Bestimmungen zur Auftragsverarbeitung gemäß Art. 28 DSGVO innerhalb der EU / des EWR.

Durchzuführende Verarbeitungen (Art. 4 Nr. 2 DSGVO):
Austausch von Personen- und Gesundheitsdaten der BewohnerInnen, KlientInnen und KundInnen zwischen dem Haus der Barmherzigkeit und DienstleisterInnen, die für die sichere Durchführung der vertraglich vereinbarten Dienstleistungen erforderlich sind.

1. Der Auftragsverarbeiter verpflichtet sich, Daten und Verarbeitungsergebnisse ausschließlich im Rahmen der Aufträge des Verantwortlichen zu verarbeiten und ausschließlich dem Verantwortlichen zurückzugeben oder nur nach dessen schriftlichem Auftrag zu übermitteln. Desgleichen bedarf eine Verarbeitung der übermittelten Daten für eigene Zwecke des Auftragsverarbeiters eines derartigen schriftlichen Auftrages.

2. Erhält der Auftragsverarbeiter einen behördlichen Auftrag, Daten des Verantwortlichen herauszugeben, so hat er – sofern aufgrund unmittelbar anwendbaren Unionsrechts oder gesetzlich zulässig – den Verantwortlichen unverzüglich darüber zu informieren und die Behörde an diesen zu verweisen.

3. Der Auftragsverarbeiter erklärt hiermit rechtsverbindlich, dass er alle mit der Verarbeitung von Daten beauftragten Personen vor Aufnahme der Tätigkeit zur uneingeschränkten Geheimhaltung verpflichtet hat oder diese einer angemessenen Geheimhaltungspflicht aufgrund unmittelbar anwendbaren Unionsrechts oder gesetzlicher Bestimmungen unterliegen. Diese Geheimhaltungspflicht bleibt für die mit der Verarbeitung von Daten beauftragten Personen auch nach Beendigung ihrer Tätigkeit und Ausscheiden beim Auftragsverarbeiter aufrecht.

4. Der Auftragsverarbeiter erklärt hiermit rechtsverbindlich, dass er alle erforderlichen – und insbesondere in Anhang 1 genannten – Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung gemäß Art. 32 DSGVO ergriffen hat, sodass die Verarbeitung

   a. im Einklang mit den Anforderungen der DSGVO, insbesondere deren Art. 28 und 32 sowie den in Durchführung der DSGVO erlassenen Gesetzen und Verordnungen, wie insbesondere dem Datenschutzgesetz, BGBl. I Nr. 165/1999 in der geltenden Fassung, erfolgt und
   b. den Schutz der Rechte der betroffenen Person gewährleistet.

5. Der Auftragsverarbeiter verpflichtet sich hiermit,

   a. die Erfüllung der Pflichten gemäß Pkt. 4 vor Abschluss dieser Vereinbarung sowie auf Anfrage des Verantwortlichen jederzeit während der Laufzeit dieser Vereinbarung nachzuweisen;
   b. den Verantwortlichen über geplante Verarbeitungstätigkeiten außerhalb der EU bzw. des EWR so rechtzeitig zu verständigen, dass der Verantwortliche diese allenfalls untersagen kann;
   c. den Verantwortlichen über jede unrechtmäßige Verarbeitung von Daten, bei denen den betroffenen Personen ein Schaden droht, unverzüglich zu informieren;
   d. erkannte Sicherheitslücken sowie Maßnahmen zur Beseitigung dieser, dem Verantwortlichen unverzüglich aufzuzeigen;
   e. den Verantwortlichen unverzüglich zu informieren, falls er der Ansicht ist, eine Weisung des Verantwortlichen verstößt gegen Datenschutzbestimmungen der Europäischen Union oder der Mitgliedstaaten.

6. Der Auftragsverarbeiter kann ein anderes Unternehmen („Sub-Auftragsverarbeiter“) auch ohne Zustimmung des Verantwortlichen zur Durchführung von Verarbeitungen heranziehen. Er hat jedoch den Verantwortlichen von der beabsichtigten Heranziehung eines Sub-Auftragsverarbeiters so rechtzeitig zu verständigen, dass der Verantwortliche dies allenfalls untersagen kann. Sofern der angezeigten Heranziehung eines Sub-Auftragsverarbeiters nicht seitens des Verantwortlichen widersprochen wurde, hat der Auftragsverarbeiter mit jedem Sub-Auftragsverarbeiter einen Vertrag gemäß Art. 28 Abs. 4 DSGVO abzuschließen, in dem sicherzustellen ist, dass der Sub-Auftragsverarbeiter dieselben Verpflichtungen eingeht, die dem Auftragsverarbeiter auf Grund dieser Vereinbarung obliegen. Kommt der Sub-Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten des Sub-Auftragsverarbeiters.

