Dienstleistungsvereinbarung zur Information über Entgeltumwandlung

zwischen dem / der

Insel e.V. – in Selbstbestimmung leben

Ehrenbergstraße 59

22767 Hamburg

- nachfolgend: Auftraggeber -

und der

Ecclesia Gruppe Vorsorgemanagement GmbH

Ecclesiastraße 1 – 4

32758 Detmold

- nachfolgend: Makler -

§ 1 Information der Mitarbeiter/innen

1. Der Auftraggeber hat Maklerauftrag für die betriebliche Altersversorgung erteilt. Der Makler ist zentraler Dienstleister der Auftraggeber in allen Fragen der betrieblichen Altersversorgung. Gegenstand des Maklermandates ist nicht die Zusatzversorgung, d.h. die betriebliche Altersversorgung über die Versorgungsanstalt des Bundes und der Länder (VBL) oder über andere öffentliche oder kirchliche Zusatzversorgungseinrichtungen wie z.B. Zusatzversorgungskassen.
2. Die Rahmenbedingungen für die betriebliche Altersversorgung durch Entgeltumwandlung sind in einer Versorgungsordnung festgelegt. Die Versorgungsordnung verpflichtet den Auftraggeber zu ihrer Umsetzung einschließlich der Verarbeitung der dazu erforderlichen personenbezogenen Daten im Beschäftigungskontext (Art. 88 DS-GVO, § 26 BDSG). In der Versorgungsordnung sind die Rahmenbedingungen für die Entgeltumwandlung festgelegt.
3. Die Information der Mitarbeiter/innen ist eine Rechtspflicht des Auftraggebers. Der Auftraggeber darf dazu einen Dienstleister beauftragen. Der Makler unterstützt den Auftraggeber.

§ 2 Aufgaben des Maklers im Informationsprozess

1. Mitarbeiter/innen erhalten im Postversand oder auf anderem Weg **zusammen mit der Information einen Rückmeldebogen** zur verbindlichen Rücksendung an den Auftraggeber als Arbeitgeber. Der Versand erfolgt durch den Auftraggeber. Der Makler unterstützt den Auftraggeber bei der Erstellung des Rückmeldebogens. Der Rückmeldebogen dient als Informationsnachweis. Der/die Mitarbeiter/in bestätigt den Erhalt der Information.
   1.1. Der/die Mitarbeiter/in erklärt, ob er /sie eine individualisierte Vorschlagsberechnung zur Entgeltumwandlung erhalten möchte.
   1.2. Der/die Mitarbeiter/in kann erklären, dass er/sie keine Entgeltumwandlung wünscht.
2. Mitarbeiter/innen erhalten im Postversand oder auf anderem Weg eine **individualisierte Vorschlagsberechnung zur Entgeltumwandlung**. Der Versand erfolgt durch den Makler.

2.1. Die Vorschlagsberechnung hat folgende Inhalte:

- In einer **Nettoaufwandsberechnung** wird dargestellt, wie sich ein bestimmter monatlicher Entgeltumwandlungsbetrag auf die Höhe des verbleibenden Nettoentgelts auswirken würde.
- In einer **Leistungsdarstellung** wird beschrieben, welche versicherten Leistungen auf der Basis des vorgegebenen monatlichen Beitrages (Umwandlungsbetrag zzgl. Arbeitgeberzuschuss) garantiert bzw. möglich sind. Für die individualisierte Darstellung zugrunde gelegt werden jeweils Durchführungsweg, Versicherungsunternehmen bzw. Versorgungsträger und Tarif, wie festgelegt. Stehen nach der Versorgungsordnung mehrere Varianten zur Auswahl, können sie vergleichend dargestellt werden.
- Mitarbeiter/innen erhalten einen Katalog von Fragen und Antworten („FAQ") zur betrieblichen Altersversorgung bzw. Entgeltumwandlung.
- Mitarbeiter/innen erhalten (vorbereitete) Unterlagen zum Abschluss einer Entgeltumwandlungsvereinbarung.

