Vereinbarung zur Auftragsverarbeitung für Kunden der Produkte AVAX und EVINT der compleet GmbH

Die nachstehenden Vereinbarungen zur Auftragsverarbeitung gelten ergänzend zum Hauptvertrag zwischen dem Kunden und der compleet GmbH über die Software-Produkte AVAX und EVINT.

Mit Unterzeichnung des Angebots durch den Kunden, wurden diese wirksam einbezogen.

Wenn der Kunde die unten aufgeführten Dienste nicht erwirbt, gelten diese produktspezifischen Bedingungen nicht. Wenn der Kunde einen der unten aufgeführten Dienste erwirbt, wird die entsprechende Vereinbarung zur Auftragsverarbeitung abgeschlossen.

VEREINBARUNG ZUR AUFTRAGSVERARBEITUNG AVAX

(Stand: Januar 2022)

zwischen den Kunden des Produktes AVAX der compleet GmbH als Auftraggeber („Auftraggeber“) und der compleet GmbH, Hauptstr. 8, 82008 Unterhaching als Auftragnehmer („Auftragnehmer“).

Präambel

Diese Vereinbarung konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus der im Hauptvertrag („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 Auftragnehmers oder durch den Auftragnehmer Beauftragte mit personenbezogenen Daten („Daten“) des Auftraggebers in Berührung kommen können.

1. Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung

1.1 Der Gegenstand des Auftrags ergibt sich aus dem Hauptvertrag, auf welchen hier verwiesen wird.

1.2 Soweit sich der Gegenstand nicht oder nicht vollständig aus dem Hauptvertrag ergibt, ist Gegenstand der Verarbeitung:

a) Bereitstellung eines Zugangs zum Online-Portal AVAX. Das Portal bietet unter anderem folgende Möglichkeiten:

- Kunden-/ Dienstleisterkommunikation
- Einstellen und/oder Einsicht von Personalbedarfen
- Möglichkeit Mitarbeiter- oder Bewerberdaten hochzuladen und dem Kunden anzubieten bzw. als Kunde angebotene Mitarbeiter/ Bewerber einzusehen
- Verwaltung, Bearbeitung, Monitoring von Mitarbeitern, Bewerbern und Einsätzen
- Einsicht, Verwaltung, Bearbeitung, Monitoring von Kunden-/ Dienstleisterdaten
- Auswertungen

b) Hilfestellung durch Schulungen und eine Hotline (Bedienhinweise, Arbeitsunterstützung)

c) Unterstützung bei der Datenpflege

1.3 Art und Zweck der Auftragsverarbeitung sind im Hauptvertrag beschrieben und umfassen insbesondere:

- Speicherung von (personenbezogenen) Daten des Auftraggebers auf den vom Auftragsverarbeiter bereitgestellten Speicherkapazitäten (AVAX-Portal)
- Bereitstellung der Daten im Portal
- Datenkonvertierung/ Datenimport
- Durchführung der Portalpflege
- Portaländerungen
- Behebung von eventuellen Portalfehlern
- Hilfestellung durch Schulungen
- Supportdienstleistung in Bezug auf die Portallösung
- Durchführung von Fernwartungen

1.4 Folgende Kategorien von Personen sind von der Verarbeitung betroffen:

- Kunden
- Beschäftigte
- Bewerber für ein Beschäftigungsverhältnis
- Nutzer (geben geschäftliche Kontaktinformationen zur Bewerberkommunikation an)
- Lieferanten und Dienstleister
- Auftraggeber und Geschäftspartner
- Ehemalige Beschäftigte

1.5 Die Verarbeitung umfasst die nachfolgend genannten Arten von Daten:

- Personalstammdaten
- Adressdaten
- Bankverbindungsdaten
- Kontaktdaten
- Mitarbeiterdaten
- Einsatzdaten
- Lohn- und Gehaltsdaten
- Zeiterfassungsdaten
- Urlaubsdaten
- Qualifikationsdaten
- Vertragsstammdaten
- Vertragsabrechnungsdaten
- Planungs- und Steuerungsdaten

1.6 Die Laufzeit dieser Vereinbarung richtet sich nach der Laufzeit des Hauptvertrages, sofern sich aus den Bestimmungen dieser Vereinbarung nicht darüberhinausgehende Verpflichtungen ergeben.

1.7 Das Recht zur fristlosen Kündigung aus wichtigem Grund bleibt unberührt.

2. Anwendungsbereich und Verantwortlichkeit

2.1 Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. 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 danach in schriftlicher Form oder in Textform an, die vom Auftragnehmer bezeichnete Stelle 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 Auftraggebers 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.

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 entsprechenden technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers 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. Es handelt sich hierbei um die in der Anlage 1 beschriebenen technischen und organisatorischen Maßnahmen.

3.3 Eine Änderung der getroffenen technischen und organisatorischen Maßnahmen bleibt dem Auftragnehmer 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 Auftraggebers befassten Mitarbeitern und anderen für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisungen des Auftraggebers zu verarbeiten. Ferner gewährleistet der Auftragnehmer, 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 unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers 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 Auftraggeber teilt dem Auftragnehmer die Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen sowie ggf. während der Vertragslauzeit auftretende Änderungen dieser in Textform mit. Sofern keine weisungsberechtigten Personen benannt sind, sind ausschließlich die Geschäftsführer-innen/ Inhaber-innen des Auftraggebers weisungsbefugt.

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, sofern nicht im Vertrag bereits vereinbart.

3.10 Daten, Datenträger sowie sämtliche sonstige Materialien sind nach Auftragsende auf Verlangen des Auftraggebers entweder herauszugeben oder zu löschen.

