Anlage 2: Dokumentation zugesicherter technischer und organisatorischer Maßnahmen beim Auftragnehmer (TOMs)

Auftragnehmer

Universitätsklinikum Heidelberg
Abteilung Allgemeinmedizin und Versorgungsforschung
Im Neuenheimer Feld 130.3
69120 Heidelberg

Ansprechpartner: Prof. Dr. Joachim Szecsenyi
(Zum Zeitpunkt der Unterzeichnung)

Durch den Auftragnehmer realisierte technisch-organisatorische Maßnahmen

Der Auftragnehmer hat die von ihm getroffenen technischen und organisatorischen Maßnahmen darzustellen, mit deren Hilfe er

- die gemäß Art. 32 DSGVO definierten Schutzziele im Rahmen seiner Leistungserbringung
- die gemäß §8a BSIG für kritische Infrastrukturen geforderte Einhaltung von IT-Sicherheit nach dem Stand der Technik

erfüllen und deren Angemessenheit belegen und überprüfen kann.

Hierbei dienen die Angaben in diesem Nachweis als Grundlage für Risikoanalysen der jeweiligen konkreten Verarbeitungstätigkeit. Diese erfolgen zur Sicherstellung der Schutzziele Vertraulichkeit, Integrität, Authentizität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste.

Ergänzend ist in angemessenem Umfang unter Berücksichtigung der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere von Risiken ein Sicherheitskonzept zu allen Aspekten der konkreten Verarbeitungstätigkeit vorzulegen.

1 Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO; §8a (1) BSI-Gesetz)

1.1 Zutrittskontrolle

Unbefugten Personen ist der (räumliche) Zutritt zu IT-Systemen, Netzwerkkomponenten, Speichereinrichtungen und sowie der Zugriff auf sonstige Datenträger (z. B. PCs, USB-Sticks, CDs, Aktenordner) zu verwehren.	**ja**	**nein**	**nicht erforderlich**
Festlegung der zugangsberechtigten Personen (z. B. mittels Transponder, biometrische Anlagen, Schlüssel, Magnet- oder Chipkarten, Einsatz von Werkschutz, Pförtner)	☑	☐	☐
Einsatz von Alarmanlagen	☐	☑	☐
Videoüberwachung der Eingänge	☐	☑	☐
Schließberechtigungen und Schlüsselmanagement (z. B. Vergabeprozesse für und Dokumentation der Transponder oder Schlüsselinhaber)	☑	☐	☐
Verschließen von Räumen bei Nicht-Nutzung	☑	☐	☐
Zugangsregelungen für betriebsfremde Personen (z. B. Regelung zum Umgang mit Besuchern)	☑	☐	☐
Sorgfältige Auswahl und Verpflichtung von Wach-/Reinigungspersonal	☑	☐	☐
Sonstiges:	☐	☐	☐

UNIVERSITÄTS KLINIKUM HEIDELBERG

Nachweis von Maßnahmen nach Art. 32 DSGVO und § 8a BSIG

1.2 Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass IT-Systeme von Unbefugten genutzt werden können.	ja	nein	nicht erfor-derlich
Login mit Benutzername + Passwort	☑	☐	☐
Starke Authentisierung oder biometrische Verfahren für administrative Zugänge	☑	☐	☐
Malwareschutz auf Server-Systemen	☑	☐	☐
Malwareschutz auf Client-Systemen	☑	☐	☐
Malwareschutz auf mobilen Geräten	☑	☐	☐
Zentrale Überwachung des Malwareschutzes	☑	☐	☐
Segmentierung des Netzwerkes durch Firewalls	☑	☐	☐
Einsatz VPN bei Remote-Zugriffen	☑	☐	☐
Verschlüsselung von Datenträgern mit sensiblen Daten auf Servern	☐	☑	☐
Verschlüsselung von Notebooks/Tablets	☐	☑	☐
Verschlüsselung von Datenträgern mit sensiblen Daten auf sonstigen mobilen Geräten	☐	☑	☐
Sperre externer Schnittstellen (z. B. USB)	☐	☑	☐
Automatische Desktopsperre	☑	☐	☐
Zentrale Verwaltung von Benutzeraccounts	☑	☐	☐
Vorgaben für sichere Passworte	☑	☐	☐
Sonstiges:	☐	☐	☐

