Vereinbarung über Auftragsverarbeitung

Vertrag über die Verarbeitung personenbezogener Daten im Auftrag eines Verantwortlichen gemäß Art. 28 DSGVO

zwischen

...

als Verantwortlichem - nachfolgend "Auftraggeber" genannt –

und

der CS Job-Union GmbH, Säntisstraße 139, 12277 Berlin

als Auftragsverarbeiter - nachfolgend "Auftragnehmer" genannt –

- nachfolgend jeder auch "Partei" und gemeinsam "Parteien" genannt -

Präambel

Der Auftragnehmer erbringt für den Auftraggeber Leistungen, die im Vertrag vom [...] näher spezifiziert sind (im Folgenden: "Hauptvertrag"). Teil der Durchführung des Hauptvertrags ist die Verarbeitung von personenbezogenen Daten im Sinne der Datenschutzgrundverordnung ("DSGVO"). Zur Erfüllung der Anforderungen der DSGVO an derartige Konstellationen schließen die Parteien den nachfolgenden Vertrag, dessen Erfüllung nicht gesondert vergütet wird, sofern dies nicht ausdrücklich vereinbart ist.

§ 1 Gegenstand/Umfang der Beauftragung

(1) Die Zusammenarbeit der Parteien nach Maßgabe des Hauptvertrages bringt es mit sich, dass der Auftragnehmer Zugriff auf personenbezogene Daten des Auftraggebers (nachfolgend "Auftraggeberdaten") erhält, erhebt oder anderweitig verarbeitet. Diese Verarbeitung erfolgt ausschließlich im Auftrag und nach Weisung des Auftraggebers im Sinne von Art. 4 Nr. 8 und Art. 28 DSGVO.

(2) Die Verarbeitung der Auftraggeberdaten durch den Auftragnehmer erfolgt ausschließlich im Rahmen der Erfüllung des Hauptvertrages. Art, Umfang und Zweck sind im Hauptvertrag und in Anlage 1 geregelt. Der Kreis der von der Datenverarbeitung betroffenen Personen ist in Anlage 1 zu diesem Vertrag dargestellt. Die Dauer der Verarbeitung entspricht der Laufzeit des Hauptvertrages.

(3) Dem Auftragnehmer ist eine abweichende oder über die Festlegungen im Hauptvertrag und in Anlage 1 hinausgehende Verarbeitung von Auftraggeberdaten untersagt.

(4) Die Verarbeitung der Auftraggeberdaten findet ausschließlich im Gebiet der Bundesrepublik Deutschland, 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 Art. 44 bis 49 DSGVO erfüllt sind.

(5) Die Bestimmungen dieses Vertrages finden Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei denen der Auftragnehmer und seine Beschäftigten oder durch den Auftragnehmer Beauftragte mit personenbezogenen Daten in Berührung kommen, die vom Auftraggeber stammen oder für den Auftraggeber erhoben wurden.

(6) Soweit dieser Vertrag eine Vergütung für den Auftragnehmer vorsieht, berechnet sich diese unbeschadet abweichender Vereinbarungen der Parteien nach dem tatsächlich entstandenen Aufwand (Kosten und Zeitaufwand nach Maßgabe der jeweiligen Preisliste des Auftragnehmers, in Ermangelung einer solchen unter Zugrundelegung eines angemessenen Stundensatzes) zuzüglich etwaiger Umsatzsteuer.

§ 2 Weisungsbefugnisse des Auftraggebers

(1) Der Auftragnehmer verarbeitet die Auftraggeberdaten nur im Rahmen der Beauftragung und ausschließlich im Auftrag und nach Weisung des Auftraggebers im Sinne von Art. 28 DSGVO (Auftragsverarbeitung), dies gilt insbesondere in Bezug auf die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation. Der Auftraggeber hat insoweit das alleinige Recht, Weisungen über Art, Umfang, und Methode der Verarbeitungstätigkeiten zu erteilen (nachfolgend auch "Weisungsrecht"). Wird der Auftragnehmer durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem er unterliegt, zu weiteren Verarbeitungen verpflichtet, teilt er dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit.