2.2. Individualisierte Vorschlagsberechnungen zur Entgeltumwandlung werden nach Vorgabe des Auftraggebers erstellt für einen bestimmten Personenkreis von Mitarbeiter/innen und / oder auf Anforderung von Mitarbeiter/innen und/oder im Rahmen eines Informationsgesprächs der Mitarbeiter/innen mit dem Makler.

2.3. Mit der individualisierten Vorschlagsberechnung erhält der/die Mitarbeiter/in die Kontaktdaten des Maklers. Der/die Mitarbeiter/in hat dadurch die Möglichkeit, mit dem Makler (über E-Mail, telefonisch oder in einem Videogespräch nach Terminvereinbarung) in Kontakt zu treten, zum Beispiel zur Klärung von Fragen zur Vorschlagsberechnung, zur Anforderung einer weiteren Vorschlagsberechnung mit anderen Umwandlungsbeträgen, zur Klärung von allgemeinen Fragen zur Entgeltumwandlung.

§ 3 Verarbeitung von personenbezogenen Daten

1. Der Auftraggeber entscheidet, welche Mitarbeiter/innen zu welchem Zeitpunkt die Information / den Rückmeldebogen / die individualisierte Vorschlagsberechnung zur Entgeltumwandlung erhalten.

   1.1. Bei jeglichem Versand durch den Makler werden personenbezogene Adressdaten (Vorname, Name, Adresse) automatisiert verarbeitet.

   1.2. Individualisierte Vorschlagsberechnungen zur Entgeltumwandlung werden vom Makler automatisiert erstellt. Es werden jeweils monatliche Umwandlungsbeiträge in einer bestimmten Höhe oder in unterschiedlicher Höhe unterstellt. Für die Erstellung von individualisierten Vorschlagsberechnungen zur Entgeltumwandlung müssen personenbezogene Gehaltsdaten verarbeitet werden.

2. Übermittlung der personenbezogenen Daten

   2.1. Die erforderlichen Datensätze werden vom Auftraggeber an den Makler übermittelt.

   2.2. Die erforderlichen personenbezogenen Daten sind abschließend aus der Anlage „Interessentenliste" ersichtlich.

§ 4 Datenschutz

1. Die jeweils geltenden Bestimmungen über den Datenschutz werden befolgt. Soweit es die Erfüllung dieser Vereinbarung erfordert, wird der Makler auch Daten des Auftraggebers speichern, verändern oder löschen. Der Auftraggeber ist hiermit einverstanden.
2. Die Vertragsparteien schließen einen gesonderten Vertrag zur **Auftragsverarbeitung** nach Artikel 28 DS-GVO (**Anlage**).

§ 5 Beginn und Beendigung

1. Diese Konkretisierung zum Maklerauftrag tritt an dem Tag der (letzten) Unterzeichnung in Kraft. Mündliche Nebenabreden sind nicht getroffen.
2. Diese Konkretisierung endet jedoch automatisch mit der Beendigung des Maklerauftrages; dies gilt auch, soweit der Maklerauftrag nur hinsichtlich der betrieblichen Altersversorgung (teilweise) beendet wird.
3. Der Makler ist bei Beendigung des Maklerauftrages zur Herausgabe aller relevanten Unterlagen und Daten des Auftraggebers in einer vom Auftraggeber zu benennenden Form verpflichtet.