1.3 Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können	ja	nein	nicht erfor-derlich
Zentrales Benutzer-/Berechtigungs-Management nach dem „Need to have“ Prinzip für Benutzer	☑	☐	☐
Zentrales Benutzer-/Berechtigungs-Management nach dem „Need to have“ Prinzip für Administratoren	☑	☐	☐
Regelmäßige Überprüfung und Anpassung vergebener Berechtigungen	☑	☐	☐
Zeitnaher Entzug von Berechtigungen bei Ausscheiden	☑	☐	☐
Sonstiges:	☐	☐	☐

1.4 Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.	ja	nein	nicht erfor-derlich
Physikalische Trennung von Produktiv- und Testumgebungen (Systeme/Datenbanken/Datenträger)	☐	☐	☑
Logische Trennung von Produktiv- und Testumgebungen sowohl für die Anwendungen als auch Datenbanken	☐	☐	☑
Mandantenfähigkeit relevanter Anwendungen	☑	☐	☐
Bereitstellung von Berechtigungskonzepten zur Sicherstellung der Trennung von Produktiv- und Testdaten	☐	☐	☑
Sonstiges:	☐	☐	☐

UNIVERSITÄTS KLINIKUM HEIDELBERG

Nachweis von Maßnahmen nach Art. 32 DSGVO und § 8a BSIG

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 spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen unterliegen.	**ja**	**nein**	**nicht erfor-derlich**
Trennung der Zuordnungsdaten und Aufbewahrung in getrennten und abgesicherten Systemen	☐	☐	☑
Verschlüsselte Ablage der Zuordnungsdaten	☐	☐	☑
Sonstiges:	☐	☐	☐

2 Integrität (Art. 32 Abs. 1 lit. b DSGVO; §8a (1) BSI-Gesetz)

2.1 Weitergabekontrolle

Maßnahmen, welche ein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport verhindern	**ja**	**nein**	**nicht erfor-derlich**
Einsatz von VPNs beim Transport von Daten	☐	☐	☑
Sensible Daten in E-Mails werden verschlüsselt	☐	☐	☑
Verfahren für eine elektronische Signatur beim Versand von Daten	☐	☐	☑
Protokollierung der Datenübermittlung auf Seiten des Auftragnehmers	☐	☐	☑
Protokollierung der Datenübermittlung auf Seiten des Auftraggebers	☐	☐	☑
Verschlüsselung von Datenträgern, welche für einen physischen Transport eingesetzt werden	☐	☐	☑
Absicherung der Bereiche, in welche Datenträger für den Transport aufbewahrt werden	☐	☐	☑
Sicherung des Übertragungs- und Transportweges (verschlossene/versiegelte Umschläge oder Behälter, Kurier/Bote)	☐	☐	☑
Maßnahmen gegen unbefugtes Entfernen von Datenträgern	☑	☐	☐
Sichere Entsorgung nicht mehr benötigter Datenträger (verschlossene Sammelcontainer, Aktenschredder)	☑	☐	☐
Sonstiges:	☐	☐	☐

2.2 Eingabekontrolle

Gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.	**ja**	**nein**	**nicht erfor-derlich**
Technische Protokollierung der Eingabe, Änderung und Löschung von Daten	☑	☐	☐
Manuelle oder automatisierte Kontrolle der Protokolle	☑	☐	☐
Übersicht, mit welchen Programmen welche Daten eingegeben, geändert oder gelöscht werden können	☐	☐	☑
Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts	☑	☐	☐
Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch personalisierte Benutzer	☑	☐	☐
Sonstiges:	☐	☐	☐

