Vertragsnummer/GZ: [VERTRAGSNUMMER/GZ]

DATENSCHUTZVERTRAG - Vertrag über die Verarbeitung personenbezogener Daten im Auftrag

Zwischen der

XXXXXXXXXXXXXXXXXXXXXXXXXXX

als Verantwortliche nach Art. 4 Z 7 DSGVO[1], nachfolgend kurz als **Verantwortlicher** bezeichnet,

und der

[NAME DER NATÜRLICHEN PERSON oder NAMENSBEZEICHNUNG NACH FIRMENBUCH, FIRMENBUCHNUMMER]

[UID NUMMER]

[ANSCHRIFT]

als Auftragsverarbeiter/in nach Art. 4 Z 8 DSGVO, nachfolgend kurz als **Auftragsverarbeiter** bezeichnet,

Angabe der Kontaktdaten der/des datenschutzrechtlichen Ansprechpartners des Verantwortlichen:

_____

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

[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).

1 Einleitung, Geltungsbereich und -dauer, Definitionen

(1) Verantwortlicher und Auftragsverarbeiter stehen in einer Vertragsbeziehung.

(2) Der 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 unbefristet auf alle Tätigkeiten Anwendung, bei denen der Auftragsverarbeiter, Mitarbeiter des Auftragsverarbeiters oder durch ihn zulässigerweise beauftragte Unter-Auftragsverarbeiter (Sub-Auftragsverarbeiter, Punkt 5) personen-bezogene Daten im Auftrag des Verantwortlichen verarbeiten.

(4) In diesem Vertrag verwendete Begriffe sind entsprechend ihrer Definition in der EU Datenschutz-Grundverordnung (DSGVO) zu verstehen.

2 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.

3 Pflichten des Auftragsverarbeiters

(1) Sofern im Folgenden keine ausdrückliche Einschränkung auf personenbezogene Daten erfolgt, beziehen sich die nachfolgend genannten Verpflichtungen des Auftragsverarbeiters auf sämtliche vom Verantwortlichen übermittelten Daten, über welche der Auftragsverarbeiter nicht oder nicht alleine verfügen darf.

(2) Der Auftragsverarbeiter verarbeitet personenbezogene Daten einschließlich Verarbeitungsergebnisse ausschließlich im Rahmen der Aufträge bzw. Weisungen 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 hinausgehenden Verarbeitung der Daten des Verantwortlichen verpflichtet ist oder wird, ist der Verantwortliche darüber vor der Verarbeitung nachweislich zu informieren.

(3) 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[2], sofern diese nicht einer angemessenen gesetzlichen Verschwiegenheitspflicht im Sinne von Art. 28 Abs. 3 lit. b DSGVO und § 6 DSG (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.

[2] Eine Verpflichtung hierzu im Rahmen des Dienstvertrages wird, sofern der gesetzliche Mindestinhalt eingehalten wird, als ausreichend betrachtet.

Bestehen Zweifel, ob eine Information der Geheimhaltungspflicht unterliegt, ist sie bis zur schriftlichen Freigabe durch die andere Partei als vertraulich zu behandeln.

(4) 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 Datenschutzfolgeabschätzung, unter Berücksichtigung der dem Auftragsverarbeiter zur Verfügung stehenden Informationen, zu unterstützen.

(5) 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 (innerhalb der gesetzlichen Fristen) reibungslos nachkommen kann (Art. 28 Abs. 3 lit. e DSGVO).

(6) Wird der Verantwortliche durch Datenschutzbehörde 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 Zusammenhangmit mit dem Auftrag steht.

(7) Die Auftragsverarbeitung erfolgt ausschließlich innerhalb des EWR. Jegliche Verlagerung in ein Drittland darf nur mit schriftlicher Zustimmung des Verantwortlichen (siehe Anlage 2) und unter den im Kapitel V der DSGVO enthaltenen Bedingungen erfolgen.

