SALK
SALZBURGER LANDESKLINIKEN

Anlagen zum

DATENSCHUTZ VERTRAG

Vertrag über die Verarbeitung personenbezogener Daten im Auftrag

zwischen

Gemeinnützige Salzburger Landeskliniken Betriebsgesellschaft mbH
Müllner Hauptstraße 48 | 5020 Salzburg | Austria
FN 240832s | UID: ATU57476234

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

und

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

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).

Pro Auftragsverarbeiter ist ein Datenschutzvertrag abzuschließen. Werden von einem Auftragsverarbeiter mehrere Verarbeitungstätigkeiten vorgenommen, sind diese jeweils in eigenen Anlagen abzubilden. Wird eine Anlage nachträglich dem Datenschutzvertrag beigefügt, so ist diese zu unterfertigen.

ANLAGE 1

vom Auftragsverarbeiter auszufüllen

Bezeichnung der Verarbeitungstätigkeit und ggf. betroffene Systeme samt Zweck:
(z.B. KIS)

- ☐ **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**
- ☐ **Systemadministration**
- ☐ **Backup**
- ☐ **Hosting**
- ☐ **Sonstige Verarbeitungstätigkeiten:**

Auf Seite 3 die Verarbeitungstätigkeit entsprechend beschreiben.

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“

<u>Beschreibung der Verarbeitungstätigkeit</u>:
zusätzlich vom Auftragsverarbeiter auszufüllen

ANLAGE 2

vom Auftragsverarbeiter auszufüllen

Offen gelegte Daten

Versehen Sie bitte die einzelnen Kategorien der betroffenen Personen mit einer fortlaufenden Nummer. Die jeweilige Nummer ist in weiterer Folge den entsprechenden Datenarten und Datenübermittlungs-empfängern zuzuordnen.

Kategorien der betroffenen Personen: Von der Verarbeitung betroffen sind (beim Verantwortlichen)

Nummer	Bezeichnung

Datenarten: Es werden folgende Datenarten verarbeitet

Nummer	Bezeichnung

Weitergabe von Daten: Es erfolgt eine Weitergabe (Offenlegung) personenbezogener Daten durch den Auftragsverarbeiter an

Nummer	Bezeichnung (Name, Sitz)

Weitergabe von Daten ins EWR Ausland: Es erfolgt eine Weitergabe (Offenlegung) personenbezogener Daten durch den Auftragsverarbeiter an

Nummer	Bezeichnung

ANLAGE 3

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. Unabhängig von den in Anlage 3 genannten Maßnahmen bleibt die Gültigkeit der im Rahmen zugrundeliegender Leistungsverträge, in Konzepten oder Protokollen etc. bereits schriftlich vereinbarten Sicherheitsmaßnahmen unberührt. Ziel ist die Gewährleistung insbesondere der Vertraulichkeit, Integrität und Verfügbarkeit der im Auftrag verarbeiteten Informationen.

Anforderungen an das Sicherheitskonzept des Auftragsverarbeiters

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:

1.1.	Maßnahmen für eine Alarmierung in kritischen Bereichen sind vorhanden
1.2.	Maßnahmen für manuelle Schließanlage mit Regelungen für die Schlüsselverwaltung (Schlüsselregistrierung, Schlüsselverteilungssystem) sind vorhanden
1.3.	Maßnahmen für Besucherregistrierung sind vorhanden
1.4.	Maßnahmen für ein elektronische Schließsystem mit Chipkarte/Transponder sind für sensible Bereiche vorhanden
1.5.	Maßnahmen für die Sorgfältige Auswahl und Unterweisung der Reinigungskräfte, Haustechnikkräfte, … sind vorhanden

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:

2.1.	Maßnahmen für die Authentifizierung mit Benutzername / Passwort (Passwortvergabe basiert auf gültigen Passwortregelungen) sind vorhanden
2.2.	Maßnahmen für die Verwendung von aktueller Antiviren-Software sind vorhanden
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)
2.4.	Maßnahmen zum Erstellen von Benutzerprofilen sind vorhanden
2.5.	Maßnahmen für die Verschlüsselung von mobilen Datenträgern sind vorhanden
2.6.	Maßnahmen für die Verschlüsselung von Datenträgern in Laptops/Notebooks sind vorhanden
2.7.	Maßnahmen für eine zentrale Smartphone-Verwaltungssoftware (z.B. für externes Löschen von Daten) sind vorhanden

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:

3.1.	Maßnahmen für den Einsatz von Rollen und Berechtigungen nach dem "Need-to-Know-Grundsatz" sind vorhanden
3.2.	Maßnahmen zur Minimierung der Anzahl der Administratoren (beschränkt sich auf das "absolut notwendige Minimum") sind vorhanden
3.3.	Maßnahmen zur Protokollierung der Zugriffe auf Anwendungen, Eingabe, Änderung und Löschen von Daten sind vorhanden
3.4.	Maßnahmen zum sicheren Löschen von Datenträgern vor ihrer neuerlichen Verwendung sind vorhanden
3.5.	Maßnahmen zur Physischen Vernichtung (z.B.: nach DIN 66399) oder Beauftragung eines entsprechenden Dienstleisters sind vorhanden
3.6.	Maßnahmen zur Verwaltung von Rechten durch vorgegebene Systemadministratoren oder/und einen Identitätsmanagement-System über einen definierten Prozess sind vorhanden
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
3.8.	Maßnahmen zur sicheren Aufbewahrung von Datenträgern (verschließbare Schränke und Schubladen, Datensafe, …) nach der Kritikalität der gespeicherten Daten sind vorhanden
3.9.	Maßnahmen zur Speicherung der Daten an einem sicheren Ort entsprechend der Klassifizierung der Daten und/oder deren Verschlüsselung sind vorhanden

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:

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
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

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:

5.1.	Maßnahmen zur Protokollierung von Eingaben, Änderungen oder Löschen von Daten sind vorhanden
5.2.	Maßnahmen zur Nachverfolgbarkeit von Eingaben, Änderungen oder Löschen von Daten durch individuelle Benutzernamen (nicht Benutzergruppen) sind vorhanden
5.3.	Maßnahmen zur Vergabe von Rechten für das Eingeben, Ändern oder Löschen von Daten auf der Grundlage eines Berechtigungskonzepts sind vorhanden
5.4.	Maßnahmen für das Führen einer Übersichtsliste, unter Angabe mit welchen Applikationen welche Daten eingegeben, geändert oder gelöscht werden können, sind vorhanden

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:

6.1.	Maßnahmen für die Klimatisierung in Serverräumen sind vorhanden
6.2.	Maßnahmen für Geräte zur Überwachung der Temperatur, Luftfeuchtigkeit oder anderer Messwerte in Serverräumen sind vorhanden
6.3.	Maßnahmen für den vorbeugenden Brandschutz (Brandmeldeanlage) in Serverräumen sind vorhanden
6.4.	Maßnahmen für geeignete Feuerlöscher oder Löschanlage in Serverräumen sind vorhanden
6.5.	Maßnahmen für ein Sicherungs- und Wiederherstellungskonzeptes sind vorhanden
6.6.	Maßnahmen für die Überprüfung der Wiederherstellung der Daten in der definierten Zeit sind vorhanden
6.7.	geeignete organisatorische Maßnahmen für ein PATCH-Management sind vorhanden
6.8.	Maßnahmen für die Speicherung der gesicherten Daten in einem anderen Brandabschnitt oder an einem sicheren, externen Ort
6.9.	Maßnahmen zum Schutz von Serverräume in Hochwassergebieten sind vorhanden

7. Separierungsregel

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 persönlichen Daten durch den Auftragsverarbeiter zu implementieren:

7.1.	Maßnahmen für die Festlegung der Datenbankrechte sind vorhanden
7.2.	Maßnahmen für die Trennung der Zugriffsrechte auf verschiedene Mandanten sind vorhanden
7.3.	Maßnahmen für die Trennung von Produktiv-, Qualität- und/oder Test-System sind vorhanden

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:

8.1.	Maßnahmen zur Erkennung, Bewertung und Behebung von Datenschutzverletzungen sind vorhanden
8.2.	Maßnahmen für die Überprüfung (z.B.: Audit, Simulation, …) des Notfall-Prozess sind vorhanden

Sicherheitsmaßnahmen nach Vertragsbeendigung:

☐ Vernichtung offen gelegter Daten

oder

☐ Übergabe der Daten an den Verantwortlichen

ANLAGE 4

vom Auftragsverarbeiter auszufüllen

Sub-Auftragsverarbeiter

Mindestangaben: Name der natürlichen Person oder Firmenwortlaut gemäß Firmenbuch, Firmenbuchnummer, UID-Nr., Länderkennzeichen, Postleitzahl, Ort, Straße/Gasse, ausgelagerte Verarbeitungstätigkeit