Vertragsnummer/GZ:

DATENSCHUTZVERTRAG

Dienstleister/Auftragnehmer

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 **Auftraggeber** bezeichnet,

und

Firmenbuchnummer:

UID:

nachfolgend kurz als **Auftragnehmer** bezeichnet,

gemeinsam in der Folge „Vertragsparteien“ bzw. einzeln „Vertragspartei“.

# Einleitung, Geltungsbereich, Definitionen

1. Auftraggeber und Auftragnehmer stehen in einer Vertragsbeziehung.
2. Dieser nun vorliegende Datenschutzvertrag regelt die datenschutzrechtlichen Rechte und Pflichten des Auftraggebers und des Auftragnehmers im Rahmen ihrer Vertragsbeziehung.
3. Dieser Vertrag findet auf alle Tätigkeiten Anwendung, bei denen der Auftragnehmer, Mitarbeiter des Auftragnehmers oder durch ihn zulässigerweise beauftragte Sub- Auftragnehmer (siehe Punkt 4) im Rahmen der Vertragsbeziehung Kenntnis von personenbezogenen Daten des Auftraggebers erlangen.
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.

# Pflichten des Auftragnehmers

1. Der Auftragnehmer verpflichtet sich, seine Leistungen ausschließlich im Rahmen des Auftrags und der Anweisungen des Auftraggebers zu erbringen. Der Auftragnehmer darf Daten des Auftraggebers nur insoweit verwenden, als dies zum Zwecke der Erfüllung seiner vertraglichen Verpflichtungen notwendig ist. Eine Verwendung von Daten des Auftraggebers für eigene Zwecke des Auftragnehmers ist ausgeschlossen.
2. Der Auftragnehmer verpflichtet sich, personenbezogene Daten sowie sonstige Informationen des Auftraggebers (wie etwa Geschäfts- und Betriebsgeheimnisse) die ihm im Zusammenhang mit der Vertragsbeziehung zur Kenntnis gelangen, streng vertraulich zu behandeln und diese Verpflichtung vertraglich allen Personen zu überbinden, die für ihn im Rahmen des Vertragsverhältnisses zwischen den Vertragsparteien tätig werden, sofern diese nicht einer angemessenen gesetzlichen Verschwiegenheitspflicht ([§ 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 beauftragten Personen auch nach Beendigung ihrer Tätigkeit bzw. Ausscheiden beim Auftragnehmer aufrecht.

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

Die mit der Dienstleistung 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 Auftragnehmer hat die vertraglichen Verpflichtungserklärungen zum Datengeheimnis dem Auftraggeber auf dessen Verlangen vorzulegen.

1. Der Auftragnehmer wird Anfragen von betroffenen Personen, soweit diese Bezüge zur Vertragsbeziehung zwischen den Vertragsparteien aufweisen, unverzüglich an den Auftraggeber weiterleiten. Der Auftragnehmer hat die technischen und organisatorischen Voraussetzungen dafür zu treffen, dass der Auftraggeber 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/)).
2. Wird der Auftraggeber durch Aufsichtsbehörden oder andere hierzu berechtigte Stellen einer Kontrolle unterzogen oder machen betroffene Personen ihm gegenüber Rechte geltend, verpflichtet sich der Auftragnehmer, den Auftraggeber im erforderlichen Umfang zu unterstützen.
3. Die Dienstleistung wird ausschließlich innerhalb des EWR erbracht. Jegliche Verlagerung in ein Drittland darf ausschließlich nach vorheriger schriftlicher Genehmigung des Auftraggebers sowie im Einklang mit Art 44 ff DSGVO erfolgen.

# Technische und organisatorische Maßnahmen

1. Der Auftragnehmer 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 des Auftraggebers 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 Auftragnehmer 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 Auftragnehmer geschuldete Minimum. Dieses Niveau darf nicht unterschritten werden.
3. Auf Aufforderung hat der Auftragnehmer dem Auftraggeber 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. Der Auftragnehmer darf Datenbestände des Auftraggebers nur insoweit in seine eigene Sphäre verbringen und Kopien der Datenbestände (partiell oder gesamt) des Auftraggebers nur insoweit erstellen, als dies für die Erfüllung der vertragsgegenständlichen Leistungen des Auftragnehmers tatsächlich notwendig ist. Alle anderen Kopien von Daten bedürfen der schriftlichen Genehmigung des Auftraggebers. Der Auftragnehmer hat Daten des Auftraggebers unwiederbringlich zu löschen, sobald diese zur Erreichung des Zwecks nicht mehr erforderlich sind, spätestens jedoch nach Beendigung des jeweiligen Auftrags.

