlüsselung von Datenträgern (Pflicht)	☐	
☐	Verschlüsselung Smartphones (Pflicht)	☐	
☐	Gehäuseverriegelung	☐	
☐	BIOS Schutz (separates Passwort)	☐	
☐	Sperre externer Schnittstellen (USB)	☐	
☐	Automatische Desktopsperre	☐	
☐	Verschlüsselung von Notebooks / Tablet (Pflicht)	☐	
☐		☐	
☐		☐	

1.3. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Die Zugriffskontrolle kann unter anderem gewährleistet werden durch geeignete Berechtigungskonzepte, die eine differenzierte Steuerung des Zugriffs auf Daten ermöglichen. Dabei gilt, sowohl eine Differenzierung auf den Inhalt der Daten vorzunehmen als auch auf die möglichen Zugriffsfunktionen auf die Daten. Weiterhin sind geeignete Kontrollmechanismen und Verantwortlichkeiten zu definieren, um die Vergabe und den Entzug der Berechtigungen zu dokumentieren und auf einem aktuellen Stand zu halten (z.B. bei Einstellung, Wechsel des Arbeitsplatzes, Beendigung des Arbeitsverhältnisses). Besondere Aufmerksamkeit ist immer auch auf die Rolle und Möglichkeiten der Administratoren zu richten.

Technische Maßnahmen		Organisatorische Maßnahmen	
☐	Aktenschredder (DIN 66399) (Pflicht)	☐	Einsatz Berechtigungskonzepte (Pflicht)
☐	Externer Aktenvernichter (DIN 66399)	☐	Minimale Anzahl an Administratoren (Pflicht)
☐	Physische Löschung von Datenträgern (Pflicht)	☐	Verwaltung Benutzerrechte durch Administratoren (Pflicht)
☐	Protokollierung von Zugriffen auf Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten (Pflicht)	☐	
☐		☐	
☐		☐	

1.4. Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Dieses kann beispielsweise durch logische und physikalische Trennung der Daten gewährleistet werden.

Technische Maßnahmen		Organisatorische Maßnahmen	
☐	Trennung von Produktiv- und Test-Umgebung (Pflicht)	☐	Steuerung über Berechtigungskonzept (Pflicht)
☐	Physikalische Trennung (Systeme / Datenbanken / Datenträger)	☐	Festlegung von Datenbankrechten
☐	Mandantenfähigkeit relevanter Anwendungen (Pflicht)	☐	Datensätze sind mit Zweckattributen versehen
☐		☐	
☐		☐	

1.5. Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)

Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen;

Technische Maßnahmen		Organisatorische Maßnahmen	
☐	Im Falle der Pseudonymisierung: Trennung der Zuordnungsdaten und Aufbewahrung in getrenntem und abgesicherten System (mögl. verschlüsselt)	☐	Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst zu anonymisieren / pseudonymisieren
☐		☐	
☐		☐	

2. Integrität und Vertraulichkeit

2.1. Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist. Zur Gewährleistung der Vertraulichkeit bei der elektronischen Datenübertragung können z.B. Verschlüsselungstechniken und Virtual Private Network eingesetzt werden. Maßnahmen beim Datenträgertransport bzw. Datenweitergabe sind Transportbehälter mit Schließvorrichtung und Regelungen für eine datenschutzgerechte Vernichtung von Datenträgern.

Technische Maßnahmen		**Organisatorische Maßnahmen**	
☐	E-Mail-Verschlüsselung (Pflicht)	☐	Dokumentation der Datenempfänger sowie der Dauer der geplanten Überlassung bzw. der Löschfristen (Pflicht)
☐	Einsatz von VPN	☐	Übersicht regelmäßiger Abruf- und Übermittlungsvorgänge (Pflicht)
☐	Protokollierung der Zugriffe und Abrufe (Pflicht)	☐	Weitergabe in anonymisierter oder pseudonymisierter Form
☐	Sichere Transportbehälter	☐	Sorgfalt bei Auswahl von Transport-Personal und Fahrzeugen
☐	Bereitstellung über verschlüsselte Verbindungen wie sftp, https (Pflicht)	☐	Persönliche Übergabe mit Protokoll
☐	Nutzung von Signaturverfahren	☐	
☐		☐	
☐		☐	

2.2. Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Eingabekontrolle wird durch Protokollierungen erreicht, die auf verschiedenen Ebenen (z.B. Betriebssystem, Netzwerk, Firewall, Datenbank, Anwendung) stattfinden können. Dabei ist weiterhin zu klären, welche Daten protokolliert werden, wer Zugriff auf Protokolle hat, durch wen und bei welchem Anlass/Zeitpunkt diese kontrolliert werden, wie lange eine Aufbewahrung erforderlich ist und wann eine Löschung der Protokolle stattfindet.