7. Der Auftragsverarbeiter trägt für die technischen und organisatorischen Voraussetzungen Vorsorge, dass der Verantwortliche die Bestimmungen der DSGVO, insbesondere

   a. des Kapitels III über die Rechte der betroffenen Person *(Transparenz; Informationspflicht; Recht auf Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit, Widerspruch; Mitteilungspflicht; Automatisierte Entscheidungen im Einzelfall einschließlich Profiling; Beschränkungen)* sowie
   b. des Kapitels IV Abschnitt 1 bis 3 über die Pflichten von Verantwortlichen und Auftragsverarbeitern *(Allgemeine Pflichten; Technikgestaltung und datenschutzfreundliche Voreinstellungen; Vertreter; Auftragsverarbeiter; Verarbeitung unter Aufsicht; Verzeichnis von Verarbeitungstätigkeiten; Zusammenarbeit mit der Aufsichtsbehörde; Sicherheit der Verarbeitung; Meldung und Benachrichtigung von Verletzungen des Schutzes personenbezogener Daten; Datenschutz-Folgenabschätzung und vorherige Konsultation)*

   gegenüber den betroffenen Personen innerhalb der in der DSGVO oder sonst gesetzlich vorgesehenen Fristen jederzeit erfüllen kann und überlässt dem Verantwortlichen alle dafür notwendigen Informationen. Wird ein entsprechender Antrag an den Auftragsverarbeiter gerichtet und lässt dieser erkennen, dass der Antragsteller ihn irrtümlich für den Verantwortlichen der von ihm betriebenen Datenanwendung hält, hat der Auftragsverarbeiter den Antrag unverzüglich an den Verantwortlichen weiterzuleiten und dies dem Verantwortlichen mitzuteilen.

8. Der Auftragsverarbeiter verpflichtet sich hiermit zur Unterstützung des Verantwortlichen bei der Einhaltung der in den Art 32 bis 36 DSGVO genannten Pflichten *(Datensicherheitsmaßnahmen, Meldungen von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde, Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person, Datenschutz-Folgenabschätzung, vorherige Konsultation)*.

9. Der Auftragsverarbeiter wird darauf hingewiesen, dass er für die vorliegende Auftragsverarbeitung ein Verarbeitungsverzeichnis nach Art 30 DSGVO zu errichten und auf Anfrage dem Verantwortlichen innerhalb eines Werktags zur Verfügung zu stellen hat.

10. Der Auftragsverarbeiter ist nach Beendigung der Auftragsverarbeitung verpflichtet, alle Verarbeitungsergebnisse und Unterlagen, die Daten enthalten, dem Verantwortlichen zu übergeben bzw. in dessen Auftrag für ihn weiter vor unbefugter Einsicht gesichert aufzubewahren oder auftragsgemäß zu vernichten. Wenn der Auftragsverarbeiter die Daten in einem speziellen technischen Format verarbeitet, ist er verpflichtet, die Daten nach Beendigung dieser Vereinbarung entweder in diesem Format oder nach Wunsch des Verantwortlichen in dem Format, in dem er die Daten vom Verantwortlichen erhalten hat oder in einem anderen, gängigen Format herauszugeben.

11. Dem Verantwortlichen wird hinsichtlich der Verarbeitung der von ihm übermittelten Daten das Recht jederzeitiger Einsichtnahme und Kontrolle der Datenverarbeitungseinrichtungen vor Ort eingeräumt (Audits zum Thema Datensicherheit und Datenschutz). Der Auftragsverarbeiter verpflichtet sich hiermit,

    a. dem Verantwortlichen jene Informationen zur Verfügung zu stellen, die zur Kontrolle der Einhaltung der in dieser Vereinbarung genannten Verpflichtungen notwendig sind;

Institut
Haus der Barmherzigkeit
Seeböckgasse 30a, 1160 Wien
T +43 1 401 99-0 / **F** -1308
M info@hausderbarmherzigkeit.at
www.hausderbarmherzigkeit.at

Erste Bank
IBAN AT27 2011 1000 0800 1111
BIC GIBAATWW
Bank Austria
IBAN AT49 1200 0006 2414 5306
BIC BKAUATWW
UID ATU 16292205

Lehrkrankenhaus der Medizinischen Universität Wien und Partner der Donau-Universität Krems
Systemzertifiziert nach ISO 9001/14001

b. den Auditoren, die im Auftrag des Verantwortlichen tätig sind und soweit dies zur Erfüllung ihres Auftrags erforderlich ist,
   i. Zugang und Zugriff auf die IT-Systeme (Hardware, Software, Datenbanken, Datenbestände, etc.) zu gewähren sowie
   ii. die gemäß Art. 32 DSGVO getroffenen technischen und organisatorischen Sicherheitsmaßnahmen offenzulegen;

c. die in den Buchstaben a) und b) genannten Tätigkeiten im Ausmaß von bis zu drei Tagen pro Kalenderjahr kostenfrei zu unterstützen.

