Vertragsnummer/GZ:

DATENSCHUTZVERTRAG –

Vertrag über die Verarbeitung personenbezogener Daten im Auftrag

zwischen

**Steiermärkische Krankenanstaltengesellschaft m.b.H.**

**Stiftingtalstraße 4-6**

**8010 Graz**

als Verantwortlicher nach [Art 4 Z 7 DSGVO](https://dsgvo-gesetz.de/art-4-dsgvo/)[[1]](#footnote-1), nachfolgend kurz als **Verantwortlicher** bezeichnet,

und

Firmenbuchnummer:

UID:

als Auftragsverarbeiter nach [Art 4 Z 8 DSGVO](https://dsgvo-gesetz.de/art-4-dsgvo/), nachfolgend kurz als **Auftragsverarbeiter** bezeichnet,

gemeinsam in der Folge „Parteien“ bzw. einzeln „Partei“.

# Einleitung, Geltungsbereich, Definitionen

1. Verantwortlicher und Auftragsverarbeiter stehen in einer Vertragsbeziehung.
2. Dieser nun vorliegende Datenschutzvertrag regelt die datenschutzrechtlichen Rechte und Pflichten des Verantwortlichen und des Auftragsverarbeiters im Rahmen einer Verarbeitung von personenbezogenen Daten im Auftrag.
3. Dieser Vertrag findet auf alle Tätigkeiten Anwendung, bei denen der Auftragsverarbeiter, Mitarbeiter des Auftragsverarbeiters oder durch ihn zulässigerweise beauftragte Unter-Auftragsverarbeiter (Sub-Auftragsverarbeiter, siehe Punkt 5) personenbezogene Daten im Auftrag des Verantwortlichen verarbeiten.
4. In diesem Vertrag verwendete Begriffe sind entsprechend ihrer Definition in der EU Datenschutz-Grundverordnung ([DSGVO](https://dsgvo-gesetz.de/)) zu verstehen.
5. Ergänzungen oder Änderungen dieses Datenschutzvertrages haben schriftlich gemäß
§ 886 ABGB zu erfolgen.

# Gegenstand der Verarbeitung

1. Der Auftragsverarbeiter übernimmt die in Anlage 1 angeführten Verarbeitungstätigkeiten zum dort dargestellten Zweck.
2. Der Verantwortliche legt gegenüber dem Auftragsverarbeiter zur Durchführung der vereinbarten Tätigkeiten jene Daten aus seiner Datenverarbeitung offen, die in der Anlage 2 angeführt sind.

# Pflichten des Auftragsverarbeiters

1. Der Auftragsverarbeiter verarbeitet personenbezogene Daten einschließlich Verarbeitungsergebnisse ausschließlich im Rahmen der Aufträge des Verantwortlichen und wie vertraglich vereinbart. Der Auftragsverarbeiter verwendet somit die zur Verarbeitung überlassenen bzw. zur Kenntnis gelangten Daten für keine anderen, insbesondere nicht für eigene Zwecke und hat die verwendeten Daten ausschließlich an die vereinbarten Empfänger zu übermitteln. Sofern der Auftragsverarbeiter gesetzlich zu einer über die dokumentierte Weisung des Verantwortlichen nach [Art 28 Abs 3 lit a DSGVO](https://dsgvo-gesetz.de/art-28-dsgvo/) hinausgehenden Verarbeitung der Daten des Verantwortlichen verpflichtet ist oder wird, ist der Verantwortliche darüber vor der Verarbeitung nachweislich zu informieren.
2. Der Auftragsverarbeiter verpflichtet sich, personenbezogene Daten sowie sonstige Informationen des Verantwortlichen (wie etwa Geschäfts- und Betriebsgeheimnisse) die ihm im Rahmen des Auftragsverhältnisses zur Kenntnis gelangen, streng vertraulich zu behandeln und diese Verpflichtung vertraglich allen Personen zu überbinden, die für ihn im Rahmen des Auftragsverhältnisses tätig werden, sofern diese nicht einer angemessenen gesetzlichen Verschwiegenheitspflicht ([Art 28 Abs 3 lit b DSGVO](https://dsgvo-gesetz.de/art-28-dsgvo/) und [§ 6 DSG](https://www.ris.bka.gv.at/Dokument.wxe?ResultFunctionToken=72f73469-82d8-4c44-94b7-d8a8e7a5075e&Position=1&Abfrage=Bundesnormen&Kundmachungsorgan=&Index=&Titel=dsg&Gesetzesnummer=&VonArtikel=&BisArtikel=&VonParagraf=6&BisParagraf=&VonAnlage=&BisAnlage=&Typ=&Kundmachungsnummer=&Unterzeichnungsdatum=&FassungVom=04.12.2018&VonInkrafttretedatum=&BisInkrafttretedatum=&VonAusserkrafttretedatum=&BisAusserkrafttretedatum=&NormabschnittnummerKombination=Und&ImRisSeit=Undefined&ResultPageSize=100&Suchworte=&Dokumentnummer=NOR40195902) (2018)) unterliegen.

Diese Verpflichtung gilt auch über das Vertragsende hinaus und bleibt hinsichtlich der mit der Datenverarbeitung beauftragten Personen auch nach Beendigung ihrer Tätigkeit bzw. Ausscheiden beim Auftragsverarbeiter aufrecht. Bestehen Zweifel, ob eine Information der Geheimhaltungspflicht unterliegt, ist sie bis zur schriftlichen Freigabe durch die andere Partei als vertraulich zu behandeln.

Die mit der Auftragsverarbeitung befassten Personen sind über die einschlägigen rechtlichen Bestimmungen im Sinne des [§ 6 DSG](https://www.ris.bka.gv.at/Dokument.wxe?ResultFunctionToken=72f73469-82d8-4c44-94b7-d8a8e7a5075e&Position=1&Abfrage=Bundesnormen&Kundmachungsorgan=&Index=&Titel=dsg&Gesetzesnummer=&VonArtikel=&BisArtikel=&VonParagraf=6&BisParagraf=&VonAnlage=&BisAnlage=&Typ=&Kundmachungsnummer=&Unterzeichnungsdatum=&FassungVom=04.12.2018&VonInkrafttretedatum=&BisInkrafttretedatum=&VonAusserkrafttretedatum=&BisAusserkrafttretedatum=&NormabschnittnummerKombination=Und&ImRisSeit=Undefined&ResultPageSize=100&Suchworte=&Dokumentnummer=NOR40195902) (2018) nachweislich informiert worden.

Der Auftragsverarbeiter hat die vertraglichen Verpflichtungserklärungen zum Datengeheimnis dem Verantwortlichen auf dessen Verlangen vorzulegen.

