Vereinbarung

über eine Auftragsverarbeitung gemäß Art. 28 DSGVO

zwischen:

der Pflegeeinrichtung

Haus der Barmherzigkeit
Seeböckgasse 30a
1160 Wien

nachfolgend **Verantwortlicher** genannt,

und

nachfolgend **Auftragsverarbeiter** genannt.

Ort, Datum: Wien, 24. November 2020

HABIT

Gegenstand der Vereinbarung

§ 1. (1) Mit der vorliegenden Vereinbarung soll der Rechtsrahmen gemäß Art. 28 DSGVO geschaffen werden, um folgende Verarbeitungen (Art. 4 Nr. 2 DSGVO) rechtskonform durchführen zu können:

(2) Mit der vorliegenden Vereinbarung sollen – bei Anwendbarkeit des Gesundheitstelematikgesetzes 2012, BGBl. I Nr. 111/2012 – außerdem die im Titelblatt angeführten Identitäten und Rollen des Auftragsverarbeiters sowie Verantwortlichen gemäß § 27 Abs. 10 Z 3 GTelG 2012 bestätigt werden.

Dauer der Vereinbarung

§ 2. Diese Vereinbarung gilt solange der Auftragsverarbeiter vom Verantwortlichen bereitgestellte personenbezogene Daten verarbeitet, mindestens jedoch solange ein Beauftragungsverhältnis, etwa in Form eines Werkvertrags, zwischen dem Verantwortlichen und dem Auftragsverarbeiter besteht.

Ort der Verarbeitung

§ 3. (1) Die Verarbeitungstätigkeiten gemäß Abs. 1 werden zumindest zum Teil auch außerhalb der EU bzw. des EWR durchgeführt, und zwar in den in **Anhang 1 Spalte 3** genannten Staaten, wobei sich das angemessene Datenschutzniveau aus **Anhang 1 Spalte 4** ergibt.

(2) Ist der Auftragsverarbeiter nicht in der Union niedergelassen im Sinne des Art. 3 Abs. 2 DSGVO, ist eine allfällige Beauftragung von Verarbeitungstätigkeiten gemäß Abs. 1 – ungeachtet des für die Beauftragung herangezogenen Rechtsinstruments (Art. 28 Abs. 3 DSGVO) – ungültig, solange der Auftragsverarbeiter seinen Pflichten gemäß Art. 27 DSGVO nicht nachgekommen ist.

(3) Ist der Auftragsverarbeiter in der Union niedergelassen, erklärt er hiermit rechtsverbindlich Vertreter für alle von ihm herangezogenen Sub-Auftragsverarbeiter zu sein, solange diese nicht in der Union niedergelassen im Sinne des Art. 3 Abs. 2 DSGVO sind und ihren Pflichten gemäß Art. 27 DSGVO nicht nachgekommen sind.

Pflichten des Auftragsverarbeiters

§ 4. (1) Der Auftragsverarbeiter verpflichtet sich, Daten und Verarbeitungsergebnisse ausschließlich auf dokumentierte Weisung des Verantwortlichen (z.B. per E-Mail, mündlich mit

nachfolgendem Aktenvermerk, im Rahmen von Sitzungsprotokollen, …) 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

a) zur Einhaltung der Datenschutz-Grundverordnung sowie

b) zur uneingeschränkten Geheimhaltung

verpflichtet hat.

Die Verpflichtung gemäß b) kann insoweit entfallen, als die mit der Verarbeitung von Daten beauftragten Personen 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 2** 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 bestätigt seine Eignung durch Unterfertigung der Unbescholtenheitserklärung gemäß **Anhang 3** oder belegt diese mit seinen Datenschutz-Policy-Dokumenten (Informationssicherheits-Richtlinien, externen Auditberichten oder international anerkannten Zertifizierungen). Soweit der Auftragsverarbeiter Cloud-Dienste für die in § 1 beschriebene Verarbeitung einsetzt, hat er zu belegen, dass die Daten nicht außerhalb der Europäischen Union gespeichert werden, beispielsweise durch das Gütesiegel „Austrian Cloud“.

