Vertrag zur Auftragsdatenverarbeitung

zwischen

_____

(Kunde, bitte eintragen)

_____

(Straße, Hausnummmer)

_____

(Postleitzahl, Ort, Land)

- als Verantwortlicher (nachfolgend: Auftraggeber) -

und

Talent Engine GmbH
Rathausstraße 2
20095 Hamburg

- als Auftragsdatenverarbeiter (nachfolgend: Auftragnehmer) -

Präambel

Der Auftraggeber möchte den Auftragnehmer mit den in § 3 genannten Leistungen beauftragen. Teil der Vertragsdurchführung ist die Verarbeitung von personenbezogenen Daten. Insbesondere Art. 28 DS-GVO stellt bestimmte Anforderungen an eine solche Auftragsverarbeitung. Zur Wahrung dieser Anforderungen schließen die Parteien die nachfolgende Vereinbarung, deren Erfüllung nicht gesondert vergütet wird, sofern dies nicht ausdrücklich vereinbart ist.

§ 1 Begriffsbestimmungen

(1) Verantwortlicher ist gem. Art. 4 Ziff. 7 DS-GVO die Stelle, die allein oder gemeinsam mit anderen Verantwortlichen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

(2) Auftragsverarbeiter ist gem. Art. 4 Ziff. 8 DS-GVO eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

(3) Personenbezogene Daten sind gem. Art. 4 Ziff 1 DS-GVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person („betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

(4) Besonders schutzbedürftige personenbezogene Daten sind personenbezogenen Daten gem. Art. 9 DS-GVO, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit von Betroffenen hervorgehen, personenbezogene Daten gem. Art. 10 DS-GVO über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln sowie genetische Daten gem. Art. 4 Ziff. 13 DS-GVO, biometrischen Daten gem. Art. 4 Ziff. 14 DS-GVO, Gesundheitsdaten gem. Art. 4 Ziff. 15 DS-GVO sowie Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

(5) Verarbeitung ist gem. Art. 4 Ziff. 2 DS-GVO jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

(6) Aufsichtsbehörde ist gem. Art. 4 Ziff. 21 DS-GVO eine von einem Mitgliedstaat gem. Art. 51 DS-GVO eingerichtete unabhängige staatliche Stelle.

§ 2 Zusammenarbeit mit der Datenschutz-Aufsichtsbehörde

Der Auftraggeber und der Auftragnehmer und gegebenenfalls deren Vertreter arbeiten auf Anfrage einer Behörde mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

§ 3 Vertragsgegenstand

(1) Der Auftragnehmer erbringt für den Auftraggeber Leistungen im Bereich der Datenverarbeitung gemäß Angebot („Hauptvertrag“). Dabei erhält der Auftragnehmer Zugriff auf personenbezogene Daten und verarbeitet diese ausschließlich im Auftrag und nach Weisung des Auftraggebers. Umfang und Zweck der Datenverarbeitung durch den Auftragnehmer ergeben sich aus dieser Vereinbarung.

(2) Zur Konkretisierung der beiderseitigen datenschutzrechtlichen Rechte und Pflichten schließen die Parteien die vorliegende Vereinbarung. Die Regelungen der vorliegenden Vereinbarung gehen im Zweifel den Regelungen des Hauptvertrags vor.

(3) Die Bestimmungen dieses Vertrages finden Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei der 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.

(4) Die Laufzeit dieses Vertrags richtet sich nach der Laufzeit des Hauptvertrages, sofern sich aus den nachfolgenden Bestimmungen nicht darüber hinausgehende Verpflichtungen oder Kündigungsrechte ergeben.

§ 4 Weisungsrecht

(1) Der Auftragnehmer darf Daten nur im Rahmen des Hauptvertrags und gemäß den Weisungen des Auftraggebers erheben und verarbeiten; dies gilt insbesondere in Bezug auf die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation. 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) Die Weisungen des Auftraggebers werden anfänglich durch diesen Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in Textform durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Der Auftraggeber ist jederzeit zur Erteilung entsprechender Weisungen berechtigt. Dies

umfasst auch Weisungen in Hinblick auf die Berichtigung, Löschung und Sperrung von Daten.