(8) Ist der Auftragsverarbeiter nicht in der Europäischen Union niedergelassen, bestellt er einen verantwortlichen Ansprechpartner in der Europäischen Union gemäß Art. 27 DSGVO. Die Kontaktdaten des Ansprechpartners sowie sämtliche Änderungen in der Person des Ansprechpartners sind dem Verantwortlichen unverzüglich und nachweislich mitzuteilen.

4 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 vorgesehenen Sicherheitsmaßnahmen können durch genehmigte Verhaltensregeln oder ein genehmigtes und geeignetes Zertifizierungsverfahren – mittels Vorlage des jeweiligen Zertifikates - erbracht werden (siehe Anlage 3). Liegt ein derartiger Nachweis nicht ausreichend vor, ist die Anlage 3 (Punkte 1-8) auszufüllen. Die darin vorgesehenen Datensicherheitsmaßnahmen werden verbindlich festgelegt. Sie sind regelmäßig an den jeweils aktuellen technischen Stand anzupassen und 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.

Kopien der Datenbestände (partiell oder gesamt) des Verantwortlichen dürfen nur dann erstellt werden, wenn sie für die Erfüllung des Auftrags tatsächlich notwendig sind. Alle anderen Kopien bedürfen der nachweislichen Genehmigung des Verantwortlichen.

5 Sub-Auftragsverhältnisse

Als Subauftragsverhältnisse im Sinne dieser Regelung sind nur solche Dienstleistungen zu verstehen, die unmittelbar in der Erbringung der Hauptleistung bestehen. Nicht hierzu gehören Nebenleistungen, welche nur mittelbaren Einfluss auf die Gesamtvertragsleistung beziehungsweise das gewünschte Ergebnis haben (z.B.: HW- oder SW-Wartungsverträge). Insbesondere gelten nicht als Subauftragsverarbeiter Personen, welche unter unmittelbaren Anleitung und Verantwortung des Auftragsverarbeiters ihre Leistung erbringen (Erfüllungsgehilfen des Auftragsverarbeiters).

(1) Die Beauftragung eines weiteren Auftragsverarbeiters (Sub-Auftragsverarbeiter) durch den Auftragsverarbeiter ist nur mit schriftlicher Genehmigung des Verantwortlichen zulässig. Der Auftragsverarbeiter hat den Verantwortlichen von der beabsichtigten Heranziehung eines Sub-Auftragsverarbeiters so rechtzeitig zu verständigen, dass der Verantwortliche dies im Einklang mit Art. 28 Abs. 2 DSGVO allenfalls untersagen kann. 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.

(2) Die Verbindlichkeit der Bestimmungen dieses Datenschutzvertrages ist zwischen Auftragsverarbeiter und dem Sub-Auftragsverarbeiter schriftlich zu vereinbaren (Art. 28 Abs. 4 DSGVO). Der Verantwortliche erhält auf Verlangen Einsicht in die relevanten Verträge zwischen dem Auftragsverarbeiter und Sub-Auftragsverarbeiter.

(3) Die Verantwortlichkeiten des Auftragsverarbeiters und des Sub-Auftragsverarbeiter sind eindeutig voneinander abzugrenzen.

(4) Zum Zeitpunkt des Vertragsabschlusses sind die in Anlage 2 (Punkt „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.

6 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) Den mit der Kontrolle betrauten Personen ist vom Auftragsverarbeiter, soweit erforderlich und im notwendigen Umfang Zutritt und Einblick, zu ermöglichen.

(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 tunlichst ohne vermeidbare Störungen des Geschäftsbetriebs zu erfolgen. Soweit nicht vom Verantwortlichen zu dokumentierenden, aus dringlichen Gründen anders angezeigt, finden Kontrollen nach angemessener Vorankündigung und zu Geschäftszeiten des Auftragsverarbeiters statt.

7 Mitteilungspflichten

(1) Der Auftragsverarbeiter hat den Verantwortlichen im Falle einer Verletzung des Schutzes personenbezogener Daten unverzüglich und nachweislich zu verständigen, jedenfalls binnen 24 Stunden, nachdem die Verletzung dem Auftragsverarbeiter bekannt wurde. 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).

