Vertragsanlage zur Auftragsverarbeitung gemäß Art. 28 DS-GVO

Datenschutz – und Datensicherheitsbestimmungen

zwischen Auftraggeber und Auftragnehmer

Die nachfolgenden Datenschutz- und Datensicherheitsbestimmungen (DuD-B) finden Anwendung auf alle Leistungen oder Tätigkeiten, bei denen der AUFTRAGNEHMER, von ihm eingesetzte Personen oder durch den AUFTRAGNEHMER mit Einwilligung des AUFTRAGGEBERS beauftragte Subunternehmer personenbezogene Daten im Auftrag erheben, verarbeiten oder nutzen, Art. 28. Abs. 1 Satz 1 DSGVO. Die DuD-B finden weiterhin Anwendung bei Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen, wenn dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann, Art. 28 Abs. 2-4 DS-GVO. Diese Regelungen gelten entsprechend auch für alle sonstigen im Auftrag verarbeiteten Daten, insbesondere – unabhängig von der Rechtsform - Kundendaten oder eigene Daten des Auftraggebers oder seiner Mitarbeiter, und zwar auch dann, wenn sich die folgenden Bestimmungen ausdrücklich auf personenbezogene Daten beziehen.

I. Allgemeine Bestimmungen

(1) Der AUFTRAGGEBER ist als „Verantwortliche Stelle“ i.S.d. Art. 4 Nr. 7 EU-Datenschutzgrundverordnung (DSGVO) für die Einhaltung der DSGVO und anderer Vorschriften über den Datenschutz, für die Rechtmäßigkeit der Datenerhebung, -verarbeitung und -nutzung, insbesondere der Datenweitergabe an den AUFTRAGNEHMER, sowie für die Wahrnehmung der Rechte der Betroffenen Art. 4 Nr. 1 DSGVO verantwortlich, Art. 28 Abs. 1 Satz 1 DSGVO. Der AUFTRAGNEHMER hat den AUFTRAGGEBER hierbei in geeigneter Weise zu unterstützen, Art. 28 Abs.3 lit. e DSGVO. Darüber hinaus verpflichtet sich der AUFTRAGNEHMER zur Einhaltung sämtlicher einschlägiger datenschutz-rechtlicher Vorschriften.

(2) Bei der Erhebung, Verarbeitung und Nutzung personenbezogener Daten wird der AUFTRAGNEHMER für den AUFTRAGGEBER tätig und ist insoweit verpflichtet, die Daten ausschließlich zur Erbringung der vertraglich vereinbarten Leistungen und für Zwecke des AUFTRAGGEBERS zu erheben, zu verarbeiten oder zu nutzen und dabei gemäß Art. 28 Abs.3 lit. a DSGVO den **Weisungen** des AUFTRAGGEBERS zu folgen. Eine Verarbeitung oder Nutzung für sonstige, insbesondere eigene Zwecke ist dem AUFTRAGNEHMER nicht erlaubt.

Darüber hinaus sind im Einzelnen der Gegenstand und die Dauer des Auftrags, der Umfang, die Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen sowie der Umfang der Weisungsbefugnisse, die sich der AUFTRAGGEBER gegenüber dem AUFTRAGNEHMER vorbehält, im Hauptvertrag festgelegt.

(3) Soweit der AUFTRAGNEHMER seine Leistung in den Räumlichkeiten oder unter Zugriff auf die Systeme des AUFTRAGGEBERS erbringt, unterliegt er den Kontrolleinrichtungen des AUFTRAGGEBERS (insbesondere Zutritts-, Zugangs- und Zugriffskontrolle).

(4) Bei der E-Mail-Kommunikation werden die Parteien die Vertraulichkeit beachten, indem sie vertrauliche Informationen gegen unberechtigte Kenntnisnahme oder Manipulationen schützen. Hierzu können die Parteien entsprechende technische Maßnahmen, z.B. Verschlüsselungs- und Signaturverfahren, abstimmen.