4. Pflichten des Auftraggebers

4.1 Der Auftraggeber ist als Verantwortlicher für die Datenverarbeitung selbstständig zur Einhaltung seiner Verpflichtungen aus der DS-GVO verantwortlich. Die vom Auftragnehmer zur Verfügung gestellten Tools zur Umsetzung der Verpflichtungen aus der DS-GVO stellen lediglich Hinweise dar, für deren Nutzung der Auftraggeber die Verantwortung trägt. Auf die Nutzungsweise der jeweiligen Tools durch den Auftraggeber hat der Auftragnehmer keinerlei Einfluss.

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

4.3 Der Auftraggeber nennt dem Auftragnehmer den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

5. Anfragen Betroffener

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

6. Nachweismöglichkeiten

6.1 Der Auftragnehmer weist dem Auftraggeber die Einhaltung der in Art 28 DS-GVO und in diesem Vertrag niedergelegten Pflichten mit geeigneten Mitteln nach. Zum Nachweis der Einhaltung der vereinbarten

Pflichten kann der Auftragnehmer, dem Auftraggeber Zertifikate und Prüfergebnisse Dritter 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 Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht

6.3 Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Auftraggebers 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 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 Auftragnehmers 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 Subunternehmer hinzuzieht. Vor der Hinzuziehung oder Ersetzung von Subunternehmern informiert der Auftragnehmer den Auftraggeber mit einer Frist von vier Wochen in Textform. Der Auftraggeber kann der Änderung nur aus wichtigem Grund widersprechen. Der Widerspruch hat binnen 14 Tagen zu erfolgen und hat alle wichtigen Gründe ausdrücklich zu benennen. Erfolgt innerhalb der Frist kein Widerspruch, so erlischt das Widerspruchsrecht. Liegt ein wichtiger Grund vor, der vom Auftragnehmer nicht durch Anpassung des Auftrages beseitigt werden kann, wird dem Auftraggeber ein Sonderkündigungsrecht eingeräumt. Über die in der Anlage 2 aufgeführten, bei Vertragsschluss bereits bestehenden, Subunternehmer und Teilleistungen erfolgt keine gesonderte Information. Ein Widerspruchsrecht des Auftraggebers besteht für diese Subunternehmer nicht.

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

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

8. Datenverarbeitung im Drittland

Die Vorgaben des EuGH aus der Schrems II Entscheidung vom 16. Juli 2020 (Az. C 311/18) werden beachtet.

9. Informationspflichten, Schriftformklausel, Rechtswahl

9.1 Sollten die Daten des Auftraggebers beim Auftragnehmer 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 als „Verantwortlicher“ im Sinne der Datenschutz-Grundverordnung liegen.

9.2 Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – 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.

9.3 Bei etwaigen Widersprüchen gehen Regelungen dieser Vereinbarung zum Datenschutz den Regelungen der Nutzungsbedingungen und dem Bestellschein vor. Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

9.4 Es gilt deutsches Recht.

Anlage 1: Technische und organisatorische Maßnahmen
Anlage 2: Subunternehmer

Anlage 1
zur Vereinbarung zur Auftragsverarbeitung

TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen hat die compleet GmbH nachfolgend dargelegte technische und organisatorische Maßnahmen getroffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

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

Zutrittskontrolle

Ein unbefugter Zutritt ist zu verhindern, wobei der Begriff räumlich zu verstehen ist. Technische und organisatorische Maßnahmen zur Zutrittskontrolle, insbesondere auch zur Legitimation der Berechtigten:

- ☑ Festlegung befugter Personen inklusive Umfang der jeweiligen Befugnisse
- ☑ Sorgfältige Auswahl von Reinigungspersonal
- ☑ Existenz von Regelungen für Unternehmensexterne (Besucherbegleitung durch Mitarbeiter, Trennung von Bearbeitungs- und Publikumszonen)
- ☑ Umsetzung einer Schlüsselregelung
- ☑ Anweisung zur Ausgabe von Schlüsseln
- ☑ Protokollierung der ein- und ausgehenden Personen
- ☑ Physische Maßnahmen vorhanden und regelmäßig überprüft:
    - ☑ Gesicherter Hauseingang (z. B. abschließbare Türen, Sicherheitsschlösser)
    - ☑ Türsicherung Hauseingang (elektrische Türöffner)

Zugangskontrolle

Das Eindringen Unbefugter in die DV-Systeme und die unbefugte Systemnutzung sind zu verhindern.
Technische und organisatorische Maßnahmen hinsichtlich der Benutzeridentifikation und Authentifizierung:

- ☑ Konzeption und Implementierung eines Berechtigungskonzepts
- ☑ Berechtigungskonzept für Endgeräte (Rechner)
- ☑ Berechtigungskonzept für Software/ Systeme
- ☑ Identifikation und Berechtigungsprüfung eines Benutzers
- ☑ Implementierung eines Systems zur Verwaltung von Benutzeridentitäten
- ☑ Monitoring der Zugangsversuche mit Reaktion auf Sicherheitsvorfälle
- ☑ Festlegung und Kontrolle der Zugangsbefugnisse
- ☑ Passwort-Richtlinie
- ☑ Spezielle Sicherheitssoftware
- ☑ Existenz von Regelungen für Unternehmensexterne

Zugriffskontrolle

Unerlaubte Tätigkeiten in DV-Systemen außerhalb eingeräumter Berechtigungen sind zu verhindern.
Bedarfsorientierte Ausgestaltung des Berechtigungskonzepts und der Zugriffsrechte sowie deren Überwachung und Protokollierung anhand:

- ☑ Berechtigungs- und Rollenkonzept für Applikationen
- ☑ Umsetzung von Regelungen zur Zugriffs- und Benutzerberechtigung