(6) Der Auftragsverarbeiter verpflichtet sich hiermit,

a) die Erfüllung der Pflichten gemäß Abs. 4 vor Abschluss dieser Vereinbarung sowie auf Anfrage des Verantwortlichen jederzeit, mindestens jedoch einmal im Jahr unaufgefordert, etwa per E-Mail an datenschutz@hb.at, während der Laufzeit dieser Vereinbarung nachzuweisen;

b) hinsichtlich der in **Anhang 1** angeführten Verarbeitungstätigkeiten die Einhaltung der DSGVO (**Anhang 1 Spalte 4**) dem Verantwortlichen durch Vorlage geeigneter Dokumente nachzuweisen sowie den Verantwortlichen über geplante Verarbeitungstätigkeiten außerhalb der EU bzw. des EWR, die nicht in **Anhang 1** angeführt sind, so rechtzeitig zu verständigen, dass der Verantwortliche diese allenfalls untersagen kann;

c) jedwede Art von möglichen Interessenkonflikten, auch bei beteiligten Mitarbeiter*innen, unverzüglich bekanntzugeben;

d) den Verantwortlichen über jede unrechtmäßige Verarbeitung von Daten, bei denen den betroffenen Personen ein Schaden droht, unverzüglich zu informieren;

e) erkannte Sicherheitslücken sowie Maßnahmen zur Beseitigung dieser, dem Verantwortlichen unverzüglich aufzuzeigen;

f) den Verantwortlichen unter datenschutz@hb.at unverzüglich zu informieren, falls er der Ansicht ist, eine Weisung des Verantwortlichen verstößt gegen Datenschutzbestimmungen der Europäischen Union oder der Mitgliedstaaten; der Verantwortliche sichert dem Auftragsverarbeiter in diesem Zusammenhang ausdrücklich zu, dass dem Auftragsverarbeiter aus der Wahrnehmung der Warnpflicht bzw. der Ablehnung von Aufträgen des Verantwortlichen, die Datenschutzbestimmungen der Europäischen Union oder der Mitgliedstaaten widersprechen, keinerlei Nachteile seitens des Verantwortlichen erwachsen.

Sub-Auftragsverarbeiter

§ 5. Der Auftragsverarbeiter kann ein anderes Unternehmen („Sub-Auftragsverarbeiter“) auch ohne Zustimmung des Verantwortlichen zur Durchführung von Verarbeitungen heranziehen. Er hat jedoch dem Verantwortlichen vor Heranziehung eines neuen Sub-Auftragsverarbeiters eine unterschriebene Datenschutz-Unbescholtenheitserklärung gemäß **Anhang 3** vorzulegen und den Verantwortlichen von der beabsichtigten Heranziehung des neuen 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.

Technische und organisatorische Maßnahmen

§ 6. (1) 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 den 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.

(2) Der Auftragsverarbeiter verpflichtet sich hiermit

a) 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)*,

b) insbesondere zur Einhaltung der rechtlich erforderlichen Datensicherheit, wie etwa der Verschlüsselungspflicht nach § 6 des Gesundheitstelematikgesetzes 2012, BGBl. I Nr. 111/2012, durch

   i. Einhaltung der unterfertigten Vereinbarung gemäß **Anhang 4**, wobei durch Unterfertigung bestätigt wird, dass nur der Auftragsverarbeiter die Einstellungen an seinem Mailserver ändern kann, die für die verschlüsselte Übermittlung erforderlichen Einstellungen getroffen hat und garantiert, die für die verschlüsselte Übermittlung getroffenen Einstellungen nicht – ohne Rücksprache mit dem Verantwortlichen – einseitig zu ändern oder

   ii. Verschlüsselung der Gesundheitsdaten vor Übermittlung, etwa in Form verschlüsselter PDFs, oder

   iii. Übermittlung von Gesundheitsdaten mittels Fax, verschlüsselter Server-Lösungen, wie etwa Sharefile, oder anderer technischer Lösungen, bei denen eine Verschlüsselung im Sinne des Gesundheitstelematikgesetzes 2012 gewährleistet ist sowie

c) die Unterhaltung oder Begründung von Niederlassungen (auch durch kontrollierte Tochterunternehmen) in Drittstaaten ohne angemessenen Datenschutz, wie etwa in den USA, oder das Hosting von Daten auf Servern von Unternehmen mit US-Bezug, dem Verantwortlichen so rechtzeitig zu melden, dass dieser seine Rechte gemäß § 8 der vorliegenden Vereinbarung ausüben kann.