(2) Weisungen werden vom Auftraggeber grundsätzlich mindestens in Textform erteilt; mündlich erteilte Weisungen sind vom Auftraggeber in Textform zu bestätigen. Die weisungs- und empfangsberechtigten Personen ergeben sich aus Anlage 2. Bei einem Wechsel oder einer längerfristigen Verhinderung der in Anlage 2 benannten Personen ist der anderen Partei unverzüglich der Nachfolger bzw. Vertreter in Textform zu benennen. Der Auftragnehmer wird dem Auftraggeber einen Wechsel der Person des Weisungsberechtigten frühzeitig anzeigen. Bis zum Zugang einer solchen Mitteilung beim Auftraggeber gelten die gesetzlichen Vertreter des Auftraggebers als empfangsberechtigt.

(3) Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen datenschutzrechtliche Bestimmungen verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird.

§ 3 Schutzmaßnahmen des Auftragnehmers

(1) Der Auftragnehmer ist verpflichtet, die gesetzlichen Bestimmungen über den Datenschutz zu beachten und die aus dem Bereich des Auftraggebers erlangten Informationen nicht an Dritte weiterzugeben oder deren Zugriff auszusetzen. Unterlagen und Daten sind gegen die Kenntnisnahme durch Unbefugte unter Berücksichtigung des Stands der Technik zu sichern. Die Einhaltung der in diesem Vertrag niedergelegten Pflichten wird er mit geeigneten Mitteln nachweisen.

(2) Ferner wird der Auftragnehmer alle Personen, die von ihm mit der Bearbeitung und der Erfüllung dieses Vertrages betraut werden (im folgenden "Mitarbeiter" genannt), in Schriftform zur Vertraulichkeit verpflichten (Art. 28 Abs. 3 lit. b DSGVO) und die Einhaltung dieser Verpflichtung mit der gebotenen Sorgfalt sicherstellen. Auf Verlangen des Auftraggebers wird der Auftragnehmer dem Auftraggeber die Verpflichtung der Mitarbeiter schriftlich oder in elektronischer Form nachweisen.

(3) Der Auftragnehmer wird seine innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er verpflichtet sich, alle geeigneten technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Auftraggeberdaten gem. Art. 32 DSGVO, insbesondere die in Anlage 3 zu diesem Vertrag aufgeführten Maßnahmen, zu ergreifen und diese für die Dauer der Verarbeitung der Auftraggeberdaten aufrecht zu erhalten.

(4) Eine Änderung der getroffenen technischen und organisatorischen Maßnahmen bleibt dem Auftragnehmer vorbehalten, wobei er sicherstellt, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird. Der Auftragnehmer hat den Auftraggeber unverzüglich in Textform zu informieren, wenn er Grund zu der Annahme hat, dass die Maßnahmen gemäß Anlage 3 nicht mehr ausreichend sind und wird sich mit ihm hinsichtlich weiterer technischer und organisatorischer Maßnahmen abstimmen.

(5) Auf Verlangen des Auftraggebers wird der Auftragnehmer dem Auftraggeber die Einhaltung der in Anlage 3 bestimmten technischen und organisatorischen Maßnahmen durch geeignete Nachweise nachweisen.

§ 4 Informations- und Unterstützungspflichten des Auftragnehmers

(1) Bei Störungen, Verdacht auf Datenschutzverletzungen oder Verletzungen vertraglicher Verpflichtungen des Auftragnehmers, Verdacht auf sicherheitsrelevante Vorfälle oder andere Unregelmäßigkeiten bei der Verarbeitung der Auftraggeberdaten durch den Auftragnehmer, bei ihm im Rahmen des Auftrags beschäftigten Personen oder durch Dritte wird der Auftragnehmer den Auftraggeber unverzüglich, spätestens aber innerhalb von 48 Stunden nach Kenntnis in elektronischer Form informieren. Maßgeblich zur Wahrung der Frist ist der Zugang beim Auftraggeber. Dasselbe gilt für Prüfungen des Auftragnehmers durch die Datenschutz-Aufsichtsbehörde. Die Meldungen gemäß § 4 Abs. 1 Satz 1 enthalten jeweils zumindest die in Art. 33 Absatz 3 DSGVO genannten Angaben.