1. Im Zusammenhang mit der beauftragten Verarbeitung hat der Auftragsverarbeiter den Verantwortlichen bei Erstellung (und allenfalls erforderlichen Aktualisierungen) des Verzeichnisses der Verarbeitungstätigkeiten sowie bei Durchführung einer allenfalls erforderlichen Datenschutzfolgenabschätzung, unter Berücksichtigung der dem Auftragsverarbeiter zur Verfügung stehenden Informationen, zu unterstützen.
2. Auskünfte an betroffene Personen sowie an sonstige Dritte darf der Auftragsverarbeiter nur nach vorheriger schriftlicher Zustimmung durch den Verantwortlichen erteilen. Direkt an ihn gerichtete Anfragen, soweit diese Bezüge zur Auftragsverarbeitung aufweisen, wird er unverzüglich an den Verantwortlichen weiterleiten. Der Auftragsverarbeiter hat die technischen und organisatorischen Voraussetzungen dafür zu treffen, dass der Verantwortliche seiner Pflicht zur Behandlung von Anträgen betreffend die Wahrnehmung der Rechte der betroffenen Person gemäß [Kapitel III der DSGVO](https://dsgvo-gesetz.de/kapitel-3/) (innerhalb der gesetzlichen Fristen) nachkommen kann ([Art 28 Abs 3 lit e DSGVO](https://dsgvo-gesetz.de/art-28-dsgvo/)).
3. Wird der Verantwortliche durch Aufsichtsbehörden oder andere hierzu berechtigte Stellen einer Kontrolle unterzogen oder machen betroffene Personen ihm gegenüber Rechte geltend, verpflichtet sich der Auftragsverarbeiter den Verantwortlichen im erforderlichen Umfang zu unterstützen, soweit die Verarbeitung im Auftrag betroffen ist.
4. Die Auftragsverarbeitung erfolgt ausschließlich innerhalb des EWR. Jegliche Verlagerung in ein Drittland darf nur mit schriftlicher Zustimmung des Verantwortlichen und unter den [im Kapitel V der DSGVO](https://dsgvo-gesetz.de/kapitel-5/) enthaltenen Bedingungen erfolgen.
5. Ist der Auftragsverarbeiter nicht in der Europäischen Union niedergelassen, bestellt er einen verantwortlichen Ansprechpartner in der Europäischen Union gem. [Art 27 DSGVO](https://dsgvo-gesetz.de/art-27-dsgvo/). Die Kontaktdaten des Ansprechpartners sowie sämtliche Änderungen in der Person des Ansprechpartners sind dem Verantwortlichen unverzüglich und nachweislich mitzuteilen.

# Technische und organisatorische Maßnahmen

1. Der Auftragsverarbeiter verpflichtet sich ausreichende (technische und organisatorische) Sicherheitsmaßnahmen gemäß Art 32 DSGVO zu ergreifen und diese stets auf dem aktuellen Stand der Technik zu halten, um zu verhindern, dass Daten ordnungswidrig verwendet oder Dritten unbefugt zugänglich werden.
2. Die gemäß [Art 32 DSGVO](https://dsgvo-gesetz.de/art-32-dsgvo/) vorgesehenen Sicherheitsmaßnahmen sind durch den Auftragsverarbeiter in einem Sicherheitskonzept zu beschreiben, welches die Mindeststrukturierung der Anlage 3 „Technische und Organisatorische Maßnahmen (TOM)“ zu berücksichtigen hat und regelmäßig auf den jeweils aktuellen technischen Stand zu aktualisieren ist. Die darin vorgesehenen Datensicherheitsmaßnahmen werden verbindlich festgelegt. Sie definieren das vom Auftragsverarbeiter geschuldete Minimum. Dieses Niveau darf nicht unterschritten werden.
3. Auf Aufforderung hat der Auftragsverarbeiter dem Verantwortlichen zu belegen, dass er seine Pflichten, insbesondere die vollständige Umsetzung der vereinbarten technischen und organisatorischen Maßnahmen, erfüllt hat. Der Nachweis kann auch durch genehmigte Verhaltensregeln oder ein genehmigtes und geeignetes Zertifizierungsverfahren erbracht werden.
4. Kopien der Datenbestände (partiell oder gesamt) des Verantwortlichen dürfen nur dann erstellt werden, wenn sie für die Erfüllung des Auftragstatsächlich notwendig sind. Alle anderen Kopien bedürfen der nachweislichen Genehmigung des Verantwortlichen.

# Sub-Auftragsverhältnisse

1. Sub-Auftragsverhältnisse im Sinne dieses Vertrags sind ausschließlich solche Leistungen, die einen direkten Zusammenhang mit der Erbringung der Hauptleistung aufweisen.
2. Die Beauftragung eines weiteren Auftragsverarbeiters (Sub-Auftragsverarbeiters) durch den Auftragsverarbeiter ist nur mit vorheriger gesonderter oder allgemeiner schriftlicher Genehmigung des Verantwortlichen zulässig. Im Falle einer allgemeinen schriftlichen Genehmigung informiert der Auftragsverarbeiter den Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder Ersetzung anderer Auftragsverarbeiter, wodurch der Verantwortliche die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben. Darüber hinaus stellt der Auftragsverarbeiter sicher, dass der Verantwortliche dem Sub-Auftragsverarbeiter auch direkt Weisungen nach der DSGVO erteilen kann, sofern dies aus datenschutzrechtlicher Sicht erforderlich ist.
3. Die Verbindlichkeit der Bestimmungen dieses Datenschutzvertrages ist zwischen Auftragsverarbeiter und dem Sub-Auftragsverarbeiter schriftlich zu vereinbaren ([Art 28 Abs 4 DSGVO](https://dsgvo-gesetz.de/art-28-dsgvo/)). Der Verantwortliche erhält auf Verlangen Einsicht in die relevanten Verträge zwischen dem Auftragsverarbeiter und Sub-Auftragsverarbeiter.
4. Die Verantwortlichkeiten des Auftragsverarbeiters und des Sub-Auftragsverarbeiter sind eindeutig voneinander abzugrenzen.
5. Zum Zeitpunkt des Vertragsabschlusses sind die in Anlage 4 „Zugelassene Sub-Auftragsverarbeiter“ mit Namen, Anschrift und Auftragsinhalt angeführten Sub-Auftragsverarbeiter mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beauftragt und durch den Verantwortlichen genehmigt.

# Rechte und Pflichten des Verantwortlichen

1. Der Verantwortliche ist berechtigt, die Einhaltung der Vorschriften über den Datenschutz und die Datensicherheit beim Auftragsverarbeiter in angemessenem Umfang selbst oder durch von ihm beauftragte Dritte, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme, zu überprüfen sowie allfällige Kontrollen vor Ort durchzuführen.
2. Der Auftragsverarbeiter hat dafür Sorge zu tragen, dass einer zweckmäßigen Kontrolle durch den Verantwortlichen oder einem von diesem beauftragten Dritten keine Geschäfts- und Betriebsgeheimnisse entgegenstehen.
3. Der Auftragsverarbeiter ist verpflichtet, erforderliche Auskünfte zu erteilen, Abläufe zu demonstrieren und Nachweise zu führen, die zur Durchführung einer Kontrolle erforderlich sind.
4. Kontrollen beim Auftragsverarbeiter haben ohne vermeidbare Störungen des Geschäftsbetriebs zu erfolgen. Soweit nicht aus vom Verantwortlichen zu dokumentierenden, dringlichen Gründen anders angezeigt, finden Kontrollen nach angemessener Vorankündigung und zu Geschäftszeiten des Auftragsverarbeiters statt.