- ☑ Überprüfung der Berechtigungen
- ☑ Funktionsbegrenzung
- ☑ Zugriffsbeschränkungen („Need-to-Know“)
- ☑ Passwortgesicherte Speicherung der Daten
- ☑ Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
- ☑ Protokollierung von unberechtigten Zugriffsversuchen Anlassbezogene Auswertung
- ☑ Umsetzung von Regelungen zur Entsorgung von Speichermedien (Einsatz von Aktenvernichtern bzw. Dienstleistern gem. DIN 66933)
- ☑ Umsetzung von Regelungen zum Umgang mit elektronischen Speichermedien

Trennungskontrolle

Daten, die zu unterschiedlichen Zwecken erhoben wurden, sind getrennt zu verarbeiten.
Maßnahmen zur getrennten Verarbeitung (Speicherung, Veränderung, Löschung, Übermittlung) von Daten mit unterschiedlichen Zwecken:

- ☑ Mandantenfähigkeit:
- ☑ Logische Mandantentrennung
- ☑ Trennung von Produktiv- und Testsystemen
- ☑ Festlegung von Datenbankrechten
- ☑ Vorhandensein von Richtlinien und Arbeitsanweisungen
- ☑ Vorhandensein von Verfahrensdokumentationen
- ☑ Anlassbezogene Prüfung der bestimmungsgemäßen Nutzung der Informationen und IT-Systeme

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

Weitergabekontrolle

Aspekte der Weitergabe und Übertragung personenbezogener Daten sind zu regeln: Elektronische Übertragung, Datentransport, Übermittlungskontrolle.
Maßnahmen bei Transport, Übertragung und Übermittlung oder Speicherung auf Datenträger (manuell oder elektronisch) sowie bei der nachträglichen Überprüfung:

- ☑ Verschlüsselung der Datenübermittlung (z. B. VPN, S/MIME)
- ☑ Protokollierungen der Datenweitergabe
- ☑ Anlassbezogene Durchführung von Plausibilitäts-, Vollständigkeits- und Richtigkeitsprüfungen
- ☑ Organisatorische Maßnahmen zur Verhinderung von unkontrollierten Informationsabflüssen
- ☑ Dokumentationen der Schnittstellen und der Abruf- und Übermittlungsprogramme

Eingabekontrolle

Die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege ist zu gewährleisten.
Maßnahmen zur nachträglichen Überprüfung, ob und von wem Daten eingegeben, verändert oder entfernt (gelöscht) worden sind:

- ☑ Protokollierung der Eingaben und Überprüfung der Protokolle
- ☑ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- ☑ Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen wurden
- ☑ Rechtevergabe zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzeptes
- ☑ Organisatorisch festgelegte Zuständigkeiten für die Eingabe

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b, c DS-GVO)

Verfügbarkeitskontrolle

Die Daten sind gegen zufällige Zerstörung oder Verlust zu schützen.
Maßnahmen zur Datensicherung (physisch/logisch):

- ☑ Regelmäßige Kontrolle des Systemzustands (Monitoring)
- ☑ Kurzfristige Wiederherstellbarkeit des normalen Systemzustands
- ☑ Backup- und Wiederanlaufkonzept (regelmäßige Datensicherungen)
- ☑ Disaster Recovery Konzept
- ☑ Regelmäßige Tests des Notfallkonzepts
- ☑ Vorhandensein von redundanten IT-Systemen
- ☑ Replizierbarkeit virtueller Maschinen
- ☑ Funktionsfähige physische Schutzeinrichtungen (Brandschutz, Energie: USV, Klima)
- ☑ Meldewege und Notfallpläne

Belastbarkeitskontrolle

Die Verarbeitung der Daten soll tolerant gegenüber Störungen und Fehlern sein.

- ☑ Virenschutz/Anti-Malware/
- ☑ großzügig vorhandene Netzwerkkapazität
- ☑ Firewall

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

- ☑ Schriftlich fixierte Regelungen der Verantwortlichkeiten für Datenschutz
- ☑ Schriftlich fixierte Regelungen der Verantwortlichkeiten für Informationssicherheit
- ☑ Existenz eines angemessenen Incident Response Managements
- ☑ Regelmäßige Aufklärung und Sensibilisierung der Mitarbeiter und Führungskräfte
- ☑ Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)
- ☑ Auftragskontrolle, um weisungsgemäße Auftragsverarbeitung zu gewährleisten:
    - ☑ Strikte Einhaltung der festgeschriebenen Vereinbarungen und deren Überprüfungen
    - ☑ Konzept dahingehend, wie die regelmäßige Kontrolle des Auftragsprozesses erfolgt (z. B. Vorlage von Self-Assessments, Vorlage der Verträge mit Unterauftragnehmern, Durchführung von Kontrollen bei Subunternehmern durch den Auftragnehmer)
    - ☑ Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z. B. anhand: eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen

Stand: November 2021

Anlage 2
zur Vereinbarung zur Auftragsverarbeitung (Stand: Januar 2022):

SUBUNTERNEHMER

FIRMA SUBUNTERNEHMER	ANSCHRIFT/ LAND	LEISTUNG
Amazon Web Services EMEA	SARL, 38 avenue John F. Kennedy, 1855, Luxemburg	Hosting des AVAX-Portals
Hetzner Online GmbH	Industriestr. 25, 91710 Gunzenhausen, Deutschland	Backup

VEREINBARUNG ZUR AUFTRAGSVERARBEITUNG EVINT

(Stand: Januar 2022)

zwischen den Kunden des Produktes EVINT der compleet GmbH als Auftraggeber - im Folgenden „Kunde“ oder „Verantwortlicher“ genannt

und der compleet GmbH, Hauptstraße 8, 82008 Unterhaching als Auftragnehmer - im Folgenden „compleet“ oder „Auftragsverarbeiter“ genannt, gemeinsam „Parteien“ genannt.