II. Gegenstand und Dauer des Auftrags

(1) Gegenstand

☒ Der Gegenstand des Auftrags ergibt sich aus der Leistungsvereinbarung „CETOS - IT Support - Servicevertrag“ vom ....., auf die hier verwiesen wird (im Folgenden Leistungsvereinbarung).

oder

☐ Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer: ……

(Definition der Aufgaben)

(2) Dauer

☒ Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.

oder (insbesondere, falls keine Leistungsvereinbarung zur Dauer besteht)

☐ Der Auftrag wird zur einmaligen Ausführung erteilt.

oder

☐ Die Dauer dieses Auftrags (Laufzeit) ist befristet bis zum .....

oder

☐ Der Auftrag ist unbefristet erteilt und kann von beiden Parteien mit einer Frist von ..... zum ..... gekündigt werden. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

III. Konkretisierung des Auftragsinhalts

(1) Umfang, Art und Zweck der Erhebung, Verarbeitung und / oder Nutzung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind in der Vereinbarung „CETOS - Endpoint Manager - Nutzungsvertrag“ unter Punkt 1 und Punkt 2 beschrieben.

Es handelt sich um die Nutzung einer Eigenentwicklung der CETOS Services AG, mit der Hard- und Software verwaltet werden kann. Hierfür werden personenbezogene Daten im Zuge von Nutzerverwaltungen verarbeitet.

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Artt. 44 ff. DS-GVO erfüllt sind. Das angemessene Schutzniveau in …….

- ☐ ist festgestellt durch einen Angemessenheitsbeschluss der Kommission (Art. 45 Abs. 3 DS-GVO);
- ☒ wird hergestellt durch verbindliche interne Datenschutzvorschriften (Art. 46 Abs. 2 lit. b i.V.m. 47 DS-GVO);
- ☐ wird hergestellt durch Standarddatenschutzklauseln (Art. 46 Abs. 2 litt. c und d DS-GVO);
- ☐ wird hergestellt durch genehmigte Verhaltensregeln (Art. 46 Abs. 2 lit. e i.V.m. 40 DS-GVO);
- ☐ wird hergestellt durch einen genehmigten Zertifizierungsmechanismus (Art. 46 Abs. 2 lit. f i.V.m. 42 DS-GVO).
- ☐ wird hergestellt durch sonstige Maßnahmen: ……. (Art. 46 Abs 2 lit. a, Abs. 3 litt. a und b DS-GVO).

(2) Art der Daten

☐ Die Art der verwendeten personenbezogenen Daten ist in der Leistungsvereinbarung konkret beschrieben unter: .....

oder

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

- ☒ Name, Titel, akademischer Grad
- ☐ Berufs-, Branchen- oder Geschäftsbezeichnung
- ☒ Anschrift
- ☐ Geburtsdatum/-jahr/-tag
- ☒ Kommunikationsdaten (z.B. Telefon, E-Mail)
- ☐ TKG-Daten (Verkehrs-, Standort,- und Nutzungsdaten, Einzelverbindungsdaten i.S. des Telekommunikationsgesetzes, TKG, [Artikel 3 RiLi 2002/58/EG]
- ☒ Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- ☒ Kundenhistorie
- ☒ Vertragsabrechnungs- und Zahlungsdaten
- ☐ Sensitive Daten (Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben)
- ☐ Daten, die einem Berufsgeheimnis unterliegen
- ☐ Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten oder den Verdacht strafbarer Handlungen oder Ordnungswidrigkeiten beziehen
- ☐ Daten zu Bank- und Kreditkartenkonten
- ☐ Planungs- und Steuerungsdaten
- ☐ Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)
- ☐ Personalstammdaten
- ☐ Sozialdaten

- ☐ _____

(3) Kategorien betroffener Personen

☐ Die Kategorien der durch die Verarbeitung betroffenen Personen sind in der Leistungsvereinbarung konkret beschrieben unter: .....

oder

☒ Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- ☒ Mitarbeiter
- ☐ Angehörige von Mitarbeitern
- ☐ Pensionäre/Hinterbliebene
- ☐ Bewerber
- ☒ Kunden
- ☐ Mitarbeiter von Fremdfirmen
- ☐ Interessenten
- ☐ Mieter/Vermieter, Pächter/Verpächter
- ☐ Lieferanten
- ☐ Ansprechpartner
- ☐

IV. Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) Der Auftragnehmer hat die Sicherheit gem. Artt. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen [Einzelheiten in Anlage 1].