# Mitteilungspflichten

1. Der Auftragsverarbeiter hat den Verantwortlichen im Falle einer Verletzung des Schutzes personenbezogener Daten unverzüglich und nachweislich zu verständigen, jedenfalls aber binnen 24 Stunden, nachdem die Verletzung dem Auftragsverarbeiter bekannt wurde bzw. bekannt sein musste. Insbesondere Verstöße des Auftragsverarbeiters oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder gegen die in diesem Datenschutzvertrag getroffenen Festlegungen sind unverzüglich und nachweislich mitzuteilen.
2. Auch begründete Verdachtsfälle sind unverzüglich mitzuteilen.
3. Die Verständigung hat zumindest folgende Informationen zu enthalten:

a) Eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Gruppe 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 des Auftrags-verarbeiters oder einer sonstigen Anlaufstelle für weitere Informationen.

c) Eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten.

d) Eine Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen ([Art 33 Abs 2 und 3 DSGVO](https://dsgvo-gesetz.de/art-33-dsgvo/)).

1. Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich von Kontrollen oder Maßnahmen von Aufsichtsbehörden oder anderen Dritten, soweit diese Bezüge zur Auftragsverarbeitung aufweisen.
2. Der Auftragsverarbeiter verpflichtet sich, jeden Sicherheitsvorfall zu untersuchen und gemeinsam mit dem Verantwortlichen angemessene Maßnahmen zur Sicherung der Daten, sowie zur Minderung möglicher nachteiliger Folgen für die betroffenen Personen zu ergreifen. Der Auftragsverarbeiter sichert in diesem Zusammenhang zu, den Verantwortlichen bei Erfüllung der Pflichten nach [Art. 33](https://dsgvo-gesetz.de/art-33-dsgvo/) und [34 DSGVO](https://dsgvo-gesetz.de/art-34-dsgvo/) im erforderlichen Umfang zu unterstützen.
3. Sämtliche in diesem Abschnitt enthaltenen Pflichten sind auch auf allfällige Sub-Auftragsverarbeiter zu überbinden.

# Beendigung des Auftrags

1. Bei Beendigung des Auftragsverhältnisses oder jederzeit auf Verlangen des Verantwortlichen hat der Auftragsverarbeiter die im Auftrag verarbeiteten Daten gemäß [Art 4 Z1 DSGVO](https://dsgvo-gesetz.de/art-4-dsgvo/) nach Wahl des Verantwortlichen entweder zu vernichten oder an den Verantwortlichen in einem von diesem bestimmten Format an diesen zu übergeben und dies zu bestätigen, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Ebenfalls zu vernichten sind sämtliche vorhandene Kopien dieser Daten. Die Vernichtung hat so zu erfolgen, dass eine Wiederherstellung auch von Restinformationen mit vertretbarem Aufwand nicht mehr möglich ist. Die Art und Weise der Vernichtung bzw. der Übergabe ist verbindlich in der Anlage 3 „Technische und Organisatorische Maßnahmen (TOM)“ festgelegt. Die Vernichtung ist dem Verantwortlichen nachweislich zu bestätigen.
2. Der Auftragsverarbeiter ist verpflichtet, die unverzügliche Rückgabe bzw. dokumentierte Vernichtung dieser Daten auch bei etwaigen Sub-Auftragsverarbeitern herbeizuführen bzw. sicherzustellen.
3. Dokumentationen, die dem Nachweis der ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragsverarbeiter den jeweiligen Aufbewahrungsfristen entsprechend auch über das Vertragsende hinaus aufzubewahren. Der Auftragsverarbeiter kann die Dokumentation über die ordnungsgemäße Datenverarbeitung zu seiner Entlastung dem Verantwortlichen mit dessen Zustimmung bei Vertragsende übergeben.

# Haftung

Beide Parteien haften gemäß Art. 82 DSGVO in der jeweils gültigen Fassung.

# Sonderkündigungsrecht

1. Der Verantwortliche kann Verträge mit dem Auftragsverarbeiter jederzeit ohne Einhaltung einer Frist kündigen („außerordentliche Kündigung“), wenn in Bezug auf einen Vertrag ein schwerwiegender Verstoß des Auftragsverarbeiters oder dessen Sub-Auftragsverarbeiter gegen Datenschutzvorschriften oder die Bestimmungen dieses Datenschutzvertrages vorliegt oder der Auftragsverarbeiter bzw. dessen Sub-Auftragsverarbeiter Kontrollrechte des Verantwortlichen vertragswidrig verweigert.
2. Ein schwerwiegender Verstoß liegt insbesondere dann vor, wenn der Auftragsverarbeiter oder dessen Sub-Auftragsverarbeiter die in dieser Vereinbarung bestimmten Pflichten, insbesondere die vereinbarten technischen und organisatorischen Maßnahmen, vorsätzlich oder grob fahrlässig nicht erfüllen oder nicht erfüllt haben.
3. Bei sonstigen Verstößen gegen diesen Datenschutzvertrag setzt der Verantwortliche dem Auftragsverarbeiter eine angemessene Frist zur Abhilfe. Erfolgt die Abhilfe nicht rechtzeitig, so ist der Verantwortliche zur außerordentlichen Kündigung wie in diesem Abschnitt beschrieben berechtigt.