UNIVERSITÄTS KLINIKUM HEIDELBERG

Nachweis von Maßnahmen nach Art. 32 DSGVO und § 8a BSIG

3 Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO; §8a (1) BSI-Gesetz)

3.1 Verfügbarkeitskontrolle

Gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind	ja	nein	nicht erfor-derlich
Feuer- und Rauchmeldeanlagen in allen IT-Räumen (Serverraum, Verteilerräume, etc.)	☑	☐	☐
Klimatisierung aller IT-Räume (Serverraum, Verteilerräume, etc.)	☑	☐	☐
Unterbrechungsfreie Stromversorgung sowie Notstromversorgung in zentralen Serverräumen	☑	☐	☐
Überwachung der Temperatur und Feuchtigkeit in zentralen Serverräumen	☑	☐	☐
Redundanz in verschiedenen Serverräumen möglich (Server, Storage)	☑	☐	☐
Redundanz in Daten-Speichern (Hardware, RAID) vorhanden	☑	☐	☐
Formalisiertes und überwachtes Backup-Konzept	☑	☐	☐
Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse	☑	☐	☐
Räumlich getrennte Aufbewahrung der erstellten Datensicherungen	☑	☐	☐
Schutz gegen unberechtigten Systemzugang von Extern (Firewall)	☑	☐	☐
Vermeidung wasserführender Leitungen in den IT-Räumen	☑	☐	☐
Überwachung der Verfügbarkeit von Systemen und Anwendungen	☑	☐	☐
Vorhandene Notfallpläne bei IT-Havarien	☑	☐	☐
Sonstiges:	☐	☐	☐

4 Regelmäßige Überprüfung, Bewertung und Evaluierung

(Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO; §8a (1) BSIG)

4.1 Datenschutz- und Informationssicherheits-Management

Verfahren zum strukturierten Management der Anforderungen des Datenschutzes, der Informationssicherheit und allgemeiner Vertraulichkeitsanforderungen	ja	nein	nicht erfor-derlich
Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf/Berechtigung	☑	☐	☐
Sicherheitszertifizierung nach ISO 27001, BSI IT-Grundschutz, ISAE 3402.	☐	☑	☐
Sonstige Zertifizierungen: _____	☐	☑	☐
Eine Überprüfung der Wirksamkeit der Technischen Schutzmaßnahmen wird mind. jährlich durchgeführt	☑	☐	☐
Mitarbeiter werden regelmäßig geschult und auf Vertraulichkeit verpflichtet	☑	☐	☐
Ein Datenschutzbeauftragter ist bestellt	☑	☐	☐
Ein Informationssicherheits-Beauftragter ist bestellt	☐	☑	☐
Die Datenschutz-Folgenabschätzung (DSFA) wird nach festgelegten Verfahren durchgeführt	☐	☐	☑
Die Organisation kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach	☑	☐	☐
Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden	☑	☐	☐
Sonstiges:	☐	☐	☐

UNIVERSITÄTS KLINIKUM HEIDELBERG

Nachweis von Maßnahmen nach Art. 32 DSGVO und § 8a BSIG

4.2 Incident-Response-Management

Unterstützung bei der Reaktion auf Sicherheitsverletzungen	ja	nein	nicht erfor-derlich
Einsatz eines Intrusion Detection oder Prevention Systems (IDS/IPS)	☐	☑	☐
Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen/Datenpannen	☑	☐	☐
Verfahren zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen	☑	☐	☐
Verfahren zur Meldung von Sicherheitsvorfällen/Datenpannen an Aufsichtsbehörden	☑	☐	☐
Einbindung des Datenschutzbeauftragten in die Bewertung und Bearbeitung von Sicherheitsvorfällen & Datenpannen	☑	☐	☐
Dokumentation von Sicherheitsvorfällen und Datenpannen (z. B. in Ticketsystemen)	☑	☐	☐
Sicherheitsrelevante Schwachstellen werden systematisch identifiziert	☑	☐	☐
Es sind Vorkehrungen getroffen und Kommunikationswege etabliert um sicherheitsrelevante Vorfälle an das Uniklinikum zu melden.	☑	☐	☐
Sonstiges:	☐	☐	☐

