Vertrag über Auftragsverarbeitung

zwischen

KUNDE

(Verantwortlicher)

und der

compass Computer Anwendungs- u. Service GmbH

Steinbeisstr. 40

73730 Esslingen

(Auftragsverarbeiter)

1. Gegenstand und Dauer des Auftrags

1.1 Gegenstand

Gegenstand dieses Vertrages ist die Verarbeitung personenbezogener Daten (im Weiteren 'Daten') durch die compass GmbH für den Auftraggeber im Zusammenhang mit der Nutzung, insbesondere im Zusammenhang mit Supporttätigkeiten des DV-Programmes/Verfahrens:

Remote Support Unterstützung via compass QuickSupport

1.2 Dauer

Die Dauer dieses Auftrags (Laufzeit) entspricht der gesamten Zeitspanne der IT-Betreuung der Hard- u. Softwareinstallation des Kunden.

2. Konkretisierung des Auftragsinhalts

2.1 Art und Zweck der vorgesehenen Verarbeitung von Daten

Im Supportfall ist es dem Auftragsverarbeiter möglich, sich unter direkter/aktiver Mitwirkung auf einen Rechner/Server des Verantwortlichen mit Sicht,- oder Steuerungsrechten (z.B. zur Anpassung von produktspezifischen Systemeinstellungen) zu verbinden.

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union, in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Verantwortlichen und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

2.2 Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien)

- Namen der Kunden des Auftraggebers
- Namen von Beschäftigten des Auftraggebers
- Software-Applikationsdaten der Produkte des Kunden
- Bildschirminhalt (Live-Desktop) des Verantwortlichen

2.3 Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- Kunden des Auftraggebers
- Beschäftigte des Auftraggebers

3. Technisch-organisatorische Maßnahmen

3.1 Der Auftragsverarbeiter 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 Verantwortlichen zur Prüfung zu übergeben. Bei Akzeptanz durch den Verantwortlichen werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Verantwortlichen einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

3.2 Der Auftragsverarbeiter 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 1).

3.3 Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragsverarbeiter 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

4.1 Der Auftragsverarbeiter darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Verantwortlichen berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragsverarbeiter wendet, wird der Auftragsverarbeiter dieses Ersuchen unverzüglich an den Verantwortlicher weiterleiten.

4.2 Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Verantwortlichen unmittelbar durch den Auftragsverarbeiter sicherzustellen.

5. Qualitätssicherung und sonstige Pflichten des Auftragsverarbeiters

Der Auftragsverarbeiter 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:

5.1 Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DSGVO ausübt.

Verantwortlicher für den Datenschutz beim Auftragsverarbeiter ist:
Herr Norbert Jakob. Kontaktdaten: datenschutz@compass-es.de, Tel.: 0711-930707-0

5.2 Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO. Der Auftragsverarbeiter 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 Auftragsverarbeiter und jede dem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend

der Weisung des Verantwortlichen verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

5.3 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 1).

5.4 Der Verantwortliche und der Auftragsverarbeiter arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

5.5 Die unverzügliche Information des Verantwortlichen 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 Auftragsverarbeiter ermittelt.

5.6 Soweit der Verantwortliche 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 Auftragsverarbeiter ausgesetzt ist, hat ihn der Auftragsverarbeiter nach besten Kräften zu unterstützen.

5.7 Der Auftragsverarbeiter 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.

5.8 Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Verantwortlicher im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

6. Unterauftragsverhältnisse

6.1 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 Auftragsverarbeiter 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 Auftragsverarbeiter ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Verantwortlichen auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

6.2 Die Auslagerung auf Unterauftragnehmer oder der Wechsel der bestehenden genehmigten Unterauftragnehmer sind zulässig, soweit der Auftragnehmer eine solchen Einschaltung von Unterauftragnehmern 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 DSGVO oder Art. 46 Abs. 2 litt. c und d DSGVO zugrunde gelegt wird. Im Falle des Einspruchs des Auftraggebers steht dem Auftragnehmer ein

außerordentliches Kündigungsrecht sowohl hinsichtlich dieser Vereinbarung als auch bezüglich der Leistungsvereinbarung zu.