§ 6 Schlussbestimmungen

1. Ergänzungen oder Änderungen dieses Vertrages bedürfen zur Rechtswirksamkeit der Schriftform. Das Gleiche gilt für den Verzicht auf das Schriftformerfordernis.
2. Die Parteien können mit einer gesonderten Vereinbarung Festlegungen zur Wirksamkeit von Erklärungen treffen, die im Rahmen dieser Vereinbarung von den Parteien und von den Mitarbeiter/innen abgegeben werden (z.B. zur Wirksamkeit von digital signierten Dokumenten wie z.B. Entgeltumwandlungsvereinbarungen).
3. Sollten einzelne Bestimmungen der Vereinbarung unwirksam oder undurchführbar sein, wird die Wirksamkeit der übrigen Bestimmungen hierdurch nicht berührt. Die Vertragsparteien sind verpflichtet, die unwirksamen oder undurchführbaren Bestimmungen unverzüglich durch wirksame oder durchführbare zu ersetzen, die dem von den Vertragsparteien bei Vertragsschluss beabsichtigten Sinn und Zweck der Regelung und den wirtschaftlichen Interessen beider Vertragsparteien so nahe wie möglich kommt. Dies gilt auch für den Fall, dass die Vereinbarung Regelungslücken enthält.
4. Die Vertragsparteien bestätigen mit ihrer Unterschrift zugleich, jeweils eine gleichlautende Ausfertigung dieser Vereinbarung nebst der darin ggf. erwähnten, einbezogenen Anlagen erhalten zu haben.

Hamburg, den 29.11.22

Insel e.V.

insel e.V.
in Selbstbestimmung leben

insel e.V.
in Selbstbestimmung leben
Geschäftsstelle
Ehrenbergstraße 59
22767 Hamburg
Tel. 040 - 380 38 36 - 0
www.insel-ev.de

Detmold, den 18.01.2023

Ecclesia Gruppe
Vorsorgemanagement GmbH

Ecclesia Gruppe
Vorsorgemanagement GmbH
Ecclesiastraße 1-4
32758 Detmold

Anlage

Vertrag zur Auftragsverarbeitung nach Artikel 28 DS-GVO

Zwischen der / dem

Insel e.V. – in Selbstbestimmung leben

Ehrenbergstraße 59

22767 Hamburg

- nachstehend „Auftraggeber" genannt -

und der

Ecclesia Gruppe Vorsorgemanagement GmbH

Ecclesiastraße 1 – 4

32758 Detmold

- nachstehend „Auftragnehmer" genannt –

§ 1 Gegenstand und Dauer des Auftrags

1. Der Auftraggeber beauftragt den Auftragnehmer mit der Verarbeitung personenbezogener Daten.
2. Dieser Vertrag beginnt mit seiner Unterzeichnung durch beide Vertragspartner und endet mit der Auftragserledigung.

   Das Recht zur Kündigung aus wichtigem Grund bleibt unberührt. Der Auftraggeber kann diesen Vertrag insbesondere jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen die Bestimmungen dieses Vertrages vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer den Zutritt des Auftraggebers in seinen Geschäftsbetrieb vertragswidrig verweigert.

   Jede Kündigung bedarf zu ihrer Wirksamkeit der Textform.

§ 2 Konkretisierung des Auftragsinhalts

1. Ziel ist die datenschutzgerechte Durchführung der Dienstleistungen des Auftragnehmers als Versicherungsmakler, der für die betriebliche Altersversorgung vom Auftraggeber beauftragt ist – und zwar bezogen auf den Umgang mit den dazu erforderlichen personenbezogenen Daten, die der Auftraggeber an den Auftragnehmer übergibt bzw. die im Auftrag des Auftraggebers erhoben, verarbeitet oder genutzt werden.
2. Gegenstand des Auftrags ist die Verwaltung und Betreuung des Vertragsbestandes zur betrieblichen Altersversorgung im Rahmen des erteilten Maklermandates. Gegenstand des Auftrags ist auch die Information von Mitarbeiter/innen. Der Auftragnehmer erbringt als Makler die Dienstleistungen, *wie sie zwischen den Vertragsparteien in der Dienstleistungsvereinbarung festgehalten sind.*

3. Zur Auftragserfüllung erforderliche personenbezogene Daten sind Daten der Beschäftigten, d.h. der Mitarbeiter/innen, die der jeweiligen Versorgungsordnung im Sinne der Dienstleistungsvereinbarung unterfallen. Insbesondere handelt es sich um folgende Daten:

   3.1. Daten mit Bezug zum Arbeitsverhältnis: Name, Vorname, Adresse, Geburtsdatum, Gehaltsdaten, steuerliche Merkmale, Datum des Beginns / Entgeltumwandlungsbeträge / Zuschuss zur Entgeltumwandlung.