(3) Alle erteilten Weisungen sind sowohl vom Auftraggeber als auch vom Auftragnehmer zu dokumentieren. Weisungen, die über die hauptvertraglich vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt.

(4) 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. Der Auftragnehmer darf die Durchführung einer offensichtlich rechtswidrigen Weisung ablehnen.

§ 5 Art der Verarbeitung, Art der personenbezogenen Daten, Kreis der Betroffenen

(1) Der Auftraggeber ermöglicht der betroffenen Person ggfls., sich über seine Webseiten oder Apps oder vom Auftragnehmer zur Verfügung gestellten Webseiten oder Apps für den JMT-App-Service zu registrieren und seine Daten zu verwalten. Die Verarbeitung selbst erfolgt über den Auftragnehmer.

(2) Im Rahmen der Durchführung des Hauptvertrags und des Absatzes 1 kann der Auftragnehmer Zugriff auf folgende personenbezogenen Daten der betroffenen Person erhalten:

Stammdaten (z.B. Name, Geburtsdatum, Adresse, Telefonnummer, Größe, Gewicht), Teilnahme an Events (z.B. Feriencamps), Einwilligungen (z.B. Newsletter Opt-ins), Custom Attribute (z.B. Mitgliedsnummer), Nutzer-Events (z.B. Login), Talentbewertung im Rahmen der Talent ID.

Vorgenannte personenbezogene Daten werden zur Durchführung der Kommunikation mit den Nutzern des Auftraggebers zweckgerichtet verarbeitet, insbesondere erhoben, organisiert und gespeichert.

(3) Folgende Kategorien von Betroffenen werden von der Datenverarbeitung erfasst: Nutzer, Daten der Teilnehmer und deren Erziehungsberechtigten

§ 6 Schutzmaßnahmen des Auftragnehmers

(1) Der Auftragnehmer ist verpflichtet, die gesetzlichen Bestimmungen über den Datenschutz zu beachten. Unterlagen und Daten sind gegen die Kenntnisnahme durch Unbefugte unter Berücksichtigung des Stands der Technik zu sichern.

Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er trifft alle erforderlichen technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers gem. Art. 32 DS-GVO, insbesondere mindestens die in Anlage 1 aufgeführten Maßnahmen der a) Zutrittskontrolle, b) Zugangskontrolle, c) Zugriffskontrolle, d) Trennungskontrolle, e) Weitergabekontrolle, f) Eingabekontrolle, g) Verfügbarkeitskontrolle und h) Auftragskontrolle.

Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei er sicherstellt, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

(2) Der Auftragnehmer hat einen Datenschutzbeauftragten bestellt. Veröffentlichung und Mitteilung weist der Auftragnehmer auf Anforderung des Auftraggebers in geeigneter Weise nach.

(3) Den bei der Datenverarbeitung durch den Auftragnehmer beschäftigten Personen ist es untersagt, personenbezogene Daten unbefugt zu erheben oder zu verarbeiten. Der Auftragnehmer wird alle Personen, die von ihm mit der Bearbeitung und der Erfüllung dieses Vertrages betraut werden (“Mitarbeiter”), entsprechend verpflichten (Verpflichtung zur Vertraulichkeit, Art. 28 Abs. 3 lit. b DS-GVO) und mit der gebotenen Sorgfalt die Einhaltung dieser Verpflichtung sicherstellen. Diese Verpflichtungen müssen so gefasst sein, dass sie auch nach Beendigung dieses Vertrages oder des Beschäftigungsverhältnisses zwischen dem Mitarbeiter und dem Auftragnehmer bestehen bleiben. Dem Auftraggeber sind die Verpflichtungen auf Verlangen in geeigneter Weise nachzuweisen.

§ 7 Informationspflichten 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 personenbezogenen Daten durch den Auftragnehmer, bei ihm im Rahmen des Auftrags beschäftigten Personen oder durch Dritte wird der Auftragnehmer den Auftraggeber unverzüglich in Schriftform oder Textform informieren. Dasselbe gilt für

Prüfungen des Auftragnehmers durch die Datenschutz-Aufsichtsbehörde. Die Meldung über eine Verletzung des Schutzes personenbezogener Daten enthält zumindest folgende Informationen:

a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der Zahl der betroffenen Personen, der betroffenen Kategorien und der Zahl der betroffenen personenbezogenen Datensätze;

b) eine Beschreibung der von dem Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

(2) Der Auftragnehmer trifft unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der Betroffenen, informiert hierüber den Auftraggeber und ersucht um weitere Weisungen.