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

V. Pflichten des AUFTRAGNEHMERS

(4) Zum Schutz personenbezogener Daten vor Missbrauch und Verlust wird der AUFTRAGNEHMER die technischen und organisatorischen Vorkehrungen treffen, die in der beigefügten **„Vereinbarung zu den technischen und organisatorischen Maßnahmen“** zwischen den Parteien festgelegt wurden. Die Vereinbarung ist Bestandteil dieser Anlage. Die vereinbarten Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Beabsichtigte wesentliche Änderungen (z.B. wesentliche Änderung von Verschlüsselungsverfahren oder Anmeldeprozeduren) sind zu dokumentieren und dem AUFTRAGGEBER mitzuteilen sowie einvernehmlich in einer geänderten Fassung der „Vereinbarung zu den technischen und organisatorischen Maßnahmen“ festzuhalten, wobei der AUFTRAGGEBER Änderungen nicht ohne erheblichen Grund widerspricht.

(5) Der AUFTRAGNEHMER bestätigt und stellt sicher, dass die für die Durchführung des Auftrags eingesetzten Personen abgeleitet aus Art. 28 Abs. 3 lit. b) DSGVO (**Datengeheimnis**) schriftlich verpflichtet und in die Schutzbestimmungen der DSGVO sowie weiterer maßgeblicher Bestimmungen zum Datenschutz (z.B. § 88 TKG sowie §§ 203, 206 StGB) eingewiesen worden sind. Auf Verlangen des AUFTRAGGEBERS wird der AUFTRAGNEHMER die Verpflichtung und Einweisung nachweisen.

(6) Der AUFTRAGNEHMER darf **Zugriffsberechtigungen** nur an Personen vergeben, die mit der Durchführung des Auftrags befasst sind. Die Berechtigungen sind in dem für die Erfüllung der jeweiligen Aufgaben erforderlichen Umfang zu vergeben. Auf Verlangen wird der AUFTRAGNEHMER dem AUFTRAGGEBER die zugriffsberechtigten Personen und deren Berechtigungen benennen.

(7) Die Verarbeitung von Daten in Privatwohnungen ist nur mit Einwilligung des AUFTRAGGEBERS im Einzelfall gestattet. Soweit die Daten in einer Privatwohnung verarbeitet werden, ist der Zugang zur Wohnung durch den AUFTRAGGEBER vorher mit dem AUFTRAGNEHMER abzustimmen. Der AUFTRAGNEHMER sichert zu, dass alle Bewohner dieser Privatwohnung mit dieser Regelung einverstanden sind.

(8) Der AUFTRAGNEHMER hat den AUFTRAGGEBER unverzüglich darauf aufmerksam zu machen, wenn eine vom AUFTRAGGEBER erteilte Weisung seiner Meinung nach gegen die DSGVO oder eine andere Vorschrift über den Datenschutz verstößt, Art. 28 Abs. 3 lit. f) DSGVO.

(9) Der AUFTRAGNEHMER gewährleistet die ordnungsgemäße Durchführung der mit dem AUFTRAGGEBER in der Anlage „**Vereinbarung zu den technischen und organisatorischen Maßnahmen“** vereinbarten, nach Art. 32 DSGVO zu treffenden technischen und organisatorischen Maßnahmen. Die Einhaltung der technischen und organisatorischen Maßnahmen wird der AUFTRAGNEHMER regelmäßig durch geeignete Nachweise z.B. von der Revision, seinem betrieblichen Datenschutzbeauftragten oder einer anerkannten Wirtschaftsprüfungsgesellschaft belegen. Die Aktualität der Nachweise darf im Regelfall 3 Jahre nicht überschreiten. Die Nachweise sind dem AUFTRAGGEBER unaufgefordert vorzulegen. Unabhängig davon räumt der AUFTRAGNEHMER dem AUFTRAGGEBER und dessen Bevollmächtigten bezüglich der getroffenen Datenschutz- und Datensicherungsvorkehrungen ein Besichtigungs-, Einsichtnahme-, Auskunfts- und

Kontrollrecht, grundsätzlich nach vorheriger Abstimmung mit dem AUFTRAGNEHMER und während dessen gewöhnlichen Geschäftszeiten, ein. Der AUFTRAGNEHMER ist verpflichtet, im Falle von Auskünften und Einsichtnahmen die erforderliche Unterstützung bereitzustellen. Im Übrigen wird der AUFTRAGNEHMER sämtlichen Personen, die Prüfungen oder sonstige Maßnahmen gemäß DSGVO vornehmen, den Zugang zu allen seinen Räumlichkeiten gestatten, sofern dies nach datenschutzrechtlichen Bestimmungen erforderlich ist, und seinen weiteren Pflichten gemäß Art. 58 DSGVO nachkommen.

