Allgemeine Nutzungsbedingungen

1. Allgemeine Regelungen

Das Unternehmen bond:in GmbH [Pflügerstr. 18, 12047 Berlin, HRB folgt] (nachfolgend „bond:in“ oder „Plattformbetreiber“), vertreten durch den Geschäftsführer, bietet Handelsvertretern und (gebundenen) Vermittler:innen im Sinne des Handelsgesetzbuchs (nachfolgend „Nutzer“) im Rahmen eines Dienstvertrages die Möglichkeit, die Plattform „bav: hub“ gemäß den Vorgaben dieser Nutzungsbedingungen auf Zeit zu nutzen. Nutzer können über die Plattform Versicherungsleistungen zur betrieblichen Altersvorsorge ihren Kunden und/oder Mitarbeitenden (nachfolgend „Client“) anbieten und/oder vermitteln. Von diesen Nutzungsbedingungen abweichende Regelungen gelten nur dann, wenn diese von A schriftlich bestätigt werden. Mit der Registrierung gem. Ziffer 3 erkennt der Nutzer diese Nutzungsbedingungen als maßgeblich an.

2. Leistungsbeschreibung

2.1. Die Plattform wird von bond:in technisch betrieben und den Nutzern im Rahmen einer Auftragsverarbeitung (Anhang) angeboten. Die Leistungen des Plattformbetreibers bestehen u.a. in der Bereithaltung der Nutzungsmöglichkeiten der Plattform nach Registrierung des Nutzers und dessen Möglichkeit dem Client Informationen für eine betriebliche Altersvorsorge zur Verfügung zu stellen.

2.2. Beratung und Angebote an die Clients erfolgt im Rahmen einer unmittelbaren Vertragsbeziehung zwischen Kunde und dem Nutzer bzw. der jeweiligen Einrichtung des Nutzers. bond:in ist nicht Partei des Versicherungsvertrags und hat keinerlei Ansprüche aus daraus resultierenden Provisionen.

2.3. Die Plattform besteht aus komplexen Hard- und Softwarekomponenten, deren einzelne Bestandteile ständig miteinander interagieren und die gleichzeitig einer ständigen Anpassung durch Weiterentwicklungen, veränderte gesetzliche Anforderungen oder Sicherheitsupdates unterliegen. BOND:IN wird sämtliche Anpassungen an den Hard- und Softwarekomponenten im Rahmen der bestehenden technischen und betrieblichen Möglichkeiten sorgfältig vornehmen, kann aber eine ununterbrochene Verfügbarkeit der Plattform nicht zusichern. bond:in sichert eine Verfügbarkeit der Plattform von 98% im Jahresmittel zu. Dies schließt erforderliche Wartungsarbeiten nicht mit ein. Der Plattformbetreiber wird die Nutzer hierüber rechtzeitig informieren. Die Wartung wird regelmäßig außerhalb der üblichen Geschäftszeiten der Nutzer durchgeführt, es sei denn aufgrund zwingender Gründe muss eine Wartung zu einer anderen Zeit vorgenommen werden.

3. Registrierung

3.1. Voraussetzung für die Nutzung der Plattform ist die Registrierung. Die Plattform steht nur Kaufleuten im Sinne des HGB und juristischen Personen des öffentlichen Rechts zur Verfügung. Ein Anspruch auf Registrierung oder Nutzung der Plattform besteht nicht.

3.2. Der Nutzer hat im Registrierungsantrag seine Unternehmensdaten, Rechnungsdaten und einen Ansprechpartner zu benennen. Die Annahme des Zulassungsantrags erfolgt durch Zulassungsbestätigung per E-Mail. Durch die Zulassung kommt ein kostenpflichtiger Dienstvertrag auf die festgelegte Zeit zwischen bond:in und dem jeweiligen Nutzer nach diesen

Nutzungsbedingungen zustande. Die vom Nutzer zu zahlende Vergütung richtet sich nach den aktuellen Preiskonditionen, welche auf der Bestellseite einsehbar sind.

3.3. Die jeweils anfallenden Vergütungen werden – sofern nicht anders vereinbart – jährlich im Voraus abgerechnet und unmittelbar nach Rechnungsstellung ohne Abzug, jedoch zzgl. Mehrwertstellung, zum jeweils geltenden Steuersatz fällig.