# Sonstiges

1. Änderungen oder Ergänzungen der vorliegenden Vereinbarung bedürfen der Schriftform. Es bestehen keine mündlichen Nebenabreden.
2. Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.
3. Dieser Vertrag ersetzt alle bestehenden datenschutzrechtlichen Vereinbarungen zwischen den Vertragsparteien und gilt sowohl während als auch nach Beendigung einzelner oder aller Vertragsverhältnisse.
4. Abweichende Bedingungen des Auftragsverarbeiters (z. B. in Allgemeinen Geschäftsbedingungen) gelten rechtlich als nicht beigelegt und haben damit keine Gültigkeit. Die Unwirksamkeit gilt auch für den Fall, dass derartige Bedingungen des Auftragsverarbeiters auf Lieferscheinen, Fakturen etc. angebracht sind und diesen Aufdrucken bzw. sonstigen Beilagen vom Verantwortlichen nicht widersprochen wird.
5. Dieser Vertrag unterliegt österreichischem Recht. Die Anwendung des UN-Kaufrechts (Convention on Contracts for the International Sale of Goods vom 11. April 1980, UNCITRAL-Kaufrecht) und der Verweisnormen des IPRG wird ausgeschlossen. Alle sich aus dem Datenschutzvertrag ergebenden Rechtsstreitigkeiten unterliegen der ausschließlichen Gerichtsbarkeit des sachlich zuständigen Gerichts in Graz.
6. Der Vertrag kann analog (handschriftlich) oder mittels qualifizierter oder fortgeschrittener elektronischer Signatur unterfertigt werden. Die Unterfertigung einer Ausfertigung, welche bereits von einer oder mehreren Vertragspartei(en) handschriftlich oder mittels qualifizierter oder fortgeschrittener elektronischer Signatur unterfertigt und elektronisch weitergeleitet wurde, ist zulässig und wird das Erfordernis der Schriftlichkeit erfüllt. Auf Seiten der Steiermärkischen Krankenanstaltengesellschaft m.b.H. wird hiefür die E-Mail-Adresse fa.recht@kages.at bereitgestellt.
7. Jede Partei kann identische Gegenstücke dieses Vertrags mit derselben Wirkung unterzeichnen, als ob die Parteien dasselbe Dokument unterzeichnet hätten. Die Parteien vereinbaren, dass Unterschriften elektronisch oder handschriftlich zu diesem Vertrag, die per Fax, per E-Mail im „Portable Document Format“ („PDF“) oder durch ein anderes elektronisches Mittel zur Erhaltung des ursprünglichen Erscheinungsbildes dieses Vertrags übermittelt werden, dieselbe Wirkung haben wie die physische Übergabe des Papierdokuments mit einer Originalunterschrift und ausreichen, um das Schriftformerfordernis zu erfüllen.

# 12 Anlagen

Anlage 1 Verarbeitungstätigkeiten/Zweck

Anlage 2 Betroffenenkategorien/Datenarten

Anlage 3 Technische und Organisatorische Maßnahmen (TOM)

Anlage 4 Zugelassene Offenlegungen

# 13 Unterschriften

**Für die Steiermärkische Krankenanstaltengesellschaft m.b.H.:**

 ……………, am ……………….. ……………, am ……………….

 (Ort, Datum) (Ort, Datum)

 ……………………………………………. …………………………………………….

 Name und Funktion, Unterschrift Name und Funktion, Unterschrift

**Für den Auftragsverarbeiter:**

 ……………, am ……………….. ……………, am ……………….

 (Ort, Datum) (Ort, Datum)

 ……………………………………………. …………………………………………….

 Name und Funktion, Unterschrift Name und Funktion, Unterschrift

# Anlage 1 – Verarbeitungstätigkeiten/Zweck

zu [VERTRAGSNUMMER/GZ]

* **Bezeichnung der Verarbeitung**:

Klicken oder tippen Sie hier, um Text einzugeben.

* **Beschreibung und Zweck der Verarbeitung:**

Klicken oder tippen Sie hier, um Text einzugeben.

* **verwendete Systeme des Verantwortlichen und des Auftragsverarbeiters (z.B. KIS des Verantwortlichen):**

Klicken oder tippen Sie hier, um Text einzugeben.

* **Dauer der Verarbeitung**: [ ]  einmalig [ ]  unbefristet
 [ ]  befristet Klicken oder tippen Sie hier, um Text einzugeben.

|  |
| --- |
| [ ]  **Systemadministration**[ ]  **Cloud-Dienst** [ ]  **Fernzugriff** [ ]  **Wartung und Support** [ ]  **vor Ort** [ ]  **nicht vor Ort**[ ]  **Backup**[ ]  **Hosting**[ ]  **Sonstiges:** Klicken oder tippen Sie hier, um Text einzugeben. |
|  |
|  |

**Die Verarbeitungstätigkeit der Beauftragung bzgl. personenbezogene Daten umfasst:**

**Kontaktstelle für Datenschutz und IKT-Sicherheitsfragen des Auftragsverarbeiters:**

z.B. Betroffenenrechtsanfragen, Sicherheitsanfragen

1. Funktion, Titel, Vorname, Nachname, E-Mail-Adresse, mobile Telefonnummer
2. Funktion, Titel, Vorname, Nachname, E-Mail-Adresse, mobile Telefonnummer
3. Funktion, Titel, Vorname, Nachname, E-Mail-Adresse, mobile Telefonnummer

# Anlage 2 – Betroffenenkategorie/Datenarten

zu [VERTRAGSNUMMER/GZ]

# Offen gelegte Daten

2.1 Kategorien der betroffenen Personen & Datenarten

Von der Verarbeitung betroffen sind:

|  |  |
| --- | --- |
| Betroffenenkategorie \*  | Datenarten |
| **Mitarbeiter\*innen** | **Klicken oder tippen Sie hier, um Text einzugeben.** |
| **Patient\*innen** | **Klicken oder tippen Sie hier, um Text einzugeben.** |
| **Angehörige / Kontaktperson** | **Klicken oder tippen Sie hier, um Text einzugeben.** |
| **Lieferant** | **Klicken oder tippen Sie hier, um Text einzugeben.** |
| **Sonstige** | **Klicken oder tippen Sie hier, um Text einzugeben.** |

\* nicht verwendete Zeilen bitte löschen

2.2 Form der Datenübermittlung/Offenlegung

**Datenübermittlung/Offenlegung zwischen Verantwortlichem und Auftragsverarbeiter:**(Wie, wann und in welcher Form findet die Datenübermittlung/Offenlegung zw. Verantwortlichem und Auftragsverarbeiter statt.)

* + **Form der Übermittlung/Offenlegung:**[ ]  Papierform [ ]  Elektronisch

[ ]  Sonstiges: Klicken oder tippen Sie hier, um Text einzugeben.

* + **Häufigkeit der Übermittlung/Offenlegung**:
	[ ]  einmalig [ ]  regelmäßig/kontinuierlich
	[ ]  Sonstiges: Klicken oder tippen Sie hier, um Text einzugeben.

2.3 Datenspeicherung

**Werden Daten des Verantwortlichen beim Auftragsverarbeiter gespeichert (allenfalls auch nur kurzzeitig):**

[ ]  Ja, zu folgendem Zweck: Klicken oder tippen Sie hier, um Text einzugeben.
 **Dauer der Speicherung** der personenbezogenen Daten, allenfalls, die Kriterien für die Festlegung dieser Dauer: Klicken oder tippen Sie hier, um Text einzugeben.

[ ]  Nein

**HINWEIS!** Wird **die Frage** mit **„Ja“** beantwortet, sind alle in der Anlage 3 angeführten **Fragen** welche **mit „AV“** (Auftragsverarbeiter) vor der Nummerierung **gekennzeichnet** sind **zu beantworten**. Wird die Frage mit **„Nein“** beantwortet sind **nur jene Fragen** zu beantworten, welche vor der Nummerierung **mit „DL“** (Dienstleister) gekennzeichnet sind.