(2) Der Auftragnehmer wird den Auftraggeber im Falle des § 4 Abs. 1 bei der Erfüllung seiner diesbezüglichen Aufklärungs-, Abhilfe- und Informationsmaßnahmen im Rahmen des zumutbaren unterstützen. Der Auftragnehmer wird insbesondere unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der Betroffenen durchführen, den Auftraggeber hierüber informieren und diesen um weitere Weisungen ersuchen.

(3) Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf dessen mündliche oder schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte und Nachweise zur Verfügung zu stellen, die zur Durchführung einer Kontrolle gemäß § 7 Abs. 1 dieses Vertrages erforderlich sind. Ferner wird der Auftragnehmer dem Auftraggeber auf dessen Wunsch ein umfassendes und aktuelles Datenschutz- und Sicherheitskonzept für die Auftragsverarbeitung sowie über zugriffsberechtigte Personen zur Verfügung stellen.
(4) Für Unterstützungsleistungen nach dieser Regelung steht dem Auftragnehmer eine Vergütung zu.

§ 5 Sonstige Verpflichtungen des Auftragnehmers

(1) Der Auftragnehmer ist auf Anforderung des Auftraggebers verpflichtet, ein Verzeichnis zu allen Kategorien von im Auftrag des Auftraggebers durchgeführten Tätigkeiten der Verarbeitung gem. Art. 30 Absatz 2 DSGVO zu führen. Das Verzeichnis ist dem Auftraggeber auf Verlangen zur Verfügung zu stellen.
(2) Der Auftragnehmer ist verpflichtet, den Auftraggeber bei der Erstellung einer Datenschutz-Folgenabschätzung nach Art. 35 DSGVO und einer etwaigen vorherigen Konsultation der Aufsichtsbehörde nach Art. 36 DSGVO zu unterstützen.
(3) Der Auftragnehmer bestätigt, dass er – soweit eine gesetzliche Verpflichtung hierzu besteht – einen Datenschutzbeauftragten bestellt hat. Die vollständigen Kontaktdaten des Datenschutzbeauftragten sind dem Auftraggeber mit Vertragsschluss in Textform zu übermitteln. Ein Wechsel in der Person des betrieblichen Datenschutzbeauftragten/Ansprechpartners für den Datenschutz ist dem Auftraggeber unverzüglich in Textform mitzuteilen.
(4) Sollten die Auftraggeberdaten 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, sofern ihm dies nicht durch gerichtliche oder behördliche Anordnung untersagt ist. Der Auftragnehmer wird in diesem Zusammenhang alle zuständigen Stellen unverzüglich darüber informieren, dass die Entscheidungshoheit über die Daten ausschließlich beim Auftraggeber als „Verantwortlichem“ im Sinne der DSGVO liegt.
(5) Für Leistungen nach dieser Regelung steht dem Auftragnehmer eine Vergütung zu.

§ 6 Subunternehmerverhältnisse

(1) Der Auftragnehmer ist im Rahmen seiner vertraglichen Verpflichtungen nicht zur Begründung von Unterauftragsverhältnissen mit Subunternehmern ("Subunternehmerverhältnis") befugt. Ausnahmen sind nur nach vorheriger ausdrücklicher Zustimmung des Auftraggebers im Einzelfall zulässig; diese gilt für die in Anlage 4 genannten Subunternehmen als erteilt. In jedem Fall hat der Auftragnehmer dafür Sorge zu tragen, dass die in diesem Vertrag vereinbarten Regelungen auch gegenüber den von ihm beauftragten Subunternehmen gelten, wobei dem Auftraggeber gegenüber dem Subunternehmer sämtliche Kontrollrechte gemäß § 7 dieses Vertrages einzuräumen sind. Subunternehmerverhältnisse zu Dritten

außerhalb des Europäischen Wirtschaftsraumes sind nicht gestattet. Die vorgenannten Regelungen, insbesondere auch die Genehmigungserteilung durch die Nennung in Anlage 4, gelten entsprechend für die Begründung von weiteren Unterauftragsverhältnissen durch Subunternehmer.