   3.2. Daten mit Bezug zum Versicherungsvertrag bzw. zur versicherungstechnischen Rückdeckung: Name, Vorname, Adresse, Geburtsdatum, Entgeltumwandlungsbeträge / Zuschuss zur Entgeltumwandlung, Versicherer, Versicherungstarif, Datum des Beginns / des Endes der Beitragszahlung, versicherte Leistungen (Rentenleistung, Kapitalleistung), Rückkaufswert.

4. Der Auftraggeber übermittelt Daten der Mitarbeiter/innen, die zur betrieblichen Altersversorgung bzw. Entgeltumwandlung zu informieren sind,

   an den Auftragnehmer jeweils auf sicherem Weg. Übermittelt wird eine Excel-Datei mit den erforderlichen personenbezogenen Daten seiner Mitarbeiter /innen. Die Übermittlung der Daten erfolgt vorzugsweise auf nicht körperlichem Weg, zum Beispiel durch

   - den Transfer über ein Down-/Upload-Portal mit verschlüsselter Verbindung,
   - die Übersendung einer Excel-Datei per E-Mail, wenn zuvor beidseitig TLS-Verschlüsselung etabliert wurde,
   - die Übersendung einer Excel-Datei via E-Mail unter Kennwortschutz der Excel-Datei (bei gesonderter Übermittlung des Kennworts auf einem anderen Übertragungsweg).

5. Die Excel Datei wird im Unternehmensnetzwerk der Ecclesia Holding GmbH, die als Unterbeauftragter (siehe unten Ziffer 6) tätig wird, gespeichert und damit auch der täglichen Sicherung unterzogen.

6. Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt.

§ 3 Technisch-organisatorische Maßnahmen

1. Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

2. Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, er Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen [Einzelheiten im Anhang 1].

3. Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten

Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

§ 4 Berichtigung, Einschränkung und Löschung von Daten

1. Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.
2. Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

§ 5 Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DS-GVO ausübt.
Beim Auftragnehmer ist als externer Beauftragter für den Datenschutz

Herr Oliver Baldner

Tel. +49 5231 6036129

Fax: +49 5231 603606129

E-Mail: dsb@ecclesia-gruppe.de

bestellt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

b) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten, einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

c) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO. Einzelheiten sind beschrieben in dem Anhang 1 (Beschreibung der technischen und organisatorischen Maßnahmen), der Bestandteile dieses Vertrages zur Auftragsverarbeitung ist.

d) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

e) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeiten- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

f) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeiten- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

g) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Personen gewährleistet wird.

h) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

§ 6 Unterauftragsverhältnisse

1. Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer zum Beispiel als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers, auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen. Diese haben mindestens den in dieser Vereinbarung getroffenen technisch-organisatorischen Maßnahmen zu entsprechen.
2. Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.
3. Der Auftraggeber stimmt der Beauftragung der nachfolgenden Unterauftragnehmer unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zu:

Firma Unterauftragnehmer	Anschrift/Land	Leistung
Ecclesia Holding GmbH	Ecclesiastraße 1-4 32758 Detmold	Betrieb des Rechenzentrums

Ein Wechsel des bestehenden Unterauftragnehmers ist zulässig, soweit:

- Der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und
- der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
- eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde gelegt wird.

4. Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.
5. Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.
6. Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen Zustimmung des Hauptauftraggebers. Sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

§ 7 Kontrollrechte des Auftraggebers

1. Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.
2. Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.
3. Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch
   - die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;
   - die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO;
   - aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (zum Beispiel Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
   - eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (zum Beispiel nach BSI-Grundschutz).