3.4. Alle Logins sind individualisiert und dürfen nur vom jeweils berechtigten Nutzer verwendet werden. Der Nutzer ist verpflichtet, Login und Passwort geheim zu halten und vor dem unberechtigten Zugriff Dritter zu schützen. Bei Verdacht des Missbrauchs durch einen Dritten wird der Nutzer bond:in hierüber unverzüglich informieren. Sobald bond:in von der unberechtigten Nutzung Kenntnis erlangt, wird bond:in den Zugang des unberechtigten Nutzers sperren. Bond:in behält sich das Recht vor, Login und Passwort eines Nutzers zu ändern; in einem solchen Fall wird bond:in den Nutzer hierüber unverzüglich informieren.

3.5. Der Nutzer steht dafür ein, dass die von ihm, insbesondere im Rahmen seines Antrages auf Registrierung gemäß Abs. 2 gegenüber bond:in gemachten Angaben wahr und vollständig sind. Er verpflichtet sich, bond:in alle künftigen Änderungen der gemachten Angaben unverzüglich mitzuteilen. Gleiches gilt auch für alle Angaben, die vom Nutzer bei der Einrichtung von Mitarbeiter-Logins gemacht werden.

3.6. Bond:in ist berechtigt, einem Nutzer die Zulassung zu entziehen oder den Zugang zur Plattform zu sperren, falls ein hinreichender Verdacht besteht, dass er gegen diese Nutzungsbedingungen verstoßen hat. Der Nutzer kann diese Maßnahmen abwenden, wenn er den Verdacht durch Vorlage geeigneter Nachweise auf eigene Kosten ausräumt.

4. Nutzungsrechte

4.1. Eine physische Überlassung von Software an den Nutzer erfolgt nicht. Der Nutzer erhält Zugriff an der jeweils aktuellen Version der Plattform für die vertraglich festgelegte Anzahl an Nutzern einfache, d. h. nicht unterlizenzierbare und nicht übertragbare, zeitlich auf die Dauer des Vertrags beschränkte Rechte die Plattform mittels Zugriff über einen Browser nach Maßgabe der Regelungen dieser AGB zu nutzen.

4.2. Der Nutzer darf die Plattform nur im Rahmen seiner eigenen geschäftlichen Tätigkeit durch eigenes Personal nutzen. Dem Nutzer ist eine weitergehende Nutzung der Plattform nicht gestattet.

4.3. Nutzer erhalten an den von bond:in bereitgestellten Dokumenten ein einfaches, nicht exklusives Nutzungsrecht für die Verwendung gegenüber Clients auf der Plattform.

5. Verfügbarkeit der Plattform

5.1. Sofern eine Nichtverfügbarkeit der Plattform auf Vorsatz oder grober Fahrlässigkeit von bond:in oder eines Erfüllungsgehilfen von bond:in beruht, kann sich bond:in nicht auf eine Einhaltung der Verfügbarkeitszusage nach der Leistungsbeschreibung (Ziffer 2) berufen.

5.2. Bond:in ist für eine Unterschreitung der Verfügbarkeitszusage nicht verantwortlich, sofern die Nichterreichbarkeit auf höhere Gewalt, auf technische Störungen bei Dritten, die nicht Erfüllungsgehilfen von bond:in sind, oder auf einem rechtswidrigen Angriff auf bond:in oder einen von bond:in beauftragten Dienstleister beruhen.

6. Haftung

6.1. Bei Vorsatz, Arglist oder grober Fahrlässigkeit sowie bei Fehlen einer garantierten Eigenschaft oder im Fall einer gesetzlichen, verschuldensunabhängigen Haftung, sowie im Fall der Verletzung des Lebens, des Körpers oder der Gesundheit steht der Systemanbieter unbeschränkt für aus der Pflichtverletzung entstandene Schäden ein.

6.2. Für leichte Fahrlässigkeit haftet der Systemanbieter nur bei Verletzung einer wesentlichen Vertragspflicht. Vertragswesentliche Pflichten sind solche Pflichten, die der Systemanbieter nach Inhalt und Zweck dieses Vertrages und seiner Ergänzungen zu erbringen hat, deren Erfüllung die ordnungsgemäße Durchführung dieses Vertrages erst ermöglicht und auf deren Einhaltung der Nutzer regelmäßig vertraut und vertrauen darf. Zu den vertragswesentlichen Pflichten dieses Vertrages gehört danach insbesondere die Ermöglichung, onlinebasierte Bezahlungen abzuwickeln. Nicht zu den vertragswesentlichen Pflichten dieses Vertrages gehört insbesondere die Haftung für die ununterbrochene technische Verfügbarkeit des Dienstes. Diese Haftungsbeschränkung gilt auch zugunsten der gesetzlichen Vertreter und Erfüllungsgehilfen des Systemanbieters.