(2) Ein Subunternehmerverhältnis im Sinne dieser Bestimmungen liegt nicht vor, wenn der Auftragnehmer Dritte mit Dienstleistungen beauftragt, die als reine Nebenleistungen anzusehen sind. Dazu gehören zum Beispiel Post-, Transport- und Versandleistungen, Reinigungsleistungen, Bewachungsdienste, Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen. Die Pflicht des Auftragnehmers, auch in diesen Fällen die Beachtung von Datenschutz und Datensicherheit sicherzustellen, bleibt unberührt.

§ 7 Kontrollrechte

(1) Der Auftraggeber ist berechtigt, sich regelmäßig von der Einhaltung der Regelungen dieses Vertrages, insbesondere der Umsetzung und Einhaltung der technischen und organisatorischen Maßnahmen gemäß § 3 Abs. 3 dieser Vereinbarung, zu überzeugen. Hierfür kann er zum Beispiel Auskünfte des Auftragnehmers einholen, sich vorhandene Testate von Sachverständigen, Zertifizierungen oder internen Prüfungen vorlegen lassen oder die technischen und organisatorischen Maßnahmen des Auftragnehmers zu den üblichen Geschäftszeiten selbst persönlich bzw. durch einen sachkundigen Dritten prüfen lassen, sofern dieser nicht in einem Wettbewerbsverhältnis zum Auftragnehmer steht.

(2) Der Auftraggeber wird Kontrollen nur im erforderlichen Umfang durchführen und angemessene Rücksicht auf die Betriebsabläufe des Auftragnehmers nehmen. Über den Zeitpunkt sowie die Art der Prüfung verständigen sich die Parteien rechtzeitig.

(3) Der Auftraggeber dokumentiert das Kontrollergebnis und teilt es dem Auftragnehmer mit. Bei Fehlern oder Unregelmäßigkeiten, die der Auftraggeber insbesondere bei der Prüfung von Auftragsergebnissen feststellt, hat er den Auftragnehmer unverzüglich zu informieren. Werden bei der Kontrolle Sachverhalte festgestellt, deren zukünftige Vermeidung Änderungen des angeordneten Verfahrensablaufs erfordern, teilt der Auftraggeber dem Auftragnehmer die notwendigen Verfahrensänderungen unverzüglich mit.

§ 8 Rechte Betroffener

(1) Der Auftragnehmer unterstützt den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von dessen Pflichten nach Art. 12 bis 22 sowie Art. 32 bis 36 DSGVO. Er wird dem Auftraggeber unverzüglich, spätestens aber innerhalb von fünf Arbeitstagen, die gewünschte Auskunft über Auftraggeberdaten geben, sofern der Auftragnehmer nicht selbst über die entsprechenden Informationen verfügt und vom Auftragnehmer hierauf unter Nennung des Speicherorts hingewiesen wird.

(2) Macht der Betroffene seine Rechte gemäß Art. 16 bis 18 DSGVO geltend, ist der Auftragnehmer dazu verpflichtet, die Auftraggeberdaten auf Weisung des Auftraggebers unverzüglich, spätestens binnen einer Frist von drei Arbeitstagen zu berichtigen, löschen oder einzuschränken. Der Auftragnehmer wird dem Auftraggeber die Löschung, Berichtigung bzw. Einschränkung der Daten auf Verlangen nachweisen.
(3) Macht ein Betroffener Rechte, etwa auf Auskunftserteilung, Berichtigung oder Löschung hinsichtlich seiner Daten, unmittelbar gegenüber dem Auftragnehmer geltend, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten und wartet dessen Weisungen ab. Ohne entsprechende Einzelweisung wird der Auftragnehmer nicht mit der betroffenen Person in Kontakt treten.
(4) Für Unterstützungsleistungen nach dieser Regelung steht dem Auftragnehmer eine Vergütung zu.