§ 8 Mitteilung bei Verstößen des Auftragnehmers

1. Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören unter anderem:
   a) Die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen;
   b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden;
   c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen;

d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung;

e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

2. Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

§ 9 Weisungsbefugnis des Auftraggebers

1. Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mindestens in Textform).
2. Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

§ 10 Löschung und Rückgabe von personenbezogenen Daten

1. Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.
2. Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.
3. Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

§ 11 Vergütung

Eine gesonderte Vergütung schuldet der Auftraggeber dem Auftragnehmer für dessen Leistungen im Zusammenhang mit diesem Vertrag nicht.

§ 12 Schlussbestimmungen

1. Sollte das Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu informieren. Der Auftragnehmer wird die Gläubiger über die Tatsache, dass es sich um Daten handelt, die im Auftrag verarbeitet werden, unverzüglich informieren.
2. Die Anhänge zu diesem Vertrag sind Bestandteil dieses Vertrages.
3. Änderungen und Ergänzungen sowie die Aufhebung dieses Vertrages, seiner Anhänge sowie dieser Schriftformklausel bedürfen zu ihrer Wirksamkeit der gesetzlichen Schriftform.
4. Sollten Bestimmungen dieses Vertrages oder seiner Anhänge ganz oder teilweise unwirksam oder undurchführbar sein oder werden, so wird die Wirksamkeit der Bestimmungen

im Übrigen hiervon nicht berührt. Die Vertragspartner verpflichten sich, die unwirksamen oder undurchführbaren Bestimmungen oder Teile der Bestimmungen durch wirksame und durchführbare Bestimmungen zu ersetzen, die dem von den Vertragspartnern mit den ganz oder teilweise unwirksamen oder undurchführbaren Bestimmungen verfolgten wirtschaftlichen Zweck am nächsten kommen. Dies gilt auch für den Fall, dass dieser Vertrag oder seine Anhänge Regelungslücken enthalten.

5. Die Einrede des Zurückbehaltungsrechts i.S.v. § 273 BGB und die Einrede des nicht erfüllten Vertrages gemäß § 320 BGB werden hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

Hamburg, den 24.11.22

Insel. e.V.

insel e.V.
in Selbstbestimmung leben

insel e.V.
in Selbstbestimmung leben
Geschäftsstelle
Ehrenbergstraße 59
22767 Hamburg
Tel. 040 - 380 38 36 - 0
www.insel-ev.de

Detmold, den 18.01.2023

Ecclesia Gruppe
Vorsorgemanagement GmbH

Ecclesia Gruppe
Vorsorgemanagement GmbH
Ecclesiastraße 1-4
32758 Detmold

Anhang zum Vertrag zur Auftragsverarbeitung

Technische und organisatorische Maßnahmen

Geltungszeitraum ab 12.10.2021

1. Allgemeines

Personenbezogene Kundendaten werden nur auf den beschriebenen Anlagen in den Rechenzentren gespeichert. An anderen Orten, auch in den Büroräumen, befinden sich regelmäßig keine Kundendaten. Einzige Ausnahmen sind temporäre Kopien einzelner Datensätze für spezielle Aufgaben (z.B. Bearbeitung einer Anfrage des Auftraggebers, Bearbeitung eines Auftrags des Auftraggebers zur Fehleranalyse oder -behebung).

Alle Mitarbeitenden des Auftragnehmers werden vor Aufnahme der Tätigkeit auf die Vertraulichkeit verpflichtet. Darüber hinaus existiert eine verbindliche Verfahrensanweisung zum Umgang mit den datenschutzrelevanten Daten.

Die Wirksamkeit der im Folgenden beschriebenen technischen und organisatorischen Maßnahmen wird regelmäßig durch Penetrationstests sowie regelmäßige interne Audits durch den Datenschutzbeauftragten überprüft.

2. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

- **Zutrittskontrolle**

  Die Zutrittskontrolle wird durch die folgenden Maßnahmen gewährleistet:

  - Durch ein elektronisches Zutrittskontrollsystem wird der Zutritt auf Personen beschränkt, die den Zutritt für ihre dienstliche Aufgabenerfüllung zwingend benötigen. Jeder Zutritt wird protokolliert. Zu den Serverräumen haben nur die verantwortlichen Mitarbeitenden der IT-Abteilung sowie die zuständigen Personen der Notfallbewältigung gemäß IT-Notfallhandbuch Zutritt. Die Liste der zutrittsberechtigten Personen wird in regelmäßigen Abständen im Rahmen eines internen Audits geprüft und bei Bedarf angepasst.
  - Besucher müssen sich am Empfang anmelden und werden durch den jeweiligen Ansprechpartner abgeholt.
  - Die Systeme werden durch Kameras im Außenbereich, in den Zugängen zum Gebäude und separat in den Rechenzentren überwacht und durch eine Einbruchmeldeanlage sowie durch regelmäßige Kontrollgänge des Wachschutzes gesichert (24h/365 Tage).
  - Die Serverräume sind mit Sicherheitstüren ausgestattet. Fenster sind in den Serverräumen nicht vorhanden.

- **Zugangskontrolle**

  Der Zugang zu allen Anwendungen und Daten wird über die Benutzerkennung des Active Directory gesteuert und unterliegt den folgenden Richtlinien:

  - Die Kennwörter sind 90 Tage gültig und müssen nach Ablauf vom Benutzer geändert werden
  - Komplexität: mindestens 8 Zeichen, mindestens drei der Kategorien Groß- und Kleinbuchstaben, Ziffern sowie Sonderzeichen müssen enthalten sein
  - Historie: die letzten acht Kennwörter dürfen nicht verwendet werden
  - Nach 10 Fehlversuchen erfolgt eine automatische Sperrung des Zugangs

- Externe Zugänge sind durch ein wirksames Firewallkonzept und eine verschlüsselte VPN-Verbindung abgesichert.

- **Zugriffskontrolle**

  Die Zugriffskontrolle ist wirksam umgesetzt durch Implementierung eines Berechtigungskonzepts. Das Berechtigungskonzept ist dokumentiert und wird regelmäßig in Bezug auf die betrieblichen Erfordernisse überprüft. Die Zugriffsrechte sind sowohl personenbezogen auf Benutzerebene als auch funktionsbezogen vergeben.

- **Trennungskontrolle**

  Durch strikte Kunden und Mandantentrennung ist sichergestellt, dass die zu unterschiedlichen Zwecken erhobenen Daten getrennt verarbeitet werden können.

- **Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)**

  Eine automatisierte Pseudonymisierung scheidet aus organisatorischen bzw. auftragsspezifischen Gründen aus.

3. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

- **Weitergabekontrolle**

  Sofern Daten auf elektronischem Wege übermittelt werden, ist sichergestellt, dass die Übertragung ausschließlich in verschlüsselter Form erfolgt. Jede Übermittlung von Daten auf mobilen Datenträgern ist nur in Ausnahmefällen und auf Anfrage zulässig. Schnittstellen (z.B. USB) sind gesperrt und werden nur auf Antrag des jeweiligen Vorgesetzten durch die IT-Abteilung selektiv freigeschaltet.

  Datenträger von mobilen Geräten (z.B. Notebooks) sind verschlüsselt. Sofern im Ausnahmefall auf Anweisung des Auftraggebers Daten auf mobilen Datenträgern zur Verfügung gestellt werden, ist in der Verfahrensanweisung festgelegt, dass hierzu nur verschlüsselte Datenträger zu verwenden sind.

  Sensible Daten in Papierform werden durch Aktenvernichter unkenntlich gemacht bzw. durch einen Dienstleister im Rahmen einer Auftragsverarbeitung datenschutzkonform vernichtet. Nicht mehr benötigte Datenträger werden durch einen Dienstleister im Rahmen einer Auftragsverarbeitung fachgerecht und datenschutzkonform vernichtet.

