Vereinbarung

Zwischen der

_____

- Verantwortlicher - nachstehend Auftraggeber genannt -

und der

venabo GmbH

- Auftragsverarbeiter - nachstehend Auftragnehmer genannt

Inhaltsverzeichnis

1. Gegenstand und Dauer des Auftrags 3
2. Technisch-organisatorische Maßnahmen 3
3. Berichtigung, Einschränkung und Löschung von Daten 3
4. Qualitätssicherung und sonstige Pflichten des Auftragnehmers 4
5. Unterauftragsverhältnisse 5
6. Erfüllung der Betroffenenrechte 5
7. Kontrollrechte des Auftraggebers 6
8. Mitteilung bei Verstößen des Auftragnehmers 6
9. Weisungsbefugnis des Auftraggebers 7
10. Haftung 7
11. Löschung und Rückgabe von personenbezogenen Daten 7
12. Salvatorische Klausel 7
13. Formerfordernis 7
14. Beginn der Vereinbarung, Auswirkung von Kündigungen 8

Anlage 1 - Auflistung der beauftragten Dienstleistungen

Anlage 2 - Liste der beauftragten Unterauftragnehmer einschließlich der Verarbeitungsstandorte

Anlage 3 - Technisch-organisatorische Maßnahmen

1. Gegenstand und Dauer des Auftrags

(1) Der Auftragnehmer führt die im Anhang 1 beschriebenen Dienstleistungen für den Auftraggeber durch. Gegenstand, Art und Zweck der Verarbeitung, die Art der Daten sowie die Kategorie betroffener Personen werden dort beschrieben.

(2) Dieser Vertrag tritt – solange keine anderweitigen Regelungen vereinbart wurden – mit Unterzeichnung beider Parteien in Kraft und gilt, solange der Auftragnehmer für den Auftraggeber personenbezogene Daten verarbeitet.

(3) Die in den jeweiligen vertraglichen Vereinbarungen geregelten Kündigungsfristen bleiben unberührt.

2. 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 im Anhang 3 dieses Vertrages 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 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO 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, der 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 DSGVO zu berücksichtigen [Einzelheiten in Anlage 3].

(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) Fernzugriffe zu Prüfungs- und/oder Wartungsarbeiten von unterwegs mit einem mobilen Gerät oder von einem Home-Office aus bedürfen keiner gesonderten Zustimmung des Verantwortlichen. Bei diesen besonderen Fernzugriffen kann der Auftragnehmer die technischen und organisatorischen Maßnahmen nicht vollumfänglich gewährleisten.

3. 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.

4. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

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

a) Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DSGVO ausübt. Dessen jeweils aktuelle Kontaktdaten sind auf der Homepage des Auftragnehmers leicht zugänglich hinterlegt.

b) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO. 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 DSGVO [Einzelheiten in Anlage 3].

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 Ordnungswidrigkeits- 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 Ordnungswidrigkeits- 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 Person gewährleistet wird.

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

5. 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 z.B. 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.
(2) Der Auftraggeber stimmt zu, dass der Auftragnehmer Unterauftragnehmer hinzuzieht. Vor Hinzuziehung oder Ersetzung der Unterauftragnehmer informiert der Auftragnehmer den Auftraggeber. Der Auftraggeber kann der Änderung – innerhalb von 7 Tagen – aus wichtigem Grund –widersprechen. Erfolgt kein Widerspruch innerhalb der Frist gilt die Zustimmung zur Änderung als gegeben.
(3) Der Auftraggeber stimmt der Beauftragung der in Anlage 2 dieser Vereinbarung genannten Unterauftragnehmer zu, die Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO ist zu erfüllen.
(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) Der Auftragnehmer sorgt bei einer Beauftragung von Unterauftragnehmern dafür, dass sämtliche Regelungen dieser Vereinbarung auch vom Unterauftragnehmer eingehalten und gegenüber weiterer Unterauftragnehmer in der gesamten Auftragskette durchgesetzt werden.