6.3. Gegenüber Unternehmern ist die Haftung, außer im Fall der Verletzung von Leben, Körper oder Gesundheit oder der Verletzung wesentlicher Vertragspflichten, auf den typischerweise vorhersehbaren Schaden begrenzt.

6.4. Für von bond:in nicht verschuldete Störungen innerhalb des Leitungsnetzes übernimmt bond:in keine Haftung. Für den Verlust von Daten haftet bond:in nach Maßgabe der vorstehenden Absätze nur dann, wenn ein solcher Verlust durch angemessene Datensicherungsmaßnahmen seitens des Nutzers nicht vermeidbar gewesen wäre. Die Haftung erstreckt sich nicht auf Beeinträchtigungen des vertragsgemäßen Gebrauchs der von bond:in erbrachten Leistungen, die durch eine unsachgemäße oder fehlerhafte Inanspruchnahme durch den Nutzer verursacht worden sind.

6.5. Die vorstehenden Haftungsbeschränkungen gelten sinngemäß auch zugunsten der Erfüllungsgehilfen von bond:in.

6.6. Soweit über die Plattform eine Möglichkeit der Weiterleitung auf Datenbanken, Websites, oder sonstige Dienste Dritter, z.B. durch die Einstellung von Links oder Hyperlinks gegeben ist, haftet bond:in weder für Zugänglichkeit, Bestand oder Sicherheit dieser Datenbanken oder Dienste, noch für den Inhalt derselben. Insbesondere haftet bond:in nicht für deren Rechtmäßigkeit, inhaltliche Richtigkeit, Vollständigkeit und Aktualität.

6.7. Sofern bond:in dem Nutzer Dokumente zur Verfügung stellt, gelten diese lediglich als Anregungen oder Hilfestellungen für die umfassende und eigenverantwortliche Beratung von Client durch den Nutzer.

7. Fremde Inhalte

7.1. Den Nutzern ist es untersagt, Inhalte, z.B. durch Links oder Frames, auf der Plattform einzustellen, die gegen gesetzliche Vorschriften, behördliche Anordnungen oder gegen die guten Sitten verstoßen. Ferner ist es ihnen untersagt, Inhalte einzustellen, die Rechte, insbesondere Urheber- oder Markenrechte Dritter verletzen. Der Plattformbetreiber macht sich fremde Inhalte unter keinen Umständen zu Eigen.

7.2. Bond:in behält sich vor, fremde Inhalte zu sperren, wenn diese nach den geltenden Gesetzen strafbar sind oder erkennbar zur Vorbereitung strafbarer Handlungen dienen.

7.3. Der Nutzer wird bond:in von sämtlichen Ansprüchen freistellen, die Dritte gegen bond:in wegen der Verletzung ihrer Rechte oder wegen Rechtsverstößen aufgrund der vom Nutzer eingestellten Angebote und/oder Inhalte geltend machen, sofern der Nutzer diese zu vertreten

hat. Der Nutzer übernimmt diesbezüglich auch die Kosten der Rechtsverteidigung von bond:in einschließlich sämtlicher Gerichts- und Anwaltskosten.

8. Sonstige Pflichten des Nutzers

8.1. Der Nutzer ist verpflichtet,

(a) die erforderlichen Datensicherungsvorkehrungen während der gesamten Vertragslaufzeit einzurichten und aufrechtzuerhalten. Dies bezieht sich im Wesentlichen auf den sorgfältigen und gewissenhaften Umgang mit Logins und Passwörtern;

(b) in seinem Bereich eintretende technische Änderungen bond:in umgehend mitzuteilen, wenn sie geeignet sind, die Leistungserbringung oder die Sicherheit der Plattform zu beeinträchtigen;

(c) bei der Aufklärung von Angriffen Dritter auf die Plattform mitzuwirken, soweit diese Mitwirkung durch den Nutzer erforderlich ist;

8.2. Der Nutzer verpflichtet sich, alle Maßnahmen zu unterlassen, welche die Funktionsweise der Plattform gefährden oder stören, sowie nicht auf Daten zuzugreifen, zu deren Zugang er nicht berechtigt ist. Weiterhin muss er dafür Sorge tragen, dass seine über die Plattform übertragenen Informationen und eingestellten Daten nicht mit Schadsoftware behaftet sind. Der Nutzer verpflichtet sich, A alle Schäden zu ersetzen, die aus der von ihm zu vertretenden Nichtbeachtung dieser Pflichten entstehen und darüber hinaus bond:in von allen Ansprüchen Dritter, einschließlich der Anwalts- und Gerichtskosten, freizustellen, die diese aufgrund der Nichtbeachtung dieser Pflichten durch den Nutzer gegen A geltend machen.