Dem Verantwortlicher sind vor Beginn der Verarbeitung die Unterauftragnehmer nach **Anlage 2** mitgeteilt worden.

6.3 Die Weitergabe von personenbezogenen Daten des Verantwortlichen an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

6.4 Sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

7. Kontrollrechte des Verantwortlichen

7.1 Der Verantwortliche hat das Recht, im Benehmen mit dem Auftragsverarbeiter 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 Auftragsverarbeiter in dessen Geschäftsbetrieb zu überzeugen.

7.2 Der Auftragsverarbeiter stellt sicher, dass sich der Verantwortlicher von der Einhaltung der Pflichten des Auftragsverarbeiters nach Art. 28 DSGVO überzeugen kann. Der Auftragsverarbeiter verpflichtet sich, dem Verantwortlicher auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

7.3 Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch

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

7.4 Für die Ermöglichung von Kontrollen durch den Kunden kann der Auftragsverarbeiter einen Vergütungsanspruch geltend machen.

8. Mitteilung bei Verstößen des Auftragsverarbeiters

8.1 Der Auftragsverarbeiter unterstützt den Verantwortlicher 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 Verantwortlicher zu melden

c) die Verpflichtung, dem Verantwortlicher 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 Verantwortlichen für dessen Datenschutz-Folgenabschätzung
e) die Unterstützung des Verantwortlichen im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

8.2 Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragsverarbeiters zurückzuführen sind, kann der Auftragsverarbeiter eine Vergütung beanspruchen.

9. Weisungsbefugnis des Verantwortlichen

9.1 Mündliche Weisungen bestätigt der Verantwortliche unverzüglich (mind. Textform).

9.2 Der Auftragsverarbeiter hat den Verantwortlichen unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragsverarbeiter ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen bestätigt oder geändert wird.

10. Löschung und Rückgabe von personenbezogenen Daten

10.1 Kopien oder Duplikate der Daten werden ohne Wissen des Verantwortlichen 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.

10.2 Remote-Sitzungen werden vollständig aufgezeichnet und gespeichert. Diese Remote-Sitzungen werden nach Ablauf von 3 Monaten automatisiert gelöscht.

10.3 Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragsverarbeiter entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Verantwortlichen übergeben.

11. Schlussbestimmungen

Im Falle einer bereits bestehenden Vereinbarungen nach § 11 BDSG (alte Fassung) wird diese durch die vorliegende Vertragsregelung ersetzt.

Anlagen:

Anlage 1 - Technisch organisatorische Maßnahmen

Anlage 2 - Unterauftragnehmer

Stand: 25.05.2018

Anlage 1 – Technisch-organisatorische Maßnahmen

A. compass GmbH

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

- **Zutrittskontrolle**
  Gebäude allgemein:
  - Schlüssel-/Chipkartenregelung
  - Tragen von Firmenausweisen
  - Videoüberwachung
- Rechenzentrumsräume zusätzlich:
  - verschlossene Türen in Rechenzentren, keine Fenster
  - Aufenthalt von Besuchern nur in Anwesenheit von Mitarbeitern
  - Alarmanlage
- **Zugangskontrolle**
  - Benutzername und Passwort
  - Vorgaben per Passwortrichtlinie
  - Protokollierung aller erfolgreichen und erfolglosen Logins
  - Einsatz von Spamfilter und Virenscanner (Exchange, Gateway)
- **Zugriffskontrolle**
  - Zuordnung von Zugriffsrechten zu jedem Benutzer
  - Einrichten von Administrationsrechten
  - Verschlüsselung von Funknetzen (WLAN)
  - Berechtigungskonzept

- **Trennungskontrolle**
  Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, über die Zuordnung der individuellen ID, auf die nur der jeweilige Bearbeiter Zugriffsrechte hat.