1. Präambel

1.1. Die Vertragsparteien sind mit der Freischaltung durch die compleet zur Nutzung des Portals *www.evint.net* und *mein-evint.gbg-ag.com* durch den Kunden ein Auftragsverarbeitungsverhältnis gemäß EU Datenschutz Grundverordnung (DS-GVO) eingegangen. Um die Rechte und Pflichten aus diesem Auftragsverarbeitungsverhältnis gemäß der gesetzlichen Verpflichtung zu konkretisieren, schließen die Vertragsparteien die nachfolgende Vereinbarung.

1.2. Diese Vereinbarung bezieht sich nur auf die Durchführung der technischen Erhebung, Verarbeitung und Nutzung personenbezogener Daten nach einem vom Kunden vorgegebenen Verfahren und Umfang in Verbindung mit dem Produkt EVINT der compleet. Dadurch begründet sich eine Auftragsverarbeitung nach Art. 28 DS-GVO.

1.3. Es gelten die Begrifflichkeiten gemäß Art. 4 DS-GVO.

2. Gegenstand und Dauer der Vereinbarung

2.1. Gegenstand dieser Vereinbarung ist die Verarbeitung personenbezogener Daten durch die compleet für den Kunden im Zusammenhang mit der Nutzung des Portals *www.evint.net* und *mein-evint.gbg-ag.com.*

2.2. Die Vereinbarung gilt bis zur Beendigung der Inanspruchnahme der Leistungen des Auftragsverarbeiters. Etwaige Sonderkündigungsrechte bleiben davon unberührt. Diese Vereinbarung ersetzt alle bisherigen geschlossenen Vereinbarungen zur Auftragsdatenverarbeitung im Zusammenhang mit dem Produkt EVINT zwischen der compleet und dem Kunden.

2.3. Dies umfasst alle Tätigkeiten, die die compleet gemäß den „*Nutzungsbedingungen für EVINT*“ und den vertraglichen Vereinbarungen mit dem Kunden (Bestellungen von Standardprodukten und Verträge über individuelle Leistungen) erbringt und die eine Auftragsverarbeitung darstellen.

2.4. Bei Widersprüchen zwischen einer Vereinbarung der Parteien und dieser Vereinbarung zur Auftragsverarbeitung geht diese Vereinbarung zur Auftragsverarbeitung vor.

3. Konkretisierung der Vereinbarung

3.1. Art und Zweck der vorgesehenen Verarbeitung von Daten

3.1.1. Inhaltliche Vereinbarungen mit Kunden und deren Anwendern umfassen die Möglichkeiten des Verantwortlichen zur Nutzung der Funktionen des Portals EVINT.

3.1.2. Die Art der Verarbeitung umfasst alle Arten von Verarbeitungen im Sinne der DS-GVO.

3.1.3. Die Erbringung der vertraglich vereinbarten Datenverarbeitung hinsichtlich EVINT 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 Verantwortlichen und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.

3.2. Art der Daten und Kategorien betroffener Personen

3.2.1. Art der personenbezogenen Daten sind alle Arten personenbezogener Daten, die die compleet im Auftrag des Kunden verarbeitet. Darunter können ggf. auch besondere Kategorien personenbezogener Daten fallen.

3.2.2. Hinsichtlich der Verarbeitung von personenbezogenen Daten besonderer Art ist der Kunde verpflichtet, in eigener Verantwortung dafür Sorge zu tragen, dass die hierzu geltenden gesetzlichen Vorgaben eingehalten werden.

3.2.3. Kategorien betroffener Personen sind insbesondere:

- Beschäftigte und Geschäftspartner/ Mandanten des Kunden;
- Beschäftigte und Geschäftspartner des Geschäftspartners/ Mandanten;
- Nutzer einer der compleet-Leistungen.

3.2.4. Ein detaillierter Umfang der einzelnen Leistungen ergibt sich aus den jeweiligen Einzelaufträgen. Die von den Vertragsparteien vereinbarte Auftragsverarbeitung beinhaltet unter anderem:

- Pflege und Verwaltung von Arbeitnehmerdaten;
- Erfassung und Verarbeitung von Arbeitszeiten und Abwesenheiten;
- Erfassung und Verarbeitung von Überlassungsverhältnissen;
- Abrechnung von Personalleistungen;
- Erfassung qualifiziert signierter Verträge;
- Zutrittskontrolle und Verwaltung von Sicherheitsbereichen.

3.2.5. Folgenden Datenarten oder -kategorien können dabei Gegenstand der Erhebung, Verarbeitung und/ oder Nutzung durch den Auftragsverarbeiter sein:

- Personenstammdaten;
- Kommunikationsdaten (z. B. Telefon, E-Mail);
- Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse);
- Kundenhistorie;
- Planungs- und Steuerungsdaten;
- Vertragsabrechnungs- und Zahlungsdaten;
- Ggf. Ausweisdokumente und Qualifikationen.

Der Kreis derer, die durch den Umgang mit ihren personenbezogenen Daten betroffen sind, umfasst:

- Kunden;
- Beschäftigte (auch Auszubildende, Praktikanten, Zeitarbeitnehmer, Lieferanten);
- Ansprechpartner bei anderen Unternehmern.

4. Verantwortlichkeit und Weisungsbefugnis

4.1. Der Verantwortliche ist für die Einhaltung der datenschutzrechtlichen Bestimmungen, insbesondere für die Rechtmäßigkeit der Datenverarbeitung verantwortlich. Er kann jederzeit die Herausgabe, Berichtigung, Löschung und Sperrung der Daten verlangen. Soweit ein Betroffener sich zwecks Ausübung seiner Rechte nach Art. 12 – 23 DS-GVO (z.B. Löschung, Berichtigung oder Datenübertragung) unmittelbar an den Auftragsverarbeiter wendet, wird der Auftragsverarbeiter dieses Ersuchen unverzüglich an den Verantwortlichen weiterleiten.