(3) 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 von 14 Tagen zur Verfügung zu stellen hat. Das Verarbeitungsverzeichnis hat – gegliedert nach Verarbeitungstätigkeit – zumindest Folgendes zu enthalten:

a) die Datenarten auf Ebene von Attributen von Informationsobjekten, z.B. Name einer Person,

b) einen technischen Ansprechpartner,

c) eine Liste sämtlicher Sub-Auftragsverarbeiter,

d) Angaben zu den Löschfristen sowie

e) Angaben zu den eingehaltenen technischen und organisatorischen Maßnahmen.

(4) Der Auftragsverarbeiter ist nach Beendigung der Auftragsverarbeitung verpflichtet, alle Verarbeitungsergebnisse und Unterlagen, die Daten enthalten,

a) dem Verantwortlichen herauszugeben, wobei der Auftragsverarbeiter, wenn er die Daten in einem speziellen technischen Format verarbeitet, verpflichtet ist, 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, oder

b) in dessen Auftrag für ihn weiter vor unbefugter Einsicht gesichert aufzubewahren oder

c) in dessen Auftrag in maschinenlesbarer Form einem anderen Auftragsverarbeiter des Verantwortlichen zu übermitteln oder

d) auftragsgemäß zu vernichten, wobei im Falle der Nichtlöschbarkeit der Verantwortliche unverzüglich zu informieren ist.

Kontrolle

§ 7. 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;

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.

Haftung und Schadenersatz

§ 8. 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. Zu solchen Verstößen zählen insbesondere die Unterhaltung oder Begründung von Niederlassungen (auch durch mehrheitlich kontrollierte Tochterunternehmen) in Drittstaaten ohne angemessenen Datenschutz, wie etwa den USA, oder das Hosting von Daten auf Servern von Unternehmen mit US-Bezug. Der Auftragsverarbeiter hat den Verantwortlichen schad- und klaglos zu halten, insbesondere hinsichtlich der gemäß Art. 32 DSGVO zu treffenden Maßnahmen, Überschreitungen des vom Verantwortlichen erteilten Auftrags sowie der Unterhaltung oder Begründung von Niederlassungen (auch durch mehrheitlich kontrollierte Tochterunternehmen) in Drittstaaten ohne angemessenen Datenschutz, wie etwa den USA, oder das Hosting von Daten auf Servern von Unternehmen mit US-Bezug.

Sonstiges

§ 9. (1) Änderungen und Ergänzungen dieser Vereinbarung – einschließlich etwaiger Zusicherungen des Auftragsverarbeiters – bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt.

(2) Sollten einzelne Bestimmungen dieser Vereinbarung unwirksam oder undurchführbar sein oder nach Abschluss dieser Vereinbarung unwirksam oder undurchführbar werden, bleibt davon die Wirksamkeit dieser Vereinbarung im Übrigen unberührt.

(3) Es gilt österreichisches Recht. Für allfällige Streitigkeiten aus dieser Vereinbarung ist das sachlich zuständige Gericht in Wien zuständig.

	Für den Verantwortlichen	Für den Auftragsverarbeiter
Vor- und Zuname (BLOCKSCHRIFT)		
Funktion		

Firmenmäßige-zeichnung		
unterzeichnet am (tt.mm.jjjj)		
Ort		

HABIT –
Haus der Barmherzigkeit
Integrationsteam GmbH
Büro der Geschäftsführung
Seeböckgasse 30a, 1160 Wien
T +43 1 401 99-8008/ **F** -8004
M habit@hb.at

Erste Bank
IBAN AT11 2011 1284 0155 3600
BIC GIBAATWW
FN 257249 h, HG Wien
UID ATU 61604437
Systemzertifiziert nach ISO 9001

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

Spenden an HABIT sind steuerlich absetzbar.
IBAN AT79 2011 1280 2410 1514
BIC GIBAATWW
Konto lautend auf: Institut Haus der Barmherzigkeit
Verwendungszweck: HABIT

