Auftragsbedingungen

1. Präambel

Der folgende Softwarenutzungsvertrag ermöglicht dem Lizenznehmer die widerrufliche Nutzung ausgewählter, vom Lizenzgeber entwickelter Softwaremodule; im Übrigen verbleiben alle Rechte an Software und Dokumentation beim Lizenzgeber. Der Funktionsumfang der Software ergibt sich aus den jeweils gebuchten Softwaremodulen. Hiernach richtet sich auch die monatliche Nutzungsgebühr. Soweit in diesem Softwarenutzungsvertrag nicht ausdrücklich abweichend vorgesehen, gelten ergänzend die zum Zeitpunkt des Vertragsabschlusses gültigen „Nutzungsbedingungen für PERSY" des Lizenzgebers (**Nutzungsbedingungen für PERSY**).

Sämtliche vorgenannten wie auch nachbestellten Softwaremodule bleiben während der gesamten Nutzungsdauer uneingeschränktes Eigentum des Lizenzgebers. Alle geistigen Eigentumsrechte an der Software, deren Nutzung Gegenstand dieses Vertrages ist, stehen dem Lizenzgeber zu. Der Lizenznehmer erwirbt keinerlei Rechte an der Software, deren Entwicklungen und dem Know-How des Lizenzgebers.

2. Nutzungssache und Nutzungsgebühren

Die auf Seite 1 aufgeführten Softwaremodule bzw. Leistungen werden im Rahmen dieses Vertrages dem Lizenznehmer vom Lizenzgeber zur Verfügung gestellt.

3. Nachbestellungen, Kontingente, Bundesagentur für Arbeit

Für nachbestellte Softwaremodule und Leistungen gem. Ziffer 5 „Vertragslaufzeiten, Kündigungsfristen" finden die Kündigungsfristen des Hauptvertrages Anwendung. Für alle anderen Produkte wenden Sie sich bitte an Ihren zuständigen Vertriebsmitarbeiter bei compleet. Es gelten die Konditionen der zum Zeitpunkt der Nachbestellung aktuellen Preisliste von compleet. Beauftragt der Lizenznehmer den Lizenzgeber mit der Vermittlung von Stellenanzeigen des Lizenznehmers oder eines Dritten an teilnehmende Börsen zur Veröffentlichung, wird der Lizenzgeber im Rahmen des technisch und tatsächlich Möglichen alle Anstrengungen zur termingerechten und fehlerfreien Übermittlung an die gewünschten Börsen unternehmen. Der Lizenzgeber ist jedoch nicht in der Lage, die Veröffentlichungen in den gewünschten Börsen zu überprüfen und übernimmt daher keine Gewähr dafür, dass die Stellenanzeigen in sämtlichen der gewünschten Börsen tatsächlich oder in der gewünschten Form oder zu einem vom Lizenznehmer gewünschten Zeitpunkt erscheinen.

3.1 kostenloses MCP Netzwerk (Multi-Channel-Posting) / Organische Medien Kanäle

Die Stellenanzeigen des Lizenznehmers werden durch den Lizenzgeber in dessen organischen Medien-Kanal-Netzwerk ausgespielt. Ob Stellenanzeigen auf den einzelnen Medienkanälen veröffentlicht werden, obliegt im Verantwortungsbereich jedes einzelnen Medien-Kanal Betreibers. Der Lizenzgeber stellt hierfür die technischen Voraussetzungen in der Software zur Verfügung. Sofern der Lizenznehmer über das gebuchte Kontingent hinaus Stellenanzeigen veröffentlicht, wird der Lizenzgeber den Lizenznehmer auf die Kontingentüberschreitung hinweisen und ein Angebot zur Erhöhung des Kontingents unterbreiten. Sofern der Lizenznehmer trotz des Hinweises das gebuchte Kontingent zur Veröffentlichung von Stellenanzeigen auch im Folgemonat weiterhin überschreitet, gilt das Angebot als angenommen. Der Lizenzgeber ist somit berechtigt, das erhöhte Kontingent bereits für den Folgemonat in Rechnung zu stellen.

3.2 Bundesagentur für Arbeit

Sofern der Lizenznehmer mittels der bestellten Softwaremodule Stellenanzeigen auf der Jobbörse der Bundesagentur für Arbeit veröffentlicht, sind die Nutzungsbedingungen der Bundesagentur für Arbeit zu beachten. Bei Zuwiderhandlungen ist der Lizenzgeber berechtigt, den Veröffentlichungskanal der Jobbörse der Bundesagentur für Arbeit für den Lizenznehmer zu sperren.

