

# Vertrag über eine Auftragsverarbeitung gemäß Art. 28 DS-GVO

## (Fern-)Wartung und Instandhaltung

|                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Vertrags-ID                           | ⟨Vertrags-ID aus Vertragsmanagement, CUNO-Nummer⟩                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Gegenstand (kurz)                     | NNNNNNNNNNNNNNNN                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Auftraggeber/<br>Verantwortlicher     | Universitätsklinikum Heidelberg AdöR<br>Im Neuenheimer Feld 672<br>69120 Heidelberg                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Auftragnehmer/<br>Auftragsverarbeiter | ⟨Unternehmen mit Rechtsform⟩<br>⟨Straße, Hausnummer⟩<br>⟨PLZ, Ort⟩                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Bezug                                 | <i>⟨Nichtzutreffendes entfernen⟩</i><br>Hauptvertrag vom ??? (Vertrags-ID: ???)<br>EVB-IT-Vertrag vom ??? (Vertrags-ID: ???)<br>Angebot vom tt.mm.20jj und Annahme vom tt.mm.20jj<br>Auftrag vom tt.mm.20jj und Auftragsbestätigung vom tt.mm.20jj                                                                                                                                                                                                                                                                 |
| Anlagen                               | Anlage 1: Bedingungen zur Auftragsverarbeitung (BedAV)<br>Anlage 2: Dokumentation zugesicherter technischer und organisatorischer Maßnahmen beim Auftragnehmer (TOMs)                                                                                                                                                                                                                                                                                                                                              |
| Gegenstand des Auftrags (lang)        | Verarbeitung personenbezogener Daten zur Erfüllung der nachgenannten Verarbeitungszwecke                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Dauer des Auftrages                   | Die Dauer dieser Vereinbarung entspricht der Laufzeit des Hauptvertrages/Auftrages/Leistungsvereinbarung.<br>Der Vertrag ist zur einmaligen Ausführung<br>Der Vertrag ist unbefristet.<br>Das Recht zur fristlosen Kündigung aus wichtigem Grund bleibt unberührt.<br>Kündigungen bedürfen zu ihrer Wirksamkeit der Schriftform.                                                                                                                                                                                   |
| Verarbeitungsart                      | Die Verarbeitung umfasst folgende datenschutzrelevante Aspekte:<br>Die Verarbeitung personenbezogener Daten ist wesentlicher Gegenstand des Auftrags<br>Die Verarbeitung personenbezogener Daten ist nicht Gegenstand des Auftrags, eine Offenlegung/Kenntnisnahme personenbezogener Daten ist im Rahmen der Auftragserledigung aber nicht auszuschließen.<br>Die Verarbeitung personenbezogener Daten ist nicht Gegenstand des Auftrags, die Möglichkeit einer gelegentlichen Offenlegung/Kenntnisnahme ist durch |

|                   |              |                |          |               |
|-------------------|--------------|----------------|----------|---------------|
| Vorlage erstellt: | Version      | Genehmigt von: | Revision | Seitenangabe  |
| Datenschutzteam   | V1.1/2022-02 |                | 2 Jahre  | Seite 1 von 6 |