- **Eingabekontrolle**

  Soweit technisch und organisatorisch möglich und sinnvoll wird benutzerbezogen protokolliert, wenn Daten eingegeben, verändert oder gelöscht werden.

4. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

- **Verfügbarkeitskontrolle**

  Die Verfügbarkeit der Daten ist durch eine täglich durchgeführte Datensicherung gewährleistet. Die Datenträger der Datensicherung werden in einem feuerfesten Tresor gelagert. Alle Systeme sind redundant aufgebaut. Die Daten des Auftraggebers werden in zwei räumlich voneinander getrennten Rechenzentren gespiegelt vorgehalten.

  Temperatur und Luftfeuchtigkeit sowie die Funktionsfähigkeit der Klimaanlage werden automatisch überwacht. Durch den Einsatz von Systemen zur unterbrechungsfreien Stromversorgung ist im Falle eines Stromausfalls ein geordnetes Herunterfahren der Systeme gewährleistet.

  Die Integrität der Daten ist durch Einsatz eines wirksamen Firewall- und Virenschutzkonzepts gewährleistet.

  Die Brandschutzmaßnahmen beinhalten:

- Handfeuerlöscher
- Automatische Löschanlagen in den Serverschränken
- Brandmeldeanlage
- Brandfrüherkennung

- **Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO)**

  Die rasche Wiederherstellbarkeit wird durch die folgenden Maßnahmen sichergestellt:

  - Einsatz redundanter Hard- und Software in räumlich voneinander getrennten Rechenzentren
  - Vorhaltung und regelmäßige Aktualisierung eines Notfallkonzepts
  - Regelmäßige tägliche Datensicherung auf Systemen, die eine Wiederherstellung der Daten innerhalb von maximal 60 Minuten ermöglichen

5. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

- **Datenschutz-Management**

  Die erbrachte Dienstleistung unterliegt dem Datenschutz-Management der Ecclesia Gruppe, zur Sicherstellung der Einhaltung der datenschutzrechtlichen Vorgaben der DS-GVO. Hierzu gehören insbesondere die folgenden Maßnahmen:

  - Durchführung regelmäßiger Schulungen der Mitarbeiter bezüglich der Anforderungen des Datenschutzes
  - Erstellung von Anweisungen zur Einhaltung der datenschutzrechtlichen Erfordernisse und der Auftragskontrolle
  - Durchführung regelmäßiger Audits durch den Datenschutzbeauftragten der Ecclesia Gruppe
  - Durchführung regelmäßiger Penetrationstests durch externe Spezialisten

- **Incident-Response-Management**

  Die Sicherheit der Systeme sowie die Erkennung von Angriffen wird durch ein mehrstufiges Firewallsystem sichergestellt. Hierzu werden zwei Next-Generation-Firewalls (NGFW) eines führenden Herstellers verwendet. Eingehende Dokumente werden auf Schadsoftware anhand verdächtiger Signaturen und verdächtigen Verhaltens in isolierten Umgebungen (Sandbox) überprüft.

  Angriffsversuche werden durch die Firewall protokolliert und Vorfälle mit dem Status (high critical) automatisiert gemeldet. Thread logs werden täglich eingesehen und auf Bedrohungen überprüft.

- **Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)**

  Es werden ausschließlich diejenigen Daten erhoben und gespeichert, die der Auftraggeber selbst zur Verfügung stellt. Weitere Datenverarbeitung durch Protokollierung durch den Auftragnehmer findet nur insoweit statt, als dies notwendig ist zur Sicherstellung des ordnungsgemäßen Betriebs der Anwendung.

- **Auftragskontrolle**

In dem Vertrag zur Verarbeitung von Daten im Auftrag ist festgelegt, dass Daten nur gemäß den Anweisungen des Auftraggebers verarbeitet werden dürfen. Die organisatorische Umsetzung auf Auftragnehmerseite ist durch die entsprechenden Regelungen in der Verfahrensanweisung erfolgt.