4.2. Der Auftragsverarbeiter darf Daten ausschließlich im Rahmen der Weisungen des Verantwortlichen erheben, verarbeiten oder nutzen.

4.2.1. Eine Weisung ist die auf einen bestimmten Umgang des Auftragsverarbeiters mit personenbezogenen Daten gerichtete schriftliche Anordnung des Verantwortlichen.

4.2.2. Die Weisungen werden zunächst durch die Konkretisierung in Ziff. 3 dieser Vereinbarung definiert und können von dem Verantwortlichen danach in schriftlicher Form durch eine einzelne Weisung geändert, ergänzt oder ersetzt werden.

4.2.3. Trifft den Auftragsverarbeiter eine gesetzliche Verpflichtung oder eine rechtliche Anordnung zur Verarbeitung oder Herausgabe personenbezogener Daten, für die der Verantwortliche die Verantwortung trägt, informiert der Auftragsverarbeiter den Verantwortlichen unverzüglich, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

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

4.4. Verfahrensänderungen des Verarbeitungsgegenstandes dürfen nur mit dokumentierter Zustimmung des Verantwortlichen umgesetzt werden.

4.5. Auskünfte an Dritte oder Betroffene darf der Auftragsverarbeiter nur nach vorheriger schriftlicher Zustimmung durch den Verantwortlichen erteilen. Der Auftragsverarbeiter verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, diese Daten an Dritte weiterzugeben.

4.6. Der Verantwortliche führt ein Verzeichnis über Verarbeitungstätigkeiten. Der Auftragsverarbeiter stellt dem Verantwortlichen auf dessen Wunsch Informationen über das Verzeichnis zur Verfügung.

4.7. Weisungsbefugte Beschäftigte des Verantwortlichen sowie Weisungsempfänger des Auftragsverarbeiters sind im Anhang „Weisungsbefugte Beschäftigte und Weisungsempfänger“ namentlich zu nennen. Eine Änderung der benannten Personen ist der entsprechend anderen Vertragspartei dokumentiert mitzuteilen.

5. Technisch-organisatorische Maßnahmen

5.1. Der Auftragsverarbeiter stellt dem Verantwortlichen eine Beschreibung der technischen und organisatorischen Maßnahmen nach Art. 32 Abs. 1 DS-GVO vor Beginn der Verarbeitung zur Verfügung. Die in Anlage 1 „*Technische und organisatorische Maßnahmen*“ beschriebene Auswahl der technischen und organisatorischen Maßnahmen stellt nach Stand der Technik und unter Berücksichtigung der eingesetzten IT-Systeme und Verarbeitungsprozesse beim Auftragnehmer diese Maßnahmen dar.

5.2. Diese Beschreibung wird mit der Akzeptanz durch den Verantwortlichen zum Vertragsbestandteil.

5.3. Der Auftragsverarbeiter 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.

5.4. Technische und organisatorische Maßnahmen unterliegen dem technischen Fortschritt. Insoweit ist es dem Auftragsverarbeiter gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das vereinbarte Sicherheitsniveau nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

5.5. Der Kunde informiert sich vor Abschluss der Vereinbarung zur Auftragsverarbeitung und anschließend in regelmäßigen Abständen über diese technischen und organisatorischen Maßnahmen. Der Kunde trägt die Verantwortung dafür, dass die jeweils aktuell geltenden, vertraglich vereinbarten technischen und organisatorischen Maßnahmen für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten.

6. Berichtigung, Einschränkung und Löschung von Daten

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

6.2. Überlassene Datenträger und Datensätze verbleiben im Eigentum des Verantwortlichen. Kopien und Duplikate werden ohne Wissen des Verantwortlichen nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zu Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten des Auftragsverarbeiters erforderlich sind.

6.3. Nach Abschluss der vertraglich vereinbarten Leistungen oder früher nach Aufforderung des Verantwortlichen, jedoch spätestens mit Beendigung der Leistungsvereinbarung hat der Auftragsverarbeiter

sämtliche in seinen Besitz gelangte Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände (wie auch hiervon gefertigten Kopien oder Reproduktionen), die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Verantwortlichen auszuhändigen oder nach vorheriger Zustimmung des Verantwortlichen in einem dem Schutzniveau entsprechenden Verfahren zu vernichten. Gleiches gilt für Test- und Ausschussmaterial.

6.4. Der Auftragsverarbeiter kann Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufbewahren. Alternativ kann er diese zu seiner Entlastung bei Vertragsende dem Verantwortlichen übergeben.

6.5. Die compleet ist berechtigt, für diese Leistungen eine angemessene Vergütung vom Kunden zu verlangen.

6.6. Diese Vereinbarungen gelten auch im Fall einer Kündigung durch den Verantwortlichen aufgrund der Bestimmungen des Ziff. 11 dieser Vereinbarung.

7. Mitteilung bei Verstößen durch den Auftragsverarbeiter

Der Auftragsverarbeiter unterrichtet den Verantwortlichen umgehend bei schwerwiegenden Störungen seines Betriebsablaufes, bei Verdacht auf Verstöße gegen vertragliche oder gesetzliche Datenschutzbestimmungen, bei Verstößen gegen solche Bestimmungen oder anderen Unregelmäßigkeiten bei der Verarbeitung der Daten, damit dieser seiner Meldepflicht nachkommen kann.

8. Qualitätssicherung und sonstige Pflichten des Auftragsverarbeiters

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

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

8.2. Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO.