(4) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich von Kontrollen oder Maßnahmen von Datenschutzbehörden oder anderen Dritten, soweit diese Bezüge zur Auftragsverarbeitung aufweisen.

(5) 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 und 34 DSGVO im erforderlichen Umfang zu unterstützen.

(6) Sämtliche in diesem Abschnitt enthaltenen Pflichten sind auch auf allfällige Sub-Auftragsverarbeiter zu überbinden.

8 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 Z 1 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. 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 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.

9 Haftung

Der Auftragsverarbeiter haftet für den Ersatz von Schäden, die dem Verantwortlichen aufgrund von Verstößen des Auftragsverarbeiters bzw. dessen Sub-Auftragsverarbeitern gegen Datenschutzvorschriften oder diesen Datenschutzvertrag entstanden sind und hält diesbezüglich den Verantwortlichen schad- und klaglos. *Für den Fall eines Verstoßes wird eine Konventionalstrafe von € 5.000,00 pro Fall vereinbart*.

10 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, in erheblichem Maße 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 im Sinne von Abs. 1 berechtigt.

(4) Der Auftragsverarbeiter hat dem Verantwortlichen alle Kosten zu erstatten, die diesem durch die vorzeitige Beendigung dieses Datenschutzvertrages in Folge der berechtigten Wahrnehmung dieses Sonderkündigungsrechts entstehen.

11 Sonstiges

(1) Änderungen oder Ergänzungen des vorliegenden Vertrages bedürfen der Schriftform. Es bestehen keine mündlichen Nebenabreden.

(2) Sollten einzelne Teile dieses Vertrages unwirksam sein, so berührt dies die Wirksamkeit der übrigen Vereinbarung nicht.

(3) Dieser Datenschutzvertrag ersetzt allfällige frühere Datenschutzverträge.

12 Unterschriften

Ort, am 15. Juli 2019	Ort, Datum
.....	.....
Verantwortlicher	Auftragsverarbeiter

Anlage 1

zu [VERTRAGSNUMMER/GZ]Bezeichnung der Verarbeitungstätigkeit und ggf. betroffene Systeme (z.B. ERP) samt **Zweck**:

- ☐ **Fernzugriff (SW-Fehleranalyse und -Fehlerbehebung)**
- ☐ **Fernzugriff (Wartung des Programmes, SW-Updates)**
- ☐ **SW-Fehleranalyse und -behebung vor Ort**
- ☐ **Wartung des Programmes / Installation von Updates vor Ort**
- ☐ **SW-Fehleranalyse bei der/beim Auftragsverarbeiter aufgrund des übergebenen Datenträgers**
- ☐ **Tausch von defekten HW-Teilen**
- ☐ **Beseitigung von Störungen, Wiederherstellung der Funktionsfähigkeit der HW**
- ☐ **Beratungsleistungen**
- ☐ **Schulung der Nutzerinnen und Nutzer**
- ☐ **Helpdesk-Dienste**
- ☐ **Sonstige Verarbeitungstätigkeiten: ……...**

(Beschreibung der Verarbeitungstätigkeit: stichwortartig, aber dennoch so detailliert, dass ein unbeteiligter Dritte erkennen kann, worum es sich handelt, z.B. „Durchführung der Lohn- und Gehaltsabrechnung“ oder „Betrieb des CRM des Verantwortlichen in Form von Software als ein Service im Rechenzentrum des Auftragnehmers“.)