9. Datenverarbeitung und Einhaltung der Vertraulichkeit

9.1. Bond:in verpflichtet sich zur Einhaltung des Datenschutzes. Bond:in betreibt die Plattform als allein Verantwortlicher im Sinne des Art. 4 Nr. 7 DS-GVO. Die Clientanfragen verarbeitet bond:in im Auftrag des Nutzer als Auftragsverarbeiter (Art. 28 DS-GVO). Es gilt die Vereinbarung zur Auftragsverarbeitung, die als Anhang Bestandteil dieser Nutzungsvereinbarung ist.

9.2. Die Server von bond:in sind dem Stand der Technik entsprechend, insbesondere durch Firewalls, gesichert; dem Nutzer ist jedoch bekannt, dass für alle Teilnehmer die Gefahr besteht, dass übermittelte Daten im Übertragungsweg ausgelesen werden können. Dies gilt nicht nur für den Austausch von Informationen über E-Mail, die das System verlassen sowie für alle sonstigen Übertragungen von Daten. Die Vertraulichkeit, der im Rahmen der Nutzung der Plattform übermittelten Daten kann daher über den Anhang zum Datenschutz hinaus nicht gewährleistet werden.

9.3. Der Nutzer willigt darin ein, dass bond:in Informationen und nicht personenbezogene Daten über die Nutzung in anonymisierter Form speichert und ausschließlich in dieser anonymisierten Form, insbesondere für Marketingzwecke, z.B. für die Erstellung von Statistiken und Präsentationen, nutzen darf.

9.4. Der Plattformbetreiber ist berechtigt, während der Laufzeit dieses Vertrages die im Zusammenhang mit der Geschäftsbeziehung vom Nutzer erhaltenen nicht personenbezogenen Daten zu bearbeiten und zu speichern. Im Einzelnen willigt der Nutzer darin ein, dass der Plattformbetreiber:

(a) die vom Nutzer im Rahmen des Zulassungsantrags gemachten Angaben zu Unternehmensdaten und Rechnungsdaten sowie entsprechende vom Nutzer mitgeteilte Aktualisierungen speichert und bearbeitet;

(b) die vom Nutzer im Zusammenhang mit der von ihm gewünschten Firmenpräsentation und selbstständig in die Plattform eingepflegten Daten speichert und im öffentlichen

und geschlossenen Bereich der Plattform für andere registrierte und nicht registrierte Clients zum Abruf bereithält;

9.5. Der Plattformbetreiber wird im Übrigen alle den Nutzer betreffenden Daten, die von diesem als vertraulich gekennzeichnet werden, vertraulich behandeln und nur nach Maßgabe dieser Nutzungsbedingungen verwenden. Der Pattformbetreiber behält sich vor, hiervon abzuweichen, wenn dieser aufgrund gesetzlicher oder behördlicher Anordnungen Daten des Nutzers offenlegen muss.

10. Abtretung und Aufrechnung

Eine teilweise oder vollständige Übertragung der Rechte des Nutzers aus dem Vertrag mit bond:in auf Dritte ist ausgeschlossen. Zur Aufrechnung gegenüber bond:in ist der Nutzer nur mit unbestrittenen oder rechtskräftigen Gegenforderungen berechtigt.

10.1. **Vertragsdauer**

10.2. Der Vertrag beginnt mit Registrierung und läuft mindestens für einen Monat oder im Fall einer anderweitigen befristeten Lizenzierung für den Zeitraum bis zum Ablauf der Lizenz. Die Vertragsdauer richtet sich nach den aktuellen Konditionen, welche auf der Bestellseite einsehbar sind. Anschließend verlängert er sich automatisch für den identischen Zeitraum, wenn er nicht von einer der Parteien mit einer Frist von einer Woche zum Ende der einmonatigen Vertragslaufzeit, von einem Monat zum Ende einer mehrmonatigen Laufzeit oder von drei Monaten zum Ende einer einjährigen Laufzeit gekündigt wird.

