VERTRAG ZUR AUFTRAGSVERARBEITUNG GEMÄß ART. 28 DS-GVO

Vereinbarung

zwischem dem/der

Auftragnehmer, Straße, Plz, Ort

- Verantwortlicher - nachstehend Auftraggeber genannt -

und dem/der

Auctores GmbH, Amberger Straße 82, 92318 Neumarkt

- Auftragsverarbeiter - nachstehend Auftragnehmer genannt

1. Gegenstand und Dauer des Auftrags

Gegenstand des Auftrags zum Datenumgang ist die Durchführung der Aufgaben, die in Anlage 3) definiert sind. Die Dauer dieses Auftrags (Laufzeit) ist befristet auf die Gültigkeit der aktuellen Rahmenverträge.

2. Umfang, Art und Zweck der Erhebung, Verarbeitung oder Nutzung von Daten

Der Umfang, die Art und der Zweck einer etwaigen Erhebung, Verarbeitung oder Nutzung personenbezogener Daten, die Art der Daten und der Kreis der Betroffenen werden dem Auftragnehmer durch den Auftraggeber gemäß der vom Auftraggeber ausgefüllten Anlage 3 beschrieben, soweit sich das nicht aus dem Vertragsinhalt der in Ziffer 1 beschriebenen Vertragsverhältnisse ergibt.

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 Art. 44 ff. DS-GVO erfüllt sind.

3. 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.

4. 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) In Bezug auf die automatisierte Löschung von Teilnehmerdaten siehe Anlage 3.
(3) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

5. 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.

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

c) Als Datenschutzbeauftragte(r) ist beim Auftragnehmer Projekt 29 GmbH & Co. KG, Ostengasse 14, Regensburg, 93047 Regensburg bestellt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

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

e) 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.

f) 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].

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

h) 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.

i) 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.

j) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

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

6. Unterauftragsverhältnisse

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-/Transportdienstleistungen, Wartung und Benutzerservice 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. Die Liste der Unterauftragnehmer ist in Anlage 2) zu finden.

7. 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 wahlweise 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-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) und/oder eine geeignete Zertifizierung durch ITSicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

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

8. 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.

9. 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.

10. 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.

11. Sonstige Vereinbarungen

11.1. Entgelte

Ein Entgelt für diesen Auftrag wird nicht gefordert. Soweit der Auftraggeber Unterstützung nach Ziffer 4 für die Beantwortung von Anfragen Betroffener benötigt, hat er die hierdurch entstehenden Kosten zu erstatten. Soweit der Auftraggeber nach Ziffer 7 Kontrollrechte ausüben wird, orientiert sich die vorab zu vereinbarende Höhe des Entgelts an einem festzulegenden Stundensatz des für die Betreuung vom Auftragnehmer abgestellten Mitarbeiters. Erteilt der Auftraggeber dem Auftragnehmer Weisungen nach Ziffer 9, so hat er durch diese Weisung entstehende Kosten zu erstatten

11.2. Vertragsdauer

Diese Vereinbarung ist abhängig vom Bestand eines Rahmenvertrags gemäß Ziffer 1. Die Kündigung oder anderweitige Beendigung des Rahmenvertragsverhältnisses gemäß Ziffer 1 beendet gleichzeitig diese Vereinbarung. Das Recht zur isolierten, außerordentlichen Kündigung dieser Vereinbarung sowie die Ausübung gesetzlicher Rücktrittsrechte konkret für die Vereinbarung bleiben hierdurch unberührt.

11.3. Rechtswahl

Es gilt das Recht der Bundesrepublik Deutschland.

11.4. Gerichtsstand

Die Parteien vereinbaren als Gerichtsstand den Sitz des für Neumarkt i. d. OPf. zuständigen Gerichts.

11.5 Haftung

Auf Art. 82 DS - GVO wird verwiesen.

Dies ist ein Muster-Vertrag. In Ihrem Vertrag wird entsprechend Unterschrift und Firmenstempel der Auctores GmbH sein.

Anlage 1 – Technische und organisatorische Maßnahmen (TOM)