8.2.1. 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.

8.2.2. 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.

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

8.4. 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.

8.5. 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.

8.6. 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.

8.7. Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Verantwortlichen im Rahmen seiner Kontrollbefugnisse.

9. Unterauftragsverhältnisse

9.1. 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.

9.2. Die compleet informiert den Kunden, wenn sich eine Änderung in Bezug auf die Hinzuziehung weiterer oder die Ersetzung bestehender Auftragsverarbeiter ergeben hat.

9.3. Der Kunde kann gegen derartige Änderungen Einspruch innerhalb von vier Wochen erheben. Ohne Einspruch wird die Änderung nach vier Wochen rechtsverbindlich anerkannt.

9.4. Im Fall des Einspruchs kann die compleet nach eigener Wahl die Leistung ohne die beabsichtigte Änderung erbringen oder – sofern die Erbringung der Leistung ohne die beabsichtigte Änderung der compleet nicht zumutbar ist - die von der Änderung betroffene Leistung gegenüber dem Kunden innerhalb von vier Wochen nach Zugang des Einspruchs kündigen oder die gesamte Leistungserbringung kündigen.

9.5. Wenn Subunternehmer durch den Auftragsverarbeiter eingeschaltet werden, hat der Auftragsverarbeiter sicherzustellen, dass seine vertraglichen Vereinbarungen mit dem Subunternehmer so gestaltet sind, dass das Datenschutzniveau mindestens der Vereinbarung zwischen dem Verantwortlichen und dem Auftragsverarbeiter entspricht, hinreichende Garantien für die Sicherheit der Verarbeitung vorliegen und alle gesetzlichen und vertraglichen Pflichten beachtet werden.

9.6. Dem Verantwortlichen sind in der vertraglichen Vereinbarung mit dem Subunternehmer Kontroll- und Überprüfungsrechte entsprechend dieser Vereinbarung einzuräumen. Ebenso ist der Verantwortliche berechtigt, auf schriftliche Anforderung vom Auftragsverarbeiter Auskunft über den wesentlichen Vertragsinhalt, die Umsetzung der datenschutzrelevanten Verpflichtungen des Subunternehmers und die Garantien zur Sicherheit der Verarbeitung zu erhalten.

9.7. Zu Beginn der Verarbeitung sind die beauftragten Subunternehmer in der Anlage 2 „*Subunternehmer*“ aufzuführen.

10. Kontrollrechte des Verantwortlichen

10.1. 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 rechtzeitig mindestens 14 Kalendertage vorher anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragsverarbeiter in dessen Geschäftsbetrieb zu überzeugen.

10.1.1. Die Ausübung des Inspektionsrechts darf den Geschäftsbetrieb von die compleet nicht über Gebühr stören oder missbräuchlich sein.

10.1.2. Die compleet ist berechtigt, für Inspektionen eine angemessene Vergütung vom Kunden zu verlangen.

10.2. Der Auftragsverarbeiter stellt sicher, dass sich der Verantwortliche von der Einhaltung der Pflichten des Auftragsverarbeiters nach Art. 28 DS-GVO überzeugen kann. Der Auftragsverarbeiter verpflichtet sich, dem Verantwortlichen auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

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

10.3.1. die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;

10.3.2. die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO;

10.3.3. aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z. B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);

10.3.4. eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z. B. nach BSI Grundschutz).

10.4. Der Kunde hat die compleet unverzüglich und vollständig zu informieren, wenn er im Hinblick auf die Verarbeitung bezüglich datenschutzrechtlicher Bestimmungen Fehler oder Unregelmäßigkeiten feststellt.

10.5. Der Kunde nennt der compleet den Ansprechpartner für im Rahmen dieser Vereinbarung zur Auftragsverarbeitung anfallende Datenschutzfragen:

Weisungsbefugter Ansprechpartner ist: .....

11. Verarbeitung auf dokumentierte Weisung

11.1. Die compleet – und jede ihr unterstellte Person – darf die personenbezogenen Daten nur im Rahmen der Leistungsbeschreibungen und den jeweiligen vertraglichen Vereinbarungen zwischen der compleet und dem Kunden und der Weisungen des Kunden verarbeiten, außer es liegt ein Ausnahmefall im Sinne des Art. 28 Abs. 3 Satz 2 lit. a DS-GVO vor.

11.2. Die compleet nimmt Weisungen des Kunden in schriftlicher Form sowie über die hierfür von compleet angebotenen elektronischen Formate entgegen.

11.3. Mündliche Weisungen sind durch den Kunden unverzüglich schriftlich oder in einem von der compleet angebotenen elektronischen Format zu bestätigen.

11.4. Sind die Weisungen des Kunden nicht vom vertraglich vereinbarten Leistungsumfang umfasst, werden diese als Antrag auf Leistungsänderung behandelt.

11.5. Bei Änderungsvorschlägen teilt die compleet dem Kunden mit, welche Auswirkungen sich auf die vereinbarten Leistungen, insbesondere die Möglichkeit der Leistungserbringung, Termine und Vergütung ergeben.

11.6. Ist der compleet die Umsetzung der Weisung nicht zumutbar, so ist die compleet berechtigt, die Verarbeitung zu beenden.

11.7. Im Übrigen gelten die Leistungsbeschreibungen und jeweiligen vertraglichen Vereinbarungen.

12. Vereinbarung weiterer Vertragszwecke

12.1. compleet ist berechtigt, von dieser Vereinbarung umfasste personenbezogene Daten zum Zweck der Fehlerbehebung in dem compleet-Produkt, in dem die Daten gespeichert sind, zu verarbeiten.