(3) Der Auftragnehmer ist darüber hinaus verpflichtet, dem Auftraggeber jederzeit Auskünfte zu erteilen, soweit dessen Daten von einer Verletzung nach Absatz 1 betroffen sind.

(4) 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, 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 DS-GVO liegen.

(5) Über wesentliche Änderung der Sicherheitsmaßnahmen nach § 6 Abs. 2 hat der Auftragnehmer den Auftraggeber unverzüglich zu unterrichten.

(6) Ein Wechsel in der Person des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

§ 8 Kontrollrechte des Auftraggebers

(1) Der Auftraggeber darf kontrollieren, ob der Auftragnehmer seine technischen und organisatorischen Verpflichtungen u. a. gem. Art. 32 DS-GVO regelkonform nachkommt. Hierfür kann er z. B. Auskünfte des Auftragnehmers einholen, sich

vorhandene Testate von Sachverständigen, Zertifizierungen oder internen Prüfungen vorlegen lassen oder die technischen und organisatorischen Maßnahmen des Auftragnehmers nach rechtzeitiger Abstimmung zu den üblichen Geschäftszeiten selbst persönlich prüfen bzw. durch einen sachkundigen Dritten prüfen lassen, sofern dieser nicht in einem Wettbewerbsverhältnis zum Auftragnehmer steht. Der Auftraggeber wird Kontrollen nur im erforderlichen Umfang durchführen und die Betriebsabläufe des Auftragnehmers dabei nicht unverhältnismäßig stören.

(2) 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 der technischen und organisatorischen Maßnahmen des Auftragnehmers erforderlich sind.

(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.

(4) Der Auftragnehmer weist dem Auftraggeber die Verpflichtung der Mitarbeiter nach § 6 Abs. 4 auf Verlangen nach.

§ 9 Einsatz von Subunternehmern

(1) Die vertraglich vereinbarten Leistungen bzw. die nachfolgend beschriebenen Teilleistungen werden unter Einschaltung folgender Subunternehmer erbracht:

Firma Subunternehmer	Ort	Leistung des Subunternehmers	Ort der Verarbeitung
Hetzner Online GmbH	91710 Gunzenhausen	Technische Infrastruktur / Hosting	EU

Der Auftragnehmer ist im Rahmen seiner vertraglichen Verpflichtungen zur Begründung von weiteren Unterauftragsverhältnissen mit Subunternehmern („Subunternehmerverhältnis“) befugt. Er setzt den Auftraggeber hiervon unverzüglich

in Kenntnis. Der Auftragnehmer ist verpflichtet, Subunternehmer sorgfältig nach deren Eignung und Zuverlässigkeit auszuwählen. Der Auftragnehmer hat bei der Einschaltung von Subunternehmern diese entsprechend den Regelungen dieser Vereinbarung zu verpflichten und dabei sicherzustellen, dass der Auftraggeber seine Rechte aus dieser Vereinbarung (insbesondere seine Prüf- und Kontrollrechte) auch direkt gegenüber den Subunternehmern wahrnehmen kann. Sofern eine Einbeziehung von Subunternehmern in einem Drittland erfolgen soll, hat der Auftragnehmer sicherzustellen, dass beim jeweiligen Subunternehmer ein angemessenes Datenschutzniveau gewährleistet ist. Der Auftragnehmer wird dem Auftraggeber auf Verlangen den Abschluss der vorgenannten Vereinbarungen mit seinen Subunternehmern nachweisen.

(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 z. B. Post-, Transport- und Versandleistungen, Reinigungsleistungen, Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt und Bewachungsdienste. Wartungs- und Prüfleistungen stellen zustimmungspflichtige Subunternehmerverhältnisse dar, soweit diese für IT-Systeme erbracht werden, die auch im Zusammenhang mit der Erbringung von Leistungen für den Auftraggeber genutzt werden.