4.3 Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 1, 2 DSGVO)

Privacy by Design/Default/Datenschutzfreundliche Voreinstellungen	ja	nein	nicht erfor-derlich
Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind	☑	☐	☐
Nutzung von verfügbaren Konfigurationseinstellungen zur Verbesserung von Datenschutz und IT-Sicherheit	☑	☐	☐
Sonstiges:	☐	☐	☐

4.4 Auftragskontrolle (im Rahmen von Outsourcing an Dritte/Unterauftragnehmer)

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.	ja	nein	nicht erfor-derlich
Unterauftragnehmer vorhanden (folgende Punkte von 4.4 nur bei vorhandenen Unterauftragnehmern relevant)	☑	☐	☐
Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation	☑	☐	☐
Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (in Bezug auf Datenschutz und Informationssicherheit)	☑	☐	☐
Abschluss der notwendigen Vereinbarungen zur Auftragsverarbeitung bzw. EU Standard-Vertragsklauseln	☑	☐	☐
Schriftliche Weisungen an den Auftragnehmer	☑	☐	☐
Vereinbarung mit Auftragnehmer zur Verpflichtung seiner Mitarbeiter in Hinblick auf Vertraulichkeit und Aspekte des Datenschutzes	☐	☐	☑
Vereinbarung wirksamer Kontrollrechte mit dem Auftragnehmer	☑	☐	☐
Festlegung von Regelungen zum Einsatz weiterer Subunternehmer	☑	☐	☐
Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags	☑	☐	☐
Bei längerer Zusammenarbeit: Laufende Überprüfung des Auftragnehmers und seines Schutzniveaus	☑	☐	☐
Sonstiges:	☐	☐	☐

UNIVERSITÄTS KLINIKUM HEIDELBERG

Nachweis von Maßnahmen nach Art. 32 DSGVO und § 8a BSIG

5 Technik

5.1 Allgemeines

Maßnahmen zur Sicherstellung eines adäquaten Stand der Technik	ja	nein	nicht erfor-derlich
Produkte, welche durch Lieferanten bereitgestellt werden, müssen auf vom jeweiligen Hersteller unterstützten Umgebungen (z. B. Betriebssystem, Firmware) jederzeit betreibbar sein.	☑	☐	☐
Verbindungen, über welche Wartungsarbeiten am Uniklinikum ausgeführt werden, sind durch geeignete Verschlüsselungsverfahren und Authentifizierungs-Mechanismen abgesichert.	☑	☐	☐
Es werden aktuelle Schutzmaßnahmen gegen Schadcode, Viren und Malware eingesetzt	☑	☐	☐
Es gibt nachvollziehbare Verfahren (Change-Management) bei der Anpassung von Systemen und anderen administrativen Änderungen.	☑	☐	☐
Es wird eine angemessene Methodik zur Aufrechterhaltung der Aktualität der bereitgestellten Verfahren, Betriebssysteme und sonstigen Software-Bestandteilen bereitgestellt	☑	☐	☐
Bei Bekanntwerden IT-sicherheitstechnischer Mängel stellt der externe Dienstleister in angemessener Zeit Lösungen zur Behebung bereit.	☑	☐	☐
Sonstiges:	☐	☐	☐

Datum: 04.10.2018

Unterschrift
Prof. Dr. Szecsenyi
Uniklinik Heidelberg,
Abt. Allgemeinmedizin und
Versorgungsforschung (Auftragnehmer)