(10) Der AUFTRAGNEHMER hat auf Weisung des AUFTRAGGEBERS die Daten zu berichtigen, zu löschen oder zu sperren, Art. 28 Abs. 3 lit. a) DSGVO. Näheres bestimmt sich nach den Regelungen des Hauptvertrages.

(11) Der AUFTRAGNEHMER ist nicht befugt, ohne schriftliche Einwilligung des AUFTRAGGEBERS Hard- oder Software an die Systeme des AUFTRAGGEBERS anzuschließen oder darauf zu installieren.

(12) Dem AUFTRAGNEHMER ist es nicht gestattet, personenbezogene Daten in Systeme Dritter einzuspielen. Dies gilt auch für Testzwecke.

(13) Während der Entwicklung von Software werden grundsätzlich keine personenbezogenen Daten, sondern lediglich anonymisierte Original- oder fiktive Testdaten verwendet.

(14) Der AUFTRAGNEHMER wird personenbezogene Daten nach Abschluss der Arbeiten - nach den Vorgaben des AUFTRAGGEBERS - vollständig datenschutzgerecht löschen (einschließlich der verfahrens- oder sicherheitstechnisch notwendigen Kopien) oder an den AUFTRAGGEBER zurückgeben. Das gleiche gilt auch für Test- und Ausschussmaterial, das bis zur Löschung oder Rückgabe unter datenschutzgerechtem Verschluss zu halten ist. Gesetzliche Aufbewahrungspflichten insbesondere nach AO und HGB bleiben hiervon unberührt. Vertragsbezogene Daten (z.B. Ansprechpartner des AUFTRAGGEBERS), die zur Sicherung von Beweisinteressen des AUFTRAGNEHMERS erforderlich sind, dürfen in gesperrter Form bis zum Ablauf der regelmäßigen Verjährungsfrist aufbewahrt werden. Die Löschung ist auf Anforderung schriftlich zu bestätigen.

(15) Der AUFTRAGNEHMER ist verpflichtet, den AUFTRAGGEBER unaufgefordert und unverzüglich zu informieren, wenn personenbezogene Daten unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind („Datenschutzverletzung“) und Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen bestehen oder drohen (**Selbstanzeigepflicht**). Der AUFTRAGNEHMER nimmt zur Kenntnis, dass eine nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erfolgte Mitteilung mit einem Bußgeld von grundsätzlich bis zu 20 000 000 EUR oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs sanktioniert werden kann, Art. 83 DSGVO. Der AUFTRAGNEHMER hat dem AUFTRAGGEBER die aus einer Datenschutzverletzung entstehenden Schäden, insbesondere die Kosten für die Benachrichtigung der Betroffenen oder ein etwaiges Bußgeld bei Verletzung der Selbstanzeigepflicht gemäß Art. 33 DSGVO zu ersetzen, sofern dem ein schuldhaftes Verhalten des AUFTRAGNEHMERS zugrunde liegt.

(16) Der AUFTRAGNEHMER hat den AUFTRAGGEBER bei Unregelmäßigkeiten des Datenverarbeitungsablaufes, bei begründetem Verdacht der Verletzung von Vorschriften und vertraglichen Vereinbarungen zum Schutz personenbezogener Daten, sowie bei Beanstandungen durch die Datenschutzaufsichtsbehörde, die interne Revision oder in sonstigen Datenschutzprüfungsberichten, sofern ihm dies nicht aufgrund einer behördlichen Vorgabe im Rahmen eines Ermittlungsverfahrens untersagt ist, zu informieren und die Abhilfemaßnahmen aufzuzeigen.

(17) Der AUFTRAGNEHMER ist für die Durchführung des Auftrages verpflichtet, nach Maßgabe des Art. 37 Abs. 1 Satz 1DSGVO einen Beauftragten für den Datenschutz schriftlich zu bestellen, der die Aufgaben nach Art. 39 DSGVO erfüllt. Der AUFTRAGNEHMER wird dem AUFTRAGGEBER den Namen des Beauftragten für den Datenschutz benennen. Bei einem Wechsel des Beauftragten für den Datenschutz wird der AUFTRAGNEHMER den AUFTRAGGEBER unverzüglich hiervon in Kenntnis setzen.