12. Der Verantwortliche behält sich vor, im Falle eines dem Auftragsverarbeiter zuzurechnenden Verstoßes gegen die DSGVO oder die in Durchführung der DSGVO erlassenen Gesetze oder Verordnungen, wie insbesondere das Datenschutzgesetz, BGBl. I Nr. 165/1999 in der geltenden Fassung, oder diese Vereinbarung, geeignete Beweissicherungsmaßnahmen zu treffen sowie die Geschäftsbeziehung mit sofortiger Wirkung zu beenden. Der Auftragsverarbeiter hat den Verantwortlichen insbesondere schad- und klaglos zu halten, hinsichtlich der gemäß Art. 32 DSGVO zu treffenden Maßnahmen sowie Überschreitungen des vom Verantwortlichen erteilten Auftrags.

Anhang 1 – Technisch-organisatorische Maßnahmen

Vertraulichkeit

1. Zutrittskontrolle: Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen, z.B.: Schlüssel, Magnet- oder Chipkarten, elektrische Türöffner, Portier, Sicherheitspersonal, Alarmanlagen, Videoanlagen;

2. Zugangskontrolle: Schutz vor unbefugter Systembenutzung, z.B.: Kennwörter (einschließlich entsprechender Policy), automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern;

3. Zugriffskontrolle: (technischer) Ausschluss unbefugten Lesens, Kopierens, Veränderns oder Entfernens innerhalb des Systems, z.B.: Standard-Berechtigungsprofile auf Need-to-know-Basis, Standardprozess für Berechtigungsvergabe, Protokollierung von Zugriffen, periodische Überprüfung der vergebenen Berechtigungen, insb von administrativen Benutzerkonten;

4. Pseudonymisierung: sofern für die jeweilige Datenverarbeitung möglich, Entfernung der primären Identifikationsmerkmale der personenbezogenen Daten in der jeweiligen Datenanwendung und gesonderte Aufbewahrung;

5. Klassifikationsschema für Daten: aufgrund gesetzlicher Verpflichtungen oder Selbsteinschätzung (geheim/vertraulich/intern/öffentlich).

Integrität

1. Weitergabekontrolle: (technischer) Ausschluss unbefugten Lesens, Kopierens, Veränderns oder Entfernens bei elektronischer Übertragung oder Transport, z.B.: durch Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur;

2. Eingabekontrolle: Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement.

Verfügbarkeit und Belastbarkeit

1. Verfügbarkeitskontrolle: Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: durch Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV, Dieselaggregat), Virenschutz, Firewall, Meldewege und Notfallpläne; Security Checks auf Infrastruktur- und Applikationsebene, mehrstufiges Sicherungskonzept mit verschlüsselter Auslagerung der Sicherungen in Ausweichrechenzentren, Standardprozesse bei Wechsel/Ausscheiden von Mitarbeitern;

2. rasche Wiederherstellbarkeit;

3. Löschungsfristen: sowohl für Daten selbst als auch Metadaten wie Logfiles, udgl.

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

1. Datenschutz-Management, einschließlich regelmäßiger Mitarbeiterschulungen;

2. Incident-Response-Management;

3. datenschutzfreundliche Voreinstellungen;

4. Auftragskontrolle: Ausschluss von Datenverarbeitung im Sinne von Art 28 DSGVO ohne entsprechende Weisung des Verantwortlichen, z.B.: eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Auftragsverarbeiters (ISO-Zertifizierung, ISMS), Vorabüberzeugungspflicht, Nachkontrollen.

Institut
Haus der Barmherzigkeit
Seeböckgasse 30a, 1160 Wien
T +43 1 401 99-0 / **F** -1308
M info@hausderbarmherzigkeit.at
www.hausderbarmherzigkeit.at

Erste Bank
IBAN AT27 2011 1000 0800 1111
BIC GIBAATWW
Bank Austria
IBAN AT49 1200 0006 2414 5306
BIC BKAUATWW
UID ATU 16292205

Lehrkrankenhaus der Medizinischen Universität Wien und Partner der Donau-Universität Krems
Systemzertifiziert nach ISO 9001/14001