Technische Maßnahmen		Organisatorische Maßnahmen	
☐	Technische Protokollierung der Eingabe, Änderung und Löschung von Daten (Pflicht)	☐	Übersicht, mit welchen Programmen welche Daten eingegeben, geändert oder gelöscht werden können (Pflicht)
☐	Manuelle oder automatisierte Kontrolle der Protokolle	☐	Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch Individuelle Benutzernamen (nicht Benutzergruppen) (Pflicht)
☐		☐	Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts (Pflicht)
☐		☐	Klare Zuständigkeiten für Löschungen (Pflicht)
☐		☐	
☐		☐	

3. Verfügbarkeit und Belastbarkeit

3.1. Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Hier geht es um Themen wie eine unterbrechungsfreie Stromversorgung, Klimaanlagen, Brandschutz, Datensicherungen, sichere Aufbewahrung von Datenträgern, Virenschutz, Raidsysteme, Plattenspiegelungen etc.

Technische Maßnahmen		Organisatorische Maßnahmen	
☐	Feuer- und Rauchmeldeanlagen (Pflicht)	☐	Backup & Recovery-Konzept (ausformuliert) (Pflicht)
☐	Feuerlöscher Serverraum (Pflicht)	☐	Kontrolle des Sicherungsvorgangs (Pflicht)
☐	Serverraumüberwachung Temperatur und Feuchtigkeit (Pflicht)	☐	Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse (Pflicht)
☐	Serverraum klimatisiert (Pflicht)	☐	Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums (Pflicht)
☐	USV (Pflicht)	☐	Keine sanitären Anschlüsse im oder oberhalb des Serverraums
☐	Schutzsteckdosenleisten Serverraum	☐	Existenz eines Notfallplans (z.B. BSI IT-Grundschutz 100-4)
☐	Datenschutztresor (S60DIS, S120DIS, andere geeignete Normen mit Quelldichtung etc.)	☐	Getrennte Partitionen für Betriebssysteme und Daten
☐	RAID System / Festplattenspiegelung (Pflicht)	☐	
☐	Videoüberwachung Serverraum	☐	
☐	Alarmmeldung bei unberechtigtem Zutritt zu Serverraum	☐	
☐		☐	
☐		☐	

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

☐		☐	
☐		☐	

4.1. Auftragskontrolle (Outsourcing an Dritte)

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Unter diesen Punkt fällt neben der Datenverarbeitung im Auftrag auch die Durchführung von Wartung und Systembetreuungsarbeiten sowohl vor Ort als auch per Fernwartung. Sofern der Auftragnehmer Dienstleister im Sinne einer Auftragsverarbeitung einsetzt, sind die folgenden Punkte stets mit diesen zu regeln.

Technische Maßnahmen		**Organisatorische Maßnahmen**	
☐		☐	Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation (Pflicht)
☐		☐	Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit) (Pflicht)
☐		☐	Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU Standardvertragsklauseln / Privacy Shield (Pflicht)
☐		☐	
☐		☐	

Auftragnehmer, zuständiger Bereich:

Auftraggeber, zuständiger Bereich:

Anlage 4 zum Rahmen-AV-Vertrag: Weitere Angaben des Auftraggebers

1) Weisungsbefugte Personen (§ 5 Abs. 5)

☐	Geschäftsführung
☐	IT-Leitung
☐	Ärzte
☐	Pflegekräfte
☐	Weitere vom Auftraggeber mit der Betreuung seiner Daten beauftragte Personen, z. B. regionale Systembetreuer
	☐
	☐
	☐

2) Meldungen von Sicherheitsverletzungen (§ 7 Abs. 7)

Kontaktdaten des Auftraggebers für Meldungen: datenschutz@uk-koeln.de