- **Pseudonymisierung und Verschlüsselung**
  (Art. 32 Abs. 1 lit. a EU-DSGVO, Art. 25 Abs. 1 EU-DSGVO)

  Im Supportfall ist es dem Verantwortlichen möglich eine Datensicherung verschlüsselt auf einen Server des Subdienstleister netcup des Auftragnehmers zu übertragen. Die Daten sind grundsätzlich nur für den Bearbeiter beim Auftragnehmer einsehbar, der die Datensicherung analysiert/repariert und als Download für den Kunden verschlüsselt bereitstellt.

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

- **Weitergabekontrolle**
  - Einrichtung einer Standleitung
  - Verschlüsselung von Funknetzen (WLAN)
  - Dokumentation der Datenempfänger, der übermittelten Daten und der Zeitspanne für die geplante Überlassung
  - Protokollierung der Abrufe und Übermittlungsaktivitäten
  - Verwenden von VPN-Verbindungen

- **Eingabekontrolle**
  - Protokollierung

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

- **Verfügbarkeitskontrolle und rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO);**
  - Sicherungskopien und Backups
  - Konzept zur Rekonstruktion der Datenbestände
  - Notfallplan
  - Einsatz von gespiegelten Festplatten und RAID-Systemen
  - Unterbrechungsfreie Stromversorgung (USV) und Notstromaggregat
  - Feuer- und Rauchmeldeanlagen
  - Feuerlöschgeräte in den Räumen
  - Alarmanlage zur Diebstahlsicherung
  - Schutz-Steckdosenleisten (zentral in Grundversorgung)
  - Klimaanlage

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

- Datenschutz-Management und Incident-Response-Management
  Die compass GmbH verfügt über ein Incident-Response-Management und über ein Datenschutzmanagementsystem. Mit entsprechender Planung zu Maßnahmen zum Umgang mit Chancen/Risiken und die Ausstattung mit angemessenen Ressourcen, Kompetenzen, Awareness und Kommunikation. Die Überwachung, Messung, Analyse und Bewertung, zusammen mit internen Audits und Managementbewertungen finden zur fortlaufenden Verbesserung des Managementsystems kontinuierlich statt.

- Auftragskontrolle
  - Verbot, Daten unzulässiger Weise zu kopieren
  - Klare, eindeutige Weisungen (Arbeitsanweisungen)
  - Vergabe von Einzelaufträgen nur über namentlich benannte Ansprechpartner
  - Vereinbarungen über Art des Datentransfers und deren Dokumentation
  - Kontrollrechte durch den Auftraggeber

B. Dritte (Unterauftragnehmer)

Alle Unterauftragnehmer haben alle gemäß Art. 32 DSGVO erforderlichen Maßnahmen ergriffen.

Anlage 2 Verzeichnis der Unterauftragnehmer

Der Kunde stimmt der Beauftragung der nachfolgenden Unterauftragnehmer unter der Bedingung des Bestehens einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO bzw. Art. 46 Abs. 2 litt. c und d DSGVO zu. Alle Unterauftragnehmer haben alle gemäß Art. 32 DSGVO erforderlichen Maßnahmen ergriffen und unterstützen unter Berücksichtigung der Art der Verarbeitung und der ihnen zur Verfügung stehenden Informationen den Kunden bei der Einhaltung der in den Artikeln 32 bis 36 DSGVO genannten Pflichten.

Firma	Anschrift	Leistung
Netcup GmbH (*Vertragsbasis*: Vertrag nach Art. 28 DSGvO)	Daimlerstr. 25 76185 Karlsruhe	Serverhosting
Teamviewer GmbH (*Vertragsbasis*: Standarddatenschutzklauseln DSGvO)	Jahnstr. 30 73037 Göppingen	Softwareanbieter/RZ Teamviewer Quicksupport für Fernwartungsdienste/Online-Meetings