# Vertrag über eine Auftragsverarbeitung gemäß Art. 28 DS-GVO

## (Fern-)Wartung und Instandhaltung



|                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|----------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                              | technische/organisatorische Maßnahmen hinreichend ausgeschlossen (Restrisiko der Kenntnissnahme verbleibt).<br>Verarbeitung/Speicherung auf Rechnern des Auftragnehmers<br>Nicht-automatisierte Verarbeitung: ....<br>Sonstiges: ...                                                                                                                                                                                                               |
| <b>Verarbeitungszwecke</b>                   | Implementierung von Software<br>Anwendungsbetreuung<br>Support/Maintenance vor Ort oder als Fernwartung<br>Hosting Services beim Auftragnehmer<br>Managed Services (z.B. Backup-, Storage-, Helpdesk-Services, Cloud Computing, Remote Monitoring)<br>Sonstiges...                                                                                                                                                                                 |
| <b>Kategorien verarbeiteter Daten</b>        | Identitätsdaten (Name, Vorname, Patienten-ID)<br>Kontakt-/Kommunikationsdaten (z. B. IP-Adressen, Telefon, E-Mail, Nutzer, Login)<br>Administrative Daten (z.B. Vertragsdaten, Zahlungsdaten, Versicherungsdaten)<br>Gesundheitsdaten (Befunde, Diagnosen, Behandlungshistorie, Bild- und Tonaufnahmen)<br>Biometrische, genetische Daten<br>Betriebliche Beschäftigtendaten<br>Personalaktendaten, Gehaltsdaten<br>Bewerberdaten<br>Sonstige: ... |
| <b>Kategorien betroffener Personen</b>       | Stationäre und ambulante Patienten<br>Angehörige, Kontakt-/Begleitpersonen der Patienten<br>Probanden, Probandenangehörige oder -vertreter<br>Ärzte des Klinikums<br>Sonstige Beschäftigte des Klinikums<br>Beschäftigte von Dienstleistern, Geschäfts- und Kooperationspartnern des Klinikums<br>Sonstige:                                                                                                                                        |
| <b>Verarbeitungsort</b>                      | Innerhalb EU/EWR<br>○ <Stadt, Land><br>Außerhalb EU/EWR<br>○ <Stadt, Land>                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Weisungsberechtigte beim Auftraggeber</b> | <Name, Kontaktangaben>                                                                                                                                                                                                                                                                                                                                                                                                                             |

|                   |              |                |          |               |
|-------------------|--------------|----------------|----------|---------------|
| Vorlage erstellt: | Version      | Genehmigt von: | Revision | Seitenangabe  |
| Datenschutzteam   | V1.1/2022-02 |                | 2 Jahre  | Seite 2 von 6 |

# Vertrag über eine Auftragsverarbeitung gemäß Art. 28 DS-GVO

## (Fern-)Wartung und Instandhaltung

|                                                                                                                         |                                                                                                                                                                                                                                                                                                                                |
|-------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Weisungsberechtigte beim Auftragnehmer</b>                                                                           | ⟨Name, Kontaktangaben⟩                                                                                                                                                                                                                                                                                                         |
| <b>Genehmigte Subunternehmer, weitere Auftragsverarbeiter</b>                                                           | Es werden derzeit keine Subunternehmer eingesetzt.<br>Folgende Subunternehmer werden eingesetzt: <ul style="list-style-type: none"><li>○ ⟨Firmenname, Anschrift, kurze Beschreibung der Tätigkeit⟩</li><li>○ ...</li></ul>                                                                                                     |
| <b>Garantien bei einem grenzüberschreitenden Datenverkehr (auch im Verhältnis Auftragsverarbeiter – Subunternehmer)</b> | Angemessenheitsbeschluss<br>EU-Standardvertragsklauseln (EU-SCC)<br>Joint Controllership Agreement (JCA)<br>Data Transfer Agreement (DTA)<br>Binding Corporate Rules (BCR)<br>Sonstiges:<br>Zusätzlich:<br>Ausdrückliche informierte Einwilligung<br>Pseudonymisierung<br>Kryptographische Verschlüsselung<br>Sonstiges: ..... |
| <b>Datenschutzbeauftragte des Auftraggebers</b>                                                                         | Universitätsklinikum Heidelberg, Datenschutzbeauftragte,<br>im Neuenheimer Feld 672, 69120 Heidelberg<br>Tel. 06221 56-7036, datenschutz@med.uni-heidelberg.de                                                                                                                                                                 |
| <b>Datenschutzbeauftragte/r Auftragnehmers</b>                                                                          | ⟨Name, Kontaktangaben⟩                                                                                                                                                                                                                                                                                                         |

### Vertragliche Vereinbarungen

#### 1. Rechte und Pflichten der Vertragspartner

- 1.1 Die Rechte und Pflichten von Auftraggeber und Auftragnehmer für die Datenverarbeitung aufgrund der oben in Bezug genommen vertraglichen Vereinbarung ergeben sich aus den Bedingungen für die Auftragsverarbeitung (**BedAV, Anlage 1**) und der Übersicht der technischen und organisatorischen Maßnahmen (**TOMs, Anlage 2**) in der Anlage zu diesem Vertrag.
- 1.2 Anlage 1 und Anlage 2 sind wirksame Bestandteile dieses Vertrages.