3.3 Premium Kanäle

Sofern im Rahmen der Veröffentlichung von Stellenanzeigen bei sogenannten Premium-Jobboards (z.B. Monster, Stepstone, Stellenanzeigen.de, kalaydo) vorgenannte Softwaremodule verwendet werden, ist der Lizenznehmer verpflichtet, diese ausschließlich über den Lizenzgeber zu beziehen. Wenn der Lizenznehmer dieser Verpflichtung nicht nachkommt (d.h. der Erwerb dieser Stellenanzeigen über andere Bezugsquellen erfolgt), ist der Lizenzgeber berechtigt, für die Datenanlieferung bzw. Veröffentlichung mittels PERSY 15 % des vom Lizenznehmer für diese Stellenanzeigen entrichteten Einkaufspreises als Softwarenutzungsgebühr in Rechnung zu stellen. Erbringt der Lizenznehmer keinen Nachweis über den entrichteten Einkaufspreis, so ist der Lizenzgeber berechtigt, den Einkaufspreis zu schätzen.

4. Zahlungsbedingungen

Die Rechnungsstellung zu den bestellten Softwaremodulen und Leistungen beginnt mit dem Tag der Unterschrift, wenn nicht anders vereinbart. Die compleet GmbH gewährleistet nach Eingang der angeforderten Daten den Versand der Initialpasswörter innerhalb von drei bis fünf Werktagen.

5. Vertragslaufzeit, Kündigungsfristen

Der Vertrag tritt mit Unterzeichnung durch den Lizenznehmer in Kraft und wird, sofern nicht anders vereinbart, für zwölf (12) Monate geschlossen. Die Vertragslaufzeit beginnt, sofern nicht anders vereinbart, mit dem Tag der Unterschrift. Der Vertrag verlängert sich jeweils um weitere zwölf (12) Monate, sofern er nicht spätestens acht (8) Wochen vor Ablauf der Vertragslaufzeit schriftlich oder per E-Mail an sales@compleet.com gekündigt wird. Bei der automatischen Vertragsverlängerung besteht für compleet die Möglichkeit der Preisanpassung über gebuchte Leistungen aus dem Hauptvertrag an die Konditionen der aktuellen Preisliste zum Zeitpunkt der Verlängerung. Softwaremodule und Leistungen können nachbestellt und in das bestehende Vertragsverhältnis aufgenommen werden. Als Grundlage solcher Nachträge gilt hierfür grundsätzlich der Hauptvertrag (Erstvertrag). Soweit nichts anderes vereinbart wird, gelten dabei analog die Vertragslaufzeiten und Kündigungsfristen des Hauptvertrages von zwölf (12) Monaten sowie die Vertragsverlängerungsregelung um jeweils weitere zwölf (12) Monate, wenn nicht spätestens acht (8) Wochen vor Ablauf der

Vertragslaufzeit schriftlich oder per E-Mail an sales@compleet.com eine Kündigung (Unterschriebenes Dokument) erfolgt ist. Die Kündigung wird erst durch eine Kündigungsbestätigung in Text- oder Schriftform seitens des Lizenzgebers rechtswirksam.
Bei dem Produkt „PERSY lite" gilt eine abweichende Laufzeit von einem (1) Monat. Der Vertrag verlängert sich jeweils um einen (1) Monat, wenn er nicht mit einer Frist von zwei (2) Wochen zum Monatsende gekündigt wird.

6. Systemverfügbarkeit

Der Lizenzgeber stellt mit hohem Aufwand die maximale Verfügbarkeit seiner Softwaremodule sicher und garantiert eine jährliche Erreichbarkeitsquote der Server/ Applikation von 99 % im Mittel. Alle kritischen Komponenten im Bereich der Server-Hardware sind redundant ausgelegt. Systemausfälle können jedoch trotz aller Maßnahmen nicht vollständig ausgeschlossen werden. Hiervon ausgenommen sind Zeiträume, die der Lizenzgeber als sogenannte Wartungsfenster zur Optimierung und Leistungssteigerung kennzeichnet, sowie Zeitverlust bei der Störungsbeseitigung durch Gründe, die nicht durch den Lizenzgeber zu vertreten sind, sowie Ausfälle aufgrund höherer Gewalt. Wartungsarbeiten werden frühzeitig angekündigt und finden außerhalb der allgemeingültigen Geschäftszeiten statt.