Anlage 3 – Technische und organisatorische Maßnahmen (TOM) zu [VERTRAGSNUMMER/GZ]

**Datensicherheitsmaßnahmen**

Im Folgenden werden die technischen und organisatorischen Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit festgelegt, die der Auftragsverarbeiter mindestens einzurichten und laufend aufrecht zu erhalten hat. Ziel ist die Gewährleistung insbesondere der Vertraulichkeit, Integrität, Verfügbarkeit und Widerstandsfähigkeit der im Auftrag verarbeiteten Informationen und der erbrachten Dienstleistungen. Der Auftragsverarbeiter hat die Umsetzung dieser Anforderungen durch seine Subauftragsverarbeiter sicherzustellen.

Der Begriff Informationen ist gleichzusetzen mit dem Begriff Daten und umfasst alle Formen und Arten verarbeiteter Daten (personenbezogene und sonstige Daten) des Auftraggebers im Rahmen der beauftragten Dienstleistungen. Vom Begriff sind somit sowohl Papierausdrucke und Ordner, als auch digitale Daten und Datenbanken / Dateiablagen umfasst.

Die technischen und organisatorischen Maßnahmen können auch durch eine gültige facheinschlägige Informationssicherheit und / oder Datenschutz Zertifizierung (z.B. ISO 27001, ISO 27701, ISO 27018) nachgewiesen werden, wenn der Geltungsbereich die beauftragte Dienstleistung beinhaltet. Dieses kann als Begründung beim Ankreuzen von „JA“ angeführt werden.

Die folgenden technischen und organisatorischen Maßnahmen sind für die im Grundvertrag vereinbarte Erfassung, Verarbeitung und Nutzung von Daten durch den Auftragsverarbeiter zu implementieren:

1. **Zutrittskontrolle (physisch)**

Es ist sicherzustellen, dass unbefugte Personen der Zutritt zu Räumlichkeiten mit Daten und den IKT-Einrichtungen verwehrt ist, in denen Daten verarbeitet und genutzt werden. d.h. der physische Zutritt zu den Räumlichkeiten und IKT-Einrichtungen ist zu regeln.

|  |  |
| --- | --- |
| Nr. | **Zutrittskontrolle (physisch) -** Mindest-Sicherheitsniveau erfüllt durch: |
| **AV**1.1 | Zum Schutz vor unberechtigtem Zugriff sind Maßnahmen zur Speicherung der Informationen an einem sicheren Ort entsprechend der Klassifizierung der Informationen umgesetzt.  |
| [ ]  Ja | [ ]  Nein | bei „Nein“ bitte Begründung angeben |
| **AV**1.2 | Maßnahmen für eine manuelle Schließanlage mit Regelungen für die Schlüsselverwaltung (Schlüsselregistrierung, Schlüsselverteilungssystem), samt Regelungen für den Verlust von Schlüssel, sind umgesetzt |
| [ ]  Ja | [ ]  Nein | bei „Nein“ bitte Begründung angeben |
| **AV**1.3 | Maßnahmen für eine Alarmierung bei Einbruch in sensible Bereiche (z.B. Archivräume, Serverräume) sind umgesetzt. |
| [ ]  Ja | [ ]  Nein | bei „Nein“ bitte Begründung angeben |
| **AV**1.4 | Maßnahmen für die Registrierung von BesucherInnen sind umgesetzt. |
| [ ]  Ja | [ ]  Nein | bei „Nein“ bitte Begründung angeben |
| **AV**1.5 | Maßnahmen für ein elektronisches Schließsystem mit Chipkarte/Transponder sowie Regelungen für deren Verwaltung (Registrierung, Verteilung, Umgang mit Verlust) sind für sensible Bereiche (z.B. Archivräume, Serverräume) umgesetzt |
| [ ]  Ja | [ ]  Nein | bei „Nein“ bitte Begründung angeben |
| **AV**1.6 | Maßnahmen für die sorgfältige Auswahl und Unterweisung der Reinigungskräfte, Haustechnikkräfte in allen Bereichen sind umgesetzt. |
| [ ]  Ja | [ ]  Nein | bei „Nein“ bitte Begründung angeben |

1. **Zugangskontrolle (logisch)**

Jede Verwendung von elektronischen Datenverarbeitungssystemen durch unbefugte Personen ist zu verhindern, d.h. der logische Zugang zu diesen IKT-Systemen und den darin gespeicherten Daten ist zu regeln.

Die folgenden technischen und organisatorischen Maßnahmen sind für die vertragliche Erfassung, Verarbeitung und Nutzung von Daten durch den Auftragsverarbeiter zu implementieren:

|  |  |
| --- | --- |
| Nr. | **Zugangskontrolle (logisch)** - Mindest-Sicherheitsniveau erfüllt durch: |
| **AV****DL**2.1 | Maßnahmen für den Betrieb eines dokumentierten Risikomanagements, in dem Risiken für die IT Sicherheit, Informationssicherheit und Datenschutz erfasst und bewertet wurden, sind umgesetzt. |
| [ ]  Ja | [ ]  Nein | bei „Nein“ bitte Begründung angeben |
| **AV****DL**2.2 | Maßnahmen für die Verschlüsselung von eingebauten Datenträgern (z. B. in Laptops, Notebooks, Smartphone, Tablets) sind umgesetzt.  |
| [ ]  Ja | [ ]  Nein | bei „Nein“ bitte Begründung angeben |
| **AV****DL**2.3 | Maßnahmen für die Verschlüsselung von mobilen Datenträgern (z. B. mobile USB Sticks, optische Speichermedien, externe Festplatten, etc) sind umgesetzt. |
| [ ]  Ja | [ ]  Nein | bei „Nein“ bitte Begründung angeben |
| **AV****DL**2.4 | Maßnahmen für die Authentifizierung mit Benutzername / Passwort (Passwortvergabe basiert auf gültigen Passwortregelungen) bei Notebooks / Laptops, Server und PCs sind umgesetzt. |
| [ ]  Ja | [ ]  Nein | bei „Nein“ bitte Begründung angeben |
| **AV****DL**2.5 | Maßnahmen für die Authentifizierung mittels PIN Code (mindestens 4-stellig) oder Biometrie bei mobilen Endgeräten (Smartphone, Tablets) sind umgesetzt. |
| [ ]  Ja | [ ]  Nein | bei „Nein“ bitte Begründung angeben |
| **AV****DL**2.6 | Maßnahmen die sicherstellen, dass voreingestellte Standard Passwörter in eingesetzten Datenverarbeitungssystemen geändert werden, sind umgesetzt.  |
|  | [ ]  Ja | [ ]  Nein | bei „Nein“ bitte Begründung angeben |
| **AV****DL**2.7 | Maßnahmen die sicherstellen, dass vom Auftragsverarbeiter verwendete Passwörter nicht bei anderen Kunden des Auftragsverarbeiters wiederverwendet werden, sind umgesetzt.  |
| [ ]  Ja | [ ]  Nein | bei „Nein“ bitte Begründung angeben |
| **AV****DL**2.8 | Maßnahmen für eine Passwort-Richtlinie, die Komplexität, Länge sowie die Gültigkeitsdauer des Passworts bzw. die Authentifizierung über 2 Faktor und/oder biometrische Methoden definiert, sind umgesetzt. |
| [ ]  Ja | [ ]  Nein | bei „Nein“ bitte Begründung angeben |
| **AV****DL**2.9 | Maßnahmen zum Schutz mobil eingesetzter Notebooks / PCs vor unberechtigtem Zugriff aus dem Internet oder anderen Teilnehmern nicht vertrauenswürdiger Netze (Hotspots, etc.) mittels Personal Firewalls sind umgesetzt. (Regelsatz: Es ist alles verboten, was nicht explizit erlaubt ist) |
| [ ]  Ja | [ ]  Nein | bei „Nein“ bitte Begründung angeben |
| **AV****DL**2.10 | Maßnahmen zum Schutz von Netzwerken des Auftragsverarbeiters (in denen Daten des Auftraggebers verarbeitet werden) gegen unberechtigten Zugriff aus dem Internet oder anderen Netzen sind mittels Firewalls umgesetzt (Regelsatz: Es ist alles Verboten, was nicht explizit erlaubt ist). |
| [ ]  Ja | [ ]  Nein | bei „Nein“ bitte Begründung angeben |
| **AV****DL**2.11 | Maßnahmen für den Betrieb von Sicherheitssoftware zur Erkennung und Blockierung von Schadsoftware und Cyber Angriffen (z.B. Antivirus) auf vom Auftragsverarbeiter betriebenen Systemen sind umgesetzt und aktuell gehalten.  |
| [ ]  Ja | [ ]  Nein | bei „Nein“ bitte Begründung angeben |
| **AV****DL**2.12 | Maßnahmen zur Erkennung und Risikominimierung bekanntgewordener Sicherheitsschwachstellen in vom Auftragsverarbeiter betriebenen Systemen, und eingesetzten (Software-)Produkten sind umgesetzt.  |
| [ ]  Ja | [ ]  Nein | bei „Nein“ bitte Begründung angeben |
| **AV****DL**2.13 | Maßnahmen zur zeitnahen Einspielung von verfügbaren Softwaresicherheitsaktualisierungen (Sicherheitspatches, Patch Management) sind umgesetzt.  |
| [ ]  Ja | [ ]  Nein | bei „Nein“ bitte Begründung angeben |
| **AV****DL**2.14 | Maßnahmen zur Sicherstellung, dass ausschließlich berechtigte Personen des Auftragsverarbeiters über eingerichtete, verschlüsselte, Fernzugriffsverbindungen auf Systeme beim Auftraggeber zugreifen können, sind umgesetzt.Sollten Fernzugriffslösungen des Auftraggebers genutzt werden, informiert der Auftragsverarbeiter den Auftraggeber ehest über einen notwendigen Anpassungsbedarf an konfigurierten Zugriffsberechtigungen (z. B. Fernzugriffsberechtigte MitarbeiterInnen des Auftragsverarbeiters verlassen den Auftragsverarbeiter oder ändern ihren Zuständigkeitsbereich innerhalb des Auftragsverarbeiters). |
| [ ]  Ja | [ ]  Nein | bei „Nein“ bitte Begründung angeben |
| **AV****DL**2.15 | Maßnahmen zum sicheren Löschen von Datenträgern vor ihrer neuerlichen Verwendung oder Abgabe an Dritte sind umgesetzt. |
| [ ]  Ja | [ ]  Nein | bei „Nein“ bitte Begründung angeben |
| **AV****DL**2.16 | Maßnahmen zur sicheren physischen Vernichtung (z.B.: nach DIN 66399, ÖNORM S 2109) oder Beauftragung eines zertifizierten Dienstleisters für Akten- und Datenträgervernichtung sind umgesetzt.  |
| [ ]  Ja | [ ]  Nein | bei „Nein“ bitte Begründung angeben |
| **AV****DL**2.17 | Maßnahmen für das sichere Löschen gespeicherter Daten auf Smartphones, Tablets aus der Ferne sind umgesetzt. |
| [ ]  Ja | [ ]  Nein | bei „Nein“ bitte Begründung angeben |
| **AV****DL**2.18 | Maßnahmen zur Sicherstellung des datenschutzkonformen und IT sicheren Verhaltens von ArbeitnehmerInnen des Auftragsverarbeiters sind umgesetzt.Diese adressieren zumindest folgende Themen:* Sensibilität von personenbezogenen Daten und Umgang der ArbeitnehmerInnen mit diesen Daten;
* Sicherheitsbedrohungen für EndbenutzerInnen und die Reaktion darauf;
* Meldeverpflichtungen von Sicherheitsvorfällen und Datenschutzverletzungen
 |
| [ ]  Ja | [ ]  Nein | bei „Nein“ bitte Begründung angeben |
| **AV****DL**2.19 | Maßnahmen zur Absicherung der Konfiguration eingesetzter Datenverarbeitungssysteme / Applikationen gegen unberechtigten Zugriff, unter Berücksichtigung von: * Sicherheitsempfehlungen deren Hersteller und
* allgemeiner Sicherheitsempfehlungen und
* etwaiger Vorgaben des Auftraggebers und
* des Zwecks der beauftragten Datenverarbeitung

sind umgesetzt. (System Hardening). |
| [ ]  Ja | [ ]  Nein | bei „Nein“ bitte Begründung angeben |
| **AV****DL**2.20 | Sofern der Auftragsgegenstand die Entwicklung von Hardware- oder Softwarekomponenten umfasst, sind Maßnahmen zur sicheren Entwicklung von Hardware- oder Softwarekomponenten umgesetzt. |
| [ ]  Ja | [ ]  Nein | bei „Nein“ bitte Begründung angeben |

1. **Zugriffskontrolle**

Es ist sicherzustellen, dass die zur Nutzung eines Datenverarbeitungssystems befugte Person nur auf die Informationen in ihrem jeweiligen Zugriffsbereich zugreifen kann und dass keine Daten ohne entsprechende Berechtigung während der Verarbeitung oder Nutzung sowie nach der Speicherung gelesen, kopiert, geändert oder entfernt werden können; d.h. Berechtigungssysteme und Informationssicherheitsmaßnahmen sind zu entwickeln.