(18) Dem AUFTRAGNEHMER ist bekannt, dass ein Verstoß gegen datenschutzrechtliche Vorschriften eine Ordnungswidrigkeit nach Art. 83 DSGVO darstellen kann.

VI. Berichtigung, Einschränkung und Löschung von Daten

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

(2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

VII. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Artt. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) ☒ Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Artt. 38 und 39 DS-GVO ausübt.

☐ Dessen Kontaktdaten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt. Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt.

☐ Als Datenschutzbeauftragte(r) ist beim Auftragnehmer Herr/Frau [Eintragen: Vorname, Name, Organisationseinheit, Telefon, E-Mail] bestellt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

☒ Dessen jeweils aktuelle Kontaktdaten sind auf der Homepage des Auftragnehmers leicht zugänglich hinterlegt.

b) ☐ Der Auftragnehmer ist nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet. Als Ansprechpartner beim Auftragnehmer wird Herr/Frau [Eintragen: Vorname, Name, Organisationseinheit, Telefon, E-Mail] benannt.

c) ☐ Da der Auftragnehmer seinen Sitz außerhalb der Union hat, benennt er folgenden Vertreter nach Art. 27 Abs. 1 DS-GVO in der Union: [Eintragen: Vorname, Name, Organisationseinheit, Telefon, E-Mail].

d) Die Wahrung der Vertraulichkeit gemäß Artt. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

e) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Artt. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO [Einzelheiten in Anlage 1].

f) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

g) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

h) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

i) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

VIII. Subunternehmer

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transport-dienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Einsatz eines Subunternehmers durch den AUFTRAGNEHMER bedarf – soweit zwischen den Parteien nichts Abweichendes vereinbart ist - der schriftlichen Einwilligung des AUFTRAGGEBERS.

a) ☐ Eine Unterbeauftragung ist unzulässig.

b) ☐ Der Auftraggeber stimmt der Beauftragung der nachfolgenden Unterauftragnehmer zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO:

_____

Name, Anschrift, Auftragsinhalt

_____

Name, Anschrift, Auftragsinhalt

_____

Name, Anschrift, Auftragsinhalt

c) ☒ Die Auslagerung auf Unterauftragnehmer oder

☐ der Wechsel des bestehenden Unterauftragnehmers ist zulässig, soweit:

- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und
- der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
- eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde gelegt wird.

(2) Die vertraglichen Vereinbarungen zwischen dem AUFTRAGNEHMER und dem Subunternehmer sind so zu gestalten, dass sie den Regelungen der vorliegenden Vereinbarung entsprechen. Zu diesem Zweck müssen insbesondere die mit dem Subunternehmer zu vereinbarenden technischen und organisatorischen Maßnahmen ein gleichwertiges Schutzniveau aufweisen.

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

(4) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

(5) Eine weitere Auslagerung durch den Unterauftragnehmer

☐ ist nicht gestattet;
☒ bedarf der ausdrücklichen Zustimmung des Hauptauftraggebers (mind. Textform);
☒ bedarf der ausdrücklichen Zustimmung des Hauptauftragnehmers (mind. Textform);

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

(6) Auf Anforderung des AUFTRAGGEBERS wird der AUFTRAGNEHMER Auskunft über den wesentlichen Vertragsinhalt mit dem Subunternehmer und die Umsetzung der datenschutzrelevanten Verpflichtungen geben, erforderlichenfalls durch Einsicht in die relevanten Vertragsunterlagen.

(7) Der AUFTRAGNEHMER bleibt für die Erfüllung der auf den Subunternehmer übertragenen Tätigkeiten im gleichen Umfang verantwortlich, als würden diese durch den AUFTRAGNEHMER selbst ausgeführt.

IX. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch

- ☒ die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;
- ☐ die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO;
- ☐ aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheits-abteilung, Datenschutzauditoren, Qualitätsauditoren);
- ☐ eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

(4) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

X. Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen
b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden
c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen
d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung
e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

(2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

XI. Weisungsbefugnis des Auftraggebers

(1) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

(2) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

XII. Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

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