10.3. Eine Kündigung vor Ablauf einer vereinbarten Mindestvertragslaufzeit ist nicht möglich. Das Recht beider Parteien zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt. Ein wichtiger Grund liegt insbesondere dann vor, wenn über das Vermögen der jeweils anderen Partei ein Insolvenzverfahren eröffnet wird oder die Eröffnung eines solchen Verfahrens mangels Masse abgelehnt wird.

10.4. Jede Kündigung bedarf der Textform (z.B. E-Mail).

11. Änderungen dieser AGB

Der Systemanbieter behält sich das Recht vor, diese AGB, damit verbundene Leistungsbeschreibungen und Preise jederzeit und ohne Angabe von Gründen zu ändern. Diese neuen AGB werden rechtzeitig, mindestens jedoch zwei Monate vor dem Zeitpunkt, zu dem sie in Kraft treten sollen, schriftlich bekanntgegeben. Hat der Systemanbieter mit dem Nutzer einen elektronischen Kommunikationsweg vereinbart, können die Änderungen auch auf diesem Weg übermittelt werden, wenn die Art der Übermittlung es dem Nutzer erlaubt, die Änderungen in lesbarer Form zu speichern oder auszudrucken. Widerspricht der Nutzer Änderungen nicht spätestens vor dem vorgeschlagenen Zeitpunkt des Wirksamwerdens schriftlich oder auf dem vereinbarten elektronischen Weg, gelten die Änderungen als angenommen. Der Systemanbieter wird den Nutzer in dem Mitteilungsschreiben auf die Bedeutung seines Schweigens und den Zeitpunkt des beabsichtigten Wirksamwerdens der Änderungen, sowie auf das Recht zur kostenfreien und fristlosen Kündigung hinweisen. Widerspricht der Nutzer, gelten die bisherigen Bedingungen fort.

12. Salvatorische Klausel

12.1. Auf die vorliegenden AGB findet deutsches Recht unter Ausschluss des UN-Kaufrechts Anwendung. Für Streitigkeiten aus diesem Vertrag ist ausschließlicher Gerichtsstand Berlin.

12.2. Mündliche Nebenabreden sind nicht getroffen. Änderungen, Ergänzungen und Zusätze dieses Vertrages haben nur Gültigkeit, wenn sie zwischen den Vertragsparteien schriftlich vereinbart werden. Dies gilt auch für die Abänderung dieser Vertragsbestimmung.

12.3. Sollte eine Bestimmung dieses Vertrages unwirksam sein oder werden, so berührt dies die Wirksamkeit des Vertrages im Übrigen nicht. Die unwirksame Bestimmung gilt als durch eine wirksame Regelung ersetzt, die dem wirtschaftlichen Zweck der unwirksamen Bestimmung am nächsten kommt. Entsprechendes gilt im Fall einer Vertragslücke.

12.4. Anlagen, auf die in diesem Vertrag Bezug genommen wird, sind Vertragsbestandteil.

Anhang: Vereinbarung zur Auftragsverarbeitung

Diese Vereinbarung zwischen dem Nutzer (nachfolgend: Auftraggeber) und bond:in (nachfolgend Auftragnehmende) konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus der im Nutzungsvertrag (nachfolgend: Hauptvertrag) in ihren Einzelheiten beschriebenen Auftragsverarbeitung ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmenden oder durch den Auftragnehmenden Beauftragte mit personenbezogenen Daten („Daten“) des Auftraggeber n in Berührung kommen können.

1. Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung

1.1 Der Gegenstand der Auftragsverarbeitung ist im Hauptvertrag beschrieben. Im Wesentlichen handelt es sich um die Erfassung von Clientendaten für die Information zur betrieblichen Altersvorsorge. Nicht Gegenstand der Auftragsverarbeitung ist der Betrieb der Plattform selbst.

1.2 Art und Zweck der Auftragsverarbeitung sind im Hauptvertrag beschrieben und umfassen insbesondere die Registrierung und Verarbeitung der personenbezogenen Daten der Nutzer sowie der Clients.

1.3 Die Verarbeitung umfasst alle Daten, die von Nutzern oder Clients erhoben werden. Dies umfasst regelmäßig Vorname, Nachname, Kontaktdaten (Adresse, E-Mail, Telefonnummer) sowie für die betrieblichen Altersvorsorge erforderliche Daten.