§ 9 Laufzeit und Kündigung

(1) Die Laufzeit dieses Vertrags entspricht der Laufzeit des Hauptvertrags. Ist der Hauptvertrag ordentlich kündbar, gelten die Regelungen zur ordentlichen Kündigung entsprechend. Im Zweifel gilt eine Kündigung des Hauptvertrags auch als Kündigung dieses Vertrags und eine Kündigung dieses Vertrages als Kündigung des Hauptvertrages.
(2) Der Auftraggeber ist jederzeit zu einer außerordentlichen Kündigung dieses Vertrages aus wichtigem Grund berechtigt. Ein wichtiger Grund liegt vor, wenn der Auftragnehmer seinen Pflichten aus diesem Vertrag nicht nachkommt, Bestimmungen der DSGVO vorsätzlich oder grob fahrlässig verletzt oder eine Weisung des Auftraggebers nicht ausführen kann oder will. Bei einfachen – also weder vorsätzlichen noch grob fahrlässigen – Verstößen setzt der Auftraggeber dem Auftragnehmer zunächst eine angemessene Frist, innerhalb welcher der Auftragnehmer den Verstoß abstellen kann. Nach fruchtlosem Ablauf dieser Frist steht dem Auftraggeber sodann das Recht zur außerordentlichen Kündigung zu.

§ 10 Löschung und Rückgabe nach Vertragsende

(1) Der Auftragnehmer wird dem Auftraggeber nach Beendigung des Hauptvertrags oder jederzeit auf dessen Verlangen alle ihm überlassenen Unterlagen, Daten und Datenträger zurückgeben oder auf Wunsch des Auftraggebers, sofern nicht eine gesetzliche Aufbewahrungsfrist besteht, vollständig und unwiderruflich löschen. Dies gilt auch für Vervielfältigungen der Auftraggeberdaten beim Auftragnehmer, wie etwa Datensicherungen, nicht aber für Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Verarbeitung der Auftraggeberdaten dienen. Solche Dokumentationen sind vom Auftragsnehmer für eine Dauer von sechs Jahren aufzubewahren und auf Verlangen an den Auftragsgeber herauszugeben.

(2) Der Auftragnehmer wird dem Auftraggeber die Löschung bestätigen. Der Auftraggeber hat das Recht, die vollständige und vertragsgerechte Rückgabe bzw. Löschung der Daten beim Auftragnehmer in geeigneter Weise zu kontrollieren; § 7 Abs. 2 dieses Vertrags gilt hierfür entsprechend.

(3) Der Auftragnehmer ist verpflichtet, auch über das Ende des Hauptvertrags hinaus die ihm im Zusammenhang mit dem Hauptvertrag bekannt gewordenen Daten vertraulich zu behandeln.

(4) Für Leistungen nach dieser Regelung steht dem Auftragnehmer eine Vergütung zu.

§ 11 Haftung

(1) Die Haftung der Parteien richtet sich nach Art. 82 DSGVO. Eine Haftung des Auftragnehmers gegenüber dem Auftraggeber wegen Verletzung von Pflichten aus diesem Vertrag oder dem Hauptvertrag bleibt hiervon unberührt.

(2) Die Parteien stellen sich jeweils von der Haftung frei, wenn eine Partei nachweist, dass sie in keinerlei Hinsicht für den Umstand, durch den der Schaden bei einem Betroffenen eingetreten ist, verantwortlich ist. § 11 Abs. 2 Satz 1 gilt im Falle einer gegen eine Partei verhängte Geldbuße entsprechend, wobei die Freistellung in dem Umfang erfolgt, in dem die jeweils andere Partei Anteil an der Verantwortung für den durch die Geldbuße sanktionierten Verstoß trägt.