§ 10 Anfragen und 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 – 22 sowie 32 bis 36 DS-GVO.

(2) Macht ein Betroffener Rechte, etwa auf Auskunftserteilung, Berichtigung oder Löschung hinsichtlich seiner Daten, unmittelbar gegenüber dem Auftragnehmer geltend, so verweist er den Betroffenen unverzüglich an den Auftraggeber und wartet dessen Weisungen ab.

§ 11 Haftung

Für den Ersatz von Schäden, die ein Betroffener wegen einer nach den Datenschutzgesetzen unzulässigen oder unrichtigen Datenverarbeitung oder Nutzung im Rahmen der Auftragsverarbeitung erleidet, gilt Art. 82 DS-GVO.

Der Auftraggeber stellt Talent Engine GmbH unter der Maßgabe dieses gesondert vereinbarten AV-Vertrags von etwaigen Forderungen Dritter frei, welche auf dessen Verletzung datenschutzrechtlicher Vorschriften beruhen.

§ 12 Außerordentliches Kündigungsrecht

(1) Der Auftraggeber kann den Hauptvertrag und diesen Vertrag fristlos kündigen, wenn der Auftragnehmer seinen Pflichten aus diesem Vertrag nicht nachkommt, Bestimmungen der DS-GVO schuldhaft verletzt oder eine Weisung des Auftraggebers nicht ausführen kann oder will, obwohl er dazu verpflichtet ist.

(2) Vorgenannte Kündigungsmöglichkeit besteht erst nachdem der Auftraggeber dem Auftragnehmer eine angemessene Frist gesetzt hat, den Verstoß abzustellen und der Auftragnehmer diese hat ergebnislos verstreichen lassen.

(3) Das Recht zur fristlosen Kündigung aus wichtigem Grund bleibt unberührt.

§ 13 Beendigung des Hauptvertrags

(1) Der Auftragnehmer wird dem Auftraggeber nach Beendigung des Hauptvertrags oder jederzeit auf dessen Anforderung alle ihm überlassenen Unterlagen, Daten und Datenträger zurückgeben oder – auf Wunsch des Auftraggebers, sofern nicht nach dem Unionsrecht oder dem Recht der Bundesrepublik Deutschland eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht – löschen. Dies betrifft auch etwaige Datensicherungen beim Auftragnehmer. Der Auftragnehmer hat den dokumentierten Nachweis der ordnungsgemäßen Löschung noch vorhandener Daten zu führen.

(2) Der Auftraggeber hat das Recht, die vollständige und vertragsgerechte Rückgabe bzw. Löschung der Daten beim Auftragnehmer in geeigneter Weise zu kontrollieren.

(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. Die vorliegende Vereinbarung bleibt über das Ende des Hauptvertrags hinaus solange gültig, wie der Auftragnehmer über personenbezogene Daten verfügt, die ihm vom Auftraggeber zugeleitet wurden oder die er für diesen erhoben hat.

(4) Die Parteien verpflichten sich gegenseitig, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des jeweils anderen vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

§ 14 Schlussbestimmungen

(1) Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform. Dies gilt auch für den Verzicht auf dieses Formerfordernis. Der Vorrang individueller Vertragsabreden bleibt hiervon unberührt.

(2) Sollten einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise nicht rechtswirksam oder nicht durchführbar sein oder werden, so wird hierdurch die Gültigkeit der jeweils übrigen Bestimmungen nicht berührt.

(3) Diese Vereinbarung unterliegt deutschem Recht unter Ausschluss des UN-Kaufrechts.

(4) Sofern es sich bei dem Auftraggeber um einen Kaufmann, eine juristische Person des öffentlichen Rechts oder um ein öffentlich-rechtliches Sondervermögen handelt, ist Gerichtsstand für alle Streitigkeiten aus Vertragsverhältnissen zwischen dem Auftraggeber und dem Auftragnehmer Berlin.

Ort, Datum	Auftraggeber
Ort, Datum	Talent Engine GmbH

Anlage 1 – Technische und organisatorische Maßnahmen des Auftragnehmers
Durch geeignete technische und organisatorische Maßnahmen wird sichergestellt, dass die Vorschriften zum Datenschutz jederzeit eingehalten werden.