# 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 Auftragnehmers (Sub-Auftragnehmer) durch den Auftragnehmer ist nur mit vorheriger gesonderter oder allgemeiner schriftlicher Genehmigung des Auftraggebers zulässig. Im Falle einer allgemeinen schriftlichen Genehmigung informiert der Auftragnehmer den Auftraggeber immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder Ersetzung anderer Auftragnehmer, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben. Darüber hinaus stellt der Auftragnehmer sicher, dass der Auftraggeber dem Sub-Auftragnehmer auch direkt Weisungen erteilen kann, sofern dies aus datenschutzrechtlicher Sicht erforderlich ist.
3. Die Verbindlichkeit der Bestimmungen dieses Datenschutzvertrages ist zwischen Auftragnehmer und dem Sub-Auftragnehmer schriftlich zu vereinbaren ([Art 28 Abs 4 DSGVO](https://dsgvo-gesetz.de/art-28-dsgvo/)). Der Auftraggeber erhält auf Verlangen Einsicht in die relevanten Verträge zwischen dem Auftragnehmer und Sub- Auftragnehmer.
4. Die Verantwortlichkeiten des Auftragnehmers und des Sub-Auftragnehmers sind eindeutig voneinander abzugrenzen.
5. Zum Zeitpunkt des Vertragsabschlusses sind die in Anlage 4 („Zugelassene Sub- Auftragnehmer“) mit Namen, Anschrift und Auftragsinhalt angeführten Sub- Auftragnehmer durch den Auftraggeber genehmigt.

# Rechte und Pflichten des Auftraggebers

1. Der Auftraggeber ist berechtigt, die Einhaltung der Vorschriften über den Datenschutz und die Datensicherheit beim Auftragnehmer 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 Auftragnehmer hat dafür Sorge zu tragen, dass einer zweckmäßigen Kontrolle durch den Auftraggeber oder einem von diesem beauftragten Dritten keine Geschäfts- und Betriebsgeheimnisse entgegenstehen.
3. Der Auftragnehmer ist verpflichtet, erforderliche Auskünfte zu erteilen, Abläufe zu demonstrieren und Nachweise zu führen, die zur Durchführung einer Kontrolle erforderlich sind.
4. Kontrollen beim Auftragnehmer haben ohne vermeidbare Störungen des Geschäftsbetriebs zu erfolgen. Soweit nicht aus vom Auftraggeber zu dokumentierenden, dringlichen Gründen anders angezeigt, finden Kontrollen nach angemessener Vorankündigung und zu Geschäftszeiten des Auftragnehmers statt.

# Mitteilungspflichten

1. Der Auftragnehmer hat den Auftraggeber im Falle einer Verletzung des Schutzes personenbezogener Daten unverzüglich und nachweislich zu verständigen, jedenfalls aber binnen 24 Stunden, nachdem die Verletzung dem Auftragnehmer bekannt wurde bzw. bekannt sein musste. Insbesondere Verstöße des Auftragnehmers 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 Auftragnehmers 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 Auftragnehmer informiert den Auftraggeber unverzüglich von Kontrollen oder Maßnahmen von Aufsichtsbehörden oder anderen Dritten, soweit diese in Zusammenhang mit der Vertragsbeziehung zwischen den Vertragsparteien stehen.
2. Der Auftragnehmer verpflichtet sich, jeden Sicherheitsvorfall zu untersuchen und gemeinsam mit dem Auftraggeber angemessene Maßnahmen zur Sicherung der Daten, sowie zur Minderung möglicher nachteiliger Folgen für die betroffenen Personen zu ergreifen. Der Auftragnehmer sichert in diesem Zusammenhang zu, den Auftraggeber 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- Auftragnehmer zu überbinden.

# Beendigung des Auftrags

1. Sofern der Auftragnehmer bei Beendigung der Dienstleistung über Daten des Auftraggebers verfügt, ist er verpflichtet, diese Daten an den Auftraggeber zu übergeben bzw. in dessen Auftrag unwiederbringlich zu vernichten, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht.