1.4 Von der Verarbeitung betroffen sind Clients und Nutzer.

1.5 Die Laufzeit dieser Vereinbarung richtet sich nach der Laufzeit des Hauptvertrages.

2. Anwendungsbereich und Verantwortlichkeit

2.1 Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggeber. Dies umfasst Tätigkeiten, die im Hauptvertrag konkretisiert sind. Der Auftraggeber ist hinsichtlich der Verarbeitung der Daten für die Einhaltung der gesetzlichen Bestimmungen zum Datenschutz, insbesondere für die Rechtmäßigkeit der Datenverarbeitung verantwortlich.

2.2 Die Weisungen werden anfänglich durch den Hauptvertrag festgelegt und können vom Auftraggeber n danach in schriftlicher Form oder in Textform durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen, die über die vertraglich vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt.

2.3 Im Falle einer Inanspruchnahme durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, verpflichten sich Auftraggeber und Auftragnehmer, sich bei der Abwehr des Anspruches gegenseitig zu unterstützen.

3. Pflichten des Auftragnehmers

3.1 Der Auftragnehmer darf Daten von betroffenen Personen nur im Rahmen des Auftrages und der dokumentierten Weisungen des Auftraggeber n verarbeiten. Sofern der Auftragnehmer durch nationales oder europäisches Recht zu einer hiervon abweichenden Verarbeitung verpflichtet ist, weist er – sofern dies rechtlich zulässig ist – den Auftraggeber vor Beginn der Verarbeitung auf diesen Umstand hin. Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Der Auftragnehmer darf die Umsetzung der Weisung solange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde.

3.2 Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird die in Ziffer 9 beschriebenen technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Daten des Auftraggeber treffen. Die Maßnahmen sollen die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen. Dem Auftraggeber sind diese technischen und organisatorischen Maßnahmen bekannt. Er trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten.

3.3 Eine Änderung der getroffenen technischen und organisatorischen Maßnahmen bleibt dem Auftragnehmenden vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

3.4 Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten und der vertraglich geschuldeten Leistung bei der Erfüllung der Anfragen und Ansprüche Betroffener gemäß Kapitel III der DS-GVO sowie bei der Einhaltung der in Art. 33 bis 36 DS-GVO genannten Pflichten.

3.5 Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggeber befassten Mitarbeitern und anderen für den Auftragnehmenden tätigen Personen untersagt ist, die Daten außerhalb der Weisungen des Auftraggeber zu verarbeiten. Ferner gewährleistet der Auftragnehmende, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits- und Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.

3.6 Der Auftragnehmer unterrichtet den Auftraggeber n unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggeber n bekannt werden. Der Auftragnehmer trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der Betroffenen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab.

3.7 Der Auftragnehmer nennt dem Auftraggeber auf Anfrage den Ansprechpartner bzw. die Ansprechpartnerin für im Rahmen des Vertrages anfallende Datenschutzfragen.

3.8 Der Auftragnehmer gewährleistet, seinen Pflichten nach 32 Abs. 1 lit. d DS-GVO nachzukommen und ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen.

3.9 Der Auftragnehmer berichtigt oder löscht die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist und dies vom Weisungsrahmen umfasst ist. Ist eine datenschutzkonforme Löschung oder eine entsprechende Beschränkung der

Datenverarbeitung nicht möglich, übernimmt der Auftragnehmer die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien auf Grund einer Einzelbeauftragung durch den Auftraggeber n, sofern nicht im Vertrag bereits vereinbart.

3.10 Daten, Datenträger sowie sämtliche sonstige Materialien sind nach Auftragsende auf Verlangen des Auftraggeber n entweder herauszugeben oder zu löschen. Der Auftragnehmer ist berechtigt bis zur Erfüllung gesetzlicher oder vertraglicher Aufbewahrungsfristen die Daten oder eine Kopie der Daten aufzubewahren.

4. Pflichten des Auftraggeber

4.1 Der Auftraggeber hat den Auftragnehmenden unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

4.2 Der Auftraggeber nennt dem Auftragnehmenden den Ansprechpartner bzw. die Ansprechpartnerin für im Rahmen des Vertrages anfallende Datenschutzfragen.

5. Anfragen Betroffener

Wendet sich eine betroffene Person mit Forderungen zur Berichtigung oder Auskunft an den Auftragnehmenden, wird der Auftragnehmer die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber nach den Angaben der betroffenen Person möglich ist.

