compleet

Anlage 2:

VEREINBARUNG ZUR AUFTRAGSVERARBEITUNG (AVV)

(Stand: Januar 2024)

zwischen dem Kunden der compleet GmbH als Auftraggeber („Auftraggeber") und der compleet GmbH, Hermann-Weinhauser-Straße 73, 81673 München 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.

Die vertraglich vereinbarte Dienstleistung wird ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung der Dienstleistung oder von Teilarbeiten dazu in ein Drittland darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standardvertragsklauseln, genehmigte Verhaltensregeln).

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, die Art und der Zweck, die Kategorien von Personen, die von der Verarbeitung betroffen sind sowie die Arten von Daten nicht oder nicht vollständig aus dem Hauptvertrag ergibt, wird auf die folgenden Anlagen verwiesen:

1.2.1. Für das Produkt compleet vendor: Anlage 1 a)

1.2.2. Für die Produkte compleet persoprofiler, compleet PERSY, compleet recruiting: Anlage 1 b)

1.2.3. Für das Produkt compleet workforce: Anlage 1 c)

compleet

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

1.4. 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 2 beschriebenen aktuellen technischen und organisatorischen Maßnahmen.

compleet

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 Geschäftsführerinnen/ 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. Eine Verarbeitung von Daten außerhalb der Betriebsräume des Auftragnehmers (z.B. Telearbeit, Home Office, Mobile Office) ist grundsätzlich gestattet. Soweit eine solche Verarbeitung erfolgt, ist vom Auftragnehmer sicherzustellen, dass dabei ein diesem Vertrag entsprechendes Niveau an Datenschutz und Datensicherheit aufrechterhalten wird und die in diesem Vertrag bestimmten Kontrollrechte des Auftraggebers uneingeschränkt auch in den betroffenen Privatwohnungen ausgeübt werden können.

compleet

3.10. 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.

3.11. 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

5.1. Wendet sich eine betroffene Person mit Forderungen zur Berichtigung, Löschung oder Auskunft an den Auftragnehmer, wird der Auftragnehmer den Betroffenen unverzüglich 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 Berichte des betrieblichen Datenschutzbeauftragten.

compleet

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, mindestens jedoch 14 Werktage, durchgeführt. Der Auftragnehmer darf diese vom Nachweis einer angemessenen Verschwiegenheitserklärung des Prüfers abhängig machen, sofern dieser keiner berufsrechtlichen oder sonstigen gesetzlichen Verschwiegenheitsverpflichtung unterliegt, bei der ein Verstoß nach dem Strafgesetzbuch strafbewährt wäre. 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. Der Nachweis einer Verschwiegenheitsverpflichtung ist nicht erforderlich, wenn diese Aufsichtsbehörde einer berufsrechtlichen oder gesetzlichen Verschwiegenheit unterliegt, bei der ein Verstoß nach dem Strafgesetzbuch strafbewehrt wäre.

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 aus wichtigem Grund widersprechen. Der Widerspruch hat binnen 14 Tagen nach Erhalt des Informationsschreibens 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 jeweiligen Anlage 3 aufgeführten, bei Vertragsschluss bereits bestehenden, Subunternehmer und Teilleistungen erfolgt keine gesonderte Information. Ein Widerspruchsrecht des Auftraggebers besteht für diese Subunternehmer nicht.

compleet

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. Datenschutzbeauftragter

Beim Auftragnehmer ist als Datenschutzbeauftragter

Herr Rechtsanwalt Sascha Weller, Institut für Datenschutzrecht,
Ziegelbräustraße 7, 85049 Ingolstadt
Tel.: +49 (0)841 / 885 167 15
Fax: +49 (0)841 / 885 167 22
E-Mail: ra-weller@idr-datenschutz.de

bestellt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

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

compleet

die Wirksamkeit der Vereinbarung im Übrigen nicht. Die Parteien sind in diesem Fall verpflichtet, unverzüglich in eine nachträgliche Zusatzbestimmung einzuwilligen, die nach Sinn und Zweck der unwirksamen Bestimmung am nächsten kommt.

9.4 Es gilt deutsches Recht.

Anlagen 1: Spezifizierung der Datenverarbeitung:

1. Für das Produkt compleet vendor: Anlage 1 a)
2. Für die Produkte compleet persoprofiler, compleet PERSY, compleet recruiting: Anlage 1 b)
3. Für das Produkt compleet workforce: Anlage 1 c)

Anlage 2: Technische und organisatorische Maßnahmen

Anlagen 3: Subunternehmer:

1. Für das Produkt compleet vendor: Anlage 3 a)
2. Für das Produkt compleet persoprofiler: Anlage 3 b)
3. Für das Produkt compleet PERSY: Anlage 3 c)
4. Für das Produkt compleet workforce: Anlage 3 d)
5. Für das Produkt compleet recruiting: Anlage 3 e)

compleet

Anlage 1 a) – Spezifizierung der Datenverarbeitung - compleet vendor:

(Stand: Januar 2024)

1.1 Gegenstand des Auftrags:

a) Bereitstellung eines Zugangs zum Online-Portal compleet vendor. 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

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

- Speicherung von (personenbezogenen) Daten des Auftraggebers auf den vom Auftragsverarbeiter bereitgestellten Speicherkapazitäten (compleet vendor-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

compleet

1.3 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

1.4 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

compleet

Anlage 1 b) – Spezifizierung der Datenverarbeitung - compleet persoprofiler, compleet PERSY, compleet recruiting:

(Stand: Januar 2024)

1.1 Gegenstand des Auftrags:

Bewerbermanagement umfasst den Prozess von der Ausschreibung einer Stelle auf diversen Mediakanälen und über Kampagnen über die Verwaltung der Bewerberdaten bis hin zur endgültigen Personalauswahl und Personalwirtschaft. Auftragnehmer analysiert für den Auftraggeber das Nutzungsverhalten der Besucher von Kampagnenseiten und den Erfolg einzelner Kampagnen auf Grundlage pseudonymisierter Daten und erstellt Vergleichsanalysen auf Basis vollständig anonymisierter Daten (bspw. via Business Manager). Im Auftrag des Auftraggebers anonymisierte Daten nutzt Auftragnehmer auch für Vergleiche mit Kampagnen anderer Kunden.

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

- Organisation und Durchführung des Bewerbungsmanagements sowie der Distribution von Stellenanzeigen
- Durchführung von Vergleichsanalysen im Rahmen des Bewerbungsmanagements

1.3 Die Verarbeitung umfasst die nachfolgend genannten Arten von Daten:

- Personenstammdaten (z.B. Name, Vorname, Anschrift, Geburtsdatum)
- Kommunikationsdaten (z.B. Telefonnummern, E-Mail-Adressen)
- Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- Kundenhistorie
- Vertragsabrechnungs- und Zahlungsdaten
- Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)
- Bewerbungsdaten (persönliche Daten zur Anbahnung eines Arbeitsverhältnisses),
- Benutzerdaten (geschäftliche Kontaktinformationen zur Bewerberkommunikation)
- Nutzungsstatistiken (Auswertung für Administratoren und Auftraggeber)

compleet GmbH
Hermann-Weinhauser-Straße 73
81673 München
Germany

Kontakt
Tel.: +49 (0)89 2488 07 200
E-Mail: info@compleet.com
www.compleet.com

Geschäftsführung
Sophie Genty
Dr. Tobias Weigl

Handelsregister und Umsatzsteuer
Amtsgericht: München
HRB 141304
USt.-ID-Nr. 221032702

Bankverbindung
Stadtsparkasse München
IBAN: DE14 7015 0000 0061 1065 22
BIC: SSKMDEMMXXX

compleet

1.4 Folgende Kategorien von Personen sind von der Verarbeitung betroffen:

- Kunden
- Interessenten
- Abonnenten
- Beschäftigte
- Lieferanten
- Handelsvertreter
- Ansprechpartner
- Bewerber und Kandidaten für ein Beschäftigungsverhältnis
- Nutzer (geben geschäftliche Kontaktinformationen zur Kommunikation an)

Anlage 1 c) – Spezifizierung der Datenverarbeitung - compleet workforce: (Stand: Januar 2024)

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

1.2 Art der Daten und Kategorien betroffener Personen

1.2.1 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.

1.2.2 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.

1.2.3 Kategorien betroffener Personen sind:

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

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

- Pflege und Verwaltung von Arbeitnehmerdaten;
- Erfassung und Verarbeitung von Arbeitszeiten und Abwesenheiten;

compleet

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

1.2.5 Folgenden Datenarten oder -kategorien sind dabei Gegenstand der Erhebung, Verarbeitung und/ oder Nutzung durch den Auftragsverarbeiter:

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

1.3 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.

compleet

Anlage 2
zur Vereinbarung zur Auftragsverarbeitung

TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN

(Stand: Januar 2024)

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)

compleet

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

compleet

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

compleet

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

compleet

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

compleet

Anlage 3 a) – SUBUNTERNEHMER – compleet vendor:

(Stand: Januar 2024)

FIRMA SUBUNTERNEHMER	ANSCHRIFT/ LAND	LEISTUNG
Amazon Web Services EMEA Sàrl	38 avenue John F. Kennedy, 1855, Luxemburg	Hosting und Infrastruktur
AllCloud GmbH	Rosenstr. 2, Berlin 10178, Deutschland	Entwicklung, Service und Wartung der Infrastruktur bei Amazon Web Services EMEA Sàrl
Hetzner Online GmbH	Industriestr. 25, 91710 Gunzenhausen, Deutschland	Backup
Microsoft Ireland Operations Ltd	One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Irland	Technischer Dienstleister Single-Sign-On
Sentry		
Squareball Digital GmbH	Manteuffelstr. 64, 10999 Berlin	Authentifizierung-Service Okta