Anlage 2

zu [VERTRAGSNUMMER/GZ]

Offen gelegte Daten

(zutreffendes in Folge ankreuzen/ergänzen)

Kategorien der betroffenen Personen

Von der Verarbeitung betroffen sind:

Bewerber, Dienstnehmer und Funktionsträger (Verwaltungskörper und Beiräte), Sitzungsteilnehmer der Datenschutzbehörden bzw. des Bundesministeriums für Finanzen (Personaldaten)	
Mitarbeiter/Kontaktpersonen der Kunden oder Lieferanten des Auftragsverarbeiters (Empfänger und Erbringer von Lieferungen oder Leistungen)	

Versicherte, Leistungsempfänger	
Vertragspartner (Ärzte, Apotheken, etc), Dienstgeber, Vertreter	
Patienten	
Sonstige: _____	

Datenarten

Es werden folgende Datenarten verarbeitet:

Identitätsdaten (wie Namen, akad. Grade, Geburtsdaten, Geburtsort, Sterbedatum, Geschlecht, Familienstand, Staatsbürgerschaft, Kfz-Kennzeichen, Stellplatz-Nr, Zufahrtsbereich etc.)	
Organisations-/Unternehmensdaten (wie Sitz, Betriebsort, Rechtsform, Geschäftszweig, Fachsektionen, Wirtschaftsklassen, Berufsgruppen, Gründungs- und Auflösungsdaten, Scheinunternehmensdaten, Kammermitgliedschaften, etc.).	
Erreichbarkeitsdaten (wie Adressen, inkl. Abgabestellen, elektr. Postfächer, Tel.Nr., Mail-Adressen, IP-Adressen, Fax-Nr., etc.).	
arbeitsrechtliche Personalverwaltungsdaten (wie Tätigkeitsbereiche, Funktionsumfang, Ausbildung, Dienst-/Versicherungszeiten, Berechnungs-/Beitragsgrundlagen, etwaiger Behindertenstatus, Bezüge, Kurienzugehörigkeit, Gewerkschaftszugehörigkeit bei Direktverrechnung, Mitarbeitervorsorge- und Pensionskassendaten, zuständiger Sozialversicherungsträger, Bewerberdaten etc.).	
Abrechnungsdaten (wie Bankdaten, Geldadress- & Abbuchungsvereinbarungen, Zeichnungsberechtigungen, Beitragskontonummern, Insolvenzdaten, Leistungsabrechnungen, Honorare, Tarife).	
Angehörigen- & Vertretungs-(Vollmachts-) & Partnerbeziehungen (wie Erwachsenenvertreter, Kuratoren, Konzerne, Pächter, Erben, Gesellschafter, etc.	
Personenkennzeichen (wie SVNR, EKVK-Nummer, UID-, Steuer-, Kammer-, Firmenbuch-, LKF-Code, Steuernummer, bPK, in- und ausländische Betreuungsnummern, etc.).	
Meldende Stellen.	
Regressdaten (z.B. Angaben zu Schädiger, Schaden, Schadenshöhe, zuständige Haftpflicht-Versicherung, etc.).	
Vertragsdaten (z.B. Zeitraum, Fachgebiet, Befähigungen, Angebote, Nachlässe etc.).	
Patientendaten (z. B. behandelnde Einrichtung, Sterbedaten (diese sind oben unter Identifikationsdaten enthalten), Anamnesedaten, Gesundheitszustand, Indikation, etc.).	
Sonstige: _____	

Weitergabe von Daten an (zugelassene) Sub-Auftragsverarbeiter

Es erfolgt eine Weitergabe (Offenlegung) personenbezogener Daten durch den Auftragsverarbeiter an (Bezeichnung/Kontaktdaten/Auftragsinhalt):

Weitergabe von Daten ins EWR Ausland

Es erfolgt eine Weitergabe (Offenlegung) personenbezogener Daten durch den Auftragsverarbeiter (unter anderem im Rahmen von Remotezugängen/Servicedesk-leistungen) an:

Bezeichnung

Anlage 3

zu [VERTRAGSNUMMER/GZ]

Der Nachweis über das Vorliegen angemessener technischer und organisatorischer Maßnahmen kann wie folgt erbracht werden:

Die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO wird nachgewiesen: Welche:	
Eine Zertifizierung nach einem genehmigten Zertifizierungsverfahren gem. Art. 42 DS-GVO liegt vor. Welche:	
Aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen nach gängigen Standards liegen vor (z.B. Wirtschaftsprüfer, externe Datenschutzauditoren, Qualitätsauditoren) Welche:	
Eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudits (z.B. nach BSI-Grundschutz, ISO 27001) liegt vor. Welche: Der konkrete Zertifizierungsumfang ist dem Vertrag als Anlage 3a beizuschließen.	
Sonstige detaillierte Aufschlüsselung getroffener Sicherheitsmaßnahmen (zB: Link auf eigene WebSite): LINK:	

Falls keiner der oben angeführten allgemeinen Nachweise vorliegt bzw. diese vom Verantwortlichen nicht akzeptiert werden, sind die nachfolgenden Fragen auszufüllen:

1. Zutrittskontrolle (physisch)

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

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

Nr.	JA	NEIN	nicht notwendig	Mindest-Sicherheitsniveau erfüllt durch: (ACHTUNG: Wenn „NEIN“ und „nicht notwendig“ ausgefüllt wird, ist eine Begründung anzugeben.)
1.1	☐	☐	☐	Maßnahmen für eine Alarmierung in kritischen Bereichen sind vorhanden
	Begründung:			
1.2	☐	☐	☐	Maßnahmen für manuelle Schließanlage mit Regelungen für die Schlüsselverwaltung (Schlüsselregistrierung, Schlüsselverteilungssystem) sind vorhanden
	Begründung:			

1.3	☐	☐	☐	Maßnahmen für Besucherregistrierung sind vorhanden
	Begründung:			
1.4	☐	☐	☐	Maßnahmen für ein elektronische Schließsystem mit Chipkarte/Transponder sind für sensible Bereiche vorhanden
	Begründung:			
1.5	☐	☐	☐	Maßnahmen für die Sorgfältige Auswahl und Unterweisung der Reinigungskräfte, Haustechnikkräfte, … sind vorhanden
	Begründung:			

2. Zugangskontrolle (logisch)

Jede Verwendung von Datenverarbeitungssystemen durch unbefugte Personen ist zu verhindern, d.h. der logische Zugang zu diesen IKT-Systemen ist zu regeln.

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

Nr.	JA	NEIN	nicht not-wendig	Mindest-Sicherheitsniveau erfüllt durch: (ACHTUNG: Wenn „NEIN“ und „nicht notwendig“ ausgefüllt wird, ist eine Begründung anzugeben.)
2.1	☐	☐	☐	Maßnahmen für die Authentifizierung mit Benutzername / Passwort (Passwortvergabe basiert auf gültigen Passwortregelungen) sind vorhanden
	Begründung:			
2.2	☐	☐	☐	Maßnahmen für die Verwendung von aktueller Antiviren-Software sind vorhanden
	Begründung:			
2.3	☐	☐	☐	Maßnahmen für die Verwendung einer aktuellen Firewall-Version am Perimeter oder/und zwischen anderen Netzwerken sind vorhanden (Regelsatz: es ist alles verboten, was nicht erlaubt ist)
	Begründung:			
2.4	☐	☐	☐	Maßnahmen zum Erstellen von Benutzerprofilen sind vorhanden
	Begründung:			

2.5	☐	☐	☐	Maßnahmen für die Verschlüsselung von mobilen Datenträgern sind vorhanden
	Begründung:			
2.6	☐	☐	☐	Maßnahmen für die Verschlüsselung von Datenträgern in Laptops / Notebooks sind vorhanden
	Begründung:			
2.7	☐	☐	☐	Maßnahmen für eine zentrale Smartphone-Verwaltungssoftware (z.B. für externes Löschen von Daten) sind vorhanden
	Begründung:			

3. 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 personenbezogenen 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 persönlichen Daten durch den Auftragsverarbeiter zu implementieren:

Nr.	JA	NEIN	nicht not-wendig	Mindest-Sicherheitsniveau erfüllt durch: (ACHTUNG: Wenn „NEIN“ und „nicht notwendig“ ausgefüllt wird, ist eine Begründung anzugeben.)
3.1	☐	☐	☐	Maßnahmen für den Einsatz von Rollen und Berechtigungen nach dem "Need-to-know-Grundsatz" sind vorhanden
	Begründung:			
3.2	☐	☐	☐	Maßnahmen zur Minimierung der Anzahl der Administratoren (beschränkt sich auf das "absolut notwendige Minimum") sind vorhanden
	Begründung:			
3.3	☐	☐	☐	Maßnahmen zur Protokollierung der Zugriffe auf Anwendungen, Eingabe, Änderung und Löschen von Daten sind vorhanden
	Begründung:			

3.4	☐	☐	☐	Maßnahmen zum sicheren Löschen von Datenträgern vor ihrer neuerlichen Verwendung sind vorhanden
	Begründung:			
3.5	☐	☐	☐	Maßnahmen zur Physischen Vernichtung (z.B.: nach DIN 66399) oder Beauftragung eines entsprechenden Dienstleisters sind vorhanden
	Begründung:			
3.6	☐	☐	☐	Maßnahmen zur Verwaltung von Rechten durch vorgegebene Systemadministratoren oder/und einen Identitätsmanagement-System über einen definierten Prozess sind vorhanden
	Begründung:			
3.7	☐	☐	☐	Maßnahmen für eine Passwort-Richtlinie, die die Komplexität, die Länge sowie die Gültigkeitsdauer des Passworts bzw. die Authentifizierung über 2 Faktor und/oder biometrische Methoden definiert, sind vorhanden
	Begründung:			
3.8	☐	☐	☐	Maßnahmen zur sicheren Aufbewahrung (verschließbare Schränke und Schubladen, Datensafe, …) von Datenträgern nach der Kritikalität der gespeicherten Daten sind vorhanden
	Begründung:			
3.9	☐	☐	☐	Maßnahmen zur Speicherung der Daten an einem sicheren Ort entsprechend der Klassifizierung der Daten und/oder deren Verschlüsselung sind vorhanden
	Begründung:			

4. Überlassungskontrolle

Es ist sicherzustellen, dass keine personenbezogenen 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 personenbezogene 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 persönlichen Daten durch den Auftragsverarbeiter zu implementieren:

Nr.	JA	NEIN	nicht notwendig	Mindest-Sicherheitsniveau erfüllt durch: (ACHTUNG: Wenn „NEIN“ und „nicht notwendig“ ausgefüllt wird, ist eine Begründung anzugeben.)
4.1	☐	☐	☐	Maßnahmen für die Verschlüsselung bei Datenübertragung im Internet oder Netzwerken, die sich nicht in der alleinigen Verfügungshoheit befinden (z.B. TLS, …) mittels sicherer kryptographischer Verfahren (lt. Stand der Technik) sind vorhanden
	Begründung:			
4.2	☐	☐	☐	Maßnahmen zur halb- oder vollautomatischen Identifikation der Datenempfänger, zur halb- oder vollautomatischen Überprüfung der Zeiträume der geplanten Übermittlungen und zur Umsetzung der halb- oder vollautomatischen vereinbarten Löschfristen sind vorhanden
	Begründung:			

5. Eingabekontrolle

Es ist sicherzustellen, dass im Nachhinein geprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in die Datenverarbeitungssysteme 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 persönlichen Daten durch den Auftragsverarbeiter zu implementieren:

Nr.	JA	NEIN	nicht notwendig	Mindest-Sicherheitsniveau erfüllt durch: (ACHTUNG: Wenn „NEIN“ und „nicht notwendig“ ausgefüllt wird, ist eine Begründung anzugeben.)
5.1	☐	☐	☐	Maßnahmen zur Protokollierung von Eingaben, Änderungen oder Löschen von Daten sind vorhanden
	Begründung:			
5.2	☐	☐	☐	Maßnahmen zur Nachverfolgbarkeit von Eingaben, Änderungen oder Löschen von Daten durch individuelle Benutzernamen (nicht Benutzergruppen) sind vorhanden
	Begründung:			
5.3	☐	☐	☐	Maßnahmen zur Vergabe von Rechten für das Eingeben, Ändern oder Löschen von Daten auf der Grundlage eines Berechtigungskonzepts sind vorhanden
	Begründung:			

5.4	☐	☐	☐	Maßnahmen für das Führen einer Übersichtsliste, unter Angabe mit welchen Applikationen welche Daten eingegeben, geändert oder gelöscht werden können, sind vorhanden
	Begründung:			

6. Verfügbarkeitskontrolle

Es ist sicherzustellen, dass personenbezogene Daten vor unabsichtlicher Zerstörung oder Verlust geschützt werden.