12.2. compleet ist berechtigt, von dieser Vereinbarung umfasste personenbezogene Daten zum Zweck der Qualitätssicherung für das compleet-Produkt, in dem die Daten gespeichert sind bzw. für eine neuere Version des compleet-Produkts zu verarbeiten.

12.3. compleet ist berechtigt, von dieser Vereinbarung umfasste personenbezogene Daten zum Zweck der Entwicklung neuer oder Weiterentwicklung bestehender compleet-Produkte in einer angemessen gesicherten Umgebung zu verarbeiten. compleet berücksichtigt auch bei dieser Verarbeitung, dass vom Kunden gelöschte oder zur Löschung angewiesene Daten nicht mehr verarbeitet werden.

12.4. compleet ist berechtigt, von dieser Vereinbarung umfasste personenbezogene Daten zu verarbeiten,

12.4.1. soweit sie dies für die Gewährleistung der Netz- und Informationssicherheit unbedingt notwendig und verhältnismäßig erachtet,

12.4.2. soweit dadurch die Fähigkeit eines Netzes oder Informationssystems gewährleistet wird, mit dem vereinbarten Grad der Zuverlässigkeit Störungen oder widerrechtliche oder mutwillige Eingriffe abzuwehren, die die Verfügbarkeit, Authentizität, Vollständigkeit und Vertraulichkeit von gespeicherten oder übermittelten personenbezogenen Daten sowie die Sicherheit damit zusammenhängender Dienste, die über diese Netze oder Informationssysteme angeboten werden bzw. zugänglich sind, beeinträchtigen. Dies umfasst insbesondere auch, den Zugang Unbefugter zu elektronischen Kommunikationsnetzen und die Verbreitung schädlicher Programmcodes zu verhindern sowie Angriffe in Form der gezielten Überlastung von Servern („Denial of service"-Angriffe) und Schädigungen von Computer- und elektronischen Kommunikationssystemen abzuwehren.

13 Formerfordernis

Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – sind gemäß DS-GVO 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 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.

15 Schlussbestimmungen

1. Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile - einschließlich der Garantien des Auftragsverarbeiters - 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.
2. Folgende Anlagen sind Bestandteil dieser Vereinbarung:

Anlage 1: Technische und organisatorische Maßnahmen
Anlage 2: Subunternehmer

Stand: 1. Januar 2022

ANLAGE 1 TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN

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

1.1 Zutrittskontrolle

Ziel: Ein unbefugter Zutritt zu Datenverarbeitungsanlagen ist zu verhindern.

Maßnahmen: Die Zutrittskontrolle zu DV-Anlagen wird durch ein technisches Zutrittskontrollsystem gewährleistet, das Folgendes beinhaltet:

- Das Gebäude, die Büroraume und das Rechenzentrum sind mit einer Alarmanlage gesichert und werden von einem Sicherheitsdienst überwacht.
- Die Eingangstüren zu den Büroräumen sind mit einem Chipkartensystem versehen.
- Die Zutrittsberechtigungen der Mitarbeiter sind namensscharf dokumentiert.
- Der Zutritt von Fremdfirmen/ Besuchern/ Gästen wird namensscharf dokumentiert.
- Der Zutritt zu dem Rechenzentrum wird nur berechtigten Personen gewährt und dokumentiert.
- Mit Beendigung der Arbeitsverhältnisse werden die Zutrittsberechtigungen der Mitarbeiter entzogen.

1.2 Zugangskontrolle

Ziel: Eine unbefugte Systemnutzung ist zu verhindern.

Maßnahmen:

- Das Firmennetzwerk ist durch eine Firewall geschützt.
- Die Mitarbeiter sind auf ein individuell geheim zu haltendes Computerkennwort verpflichtet.
- Es werden keine Sammelkennwörter benutzt.
- Bei der Passwortvorgabe sollen folgende Komplexitätsvoraussetzungen erfüllt sein:
  alphanumerisch (Zahlen, Buchstaben und Sonderzeichen), Mindestlänge: 8 Zeichen
- Es erfolgt ein regelmäßiger Wechsel des Kennworts nach maximal 90 Tagen.
- Die Bildschirme werden nach max. 10 Minuten automatisch gesperrt.
- Auf allen Arbeitsplatzcomputern werden Virenscanner eingesetzt. Die Schutzsoftware dafür wird regelmäßig aktualisiert.
- Sicherheitsupdates werden regelmäßig installiert.

1.3 Zugriffskontrolle

Ziel: Unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems muss unmöglich sein.

Maßnahmen:

- Das Berechtigungskonzept ist dokumentiert.
- Es werden differenzierte Berechtigungen (Profile) je nach Rolle vergeben.
- Die Mitarbeiter bekommen die Zugriffsberechtigungen je zugewiesene Rolle.
- Es erfolgt eine Protokollierung sämtlicher Zugriffe.
- Fernzugriff für die Mitarbeiter erfolgt per VPN.
- Für die Notebooks wird ein Festplatten-Verschlüsselungssystem eingesetzt.

1.4 Trennungskontrolle

Ziel: Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben werden sicherstellen.

Maßnahmen:

- Kundendaten sind physisch getrennt von Entwicklungsdaten und Testdaten und innerhalb der Systeme nochmals logisch getrennt.
- Die Entwicklungsdaten sind jeweils auf getrennten Servern gespeichert (physische Trennung).
- Es wird die Mandantentrennung eingesetzt. Die Daten je Kunde werden logisch getrennt transferiert, verarbeitet und gespeichert. Zugang zu den Daten ist nur den Mitarbeitern gewahrt, die für die Datenverarbeitung zuständig sind.

1.5 Pseudonymisierung

Pseudonymisierung ist die Verarbeitung personenbezogener Daten in der Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren Person zugewiesen werden.

Maßnahmen:

- Das System bietet die Möglichkeit, mit Pseudonymen in Stammdatenfeldern zu arbeiten.