HAUS DER BARMHERZIGKEIT

Anhang 1 – Verarbeitungen außerhalb der EU

Name v. Sub-Auftragsverarbeiter / Niederlassung	Beschreibung der Verarbeitungstätigkeit(en)	Drittland / Int. Organisation	Einhaltung der DSGVO durch		Name v. Vertreter (Art. 27 DSGVO)
Spalte 1	Spalte 2	Spalte 3	Spalte 4		Spalte 5
			☐	Angemessenheitsbeschluss der Kommission (Art. 45 DSGVO)	
			☐	rechtsverbindliche Verwaltungsvereinbarung (Art. 46 Abs. 2 Buchstabe a DSGVO)	
			☐	verbindliche interne Datenschutzvorschriften (Art. 46 Abs. 2 Buchstabe b DSGVO)	
			☐	Standarddatenschutzklauseln der EU (Art. 46 Abs. 2 Buchstabe c DSGVO)	
			☐	von der EU genehmigte Standarddatenschutzklauseln (Art. 46 Abs. 2 Buchstabe d DSGVO)	
			☐	genehmigte Verhaltensregeln (Art. 46 Abs. 2 Buchstabe e DSGVO)	
			☐	genehmigte Zertifizierungsmechanismen (Art. 46 Abs. 2 Buchstabe f DSGVO)	
			☐	genehmigte Vertragsklauseln (Art. 46 Abs. 3 Buchstabe a DSGVO)	
			☐	genehmigte Verwaltungsvereinbarung (Art. 46 Abs. 3 Buchstabe b DSGVO)	
			☐	Ausnahme im Einzelfall (Art. 49 DSGVO)	
			☐	Angemessenheitsbeschluss der Kommission (Art. 45 DSGVO)	
			☐	rechtsverbindliche Verwaltungsvereinbarung (Art. 46 Abs. 2 Buchstabe a DSGVO)	
			☐	verbindliche interne Datenschutzvorschriften (Art. 46 Abs. 2 Buchstabe b DSGVO)	
			☐	Standarddatenschutzklauseln der EU (Art. 46 Abs. 2 Buchstabe c DSGVO)	

HABIT –
Haus der Barmherzigkeit
Integrationsteam GmbH
Büro der Geschäftsführung
Seeböckgasse 30a, 1160 Wien
T +43 1 401 99-8008/ **F** -8004
M habit@hb.at

Erste Bank
IBAN AT11 2011 1284 0155 3600
BIC GIBAATWW
FN 257249 h, HG Wien
UID ATU 61604437
Systemzertifiziert nach ISO 9001

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

Spenden an HABIT sind steuerlich absetzbar.
IBAN AT79 2011 1280 2410 1514
BIC GIBAATWW
Konto lautend auf: Institut Haus der Barmherzigkeit
Verwendungszweck: HABIT

HAUS DER BARMHERZIGKEIT

			☐	von der EU genehmigte Standarddatenschutz-klauseln (Art. 46 Abs. 2 Buchstabe d DSGVO)	
			☐	genehmigte Verhaltensregeln (Art. 46 Abs. 2 Buchstabe e DSGVO)	
			☐	genehmigte Zertifizierungsmechanismen (Art. 46 Abs. 2 Buchstabe f DSGVO)	
			☐	genehmigte Vertragsklauseln (Art. 46 Abs. 3 Buchstabe a DSGVO)	
			☐	genehmigte Verwaltungsvereinbarung (Art. 46 Abs. 3 Buchstabe b DSGVO)	
			☐	Ausnahme im Einzelfall (Art. 49 DSGVO)	
			☐	Angemessenheitsbeschluss der Kommission (Art. 45 DSGVO)	
			☐	rechtsverbindliche Verwaltungsvereinbarung (Art. 46 Abs. 2 Buchstabe a DSGVO)	
			☐	verbindliche interne Datenschutzvorschriften (Art. 46 Abs. 2 Buchstabe b DSGVO)	
			☐	Standarddatenschutzklauseln der EU (Art. 46 Abs. 2 Buchstabe c DSGVO)	
			☐	von der EU genehmigte Standarddatenschutz-klauseln (Art. 46 Abs. 2 Buchstabe d DSGVO)	
			☐	genehmigte Verhaltensregeln (Art. 46 Abs. 2 Buchstabe e DSGVO)	
			☐	genehmigte Zertifizierungsmechanismen (Art. 46 Abs. 2 Buchstabe f DSGVO)	
			☐	genehmigte Vertragsklauseln (Art. 46 Abs. 3 Buchstabe a DSGVO)	
			☐	genehmigte Verwaltungsvereinbarung (Art. 46 Abs. 3 Buchstabe b DSGVO)	
			☐	Ausnahme im Einzelfall (Art. 49 DSGVO)	
			☐	Angemessenheitsbeschluss der Kommission (Art. 45 DSGVO)	
			☐	rechtsverbindliche Verwaltungsvereinbarung (Art. 46 Abs. 2 Buchstabe a DSGVO)	