# Haftung

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

# Sonderkündigungsrecht

1. Der Auftraggeber kann Verträge mit dem Auftragnehmer jederzeit ohne Einhaltung einer Frist kündigen („außerordentliche Kündigung“), wenn in Bezug auf einen Vertrag ein schwerwiegender Verstoß des Auftragnehmers oder dessen Sub-Auftragnehmer gegen Datenschutzvorschriften oder die Bestimmungen dieses Datenschutzvertrages vorliegt oder der Auftragnehmer bzw. dessen Sub-Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert.
2. Ein schwerwiegender Verstoß liegt insbesondere dann vor, wenn der Auftragnehmer oder dessen Sub-Auftragnehmer die in diesem Vertrag 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 Auftraggeber dem Auftragnehmer eine angemessene Frist zur Abhilfe. Erfolgt die Abhilfe nicht rechtzeitig, so ist der Auftraggeber zur außerordentlichen Kündigung wie in diesem Abschnitt beschrieben berechtigt.

# 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 Vereinbarung im Übrigen nicht.
3. Der vorliegende Vertrag ist an etwaige geänderte datenschutzrechtliche Bestimmungen, sofern sie für die gegenständliche Vereinbarung relevant sind, anzupassen.
4. Dieser Vertrag ersetzt alle bestehenden datenschutzrechtlichen Vereinbarungen zwischen Auftraggeber und Auftragnehmer und gilt sowohl während als auch nach Beendigung einzelner oder aller Vertragsverhältnisse. Abweichende Bedingungen des Auftragnehmers (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 Auftragnehmers auf Lieferscheinen, Fakturen etc. angebracht sind und diesen Aufdrucken bzw. sonstigen Beilagen vom Auftraggeber 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 elektronischer Signatur unterfertigt werden. Die Unterfertigung einer Ausfertigung, welche bereits von einer oder mehreren Vertragspartei(en) handschriftlich oder mittels qualifizierter 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](mailto:recht@kages.at) bereitgestellt.

# Anlagen

Anlage 1 Leistungsbeschreibung

Anlage 2 Offen gelegte Daten

Anlage 3 Technische und Organisatorische Maßnahmen (TOM)

Anlage 4 Zugelassene Sub-Auftragnehmer

# Unterschriften

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

……………, am ……………….. ……………, am ……………….

(Ort, Datum) (Ort, Datum)

……………………………………………. …………………………………………….

Name und Funktion, Unterschrift Name und Funktion, Unterschrift

**Für den Auftragnehmer:**

……………, am ……………….. ……………, am ……………….

(Ort, Datum) (Ort, Datum)

……………………………………………. …………………………………………….

Name und Funktion, Unterschrift Name und Funktion, Unterschrift

## Anlage 1 zu [VERTRAGSNUMMER/GZ]

# **Leistungsbeschreibung**

Der Auftragnehmer erbringt folgende Leistungen für den Auftraggeber:

Lieferung von Medizinprodukten (z.B. bildgebende Systeme, Software, Geräte zur Labordiagnostik)

Installation von IT-Systemen

Wartung von IT-Systemen

Betreuung von IT-Systemen

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

Im Rahmen der Erbringung der oben angeführten Leistungen ist es möglich, dass Mitarbeiter des Auftragnehmers Einsicht in personenbezogene Daten des Auftraggebers nehmen. Die Einsichtnahme in personenbezogene Daten erfolgt nur insoweit, als diese zur Erfüllung der vertraglichen Verpflichtungen unabdingbar ist. Dem Auftragnehmer ist es untersagt, eine aktive Verarbeitung von personenbezogenen Daten, die über den Leistungsumfang des Auftrages hinausgehen, vorzunehmen.

Der Auftragnehmer verpflichtet sich, **dem Auftraggeber unverzüglich mitzuteilen, wenn ein Mitarbeiter des Auftragnehmers, der über einen Zugriff zum IT-System des Auftraggebers verfügt, diesen Zugriff nicht mehr benötigt** (z.B. bei Ausscheiden aus dem Unternehmen oder Übernahme eine anderen Tätigkeit, für die ein Zugriff auf das IT-System des Auftraggebers nicht mehr notwendig ist).