1.6 Verschlüsselung

Die Verschlüsselung transformiert einen Klartext in Abhängigkeit von einer Zusatzinformation, die "Schlüssel" genannt wird, in einen zugehörigen Geheimtext (Chiffrat), der für diejenigen, die den Schlüssel nicht kennen, nicht entzifferbar sein soll.

Maßnahmen:

- Nutzung von kryptografischen Tools
- Data Hashing
- Transportverschlüsselung (SSL/ TLS)
- Nutzung von VPN

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

2.1 Weitergabekontrolle

Ziel: Unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport muss unmöglich sein.

Maßnahmen:

- Der Datentransfer erfolgt immer verschlüsselt oder kryptisch auf den vereinbarten Übertragungswegen.
- . Für die verschlüsselte Übertragung werden nur sichere Protokolle (SFTP, FTPS, SSL) eingesetzt.

2.2 Eingabekontrolle

Ziel: Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Maßnahmen:

- Die Protokollierung von Zugriffen auf personenbezogene Daten erfolgt über ein Erfassungssystem.
- Die personenbezogenen Daten werden nur innerhalb des geschlossenen Systems von autorisierten Usern bearbeitet.

3. VERFÜGBARKEIT UND BELASTBARKEIT

3.1 Fähigkeit der Verfügbarkeit

Verfügbarkeit meint den Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust. Die Verfügbarkeit von Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen oder IT-Netzen oder auch von Informationen ist vorhanden, wenn diese von den Anwendern stets wie vorgesehen genutzt werden können.

Maßnahmen:

- Es erfolgt die aktive Überwachung sämtlicher Systeme während der Arbeitszeit.
- Die unternehmensrelevanten Daten werden täglich gesichert.
- Das Verfahren für Wiederherstellung und Hoch-/ Herunterfahren der Systeme wird regelmäßig dokumentiert, geprüft und getestet.
- Es wird eine unterbrechungsfreie Stromversorgung eingesetzt.

3.2 Fähigkeit der Belastbarkeit

Systeme sind belastbar, wenn sie so widerstandsfähig sind, dass ihre Funktionsfähigkeit selbst bei starkem Zugriff bzw. starker Auslastung gegeben ist.

Maßnahmen:

- Monitoring
- Managed Services
- Einsatz clusterfähiger Systeme

4. VERFAHREN ZUR REGELMÄSSIGEN ÜBERPRÜFUNG, BEWERTUNG UND EVALUIERUNG (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

Maßnahmen:

- Verfügbarkeitskontrolle
- Backup-Konzeption
- Unterbrechungsfreie Stromversorgung (USV)
- Virenschutz
- Firewall
- Meldeverfahren
- Monitoring
- Notfallplanung
- Spiegeln von Festplatten
- Klimaanlagen
- Brand- und Löschwasserschutz
- geeignete Archivierungsräumlichkeiten

4.1 Datenschutzmanagement

Die compleet verfügt über ein Incident-Response-Management und über ein Datenschutzmanagement. 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.

Es werden die gesetzlichen Bestimmungen zum Schutz natürlicher Personen bei der Verarbeitung derer personenbezogenen Daten nach DS-GVO berücksichtigt, eingehalten und periodisch überprüft.

4.2 Auftragskontrolle

Ziel: Auftragsverarbeitung im Sinne von Art. 28 DS-GVO ausschließlich aufgrund entsprechender Weisung des Verantwortlichen.

Maßnahmen:

- Es werden generell mit Kunden und Dienstleistungspartnern Vereinbarungen zur Auftragsverarbeitung geschlossen, die den Anforderungen des Art. 28 DS-GVO entsprechen.
- Es werden generell mit eingesetzten Unterauftragnehmern Vereinbarungen zur Auftragsverarbeitung geschlossen, die den Anforderungen des Art. 28 DS-GVO entsprechen.
- Nach Durchführung jedes Auftrags erfolgt eine Qualitätskontrolle des Auftragsergebnisses sowie eine Freigabe mit 4-Augen-Prinzip vor Auslieferung.
- Es ist ein betrieblicher Datenschutzbeauftragter bestellt, der im Rahmen der Datenschutzorganisation in die relevanten betrieblichen Prozesse eingebunden ist. Der Datenschutzbeauftragte führt jährlich ein Selbstaudit hinsichtlich der getroffenen technischen und organisatorischen Maßnahmen durch.

Stand: 1. Januar 2022

ANLAGE 2 SUBUNTERNEHMER

FIRMA SUBUNTER-NEHMER	ANSCHRIFT	LEISTUNG	DATENKATEGORIEN
Global Business Group AG	Ernst-Barlach-Str. 20 36041 Fulda	• Abrechnung von Lizenzen und Leistungen • Datenpflege und Verwaltung	• Personenstammdaten • Arbeitszeiten • Zeitarbeitnehmer • Mitarbeiter der Auftraggeber und deren Partner
Global Business IT GmbH	Ernst-Barlach-Str. 20 36041 Fulda	• Betrieb der IT-Infrastruktur, • technischer Support • Protokolldaten, User-Profile • Abrechnung von Lizenzen und Leistungen • Datenpflege und Verwaltung	• Personenstammdaten • Arbeitszeiten • Zeitarbeitnehmer • Mitarbeiter der Auftraggeber und deren Partner
DTS Systeme GmbH	Schrewestraße 2 32051 Herford	Betrieb des Rechenzentrums	
Alroma	Paulstraße 8 39218 Schönebeck	Rechenzentrum für Archiv und Backup	
Candis GmbH	Perleberger Straße 42 10559 Berlin	Software zur Bearbeitung der Eingangsrechnungen	

Stand: 1. Januar 2022