HAUS DER BARMHERZIGKEIT

			☐	verbindliche interne Datenschutzvorschriften (Art. 46 Abs. 2 Buchstabe b DSGVO)	
			☐	Standarddatenschutzklauseln der EU (Art. 46 Abs. 2 Buchstabe c DSGVO)	
			☐	von der EU genehmigte Standarddatenschutz-klauseln (Art. 46 Abs. 2 Buchstabe d DSGVO)	
			☐	genehmigte Verhaltensregeln (Art. 46 Abs. 2 Buchstabe e DSGVO)	
			☐	genehmigte Zertifizierungsmechanismen (Art. 46 Abs. 2 Buchstabe f DSGVO)	
			☐	genehmigte Vertragsklauseln (Art. 46 Abs. 3 Buchstabe a DSGVO)	
			☐	genehmigte Verwaltungsvereinbarung (Art. 46 Abs. 3 Buchstabe b DSGVO)	
			☐	Ausnahme im Einzelfall (Art. 49 DSGVO)	
			☐	Angemessenheitsbeschluss der Kommission (Art. 45 DSGVO)	
			☐	rechtsverbindliche Verwaltungsvereinbarung (Art. 46 Abs. 2 Buchstabe a DSGVO)	
			☐	verbindliche interne Datenschutzvorschriften (Art. 46 Abs. 2 Buchstabe b DSGVO)	
			☐	Standarddatenschutzklauseln der EU (Art. 46 Abs. 2 Buchstabe c DSGVO)	
			☐	von der EU genehmigte Standarddatenschutz-klauseln (Art. 46 Abs. 2 Buchstabe d DSGVO)	
			☐	genehmigte Verhaltensregeln (Art. 46 Abs. 2 Buchstabe e DSGVO)	
			☐	genehmigte Zertifizierungsmechanismen (Art. 46 Abs. 2 Buchstabe f DSGVO)	
			☐	genehmigte Vertragsklauseln (Art. 46 Abs. 3 Buchstabe a DSGVO)	
			☐	genehmigte Verwaltungsvereinbarung (Art. 46 Abs. 3 Buchstabe b DSGVO)	
			☐	Ausnahme im Einzelfall (Art. 49 DSGVO)	

HAUS DER BARMHERZIGKEIT

Anhang 2 – 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 Mitarbeiter*innen;

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 Schulungen, sodass sichergestellt ist, dass alle Beteiligten, d.h. insbesondere Mitarbeiter*innen, ausreichende Fähigkeiten erlangen können, die sie für die ordnungsgemäße Erfüllung ihrer Tätigkeiten benötigen;

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.

HAUS DER BARMHERZIGKEIT

Anhang 3 – Datenschutz-Unbescholtenheitserklärung

Firma / Name: .....

Straße: .....

Land / PLZ / Ort: .....

ID (zB FN, GLN, UID): .....

(in der Folge „AUFTRAGSWERBER“)

erklärt und bestätigt hiermit, dass in den letzten 3 Jahren vor Unterfertigung der HB-Auftragsverarbeitungsvereinbarung keine Geldbuße gegen ihn durch eine Aufsichtsbehörde verhängt wurde.

Außerdem verpflichtet sich der AUFTRAGSWERBER – im Falle einer Auftragserteilung – das Haus der Barmherzigkeit unter datenschutz@hb.at umgehend, jedenfalls aber binnen 72 Stunden nach rechtskräftiger Verhängung einer Geldbuße gemäß Art. 83 DSGVO, über die rechtskräftige Verhängung einer Geldbuße gemäß Art. 83 DSGVO nachweislich zu informieren.

Die Verletzung von in der Datenschutz-Grundverordnung angeführten Pflichten, kann gemäß Art. 82 DSGVO zu Schadenersatzansprüchen oder gemäß Art. 83 DSGVO zu Geldstrafen bis 20 Millionen EUR oder 4 Prozent des Vorjahresumsatzes führen. Die geltende Fassung der Datenschutz-Grundverordnung ist im Internet unter https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32016R0679 (deutsch) bzw. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679 (englisch) abrufbar.

……, …… .....