6. Erfüllung der Betroffenenrechte

(1) Ist der Auftraggeber auf Grund geltender Datenschutzgesetze gegenüber einer Einzelperson verpflichtet, Auskünfte zur Erhebung, Verarbeitung oder Nutzung von Daten dieser Person zu geben, wird der Auftragnehmer den Auftraggeber dabei unterstützen, diese Informationen bereit zu stellen, vorausgesetzt:

a) der Auftraggeber hat den Auftragnehmer hierzu schriftlich aufgefordert und
b) der Auftraggeber erstattet dem Auftragnehmer die durch diese Unterstützung entstandenen Kosten.

(2) Soweit ein Betroffener sich an den Auftragnehmer zwecks Berichtigung oder Löschung seiner Daten wenden sollte, wird der Auftragnehmer dieses Ersuchen an den Auftraggeber weiterleiten.
(3) Der Auftragnehmer unterstützt den Auftraggeber nach Möglichkeit und gegen Erstattung der hierfür entstehenden Kosten mit geeigneten technischen und organisatorischen Maßnahmen dabei, seiner Pflicht zur Beantwortung von Anträgen der Betroffenen auf Berichtigung, Löschung, Einschränkung der Verarbeitung und Datenübertragbarkeit nachzukommen. Der Auftragnehmer haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

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 vorab mit einer Frist von 14 Tagen 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 DSGVO 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 eine der nachstehenden Optionen:

- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO oder
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO oder
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

(4) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.
(5) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn der Auftraggeber Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsverarbeitung feststellt.

8. Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

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 (mind. 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 so lange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.
(3) Der Auftraggeber ist verpflichtet dem Auftragnehmer nur Weisungen zu erteilen, die im Einklang mit den datenschutzrechtlichen Vorgaben gem. der gültigen Datenschutzgesetze sind. Den Auftragnehmer trifft keinerlei Verpflichtung, Weisungen des Auftraggebers (datenschutz-) rechtlich zu prüfen

10. Haftung

(1) Die Haftung richtet sich nach Art. 82 DSGVO.

11. 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 datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial.
(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.

12. Salvatorische Klausel

Sollten sich einzelne Bestimmungen dieser Vereinbarung als ungültig erweisen, so wird hierdurch die Gültigkeit der übrigen Bestimmungen nicht berührt. Die ungültige Bestimmung ist durch eine solche Regelung zu ersetzen, die die Parteien getroffen hätten, hätten sie bei Abschluss des Vertrags an die Ungültigkeit des jeweiligen Punktes gedacht. Soweit diese Vereinbarung eine unbewusste Regelungslücke enthält, ist diese durch eine solche Regelung zu ersetzen, die die Parteien getroffen hätten, hätten sie bei Abschluss des Vertrags an die Regelungsbedürftigkeit des jeweiligen Punktes gedacht.

13. Formerfordernis

Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile - einschließlich etwaiger Zusicherungen des Auftragnehmers - sind gemäß DSGVO schriftlich abzufassen, was auch in einem elektronischen Format 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.

14. Beginn der Vereinbarung, Auswirkung von Kündigungen

(1) Diese Vereinbarung beginnt mit Bestätigung des Vertragsschlusses durch venabo.
(2) Nimmt der Kunde/Geschäftspartner Änderungen am Vertragstext vor beginnt diese Vereinbarung mit Annahme der geänderten Fassung durch venabo; venabo ist zur Annahme jedoch nicht verpflichtet.
(3) Eine Annahme der geänderten Fassung durch venabo erfolgt nicht bereits durch (fortgesetzte) Leistungserbringung, sondern erfordert eine dem Formerfordernis des Art. 28 DSGVO entsprechende Annahmeerklärung durch venabo.
(4) Diese Vereinbarung endet nicht automatisch mit der Kündigung aller Leistungsvereinbarungen und sonstigen vertraglichen Vereinbarungen, sondern bedarf des ausdrücklichen Hinweises darauf in der Kündigung, dass es sich um eine Kündigung dieser Vereinbarung zur Auftragsverarbeitung handelt.

_____	_____
Ort, Datum	Auftraggeber
_____	_____
Ort, Datum	Auftragnehmer