Anlage 3 b) – SUBUNTERNEHMER – compleet persoprofiler:

(Stand: Januar 2024)

FIRMA SUBUNTERNEHMER	ANSCHRIFT/ LAND	LEISTUNG
Google Cloud EMEA Limited	Velasco, Clanwilliam Place, Dublin 2, Irland	Geo-Location-Dienste
MONA AI GmbH	Campus Universität des Saarlandes Starterzentrum | Gebäude A1 1, 66123 Saarbrücken, Deutschland	Technischer Dienstleister
NETWAYS Managed Services GmbH	Deutschherrnstr. 15-19, 90429 Nürnberg, Deutschland	Technischer Dienstleister, Hosting der Softwarelösung
PitchYou GmbH	Campusallee 9, 51379 Leverkusen, Deutschland	Technischer Dienstleister
Sentry	45 Fremont Street, San Francisco, CA 94105, USA	Logging von technischem Monitoring der Applikation
Squareball Digital GmbH	Manteuffelstr. 64, 10999 Berlin	Authentifizierung-Service Okta

compleet

Anlage 3 c) – SUBUNTERNEHMER – compleet PERSY:

(Stand: Januar 2024)

FIRMA SUBUNTERNEHMER	ANSCHRIFT/ LAND	LEISTUNG
AllCloud GmbH	Rosenstr. 2, Berlin 10178, Deutschland	Entwicklung, Service und Wartung der Infrastruktur bei Amazon Web Services EMEA Sàrl
Amazon Web Services EMEA Sàrl	38 avenue John F. Kennedy, 1855, Luxemburg	Hosting und Infrastruktur
Google Cloud EMEA Limited	Velasco, Clanwilliam Place, Dublin 2, Irland	Geo-Location-Dienste
Google Ireland Limited	Gordon House, Barrow Street, Dublin 4, Irland	Klicktracking
Hetzner Online GmbH	Industriestr. 25, 91710 Gunzenhausen, Deutschland	Mail-Gateway
Microsoft Ireland Operations Ltd	One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Irland	Technischer Dienstleister Reporting-Platform
PitchYou GmbH	Campusallee 9, 51379 Leverkusen, Deutschland	Technischer Dienstleister
Textkernel B.V.	Nieuwendammerkade 26a5, NL1022 AB Amsterdam, Niederlande	Entwicklung, Service und Wartung der search-Suchmaschine, sowie für CV-Parsing
VONQ B.V.	Beursplein 37, 3011 AA Rotterdam, Niederlande	Buchung von Kampagnen für Stellenanzeigen

compleet

Anlage 3 d) – SUBUNTERNEHMER – compleet workforce:

(Stand: Januar 2024)

FIRMA SUBUNTERNEHMER	ANSCHRIFT/ LAND	LEISTUNG
AllCloud GmbH	Rosenstr. 2, Berlin 10178, Deutschland	Entwicklung, Service und Wartung der AWS-Infrastruktur sowie Monitoring-Lösung DataDog
Alroma	Paulstraße 8 39218 Schönebeck	Rechenzentrum für Archiv und Backup
DTS Systeme GmbH	Schrewestraße 2 32051 Herford	Betrieb des Rechenzentrums
Microsoft Ireland Operations Ltd	One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Irland	Technischer Dienstleister: Single-Sign-On, Reporting-Plattform

compleet

Anlage 3 e) – SUBUNTERNEHMER – compleet recruiting:

(Stand: Januar 2024)

FIRMA SUBUNTERNEHMER	ANSCHRIFT/ LAND	LEISTUNG
AllCloud GmbH	Rosenstr. 2, Berlin 10178, Deutschland	Entwicklung, Service und Wartung der Infrastruktur bei Amazon Web Services EMEA Sàrl
Amazon Web Services EMEA Sàrl	38 avenue John F. Kennedy, 1855, Luxemburg	Technischer Dienstleister, Hosting und Infrastruktur
MONA AI GmbH	Campus Universität des Saarlandes Starterzentrum Gebäude A1 1, 66123 Saarbrücken	Technischer Dienstleister
NETWAYS Managed Services GmbH	Deutschherrnstr. 15-19, 90429 Nürnberg, Deutschland	Technischer Dienstleister, Hosting der Softwarelösung
PitchYou GmbH	Campusallee 9, 51379 Leverkusen, Deutschland	Technischer Dienstleister
Sentry	45 Fremont Street, San Francisco, CA 94105, USA	Logging von technischem Monitoring der Applikation
Squareball Digital GmbH	Manteuffelstr. 64, 10999 Berlin	Authentifizierung-Service Okta
VONQ B.V.	Beursplein 37, 3011 AA Rotterdam, Niederlande	Buchung von Kampagnen für Stellenanzeigen