Die betroffenen Mitarbeiter des Auftraggebers unterliegen den gesetzlich erforderlichen Verschwiegenheitspflichten und/oder wurden zur Wahrung des Datengeheimnisses gemäß   
§ 6 DSG (2018) schriftlich verpflichtet. Der Auftragnehmer erbringt für den Auftraggeber die nachstehenden Leistungen, jeweils soweit dies erforderlich ist, um seine Verpflichtungen aus den mit dem Auftraggeber abgeschlossenen Verträgen zu erfüllen.

|  |
| --- |
| **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 beim Auftraggeber**  **Tausch von defekten HW-Teilen**  **Beseitigung von Störungen, Wiederherstellung der Funktionsfähigkeit der HW**  **Beratungsleistungen**  **Betreuungsleistungen (z.B. Customizing, Richtigstellen von Daten, Erstellen von Auswertungen, …)**  **Schulung der Nutzerinnen und Nutzer**  **Systemadministration**  **Backup**  **Hosting**  **Helpdesk-Dienste**  **Sonstige Leistungen:** Klicken oder tippen Sie hier, um Text einzugeben.  (Beschreibung der Verarbeitungstätigkeit: stichwortartig, aber dennoch so detailliert, dass ein unbeteiligter Dritte erkennen kann, worum es sich handelt) |

# Anlage 2

zu [VERTRAGSNUMMER/GZ]

# **Offen gelegte Daten**

## Kategorien der betroffenen Personen

|  |  |
| --- | --- |
| Nummer | Bezeichnung |
|  |  |
|  |  |

## Datenarten

|  |  |
| --- | --- |
| Nummer | Bezeichnung |
|  |  |
|  |  |

# Anlage 3

zu [VERTRAGSNUMMER/GZ]

# **Technische und organisatorische Maßnahmen (TOM)**

Der Auftragnehmer bestätigt,

hinsichtlich der vertragsgegenständlichen Leistungen über ein Zertifikat gemäß ISO 27001 (Zertifikatsnummer: Klicken oder tippen Sie hier, um Text einzugeben.)

oder

über die in nachfolgender Liste aufgeführten TOM

zu verfügen (Zutreffendes ankreuzen).

# **Zutrittskontrolle (physisch)**

Es ist sicherzustellen, dass unberechtigten Personen der Zutritt zu den Einrichtungen der Informations- und Kommunikationstechnik IKT) 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 Auftragnehmer zu implementieren:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Nr. | JA | NEIN | nicht not-wendig | 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: | | Klicken oder tippen Sie hier, um Text einzugeben. | |
| 1.2 |  |  |  | Maßnahmen für manuelle Schließanlage mit Regelungen für die Schlüsselverwaltung (Schlüsselregistrierung, Schlüsselverteilungssystem) sind vorhanden |
|  | Begründung: | | Klicken oder tippen Sie hier, um Text einzugeben. | |
| 1.3 |  |  |  | Maßnahmen für Besucherregistrierung sind vorhanden |
|  | Begründung: | | Klicken oder tippen Sie hier, um Text einzugeben. | |
| 1.4 |  |  |  | Maßnahmen für ein elektronisches Schließsystem mit Chipkarte/Transponder sind für sensible Bereiche vorhanden |
|  | Begründung: | | Klicken oder tippen Sie hier, um Text einzugeben. | |
| 1.5 |  |  |  | Maßnahmen für die Sorgfältige Auswahl und Unterweisung der Reinigungskräfte, Haustechnikkräfte, … sind vorhanden |
|  | Begründung: | | Klicken oder tippen Sie hier, um Text einzugeben. | |

# **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 Auftragnehmer 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: | | Klicken oder tippen Sie hier, um Text einzugeben. | |
| 2.2 |  |  |  | Maßnahmen für die Verwendung von aktueller Antiviren-Software sind vorhanden |
|  | Begründung: | | Klicken oder tippen Sie hier, um Text einzugeben. | |
| 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: | | Klicken oder tippen Sie hier, um Text einzugeben. | |
| 2.4 |  |  |  | Maßnahmen zum Erstellen von Benutzerprofilen sind vorhanden |
|  | Begründung: | | Klicken oder tippen Sie hier, um Text einzugeben. | |
| 2.5 |  |  |  | Maßnahmen für die Verschlüsselung von mobilen Datenträgern sind vorhanden |
|  | Begründung: | | Klicken oder tippen Sie hier, um Text einzugeben. | |
| 2.6 |  |  |  | Maßnahmen für die Verschlüsselung von Datenträgern in Laptops / Notebooks sind vorhanden |
|  | Begründung: | | Klicken oder tippen Sie hier, um Text einzugeben. | |
| 2.7 |  |  |  | Maßnahmen für eine zentrale Smartphone-Verwaltungssoftware (z.B. für externes Löschen von Daten) sind vorhanden |
|  | Begründung: | | Klicken oder tippen Sie hier, um Text einzugeben. | |