#### 2. Besondere Vereinbarungen

- 2.1 Der Auftragnehmer führt im Auftrag des Auftraggebers die vereinbarten Arbeiten aus. In diesem Zusammenhang ist nicht ausgeschlossen, dass der Auftragnehmer Zugriff auf personenbezogene Daten bekommt bzw. Kenntnis erlangt. Daher ist der Abschluss eines Auftragsverarbeitungsvertrages nach Art. 28 DS-GVO erforderlich.

|                   |              |                |          |               |
|-------------------|--------------|----------------|----------|---------------|
| Vorlage erstellt: | Version      | Genehmigt von: | Revision | Seitenangabe  |
| Datenschutzteam   | V1.1/2022-02 |                | 2 Jahre  | Seite 3 von 6 |

# Vertrag über eine Auftragsverarbeitung gemäß Art. 28 DS-GVO

## (Fern-)Wartung und Instandhaltung

- 2.2 Die Verpflichtungen der BedAV werden auf diejenigen beschränkt, die sich auf das Verbot unbefugter Verarbeitung personenbezogener Daten und die Verpflichtung des Auftragnehmers, seiner Beschäftigten und der Subunternehmer als Mitwirkende gemäß § 203 Abs.3 StGB und die daraus resultierenden Geheimhaltungspflichten beziehen.
- 2.3 Bei versehentlicher oder unbefugter Speicherung personenbezogener Daten sind diese rückstandslos unverzüglich zu löschen.
- 2.4 Der Auftragnehmer führt ein Serviceprotokoll. Es beinhaltet Datum, Uhrzeit, Dauer, Name Servicemitarbeiter/in und eine nachvollziehbare Darstellung der Aktivitäten. Das Serviceprotokoll ist mindestens ein Jahr aufzubewahren. Der Auftraggeber erhält auf Nachfrage Auszüge zu ihn betreffenden konkreten Vorgängen.
- 2.5 Der Auftragnehmer macht von den ihm eingeräumten Zugriffsrechten auf automatisierten Verfahren oder von Datenverarbeitungsanlagen (IT-Systeme, Anwendungen) des Auftraggebers nur in dem Umfang Gebrauch, wie dies für die ordnungsgemäße Durchführung der beauftragten Wartungs- und Prüfungsarbeiten notwendig ist. Nach Abschluss der einzelnen Tätigkeitserbringung wird die aktuelle Fernzugriff-Sitzung durch den Auftragnehmer unverzüglich und zuverlässig geschlossen bzw. beendet.
- 2.6 Der Auftraggeber behält sich vor, stichprobenartig oder komplett Systemzugänge oder Serviceaktivitäten zu protokollieren und mitzuverfolgen. Protokolldaten werden im 13. Monat nach Entstehen gelöscht. Der Auftragnehmer hat sein Personal hierauf hinzuweisen.
- 2.7 Fernzugriffe im Rahmen von Wartungs- und Prüfungsarbeiten sowie sämtliche in diesem Zusammenhang erforderlichen Tätigkeiten werden unter Berücksichtigung von technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten durchgeführt.
- 2.8 Bei Fernzugriffen ist der Auftraggeber, soweit technisch möglich, berechtigt, diese von einem Kontrollbildschirm aus zu verfolgen und jederzeit abzubrechen.
- 2.9 Verletzungen der Informationssicherheit beim Auftragnehmer mit eingetretenen oder möglichen negativen Auswirkungen auf den Auftraggeber sind unverzüglich dem Auftraggeber schriftlich oder in Textform zu melden. Dies schließt Verletzungen der Informationssicherheit beim Auftragnehmer mit einer Gefährdung der vertraglich definierten Leistungen ein.
- 3. Zugriffsmöglichkeiten bei Fernwartungsarbeiten**
- 3.1 Der Auftraggeber ermöglicht dem Auftragnehmer für seine vertraglichen Arbeiten einen Fernzugriff (Remote Access). Dieser kann sich damit von seinem Remote-Rechner über das Internet (öffentliches Netzwerk) mit dem Rechnernetz des Auftraggebers verbinden.
- 3.2 *«aus den folgenden Alternativen die zutreffende wählen, Rest bitte löschen»*
- 3.2.1 Der Zugriff erfolgt nicht direkt auf das interne System, sondern über ein **SSL-VPN-Gateway** (kryptographische Verschlüsselung nach dem Stand der Technik), das sich zwischen der externen und internen Firewall des Klinikums befindet. Dieses Gateway stellt den exklusiven Zugangspunkt für alle Remoteverbindungen dar. Die Kommunikation wird durch Firewallregeln des Auftraggebers auf die erforderlichen Ziel-IP-Adressen und die notwendigen Dienste eingeschränkt.