Die folgenden technischen und organisatorischen Maßnahmen sind für die vertragliche Erfassung, Verarbeitung und Nutzung von Daten durch den Auftragsverarbeiter zu implementieren:

|  |  |
| --- | --- |
| Nr. | **Zugriffskontrolle** - Mindest-Sicherheitsniveau erfüllt durch: |
| **AV****DL**3.1 | Maßnahmen für die Definition und zweckorientierte Zuweisung von Rollen und Berechtigungen anhand von Benutzerprofilen, basierend auf dem „Need-to-know-Grundsatz“, sind umgesetzt. |
| [ ]  Ja | [ ]  Nein | bei „Nein“ bitte Begründung angeben |
| **AV****DL**3.2 | Maßnahmen zur Minimierung der Anzahl der AdministratorInnen (beschränkt sich auf das "absolut notwendige Minimum") wurden ergriffen.  |
| [ ]  Ja | [ ]  Nein | bei „Nein“ bitte Begründung angeben |

1. **Sicherheit bei den übermittelten Daten**

Es ist sicherzustellen, dass keine verarbeiteten Daten während der elektronischen Übermittlung oder der Speicherung auf Datenträger von unbefugten Personen gelesen, kopiert, geändert oder entfernt werden können, und dass überprüft und festgelegt werden kann, wohin verarbeitete Daten zu übermittelt sind, d.h. die Modalität der Datenübermittlung ist zu regeln.

Die folgenden technischen und organisatorischen Maßnahmen sind für die vertragliche Erfassung, Verarbeitung und Nutzung von Daten durch den Auftragsverarbeiter zu implementieren:

|  |  |
| --- | --- |
| Nr. | **Sicherheit bei den übermittelten Daten-** Mindest-Sicherheitsniveau erfüllt durch: |
| **AV****DL**4.1 | Maßnahmen für die Verschlüsselung bei Datenübertragung im Internet oder Netzwerken, die sich nicht in der alleinigen Verfügungshoheit befinden (z. B. TLS, …), sind mittels sicherer kryptographischer Verfahren umgesetzt. |
| [ ]  Ja | [ ]  Nein | bei „Nein“ bitte Begründung angeben |
| **AV****DL**4.2 | Maßnahmen zur Sicherstellung, dass etwaige Datenübertragungen - manuell oder automationsunterstützt - ausschließlich an berechtigte, vom Verantwortlichen benannte Empfänger innerhalb zulässiger Zeiträume, durchgeführt werden, sind umgesetzt. |
| [ ]  Ja | [ ]  Nein | bei „Nein“ bitte Begründung angeben |
| **AV**4.3 | Maßnahmen zur manuellen oder automationsunterstützten Umsetzung vereinbarter Löschfristen von verarbeiteten Informationen und Daten sind umgesetzt (Adressierung des datenschutzrechtlich geforderten Prinzips der Speicherbegrenzung). |
| [ ]  Ja | [ ]  Nein | bei „Nein“ bitte Begründung angeben |

1. **Eingabekontrolle**

Es ist sicherzustellen, dass bei der Verwendung von elektronischen Datenverarbeitungssystemen im Nachhinein geprüft und festgestellt werden kann, ob und von wem Daten in eingegeben, geändert oder entfernt wurden (z. B. durch das Führen von Aufzeichnungen).

Die folgenden technischen und organisatorischen Maßnahmen sind vertraglich für die Erfassung, Verarbeitung und Nutzung von Daten durch den Auftragsverarbeiter zu implementieren:

|  |  |
| --- | --- |
| Nr. | **Eingabekontrolle** - Mindest-Sicherheitsniveau erfüllt durch: |
| **AV**5.1 | Maßnahmen zur Protokollierung der Einsichtnahme, Eingabe, Änderung oder Löschung von Daten sind umgesetzt. |
| [ ]  Ja | [ ]  Nein | bei „Nein“ bitte Begründung angeben |
| **AV**5.2 | Maßnahmen zur Nachverfolgbarkeit von Eingaben, Änderungen oder Löschungen von Daten durch individuelle Benutzernamen (nicht Benutzergruppen) sind umgesetzt. |
| [ ]  Ja | [ ]  Nein | bei „Nein“ bitte Begründung angeben |

1. **Verfügbarkeitskontrolle**

Es ist sicherzustellen, dass verarbeitete Informationen und Daten vor unabsichtlicher Zerstörung oder Verlust geschützt werden.

Die folgenden technischen und organisatorischen Maßnahmen sind für die vertragliche Erfassung, Verarbeitung und Nutzung von Informationen und Daten durch den Auftragsverarbeiter zu implementieren:

|  |  |
| --- | --- |
| Nr. | **Verfügbarkeitskontrolle** - Mindest-Sicherheitsniveau erfüllt durch: |
| **AV**6.1 | Maßnahmen für ein Sicherungs- und Wiederherstellungskonzept für verarbeitete personenbezogene Daten des Auftraggebers sind umgesetzt. |
| [ ]  Ja | [ ]  Nein | bei „Nein“ bitte Begründung angeben |
| **AV**6.2 | Maßnahmen für die Überprüfung der Wiederherstellung der Daten, unter Einhaltung etwaiger vom Auftraggeber vorgegebener Zeiten, sind umgesetzt. |
| [ ]  Ja | [ ]  Nein | bei „Nein“ bitte Begründung angeben |
| **AV**6.3 | Maßnahmen für die Klimatisierung und Steuerung der Luftfeuchtigkeit in Serverräumen sind umgesetzt.  |
| [ ]  Ja | [ ]  Nein | bei „Nein“ bitte Begründung angeben |
| **AV**6.4 | Maßnahmen zur Überwachung der Temperatur, Luftfeuchtigkeit oder anderer Messwerte in Serverräumen sind umgesetzt. |
| [ ]  Ja | [ ]  Nein | bei „Nein“ bitte Begründung angeben |
| **AV**6.5 | Maßnahmen für den vorbeugenden Brandschutz (Brandmeldeanlage) in Serverräumen sind umgesetzt. |
| [ ]  Ja | [ ]  Nein | bei „Nein“ bitte Begründung angeben |
| **AV**6.6 | Maßnahmen für geeignete Feuerlöscher oder eine Löschanlage in Serverräumen sind umgesetzt. |
| [ ]  Ja | [ ]  Nein | bei „Nein“ bitte Begründung angeben |
| **AV**6.7 | Maßnahmen zum Schutz von Serverräumen in Hochwassergebieten sind umgesetzt. |
| [ ]  Ja | [ ]  Nein | bei „Nein“ bitte Begründung angeben |
| **AV**6.8 | Maßnahmen für die Speicherung der gesicherten Daten in einem anderen Brandabschnitt oder an einem sicheren, externen Ort sind umgesetzt.  |
| [ ]  Ja | [ ]  Nein | bei „Nein“ bitte Begründung angeben |

1. **Separierung**

Es ist sicherzustellen, dass die für verschiedene Zwecke gesammelten unterschiedlichen Daten getrennt verarbeitet werden, d.h. es muss eine Funktionstrennung geben bzw. die Rechte für die Verarbeitung nur im unbedingten notwendigen Ausmaß vergeben werden (Separation of Duties). Diese Regel ist auch für Administratoren anzuwenden.