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

Nr.	JA	NEIN	nicht not-wendig	Mindest-Sicherheitsniveau erfüllt durch: (ACHTUNG: Wenn „NEIN“ und „nicht notwendig“ ausgefüllt wird, ist eine Begründung anzugeben.)
6.1	☐	☐	☐	Maßnahmen für die Klimatisierung in Serverräumen sind vorhanden
	Begründung:			
6.2	☐	☐	☐	Maßnahmen für Geräte zur Überwachung der Temperatur, Luftfeuchtigkeit oder anderer Messwerte in Serverräumen sind vorhanden
	Begründung:			
6.3	☐	☐	☐	Maßnahmen für den vorbeugenden Brandschutz (Brandmeldeanlage) in Serverräumen sind vorhanden
	Begründung:			
6.4	☐	☐	☐	Maßnahmen für geeignete Feuerlöscher oder Löschanlage in Serverräumen sind vorhanden
	Begründung:			
6.5	☐	☐	☐	Maßnahmen für ein Sicherungs- und Wiederherstellungskonzeptes sind vorhanden
	Begründung:			
6.6	☐	☐	☐	Maßnahmen für die Überprüfung der Wiederherstellung der Daten in der definierten Zeit sind vorhanden
	Begründung:			

6.7	☐	☐	☐	geeignete organisatorische Maßnahmen für ein PATCH-Management sind vorhanden
	Begründung:			
6.8	☐	☐	☐	Maßnahmen für die Speicherung der gesicherten Daten in einem anderen Brandabschnitt oder an einem sicheren, externen Ort
	Begründung:			
6.9	☐	☐	☐	Maßnahmen zum Schutz von Serverräume in Hochwassergebieten sind vorhanden
	Begründung:			

7. Separierungsregel

Es ist sicherzustellen, dass die für verschiedene Zwecke gesammelten unterschiedlichen Daten getrennt verarbeitet werden, d.h. wenn der Grund zur Datenverarbeitung nicht mehr besteht, können und müssen die entsprechenden Daten auch gelöscht werden.

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

Nr.	JA	NEIN	nicht not-wendig	Mindest-Sicherheitsniveau erfüllt durch: (ACHTUNG: Wenn „NEIN“ und „nicht notwendig“ ausgefüllt wird, ist eine Begründung anzugeben.)
7.1	☐	☐	☐	Maßnahmen für die Festlegung der Datenbankrechte sind vorhanden
	Begründung:			
7.2	☐	☐	☐	Maßnahmen für die Trennung der Zugriffsrechte auf verschiedene Mandanten sind vorhanden
	Begründung:			
7.3	☐	☐	☐	Maßnahmen für die Trennung von Produktiv-, Qualität- und/oder Test-System sind vorhanden
	Begründung:			

8. 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 persönlichen Daten durch den Auftragsverarbeiter zu implementieren:

Nr.	JA	NEIN	nicht not-wendig	Mindest-Sicherheitsniveau erfüllt durch: (ACHTUNG: Wenn „NEIN“ und „nicht notwendig“ ausgefüllt wird, ist eine Begründung anzugeben.)
8.1	☐	☐	☐	Maßnahmen zur Erkennung, Bewertung und Behebung von Datenschutzverletzungen sind vorhanden
	Begründung:			
8.2	☐	☐	☐	Maßnahmen für die Überprüfung (z.B.: Audit, Simulation, …) des Notfall-Prozess sind vorhanden
	Begründung:			

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