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

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, insbesondere:

Personenbezogene Daten sind nur für registrierte Nutzer zugänglich. Grundsätzlich besteht eine pseudonymisierten Nutzer-ID, so dass Daten-Zuordnung immer nur für den jeweiligen Use-Case und nur für berechtigte Personen möglich ist.

2. Verschlüsselung (Art. 32 Abs. 1 lit. a DS-GVO)
Kryptografische Maßnahmen, durch die personenbezogene Daten derart verändert werden, dass sie – insbes. während ihres Übertragungsvorgangs – ohne einen Schlüssel nicht mehr les- oder verstehbar sind, insbesondere Verschlüsselung mittels Zertifikate und SSL Verschlüsselung, Verschlüsselungsverfahren entsprechend dem Stand der Technik, Verschlüsselung von Passwörtern.

Passwörter werden nicht im Klartext gespeichert sondern durch den “bcrypt” Algorithmus kryptographisch verschlüsselt. Der bcrypt cost factor beträgt zum Stand März 2021 “11” und wird entsprechend gängiger Security Advisory Richtlinien angepasst sofern dies notwendig wird. Klartext Passwörter und Access tokens werden nicht protokolliert.

Jeglicher Datentransfer findet durch eine lückenlose SSL End-to-End Verschlüsselung zwischen Browser und Ursprungsserver statt. Der Zugriff auf die Anwendung erfordert Clients die mindestens TLS Version 1.2 Unterstützen. Die aktuellste TLS Version 1.3 wird ebenfalls optional unterstützt und aktuell von > 90% aller Anfragen verwendet. Zugriff über die veralteten TLS Versionen 1.0 und 1.1 wird vor der Anwendung, auf Ebene des reverse proxies unterbunden.

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

- *Zutrittskontrolle*
  Besucherregelung, Schlüsselkonzept, Alarmanlage

- *Zugangskontrolle*
  Berechtigungen zum Zugang zu Daten oder Systemen, Entzug von Berechtigungen, Protokollierungen, Periodische Überprüfung, Erforderlichkeit, Virenschutz, Regelung für Dienstleister

- *Zugriffskontrolle*
  Rollenkonzepte, Administrator-Regelungen, Protokollierung aller Zugriffe, Löschkonzepte für Datenträger

- *Trennungskontrolle*
  Trennung von Daten mit unterschiedlichen Zwecken, Mandantenkonzepte, Verfahren für Test- und Produktionssysteme

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

- *Weitergabekontrolle*

  - *Verschlüsselung der Infrastruktur, des WLAN*
  - *Back-Up Systeme*
  - *Keine Druckeranlagen und Vorgaben an Mitarbeiter bzgl. Ausdrucken von geheimen Unterlagen (Verhinderung von Zugriff auf Ausdrucke)*
  - *Kein Einsatz von USB-Sticks und CD-ROMs*

Eingabekontrolle

  - *Klare Zugriffsregelungen und Dokumentation für alle Mitarbeiter. Protokollierung von Eingaben, Änderungen und Löschung von personenbezogenen Daten*

5. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

- *Verfügbarkeitskontrolle*

  - *Regelmäßige Backup-Verfahren*
  - *Getrennte Aufbewahrung von Daten gewährleistet*
  - *Firewall*
  - *Virenschutz und Firewall entsprechen aktuellem Stand der Technik*
  - *Verwendung von Spiegelung von Festplatten (RAID), lokal getrennte Spiegelungen*

- Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO):
  - *Verwendung von Recovery / Backup-Systeme*

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

  - *Datenschutz-Management*
  - *Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz*
  - *Regelmäßige Sensibilisierung der Mitarbeiter*
  - *Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO) – „Privacy by default“ und „Privacy by design) Verwendung von vorgefertigten Datenschutzregelungen.*
  - *Incident-Response-Management*

- *<u>Auftragskontrolle</u>*
    - *Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation*
    - *Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten in Bezug auf Datenschutz und Datensicherheit*
    - *Regelmäßige Kontrolle*
    - *Regelung zum Einsatz weitere Subunternehmer*