Die folgenden technischen und organisatorischen Maßnahmen sind für die vertragliche Erfassung, Verarbeitung und Nutzung von Daten durch den Auftragsverarbeiter zu implementieren:

|  |  |
| --- | --- |
| Nr. | **Separierung -** Mindest-Sicherheitsniveau erfüllt durch: |
| **AV****DL**7.1 | Maßnahmen die sicherstellen, dass verarbeitete Daten und Informationen einzelnen Auftraggebern zugeordnet werden können, sind umgesetzt. (Mandantenzuordnung) |
| [ ]  Ja | [ ]  Nein | bei „Nein“ bitte Begründung angeben |
| **AV****DL**7.2 | Maßnahmen die sicherstellen, dass Kunden nicht auf verarbeiteten Daten anderer Kunden (ohne deren Freigabe) zugreifen können, sind umgesetzt. (Mandantentrennung)  |
| [ ]  Ja | [ ]  Nein | bei „Nein“ bitte Begründung angeben |
| **AV**7.3 | Maßnahmen für die Festlegung der Datenbankrechte sind umgesetzt.  |
| [ ]  Ja | [ ]  Nein | bei „Nein“ bitte Begründung angeben |
| **AV**7.4 | Maßnahmen für die Trennung von Produktions- und Testdaten bei Produktiv-, Qualität- und / oder Test-Systemen sind umgesetzt.  |
| [ ]  Ja | [ ]  Nein | bei „Nein“ bitte Begründung angeben |

1. **Vorfalls- und Notfallmanagement**

Es ist sicherzustellen, dass für die auftretenden Datenschutzverletzungen geeignete Managementprozesse vorhanden sind.

Die folgenden technischen und organisatorischen Maßnahmen sind für die vertragliche Erfassung, Verarbeitung und Nutzung von Daten durch den Auftragsverarbeiter zu implementieren:

|  |  |
| --- | --- |
| Nr. | **Vorfalls- und Notfallsmanagement** - Mindest-Sicherheitsniveau erfüllt durch: |
| **AV****DL**8.1 | Maßnahmen zur Erkennung, Bewertung, Analyse und Behebung von Datenschutzverletzungen, sowie für eine fristgerechte Meldung an den Verantwortlichen, sind umgesetzt. |
| [ ]  Ja | [ ]  Nein | bei „Nein“ bitte Begründung angeben |
| **AV****DL**8.2 | Maßnahmen für die Überprüfung (z.B.: Audit, Simulation, …) des Notfall-Prozess sind umgesetzt. |
| [ ]  Ja | [ ]  Nein | bei „Nein“ bitte Begründung angeben |

1. **(Sicherheits-)Maßnahmen bei Beendigung des Auftragsverhältnisses**

Es ist sicherzustellen, dass nach Beendigung des Auftrages bzw. mit Wegfall des Grundes zur Datenverarbeitung, die entsprechenden Daten auch gelöscht werden.

Die folgenden technischen und organisatorischen Maßnahmen sind für die vertragliche Erfassung, Verarbeitung und Nutzung von Daten durch den Auftragsverarbeiter zu implementieren:

|  |  |
| --- | --- |
| Nr. | **Beendigung des Auftragsverhältnisses -** Mindest-Sicherheitsniveau erfüllt durch: |
| **AV****DL**9.1 | Übergabe der Daten/Verarbeitungsergebnisse an den Verantwortlichen |
| [ ]  Ja | [ ]  Nein | **Hinweis:** Beschreiben Sie bei **„Ja“** Ihr Vorgehen bzw. begründen Sie Ihr **„Nein“**. |
| **AV****DL**9.2 | Vernichtung der Daten/Verarbeitungsergebnisse beim Auftragsverarbeiter nach Beendigung des Auftragsverhältnisses  |
| [ ]  Ja | [ ]  Nein | **Hinweis:** Beschreiben Sie bei **„Ja“** Ihr Vorgehen bzw. begründen Sie Ihr **„Nein“**. |

# Anlage 4 – Zugelassene Offenlegungen

zu [VERTRAGSNUMMER/GZ]

Erklärung: Der Begriff „Offenlegung“ umfasst grundsätzlich die Bekanntgabe von gespeicherten oder durch Datenverarbeitung gewonnen personenbezogenen Daten an einen sonstigen „Dritten“ (z.B. Sub-Auftragsverarbeiter, Behörden, andere datenschutzrechtlich Verantwortliche). Eine „Offenlegung“ kann unabhängig von deren Form (z.B. mündlich, auf Papier, elektronisch, etc.) durch „Übermittlung“, „Verbreitung“, „das Einsehen lassen“ oder „eine andere Form der Bereitstellung“ erfolgen.

Grundsätzlich wird bei der Offenlegung an sonstige „Dritte“ unterschieden zwischen:

* Der Offenlegung von personenbezogenen Daten durch den Auftragsverarbeiter an Dritte im Auftrag des Verantwortlichen
* Der Offenlegung von personenbezogenen Daten durch den Auftragsverarbeiter an dessen Sub-Auftragsverarbeiter

**Offenlegung an folgende Dritte - im Auftrag des Verantwortlichen:**

[ ]  Es erfolgt keine Datenweitergabe an Dritte.

[ ]  Es erfolgt eine Datenweitergabe an folgende Dritte:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Nr.** | **Firmenname und Anschrift** | **Zweck der Offenlegung (Beschreibung der Verarbeitung)**  | **Empfänger-land** | **Außerhalb EWR:Geeignete Garantien**  |
| 1 |  |  |  | [ ]  Angemessenheits-beschluss der EU-Kommission[ ]  genehmigte Binding Corporate Rules[ ]  Standarddatenschutz-klauseln (aktuelle Version) |
| 2 |  |  |  | [ ]  Angemessenheits-beschluss der EU-Kommission[ ]  genehmigte Binding Corporate Rules[ ]  Standarddatenschutz-klauseln (aktuelle Version) |

**Sub-Auftragsverarbeiter:**

[ ]  Es werden keine Sub-Auftragsverarbeiter eingesetzt.

[ ]  Es erfolgt eine Datenweitergabe an folgende Sub-Auftragsverarbeiter:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Nr.** | **Firmenname und Anschrift** | **Zweck der Offenlegung (Beschreibung der Verarbeitung)**  | **Empfänger-land** | **Außerhalb EWR:Geeignete Garantien**  |
| 1 |  |  |  | [ ]  Angemessenheits-beschluss der EU-Kommission[ ]  genehmigte Binding Corporate Rules[ ]  Standarddatenschutz-klauseln (aktuelle Version) |
| 2 |  |  |  | [ ]  Angemessenheits-beschluss der EU-Kommission[ ]  genehmigte Binding Corporate Rules[ ]  Standarddatenschutz-klauseln (aktuelle Version) |

1. VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung). [↑](#footnote-ref-1)