# **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 Auftragnehmer 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: | | Klicken oder tippen Sie hier, um Text einzugeben. | | |
| 3.2 |  |  |  | | Maßnahmen zur Minimierung der Anzahl der Administratoren (beschränkt sich auf das "absolut notwendige Minimum") sind vorhanden |
|  | Begründung: | | Klicken oder tippen Sie hier, um Text einzugeben. | | |
| 3.3 |  |  |  | | Maßnahmen zur Protokollierung der Zugriffe auf Anwendungen, Eingabe, Änderung und Löschen von Daten sind vorhanden |
|  | Begründung: | | Klicken oder tippen Sie hier, um Text einzugeben. | | |
| 3.4 |  |  |  | | Maßnahmen zum sicheren Löschen von Datenträgern, in jenen Fällen in denen laut Punkt 3.4 eine Kopie von Daten auf Infrastruktur des Auftragnehmers erstellt wurde, vor ihrer neuerlichen Verwendung sind vorhanden |
|  | Begründung: | | Klicken oder tippen Sie hier, um Text einzugeben. | | |
| 3.5 |  |  |  | | Maßnahmen zur physischen Vernichtung (z.B.: nach DIN 66399) oder Beauftragung eines entsprechenden Dienstleisters sind vorhanden |
|  | Begründung: | | Klicken oder tippen Sie hier, um Text einzugeben. | | |
| 3.6 |  |  |  | | Maßnahmen zur Verwaltung von Rechten durch vorgegebene Systemadministratoren oder/und ein Identitätsmanagement-System über einen definierten Prozess sind vorhanden |
|  | Begründung: | | Klicken oder tippen Sie hier, um Text einzugeben. | | |
| 3.7 |  |  |  | | Maßnahmen für eine Passwort-Richtlinie, die die Komplexität, die Länge sowie die Gültigkeitsdauer des Passworts bzw. die Authentifizierung über 2-Faktor-Authentifizierung und/oder biometrische Methoden definiert, sind vorhanden |
|  | Begründung: | | Klicken oder tippen Sie hier, um Text einzugeben. | | |
| 3.8 |  |  |  | | Maßnahmen zur sicheren Aufbewahrung (verschließbare Schränke und Schubladen, Datensafe, … ) von Datenträgern nach der Kritikalität der gespeicherten Daten sind vorhanden |
|  | Begründung: | | Klicken oder tippen Sie hier, um Text einzugeben. | | |
| 3.9 |  |  |  | | In jenen Fällen, in denen laut Punkt 3.4 eine Kopie von Daten auf Infrastruktur des Auftragnehmers erstellt wurde, sind Maßnahmen zur Speicherung der Daten an einem sicheren Ort entsprechend der Klassifizierung der Daten und/oder deren Verschlüsselung vorhanden |
|  | Begründung: | | Klicken oder tippen Sie hier, um Text einzugeben. | | |

# **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 Auftragnehmer zu implementieren:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Nr. | JA | NEIN | nicht not-wendig | 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: | | Klicken oder tippen Sie hier, um Text einzugeben. | |
| 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: | | Klicken oder tippen Sie hier, um Text einzugeben. | |

# Anlage 4

## zu [VERTRAGSNUMMER/GZ]

## Zugelassene Sub-Auftragnehmer

1. ***Name der natürlichen Person oder Firmenwortlaut gemäß Firmenbuch*,**

*Firmenbuchnummer*, *UID-Nr., Länderkennzeichen-Postleitzahl Ort, Straße/Gasse*

1. ***Name der natürlichen Person oder Firmenwortlaut gemäß Firmenbuch*,**

*Firmenbuchnummer*, *UID-Nr., Länderkennzeichen-Postleitzahl Ort, Straße/Gasse*

1. ***Name der natürlichen Person oder Firmenwortlaut gemäß Firmenbuch*,**

*Firmenbuchnummer*, *UID-Nr., Länderkennzeichen-Postleitzahl Ort, Straße/Gasse*

1. ***Name der natürlichen Person oder Firmenwortlaut gemäß Firmenbuch*,**

*Firmenbuchnummer*, *UID-Nr., Länderkennzeichen-Postleitzahl Ort, Straße/Gasse*

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)