Vereinbarung zur Auftragsverarbeitung

I. Präambel

Diese Vereinbarung wird zwischen dem Provider (Contabo GmbH; nachfolgend auch „Auftragnehmer“) und dem Kunden (nachfolgend auch „Auftraggeber“; gemeinsam die „Vertragsparteien“) zusätzlich zum auf der Bestellung des Kunden und den AGB des Providers basierenden, bereits bestehenden Hauptvertrag geschlossen. Für den nicht zwingendermaßen, gleichwohl möglicherweise eintretenden Fall, dass der Provider bei Ausführung seiner Tätigkeiten im Rahmen des Hauptvertrages personenbezogene Daten verarbeiten muss, für die der Kunde Verantwortlicher iSd Verordnung 2016/679 (Datenschutz-Grundverordnung; DS-GVO) ist, schließen die Vertragsparteien vorsorglich entsprechend Art. 28 Abs. 9 DS-GVO die nachstehende Vereinbarung zur Auftragsverarbeitung, um die wechselseitigen Rechte und Pflichten bei einer etwaigen Auftragsverarbeitung durch den Provider zu konkretisieren.

II. Gegenstand und Dauer des Auftrags

Der Gegenstand und die Dauer des Auftrags ergibt sich aus der zum Zeitpunkt der Bestellung des Kunden aktuellen Leistungsbeschreibung des bestellten Dienstes in Verbindung mit den AGB des Providers, auf die hier verwiesen wird.

III. Konkretisierung des Auftragsinhalts

1. Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind konkret in der zum Zeitpunkt der Bestellung des Kunden aktuellen Leistungsbeschreibung des bestellten Dienstes in Verbindung mit den AGB des Providers beschrieben.
2. 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. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.
3. Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenkategorien:
    - Personenstammdaten, z.B. Name, Adresse
    - Unternehmensstammdaten, z.B. Mitarbeiter, Adressen, Bankverbindungen, Steuerdaten
    - Kommunikationsdaten, z.B. Telefon, E-Mail
    - Vertragsstammdaten, z.B. Serverdaten, Logindaten
    - Logdaten, z.B. Login-Historie, verwendete IP-Adressen
    - Prozessdaten, z.B. Email- und Telefonanfragen, Netzwerkstörungen
    - Kundenhistorie
    - Vertragsabrechnungs- und Zahldaten
    - Auskunftsangaben, z.B. Schufa-Daten oder Angaben aus öffentlichen Verzeichnissen
4. Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen neben Angestellten und freien Mitarbeitern des Auftraggebers auch dessen Kunden, Interessenten, Website-Besucher, Lieferanten und sonstige Personen, deren personenbezogenen Daten der

Auftraggeber auf seinen Servern konkret speichert.

IV. Technisch-organisatorische Maßnahmen

1. Die Vertragsparteien vereinbaren die im Anhang 1 zu dieser Vereinbarung dargestellten technischen und organisatorischen Maßnahmen. Dieser Anhang 1 ist Teil der vorliegenden Vereinbarung.
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, 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 DS-GVO zu berücksichtigen [Einzelheiten in 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.

V. 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.

VI. 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:

1. Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DS-GVO ausübt. Dessen jeweils aktuelle Kontaktdaten sind auf der Homepage des Auftragnehmers leicht zugänglich hinterlegt.
2. 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.

3. 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 in Anhang 1].
4. Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
5. 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.
6. 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.
7. 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.
8. Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer VIII dieses Vertrages.

VII. 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 Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur auf Basis der folgenden Vereinbarung beauftragen:
   Die Auslagerung auf Unterauftragnehmer 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.

3. Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.
4. Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher.
5. Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen Zustimmung des Hauptauftragnehmers (mind. Textform); sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

VIII. Kontrollrechte des Auftraggebers

1. Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen. Die Kontrollen sind dem Auftragnehmer mit einer Vorlaufzeit von nicht weniger als 10 Werktagen (Mo.-Fr. – nicht 24. und 31.12.), bei Vorliegen eines Datensicherheitsvorfalles von nicht weniger als 5 Werktagen anzukündigen. Der Auftraggeber hat hierbei angemessene Rücksicht auf die Betriebsabläufe zu nehmen sowie Verschwiegenheit über Betriebs- und Geschäftsgeheimnisse des Auftragnehmers zu wahren. Eine Überprüfung durch Dritte für den Auftraggeber bedarf der vorherigen schriftlichen Zustimmung des Auftragnehmers. Beauftragt der Auftraggeber mit Zustimmung des Auftragnehmers einen Dritten mit der Durchführung der Kontrolle, hat der Auftraggeber den Dritten schriftlich zur Geheimhaltung zu verpflichten, es sei denn, dass der Dritte einer beruflichen Geheimhaltungsverpflichtung unterliegt. Auf Verlangen des Auftragnehmers hat der Auftraggeber diesem die Verpflichtungsvereinbarungen mit dem Dritten unverzüglich vorzulegen. Der Auftraggeber darf keinen Konkurrenten des Auftragnehmers mit der Kontrolle beauftragen.
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. Für die Ermöglichung von Kontrollen durch den Auftraggeber wird der Auftragnehmer einen Vergütungsanspruch geltend machen.

IX. 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 u.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
- die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden
- 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
- die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung
- 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, wird der Auftragnehmer eine Vergütung beanspruchen.

X. 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 solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

XI. 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, 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.

XII. Laufzeit und Kündigung dieser Vereinbarung

1. Die Laufzeit und Kündigung dieser Vereinbarung richtet sich nach den Bestimmungen zur Laufzeit und Kündigung des Hauptvertrages. Eine Kündigung des Hauptvertrages bewirkt automatisch auch eine Kündigung dieser Vereinbarung. Eine isolierte Kündigung dieser Vereinbarung ist ausgeschlossen. Eine Kündigung aus wichtigem Grund bleibt unberührt.
2. Eine Kündigung bedarf zu ihrer Wirksamkeit der Textform.

XIII. Schlussbestimmungen

1. Gerichtsstand für alle Streitigkeiten aus dieser Vereinbarung ist München.
2. Auf diese Vereinbarung findet das deutsche Recht unter Ausschluss des internationalen Privatrechts Anwendung.
3. Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile bedürfen einer schriftlichen Vereinbarung 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.
4. Der Auftraggeber sowie jeder Nutzer erklärt sich damit einverstanden, dass der Auftragnehmer system-oder produktrelevante Informationen per E-Mail versendet. Diese Einwilligung kann jederzeit widerrufen werden.
5. Sollten einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise unwirksam sein oder werden, wird die Wirksamkeit der übrigen Bestimmungen hierdurch nicht berührt. Die Vertragsparteien verpflichten sich für diesen Fall, die ungültige Bestimmung durch eine wirksame Bestimmung zu ersetzen, die dem wirtschaftlichen Zweck der ungültigen Bestimmung möglichst nahe kommt. Entsprechendes gilt für etwaige Lücken dieser Vereinbarung.

Anhang 1: Technisch-organisatorische Maßnahmen

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

- **Zutrittskontrolle**
  Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, z.B. Chipkarten, Schlüssel, elektrische Türöffner, Alarmanlagen, Videoanlagen;
- **Zugangskontrolle**
  Keine unbefugte Systembenutzung, z.B.: (sichere) Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Protokollierung der Besucher, Personenkontrolle
- **Zugriffskontrolle**
  Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen;
- **Trennungskontrolle**
  Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B. Sandboxing;

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

- **Weitergabekontrolle**
  Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Ermöglichung von Verschlüsselung, Virtual Private Networks (VPN), sorgfältige Auswahl des Personals bei Transport
- **Eingabekontrolle**
  Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung und Loggen von Benutzernamen

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

- **Verfügbarkeitskontrolle**
  Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (soweit im Leistungsumfang gem. Hauptvertrag enthalten), unterbrechungsfreie Stromversorgung am RZ-Standort Nürnberg (USV + Dieselgenerator), Virenschutz, Firewall, Meldewege und Notfallpläne;
- **Rasche Wiederherstellbarkeit** (Art. 32 Abs. 1 lit. c DS-GVO)

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

- **Datenschutz-Management;**
- **Incident-Response-Management**
- **Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO);**
- **Auftragskontrolle**
  Keine Auftragsverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.