7. Systemeinrichtung, Support

Nach Beauftragung informiert der Lizenzgeber den Lizenznehmer per Willkommens-Email über die für die Systemeinrichtung benötigten Unterlagen und Dateien. Der Lizenzgeber wird Fragen des Lizenznehmers zur Anwendung der vertragsgegenständlichen Softwaremodule und Leistungen werktags von 9:00 Uhr bis 12:30 Uhr und von 13:30 Uhr bis 17:00 Uhr innerhalb der nächsten drei Werktage nach Eingang der jeweiligen Frage beantworten.

8. Bedingungen und Konditionen

Der Lizenznehmer darf PERSY oder Teile davon nicht modifizieren oder bearbeiten oder durch „Reverse Engineering" nachbauen, insbesondere mit dem Ziel ein konkurrierendes Produkt oder einen konkurrierenden Service, ein Produkt unter Verwendung ähnlicher Ideen, Merkmale, Funktionen oder grafischen Darstellungen des Service zu entwickeln oder zu kopieren. Die Nutzungsbedingungen für PERSY des Lizenzgebers sind Bestandteil dieses Vertrages und werden vom Lizenznehmer akzeptiert. Die Nutzungsbedingungen für PERSY des Lizenzgebers sind in geltender Fassung hier abrufbar und können auf Wunsch zugesandt werden.

9. Nebenabreden, Schriftform und Gerichtsstand

Nebenabreden über den Inhalt dieser Vereinbarung hinaus wurden nicht getroffen. Änderungen und Ergänzungen der Vereinbarung bedürfen zu ihrer Wirksamkeit der Schriftform und müssen als solche gekennzeichnet sein. Als Gerichtsstand wird München vereinbart.

Vereinbarung zur Auftragsverarbeitung

(Stand: Dezember 2020)

zwischen [den Kunden des Produktes PERSY der compleet GmbH] als Auftraggeber („Auftraggeber")
und der compleet GmbH, Hauptstraße 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 der Auftragsverarbeitung ist im Hauptvertrag beschrieben und umfasst im Wesentlichen:
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 PERSY Business Intelligence). 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 Folgende Kategorien von Personen sind von der Verarbeitung betroffen:

- Kunden
- Beschäftigte
- Bewerber für ein Beschäftigungsverhältnis
- Nutzer (geben geschäftliche Kontaktinformationen zur Bewerberkommunikation an)

1.4 Die Verarbeitung umfasst die nachfolgend genannten Arten von Daten:
- Personenstammdaten
- Kommunikationsdaten (z.B. Telefon, E-Mail)
- Vertragsstammdaten (Vertragsbeziehung, Produkt-bzw. Vertragsinteresse)
- Kundenhistorie
- Bewerbungsdaten (persönliche Daten zur Anbahnung eines Arbeitsverhältnisses),
- Benutzerdaten (geschäftliche Kontaktinformationen zur Bewerberkommunikation)
- Nutzungsstatistiken (Auswertung für Administratoren und Auftraggeber)

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

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

3.8 Der Auftragnehmer gewährleistet, seinen Pflichten nach Art. 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 Anhang 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 vertraglich vereinbarte Dienstleistung kann in einem Staat außerhalb der Europäischen Union oder außerhalb eines Landes, das den Vertrag über den Europäischen Wirtschaftsraum unterzeichnet hat, erbracht werden. Für diesen Fall wird stets eine Einzelfallprüfung durchgeführt. 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.

Anhang 1: Technische und organisatorische Maßnahmen
Anhang 2: Subunternehmer

Anhang 1
zur Vereinbarung zur Auftragsverarbeitung

TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN

Vertraulichkeit

Zutrittskontrolle

Um Unbefugten den Zutritt zu DV-Anlagen (Datenverarbeitungsanlagen) zu verwehren, werden Besucher beim Betreten des Gebäudes in Empfang genommen und innerhalb des Gebäudes begleitet. Besucher und Arbeitsräumlichkeiten sind getrennt. compleet verfügt über separate Serverräume mit Zutrittsbeschränkungen. Weiterhin tragen ein Schließsystem und Regelungen zur Schlüsselvergabe gegen mögliche Einbrüche zur Sicherung der Zutrittskontrolle bei. Für das Rechenzentrum QSC ist ein 7-stufiges Zutrittskontrollsystem zum Gebäude sowie in den Co-Location Räumen eingerichtet. Zutritt zum Rechenzentrum ist nur für autorisierte Personen mit gültigem Ausweis möglich (Lichtbildpass und PIN). Zugang zum Server ist nur in Begleitung von Personal des Rechenzentrums möglich. Es befindet sich 24 h pro Tag, 7 Tage je Woche Sicherheitspersonal vor Ort und es wird rund um die Uhr ein Monitoring der kompletten Infrastruktur durchgeführt. Videoüberwachung und Aufzeichnung im gesamten Rechenzentrum sowie den Außenanlagen.