|                   |              |                |          |               |
|-------------------|--------------|----------------|----------|---------------|
| Vorlage erstellt: | Version      | Genehmigt von: | Revision | Seitenangabe  |
| Datenschutzteam   | V1.1/2022-02 |                | 2 Jahre  | Seite 4 von 6 |

# Vertrag über eine Auftragsverarbeitung gemäß Art. 28 DS-GVO

## (Fern-)Wartung und Instandhaltung

- 3.2.2 Der Zugriff erfolgt nicht direkt auf das interne System, sondern auf einen „Virtual Desktop / Remote Desktop“ Arbeitsplatz (bspw. Citrix) mit entsprechend darauf eingerichteten Werkzeugen (kryptographische Kommunikationsverschlüsselung nach dem Stand der Technik). Diese Anwendung stellt den exklusiven Zugangspunkt für alle Remoteverbindungen dar.
- 3.2.3 Die Anbindung erfolgt über einen Punkt-zu-Punkt-verschlüsselten **IPSEC-Tunnel** vom Auftraggebers zum Auftragnehmer (kryptographische -Verschlüsselung nach dem Stand der Technik). Die Kommunikation wird durch Firewallregeln des Auftraggebers auf die erforderlichen Ziel-IP-Adressen und die notwendigen Dienste eingeschränkt.
- 3.2.4 Der Zugriff erfolgt über eine Ende zu Ende verschlüsselte Kommunikationsverbindung nach dem Stand der Technik auf einen Arbeitsplatz- oder Serversystem des Auftraggebers. Vom Auftraggeber freigegebene Werkzeuge / Applikationen (z.B. Teamviewer, Webex) kommen auf jeweils individuelle Initiative des Auftraggebers zum Einsatz.
- 3.3 *Nur bei Varianten 3.2.1 – 3.2.3:* Der Auftragnehmer bzw. seine für die Arbeiten eingesetzten Beschäftigten authentifizieren sich mit einer Zwei-Faktor-Authentifizierung (Kennwort und Einmalpasswort eines Hardware-/Software-Tokens) *«Nichtzutreffendes streichen»*. Der Auftragnehmer hat sicherzustellen, dass Unbefugte keine Möglichkeit einer Nutzung von Hard- oder Softwaretoken erhalten. Der Softwaretoken ist dabei vom zugreifenden Gerät/System (Remote-Rechner) des Auftragnehmers zu separieren. Das Hardwaretoken ist nach Beendigung des Vertrages zurückzugeben *«oder»* Die Registrierung des Auftragnehmers für den Erhalt von Softwaretokens wird nach Beendigung des Vertrages gelöscht/gesperrt.
- Nur Variante 3.2.4:* Der Auftragnehmer erhält eine individuelle Einladung mit Session-ID und Einmalpasswort. Er hat sicherzustellen, dass Unbefugte keine Kenntnis von der Session-ID und/oder dem Einmalpasswort erhalten sowie die Authentizität der durchführenden Person des Auftragnehmers zu gewährleisten.

### Unterschriften

Für den Auftraggeber  
Heidelberg, den

Für den Auftragnehmer  
«Ort», den

N.N.  
Funktion

N.N.  
Funktion

|                   |              |                |          |               |
|-------------------|--------------|----------------|----------|---------------|
| Vorlage erstellt: | Version      | Genehmigt von: | Revision | Seitenangabe  |
| Datenschutzteam   | V1.1/2022-02 |                | 2 Jahre  | Seite 5 von 6 |

# Vertrag über eine Auftragsverarbeitung gemäß Art. 28 DS-GVO

**(Fern-)Wartung und Instandhaltung**



UNIVERSITÄTS  
KLINIKUM  
HEIDELBERG

Achtung! Ausdruck könnte veraltet sein. Aktuelle Version immer in roXtra. Druckdatum: 22.07.2026

|                   |              |                |          |               |
|-------------------|--------------|----------------|----------|---------------|
| Vorlage erstellt: | Version      | Genehmigt von: | Revision | Seitenangabe  |
| Datenschutzteam   | V1.1/2022-02 |                | 2 Jahre  | Seite 6 von 6 |