§ 12 Schlussbestimmungen

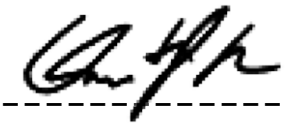
(1) Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer im Sinne des § 273 BGB hinsichtlich der zu verarbeitenden Daten und der zugehörigen Datenträger ausgeschlossen ist.

(2) Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Textform. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(3) Die Regelungen dieses Vertrags gehen im Zweifel den Regelungen des Hauptvertrags vor. Sollten sich einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise als unwirksam oder undurchführbar erweisen oder infolge Änderungen einer Gesetzgebung nach Vertragsabschluss unwirksam oder undurchführbar werden, wird dadurch die Wirksamkeit der übrigen Bestimmungen nicht berührt. An die Stelle der unwirksamen oder undurchführbaren Bestimmung soll die wirksame und durchführbare Bestimmung treten, die dem Sinn und Zweck der nichtigen Bestimmung möglichst nahekommt.

(4) Diese Vereinbarung unterliegt deutschem Recht. Der Gerichtsstand richtet sich nach den Regeln des Hauptvertrages. In Ermangelung einer solchen Bestimmung ist Gerichtsstand das Landgericht Berlin.

Berlin, den 24.01.2023 _____ Berlin, den _____



_____ _____

Christoph Sonka

Anlagen

Anlage 1 – Beschreibung der Datenarten und der Kategorien betroffener Personen

Zweck der Verarbeitung	- Bereitstellung von Software / einer Datenbank / Speicherplatz über ein Computernetzwerk (SaaS)
Art der Verarbeitung	- Ablaufenlassen der Software - Speichern von Daten in der Cloud - Zugriff auf bzw. Übermitteln von Daten über das Internet - Zwischenspeicherungen beim Zugriff über das Internet im technisch notwendigen Umfang durch Telekommunikationsanbieter - Anzeigenlassen von Daten bzw. Herunterladen auf Endgeräten des Geschäftspartners des Auftraggebers
Kategorien der betroffenen Personen und Art der Daten	- Kundendaten des Auftraggebers o Kundennummer o Firma o Position o Vorname o Nachname o Adresse o Geschlecht o Geburtstag o Foto o Anrede o Titel o Sprache o Telefon o E-Mail-Adresse - Daten von Bewerbern des Auftraggebers o Vorname (auch ein Pseudonym kann verwendet werden) o Nachname (auch ein Pseudonym kann verwendet werden) o Telefonnummer o E-Mail o Land

Anlage 2 – Weisungs- und empfangsberechtige Personen, Datenschutzbeauftragter beim Auftragnehmer

Ansprechpartner für datenschutzrechtliche Belange, insbesondere berechtigt und zuständig für die Erteilung (auf Seiten des Auftraggebers) bzw. den Empfang (auf Seiten des Auftragnehmers) sind:

Auftraggeber:

Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Vertragspartner unverzüglich und grundsätzlich in Textform die Nachfolger bzw. die Vertreter mitzuteilen.

Der Auftragnehmer hat als Datenschutzbeauftragte die

Datargus Rechtsanwaltsgesellschaft mbH,
Brachvogelstraße 1, 10961 Berlin

bestellt, Ansprechpartner dort ist:

Rechtsanwalt Erik Stamer
Rechtsanwalt | Fachanwalt für IT-Recht | Fachanwalt für Gewerblichen Rechtsschutz
Zertifizierter Datenschutzbeauftragter (TÜV)

Alle Anfragen aus dem Bereich Datenschutz an den Auftragnehmer sind bitte an die Datenschutzbeauftrage zu richten.