(Ort, Datum) (für den AUFTRAGSWERBER)

HAUS DER BARMHERZIGKEIT

Anhang 4 – Vereinbarung zu verschlüsseltem Mailserver

Folgende Vereinbarung gilt seitens des Verantwortlichen als angenommen und unterzeichnet und bedarf zu ihrer Gültigkeit der Unterfertigung durch den Auftragsverarbeiter, wobei

- Verantwortlicher und Auftragsverarbeiter gemeinsam als PARTEIEN und
- der vorliegende Anhang 4 als VEREINBARUNG

bezeichnet werden:

Gegenstand der VEREINBARUNG

§ 1. (1) Mit der vorliegenden VEREINBARUNG soll Rechtssicherheit zwischen den PARTEIEN in Bezug auf die Einhaltung der Bestimmungen des Gesundheitstelematikgesetzes 2012 (GTelG 2012), BGBl. I Nr. 111/2012, geschaffen werden, damit die PARTEIEN die ihnen obliegenden Verarbeitungen (Art. 4 Nr. 2 der Verordnung [EU] 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG [Datenschutz-Grundverordnung], ABl. Nr. L 119 vom 04.05.2016 S. 1, [DSGVO]), wie insbesondere den Versand von E-Mails, rechtskonform durchführen können.

(2) Verweist diese VEREINBARUNG auf unionsrechtliche Normen oder Normen des Bundesrechts, so sind diese – zur Sicherstellung einer langfristigen Anwendbarkeit der vorliegenden VEREINBARUNG und soweit nicht ausdrücklich anderes vereinbart ist – in ihrer jeweils geltenden Fassung anzuwenden.

Dauer der VEREINBARUNG

§ 2. Diese VEREINBARUNG gilt solange die im Gesundheitstelematikgesetz 2012 vorgesehene Verschlüsselungspflicht auf die Übermittlung von Daten (Art. 4 Nr. 1 DSGVO), insbesondere den Versand von E-Mails, zwischen den PARTEIEN Anwendung findet.

HAUS DER BARMHERZIGKEIT

Bestätigung durch die PARTEIEN

§ 3. Die PARTEIEN bestätigen hiermit rechtsverbindlich und wechselseitig, dass

1. die von ihnen verwendeten Mailserver

   a) ihrer – auch physischen – Kontrolle unterliegen und

   b) so konfiguriert sind, dass bei der Übermittlung von Daten (Art. 4 Nr. 1 DSGVO), die Voraussetzungen des Gesundheitstelematikgesetzes 2012 bzw. der auf seiner Grundlage ergangenen Verordnungen, wie insbesondere der Anlage 2 der Gesundheitstelematikverordnung 2013, BGBl. II Nr. 506/2013, erfüllt sind,

2. die ihrer Kontrolle unterliegende Infrastruktur, insbesondere die Verbindung zwischen den Mailservern und den Mailclients, verschlüsselt im Sinne des § 6 GTelG 2012 ist, d.h. insbesondere durch bauliche, kryptographische oder sonstige Maßnahmen gegenüber unbefugten Zugriffen durch Dritte abgesichert ist sowie

3. keine gemeinsame Verarbeitung im Sinne des Art. 26 DSGVO vorliegt.

Wechselseitige Informationspflicht der PARTEIEN

§ 4. (1) Die PARTEIEN verpflichten sich hiermit rechtsverbindlich zur umgehenden, d.h. maximal binnen 72 Stunden erfolgender, Information der jeweils anderen PARTEI, wenn sich Änderungen hinsichtlich der in § 3 bestätigten Umstände, wie etwa Änderungen der verwendeten kryptographischen Algorithmen, Outsourcing der Mailserver, etc., ergeben.

(2) Soweit möglich soll eine Information gemäß Abs. 1 bereits zeitgerecht vorab ergehen, um der jeweils anderen PARTEI ausreichend Reaktionszeit zuzugestehen.

HAUS DER BARMHERZIGKEIT

Sonstiges

§ 5. (1) Änderungen und Ergänzungen dieser VEREINBARUNG bedürfen – ungeachtet ihres Ausmaßes und ihrer Art – einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser VEREINBARUNG handelt.

(2) Sollten einzelne Bestimmungen dieser VEREINBARUNG unwirksam oder undurchführbar sein oder nach Abschluss dieser VEREINBARUNG unwirksam oder undurchführbar werden, bleibt davon die Wirksamkeit dieser VEREINBARUNG im Übrigen unberührt.

(3) Es gilt österreichisches Recht. Als Gerichtsstand für Streitigkeiten aus oder im Zusammenhang mit dieser VEREINBARUNG wird das sachlich zuständige Gericht in Wien vereinbart.

…….., …… .....

(Ort, Datum) (für den AUFTRAGSVERARBEITER)