Zugangskontrolle

Um zu verhindern, dass Unbefugte die Möglichkeit haben, DV-Systeme zu nutzen, verfügt compleet über Passwortrichtlinien, Authentifikationsverfahren, Verschlüsselung von Datenträgern, zertifikatsbasierte Zugangsberechtigungen (SSL) und

automatische Sperrverfahren bei Nicht-Nutzung des PCs. Zugangsberechtigungen der Mitarbeiter zu den IT-Systemen werden in einem Active-Directory dokumentiert. Nach Ausscheiden eines Mitarbeiters werden dessen Zugänge unverzüglich gelöscht. Zur weiteren Sicherung werden Anti-Viren-Software, Firewalls und SPAM-Filter eingesetzt.

Zugriffskontrolle

Mittels mehrstufigen Rollen- & Berechtigungskonzepten wird sichergestellt, dass Nutzer nur auf Daten, Dateien und Datenträger zugreifen können, die ihren Berechtigungen entsprechen. Daten in Papierform mit sensiblen Inhalten werden in Sicherheitsschränken aufbewahrt. Eine Revision der Berechtigungen und der zu löschenden Daten wird regelmäßig durchgeführt. Zugriff von außen ist ausschließlich über VPN-Verbindung möglich. Der IP-Bereich im Unternehmensnetzwerk ist eingeschränkt und Unternehmensnetzwerk vom Gästenetzwerk getrennt. Zugriffe werden protokolliert.

Trennungskontrolle

Um zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können, ist die Applikation modular aufgebaut. Je nach freigeschaltetem Modul, kann ein Nutzer nur Daten verarbeiten, die für den jeweiligen Zweck benötigt werden. Daten unterschiedlicher Auftraggeber sind logisch voneinander getrennt (Mandantenfähigkeit). Das Produktivsystem ist vom Testsystem getrennt (Sandboxing). Innerhalb der Datenbank werden Daten in separaten Tabellen gespeichert.

Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)

Personenbezogene Daten werden je nach Ergebnis einer Risikoabschätzung so verarbeitet, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können. Diese zusätzlichen Informationen werden gesondert aufbewahrt und unterliegen der IT-Sicherheitsrichtlinie.

Integrität

Weitergabekontrolle

Durch ausschließliche Nutzung IP-Adressen-gebundener VPN-Verbindungen wird sichergestellt, dass Daten im Rechenzentrum nicht unbefugt gelesen, kopiert, verändert oder bei elektronischer Übertragung entfernt werden. Benutzer können ausschließlich per SSL-Verbindung personenbezogene Daten abrufen und speichern. Weisungsbefugte bzw. weisungsempfangende Mitarbeiter werden gegenüber Dienstleistern bzw. Auftraggebern mit Beginn der Zusammenarbeit klar kommuniziert, so dass die Weitergabe an Dritte nur durch Berechtigte erfolgt. Für Dokumente mit sensiblen Daten werden entsprechende Versandwege (Versiegelung, Kurier) gewählt.

Eingabekontrolle

Eine entsprechende Protokollierung in der EDV und Authentifikationsverfahren (pro Benutzer eine Benutzerkennung, keine gemeinsamen Accounts) ermöglicht (auch nachträglich) eine Überprüfung, wer welche personenbezogenen Daten eingegeben, verändert oder entfernt hat.

Verfügbarkeit und Belastbarkeit

Verfügbarkeitskontrolle

Der Einsatz von Sicherungsmaßnahmen wie regelmäßige Backups (via Speicherabbildsicherung) für Datenbanken und Softwareentwicklungsstände schützt die Daten gegen zufällige oder mutwillige Zerstörung bzw. Verlust. Die Applikation wird auf mehreren physisch getrennten und virtualisierten Servern betrieben, durch Loadbalancer bedient und ist skalierbar. Das Hochleistungsnetz des Rechenzentrums ist redundant an mehrere Internet-Backbones angebunden und verfügt über Peerings mit mehr als 40 nationalen und internationalen ISPs (Internet-Service-Provider) und Carriern. Das Rechenzentrum gewährleistet eine unterbrechungsfreie Stromversorgung mit redundanter Gebäudezuführung, Schutz vor Spannungsschwankungen im öffentlichen Stromnetz sowie Notstromversorgung über USV und Dieselgeneratoren. 3 Brandmeldesysteme mit Früherkennung (VESDA) kombiniert mit hardwareschonender Brandlöschung unter Verwendung des Edelgases Argon reduzieren das Risiko von Datenverlust durch Feuer. Nach dem Stand der Technik erforderliche Firewall-Technologien sind implementiert und werden auf dem aktuellen Stand gehalten.

Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO)

Die Software und Konfiguration wird über ein Versionisierungssystem verwaltet, dies erlaubt schnelle Rollbacks. Ein Notfallplan existiert und steuert die rasche Wiederherstellung des Betriebes.

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Datenschutz-Management

Eine Organisationsstruktur wurde aufgebaut und Verantwortlichkeiten vergeben. Die Unterschiedlichen Rollen und Aufgaben sind in Richtlinien und Arbeitsanweisungen geregelt und werden kontinuierlich im PDCA-Zyklus (Plan-Do-Check-Act) optimiert. Durch regelmäßige Sensibilisierungsmaßnahmen und Maßnahmenplanung werden Datenschutzrisiken minimiert.

Incident-Response-Management

Regelmäßige Überprüfungen der IT-Sicherheit und des Qualitätsmanagements finden statt um Sicherheitsvorfälle zu minimieren. Meldungen über Sicherheitsvorfälle sind zentralisiert. Sicherheitsvorfällen werden genau identifiziert und eingegrenzt. Zur Vermeidung von Vorfallwiederholung werden relevante Personen im Rahmen des kontinuierlichen Verbesserungsprozesses geschult. Im Fehlerfalle werden Maßnahmen entsprechend dem Notfallplans ergriffen.

Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)

Die Verarbeitung personenbezogener Daten ist am Zweck der Auftragserfüllung ausgerichtet und standardmäßig auf ein Minimum beschränkt. Die Erfassung optionaler Informationen ist als Opt-In angelegt. In Bezug auf die Funktionen und die Verarbeitung personenbezogener Daten wird mit Hilfe von Nutzungsbedingungen und Datenschutzinformationen Transparenz hergestellt.

Auftragskontrolle

Durch eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl der Dienstleister, Vorabkontrollen und Nachkontrollen stellt compleet sicher, dass keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers stattfindet.

Stand: Dezember 2020

Anhang 2 zur Vereinbarung zur Auftragsverarbeitung (Stand: Dezember 2020):

SUBUNTERNEHMER

FIRMA SUBUNTERNEHMER	ANSCHRIFT/LAND	LEISTUNG
AllCloud GmbH, c/o DWF	Prinzregentenstraße 78, 81675 München, Deutschland	Dienstleister für Entwicklung, Service und Wartung der AWS-Infrastruktur
Amazon Web Services Inc. (AWS)	Region eu-central-1, Frankfurt, Deutschland	Rechenzentrum inkl. Service & Wartung der Hardware für PERSY, Kampagnen-Steuerung und search-Suchmaschine
Creativestyle GmbH	Erika-Mann-Straße 53, 80636 München, Deutschland	Dienstleister für Entwicklung, Service und Wartung der Kampagnen-Steuerung
DPS Business Solutions GmbH	Am Moosfeld 27, 81829 München, Deutschland	Dienstleister für Entwicklung, Service und Wartung einer Komplettlösung auf Basis der Sage Standardsoftware (CRM & ERP)
Google Analytics Ireland	Gordon House, Barrow Street, Dublin 4, Irland	Klicktracking
Hetzner Online GmbH	Industriestr. 25, 91710 Gunzenhausen, Deutschland	Rechenzentrum für Media-Server
Infopulse GmbH	Kochstr. 19, 74405 Gaildorf, Deutschland	Dienstleister für Entwicklung, Service und Wartung
Oraylis GmbH	Klaus-Bungert-Straße 4, 40468 Düsseldorf, Deutschland	Dienstleister für Entwicklung, Service und Wartung eines Datawarehouse, Beratung für Traffic & Performance Analysen
QSC AG	Balanstraße 73, 81541 München, Deutschland	Rechenzentrum inkl. Service & Wartung der Hardware für PERSY und search-Suchmaschine
Textkernel B.V.	Nieuwendammerkade 26a5, NL1022 AB Amsterdam, Niederlande	Dienstleister für Entwicklung, Service und Wartung der search-Suchmaschine, sowie für CV-parsing
Zenturion Software Development & Consulting GmbH	Knorrstraße 39, 80807 München, Deutschland	Dienstleister für Entwicklung, Service und Wartung des Videointerviews