Anlage 3 – Technische und organisatorische Maßnahmen des Auftragnehmers (Art. 32 DSGVO)

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

1. Zutrittskontrolle

Maßnahmen, um Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

a. Maßnahmen am Firmensitz

- Arbeitsbereiche und für Besucher zugängliche Bereiche sind voneinander abgegrenzt
- Zutritt für Besucher nur mit Vertraulichkeitsverpflichtung
- Sorgfalt bei Auswahl externer Dienstleister, die Zutritt zum Gebäude erhalten (Wachpersonal, Reinigungsdienste, Handwerker, etc.)
- Videoüberwachung
- Manuelles Schließsystem
- Sicherheitsschlösser
- Besucher für die gesamte Dauer ihres Besuchs in Begleitung durch Mitarbeiter
- Alle externen Dienstleister müssen vor erstmaligem Zutritt zum Gebäude eine Vertraulichkeitsverpflichtung unterzeichnen

b. Maßnahmen bzgl. Serverräumen

- Es existieren keine eigenen Serverräume.

2. Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

- Schriftliche Regelungen zur Erteilung von Benutzeraccounts vorhanden
- Protokollierung von Vergabe und Entzug von Benutzeraccounts
- Erteilung von Benutzeraccounts nur durch Administratoren
- Nur personalisierte Benutzeraccounts
- Richtlinie für Passwortsicherheit vorhanden (Mindestvorgabe für Passwortlänge und - komplexität)
- Anti-Viren-Software für Server
- Anti-Viren-Software für mobile Geräte

- Jede genutzte Anti-Viren-Software und Firewall wird regelmäßig aktualisiert
- Verschlüsselung von Smartphones
- Login mit Benutzername + Passwort
- Einhaltung der Richtlinie für Passwortsicherheit wird technisch erzwungen
- Zugangssperre bei erfolglosen Anmeldeversuchen
- Automatische Bildschirmsperre
- Anti-Viren-Software für Clients
- Firewall
- Mobile Device Policy
- Einsatz VPN bei Remote-Zugriffen

3. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden *Daten zugreifen können.*

- Benutzerberechtigungskonzept vorhanden
- Minimale Anzahl an Administratoren
- Protokollierung von Vergabe und Entzug von Berechtigungen
- Erteilung von Berechtigungen nur durch Administratoren
- Erteilung von Zugriffsrechten nach dem need-to-know-Prinzip
- Erteilung von differenzierten Berechtigungen (z.B. read-only, read-and-write, …)
- Erstellen von Benutzerprofilen
- Regelmäßige Überprüfung der erteilten Berechtigungen
- Protokollierung von versuchten und erfolgten Zugriffen auf Anwendungen und/oder Daten
- sichere Löschung/Vernichtung von nicht mehr verwendeten Datenträgern
- Datenträger-Management (Regelung der Ausgabe; Verbot der Nutzung eigener Datenträger)

4. Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

- Trennung von Produktiv- und Testumgebung
- Trennung der Daten verschiedener Verantwortlicher
- Logische Trennung

- Trennung über Berechtigungskonzept

5. Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)

Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen *Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen.*

- Personenbezogene Daten werden schnellstmöglich anonymisiert

B. Integrität (Art. 32 Abs. lit. b DSGVO)

1. Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

- Bereitstellung von personenbezogenen Daten nur über verschlüsselte Verbindungen
- Kein Versand von Datenträgern (Papier oder elektronisch) über Post, Boten etc.
- Fernwartung von Systemen, in denen personenbezogene Daten des Verantwortlichen gespeichert werden
- Clean-Desk-Policy
- Richtlinie zur Löschung und Vernichtung von Datenträgern
- Dokumentation der Löschung/Vernichtung von Datenträgern

2. Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

- Technische Protokollierung der Eingabe, Änderung und Löschung von Daten
- Übersicht, mit welchen Programmen welche Daten eingegeben, geändert oder gelöscht werden können
- Manuelle oder automatisierte Kontrolle der Protokolle
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

- Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen wurden
- Klare Zuständigkeiten für Löschungen

C. Verfügbarkeit und Belastbarkeit der Systeme und Dienste (Art. 32 Abs. lit. b, c DSGVO)

1. Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

a. Allgemeine Maßnahmen

- Nutzung eines Spamfilters
- Schriftliches Back-up- und Recovery-Konzept
- Angemessen häufige Sicherung der Daten
- Aufbewahrung der Sicherungsmedien an einem sicheren Ort
- Unterbrechungsfreie Stromversorgung

b. Maßnahmen bzgl. Serverräumen

Es existieren keine eigenen Serverräume.

2. Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO)

Maßnahmen, die gewährleisten, dass bei zufälliger Zerstörung oder zufälligem Verlust von Daten diese rasch wiederhergestellt werden können.

- Regelmäßige Tests zur Datenwiederherstellung

D. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der TOMs zur Gewährleistung der Sicherheit der Verarbeitung (Art. 32 Abs. lit d DSGVO)

1. Datenschutzmanagement (Art. 25 Abs. 1 DSGVO)

Maßnahmen, die sicherstellen, dass stets alle datenschutzrechtlichen Anforderungen eingehalten werden.

- Ein Datenschutzbeauftragter ist bestellt
- Schriftliches Datenschutz- und Datensicherheitskonzept vorhanden
- Software-Lösungen für Datenschutzmanagement im Einsatz

- Mindestens jährliche Überprüfung der Wirksamkeit der Schutzmaßnahmen; im Bedarfsfall erfolgt Anpassung der Schutzmaßnahmen
- Regelmäßige Überprüfung und Aktualisierung des Verarbeitungsverzeichnisses
- Vorhandensein eines Verarbeitungsverzeichnisses nach Art. 30 Abs. 2 DSGVO
- Alle Mitarbeiter auf Vertraulichkeit/Datengeheimnis verpflichtet oder unterliegen gesetzlicher Schweigepflicht
- Regelmäßige Schulung aller Mitarbeiter (Datenschutz sowie Datensicherheit)

2. Incident-Response-Management

Maßnahmen zur Sicherstellung der schnellen und angemessenen Reaktion auf Sicherheitsverletzungen.

- Prozess zur Erkennung und Meldung von Sicherheitsvorfällen und potentiellen Datenschutzverstößen
- Regelmäßige Kontrolle der ausselektierten Dateien / der protokollierten Angriffsversuche bei automatisierten Schutzinstallationen
- Dokumentation aller Sicherheitsvorfälle und Datenschutzverstöße
- Regelung der Verantwortlichkeit der Meldung von Sicherheitsvorfällen und Datenschutzverstößen an den Verantwortlichen

3. Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

Maßnahmen, die gewährleisten, dass die Prinzipien Privacy by design und Privacy by default eingehalten werden.

- Es werden nicht mehr personenbezogene Daten erhoben als für den jeweiligen Zweck erforderlich
- Einfache Ausübung von Betroffenenrechten möglich
- Automatische Anonymisierung von Daten nach Zweckfortfall sichergestellt

4. Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers *verarbeitet werden können.*

- Sorgfältige Auswahl von Subdienstleistern in Bezug auf Datenschutz und Datensicherheit
- Dokumentation des Auswahlprozesses
- Weisungsbefugnisse sind klar festgelegt
- Auftragsverarbeitungsverträge entsprechen den Anforderungen des Art. 28 DSGVO

- Laufende, regelmäßige Überprüfung des Subdienstleisters und seines Schutzniveaus
- Der Subdienstleister darf seinerseits weitere Dienstleister einsetzen
- Sämtliche Anforderungen aus dem Auftragsverarbeitungsvertrag mit dem Verantwortlichen werden auch vertraglich mit dem Subdienstleister vereinbart

Anlage 4 – zugelassene Subunternehmer

Name und Anschrift des Subunternehmers	Beschreibung der Teilleistung
SiDEx GmbH, Greifenhagener Straße 33, 10437 Berlin	Serverhosting und Pflege der Software
Im Unterauftrag für die SiDEx GmbH: DNS:NET Internet Service GmbH, Zimmerstraße 23, 10969 Berlin	Serverhosting