6. Nachweismöglichkeiten

6.1 Der Auftragnehmer weist dem Auftraggeber n die Einhaltung der in Art 28. DS-GVO und diesem Vertrag niedergelegten Pflichten mit geeigneten Mitteln nach. Zum Nachweis der Einhaltung der vereinbarten Pflichten kann der Auftragnehmende, dem Auftraggeber Zertifikate und Prüfergebnisse Dritter (z.B. nach Art. 42 DS-GVO oder ISO 27001) zur Verfügung stellen oder Prüfberichte des betrieblichen Datenschutzbeauftragten.

6.2 Sollten im Einzelfall Inspektionen durch den Auftraggeber oder einen von diesem beauftragten Prüfer erforderlich sein, werden diese zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit durchgeführt. Der Auftragnehmer darf diese von der Unterzeichnung einer angemessenen Verschwiegenheitserklärung abhängig machen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Auftragnehmenden stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht

6.3 Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Auftraggeber n eine Inspektion vornehmen, gilt grundsätzlich 6.2 entsprechend. Eine Unterzeichnung einer Verschwiegenheitsverpflichtung ist nicht erforderlich, wenn diese Aufsichtsbehörde einer berufsrechtlichen oder gesetzlichen Verschwiegenheit unterliegt, bei der ein Verstoß nach dem Strafgesetzbuch strafbewehrt ist.

6.4 Für die Unterstützung bei der Durchführung einer Inspektion nach Ziffer 6.2 oder 6.3 darf der Auftragnehmer eine angemessene Vergütung verlangen, sofern nicht Anlass der Inspektion der dringende Verdacht eines Datenschutzvorfalls im Verantwortungsbereich des Auftragnehmenden war. In diesem Fall sind die Verdachtsmomente mit der Ankündigung der Inspektion vom Auftraggeber vorzutragen.

7. Subunternehmer (weitere Auftragsverarbeiter)

7.1 Der Auftraggeber stimmt zu, dass der Auftragnehmer Subunternehmenden hinzuzieht. Vor der Hinzuziehung oder Ersetzung von Subunternehmenden informiert der Auftragnehmer den Auftraggeber mit einer Frist von zwei Wochen in Textform. Der Auftraggeber kann der Änderung nur aus wichtigem Grund widersprechen. Der Widerspruch hat binnen 14 Tagen zu erfolgen und alle wichtigen Gründe ausdrücklich zu benennen. Erfolgt innerhalb der Frist kein Widerspruch, gilt die Zustimmung zur Änderung als gegeben. Liegt ein wichtiger Grund vor, der vom Auftragnehmenden nicht durch Anpassung des Auftrages beseitigt werden kann, wird dem Auftraggeber n ein Sonderkündigungsrecht eingeräumt. Über die bei Vertragsschluss bereits bestehenden Subunternehmer und Teilleistungen erfolgt keine gesonderte Information. Ein Widerspruchsrecht des Auftraggeber n besteht für die bei Vertragsschluss bestehende Subunternehmenden nicht.

7.2 Erteilt der Auftragnehmer Aufträge an Subunternehmenden, so obliegt es dem Auftragnehmenden, seine datenschutzrechtlichen Pflichten aus diesem Vertrag dem Subunternehmenden zu übertragen.

7.3 Auf schriftliche Aufforderung des Auftraggeber hat der Auftragnehmer jederzeit Auskunft über die datenschutzrelevanten Verpflichtungen seiner Subunternehmenden zu erteilen.

8. Informationspflichten, Schriftformklausel, Rechtswahl

8.1 Sollten die Daten des Auftraggeber beim Auftragnehmenden durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber n als „Verantwortlicher“ im Sinne der Datenschutz-Grundverordnung liegen.

8.2 Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmenden – bedürfen einer schriftlichen Vereinbarung, die auch in elektronischer Form erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

8.3 Bei etwaigen Widersprüchen gehen Regelungen dieser Vereinbarung zum Datenschutz den Regelungen des Vertrages vor. Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

9. Technische und organisatorische Maßnahmen

Rechenzentrum

Unser Rechenzentrum unterhält ein Informationssicherheitsprogramm (einschließlich der Einführung und Durchsetzung interner Richtlinien und Verfahren), das dazu dient, (a) dem Kunden dabei zu helfen, seine Daten vor versehentlichem oder unrechtmäßigem Verlust, Zugriff oder Offenlegung zu schützen, (b) vernünftigerweise vorhersehbare und interne Risiken für die Sicherheit und den unbefugten Zugriff auf das Netzwerk zu identifizieren und (c) Sicherheitsrisiken zu minimieren, unter anderem durch Risikobewertung und regelmäßige Tests. Das Informationssicherheitsprogramm wird die folgenden Maßnahmen umfassen:

(a) Netzwerksicherheit. Das Netzwerk ist für Mitarbeiter, Auftragnehmer und alle anderen Personen, die für die Erbringung der Services erforderlich sind, elektronisch zugänglich.

Zugriffskontrollen und Richtlinien werden unterhalten, um zu verwalten, welcher Zugriff auf das Netzwerk von jeder Netzwerkverbindung und jedem Benutzer erlaubt ist, einschließlich der Verwendung von Firewalls oder funktional gleichwertiger Technologie und Authentifizierungskontrollen. Das Rechenzentrum unterhält Pläne für Abhilfemaßnahmen und Reaktionen auf Vorfälle, um auf potenzielle Sicherheitsbedrohungen zu reagieren.

(b) Physische Zugangskontrollen. Die physischen Komponenten des Netzwerks sind in nicht näher bezeichneten Einrichtungen untergebracht. Physische Schrankenkontrollen werden eingesetzt, um den unbefugten Zutritt zu den Einrichtungen sowohl an den Außengrenzen als auch an den Gebäudezugängen zu verhindern. Das Passieren der physischen Barrieren in den Einrichtungen erfordert entweder eine elektronische Zugangskontrolle (z. B. Kartenzugangssysteme usw.) oder eine Validierung durch menschliches Sicherheitspersonal (z. B. vertraglich vereinbarter oder interner Wachdienst, Empfangspersonal usw.). Mitarbeitern und Auftragnehmern werden Lichtbildausweise zugewiesen, die getragen werden müssen, während sich die Mitarbeiter und Auftragnehmer in einer der Einrichtungen aufhalten. Besucher müssen sich beim zuständigen Personal anmelden, sich ausweisen, erhalten einen Besucherausweis, den sie tragen müssen, wenn sie sich in den Einrichtungen aufhalten, und werden beim Besuch der Einrichtungen ständig von autorisierten Mitarbeitern oder Auftragnehmern begleitet.

(c) Beschränkter Zugang für Mitarbeiter und Auftragnehmer. Das Rechenzentrum gewährt denjenigen Mitarbeitern und Auftragnehmern Zugang zu den Einrichtungen, die einen legitimen geschäftlichen Grund für diese Zugangsrechte haben. Wenn ein Mitarbeiter oder Auftragnehmer kein geschäftliches Bedürfnis mehr für die ihm zugewiesenen Zugriffsrechte hat, werden die Zugriffsrechte unverzüglich entzogen, auch wenn der Mitarbeiter oder Auftragnehmer weiterhin ein Mitarbeiter des Rechenzentrum oder seinen Verbundenen Unternehmen ist.

(d) Physische Sicherheitsvorkehrungen. Alle Zugangspunkte (mit Ausnahme der Haupteingangstüren) werden in einem gesicherten (verschlossenen) Zustand gehalten. Die Zugangspunkte zu den Einrichtungen werden durch Videoüberwachungskameras überwacht, die alle Personen aufzeichnen, die die Einrichtungen betreten. Das Rechenzentrum unterhält außerdem elektronische Einbruchserkennungssysteme, die darauf ausgelegt sind, unbefugten Zutritt zu den Einrichtungen zu erkennen, einschließlich der Überwachung von Schwachstellen (z. B. Haupteingangstüren, Notausstiegstüren, Dachluken, Türen von Verladerampen usw.) mit Türkontakten, Glasbruchvorrichtungen, Bewegungserkennung im Inneren oder anderen Vorrichtungen, die darauf ausgelegt sind, Personen zu erkennen, die versuchen, sich Zugang zu den Einrichtungen zu verschaffen. Alle physischen Zugang zu den Einrichtungen durch Mitarbeiter und Auftragnehmer wird protokolliert und routinemäßig überprüft.

Fortlaufende Bewertung. Das Rechenzentrum führt regelmäßige Überprüfungen der Sicherheit seines Netzwerks und der Angemessenheit seines Informationssicherheitsprogramms durch, gemessen an den Sicherheitsstandards der Branche und seinen Richtlinien und Verfahren. Das Rechenzentrum wird die Sicherheit seines Netzwerks und der zugehörigen Services kontinuierlich bewerten, um festzustellen, ob zusätzliche oder andere Sicherheitsmaßnahmen erforderlich sind, um auf neue Sicherheitsrisiken oder Erkenntnisse aus den regelmäßigen Überprüfungen zu reagieren.