Stand 01.05.2018

Nr.	Gebiet	Beschreibung
0	**Organisation**	
	Wie ist die Umsetzung des Datenschutzes organisiert?	Ein externer Datenschutzbeauftragter wird zur Wahrnehmung der Beratungs- und Kontrollfunktionen aus dem BDSG (neu DSGVO) eingesetzt.
	Nennen Sie uns bitte den Namen und die Kontaktdaten Ihres Datenschutzbeauftragten.	Christian Volkmer +49-941-2986930 Projekt 29 GmbH & Co. KG Ostengasse 14 93047 Regensburg
	In welcher Form werden die Mitarbeiter auf die Umsetzung der vereinbarten technischen und organisatorischen Maßnahmen geschult, die für diese Verarbeitung in Anwendung kommen?	Das Schulungskonzept beinhaltet sowohl eine Datenschutzunterweisung bei Beginn der Tätigkeit, als auch eine konstante Sensibilisierung durch monatliche Datenschutznewsletter, fachbezogene Webschulungen und persönliche Sensibilisierung durch den externen Datenschutzbeauftragten.
	Sind die Verarbeitungen hinsichtlich datenschutzrechtlicher Zulässigkeit dokumentiert?	Im Rahmen des internen Verfahrens-verzeichnisses sind die Datenströme dokumentiert und die Zulässigkeit der Verarbeitung und Nutzung nach BDSG nachgewiesen. Eventuell notwendige Vorabkontrollen werden schon im Planungsstadium integriert.
1	**Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)**	
1.1	**Zutrittskontrolle**	
	Wie werden die Gebäude, in denen die Verarbeitung stattfindet, vor unbefugtem Zutritt gesichert?	Das Gebäude ist mit einer Sicherheits-Schließanlage ausgerüstet.
	Wie werden die Räume / Büros, in denen die Verarbeitung stattfindet, vor unbefugtem Zutritt gesichert?	Die Räumlichkeiten bei den Rechenzentrumsbetreibern sind mit entsprechend Schließanlagen ausgestattet.
	Wie werden die Verarbeitungsanlagen vor unbefugtem Zugriff geschützt?	Sicherheitsmaßnahmen auf verschiedenen Ebenen: - Firewall - Schließanlage

Nr.	Gebiet	Beschreibung
		- Alarm-Anlage - Aktuellste Sicherheitsupdates und Virenscanner
	Wie werden die umgesetzten Zutrittskontrollmaßnahmen auf Tauglichkeit geprüft?	Im Rahmen der Kontrollen durch den externen Datenschutzbeauftragten werden auch die Zutrittskontrollmaßnahmen überprüft.
1.2	**Zugangskontrolle**	
	Wie erfolgt die Vergabe von Benutzerzugängen?	Mitarbeiter haben Zugang zum Gebäude. Benutzerzugänge werden selektiv für Mitarbeiter ausgegeben. Sensible Daten sind nur für ausgewählte Mitarbeiter zugänglich.
	Wie wird die Gültigkeit von Benutzerzugängen überprüft?	Benutzerzugänge werden entsprechend bei Zugängen und Abgängen von Mitarbeitern aktualisiert
	Wie werden Benutzerzugänge inkl. Antragstellung, Genehmigungsverfahren etc. dokumentiert?	Es findet keine Dokumentation von Benutzerzugängen statt. Gültige Benutzer sind alle Mitarbeiter.
	Wie wird sichergestellt, dass die Anzahl von Administrationszugängen ausschließlich auf die notwendige Anzahl reduziert ist und nur fachlich und persönlich geeignetes Personal hierfür eingesetzt wird?	Die Entscheidungen zur Rechtevergabe halten sich streng an die entsprechenden Vorgaben, Datenvermeidung und Datensparsamkeit, weniger ist hier oft mehr.
	Ist ein Zugriff auf die Systeme / Anwendungen von außerhalb des Unternehmens möglich (Heimarbeitsplätze, Dienstleister etc.) und wie ist der Zugang gestaltet?	Zugriff ist selektiv geregelt. Es wird lediglich von Firmen-eigenen Geräten über verschlüsselte Zugangswege auf die Daten zugegriffen. Es gibt Heimarbeitsplätze.
1.3	**Zugriffskontrolle**	
	Wie wird erreicht, dass Passwörter nur dem jeweiligen Benutzer bekannt sind?	Die Passwörter werden vom jeweiligen Mitarbeiter selbst vergeben. Die strengen Systemvoreinstellungen zwingen zu einer hohen Passwortkomplexität. Passwörter werden nicht gespeichert. Mitarbeiter müssen beim erstmaligen Anmelden ihr Passwort ändern.
	Welche Anforderungen werden an die Komplexität von Passwörtern gestellt?	Die Vorgaben Empfehlungen des BSI dienen als Vorbild für die o.g. Systemeinstellungen
	Wie wird gewährleistet, dass der Benutzer sein Passwort regelmäßig ändern kann / muss?	Richtlinien der Domäne

Nr.	Gebiet	Beschreibung
	Welche organisatorischen Vorkehrungen werden zur Verhinderung von unberechtigten Zugriffen auf personenbezogene Daten am Arbeitsplatz getroffen?	Schulung und Sensibilisierung der Mitarbeiter. Einweisungen und regelmäßige Schulungen zu den verwendeten Geräten
	Wie wird sichergestellt, dass Zugriffsberechtigungen anforderungsgerecht und zeitlich beschränkt vergeben werden?	Siehe auch Punkt Vergabe von Benutzerzugängen Punkt 1.2; die IT-Abteilung prüft in regelmäßigen Abständen die Rechte und Benutzerstruktur
	Wie erfolgt die Dokumentation von Zugriffsberechtigungen?	Es erfolgt keine weitere Dokumentation.
	Wie wird sichergestellt, dass Zugriffsberechtigungen nicht missbräuchlich verwendet werden?	Mitarbeiter der Firma Auctores haben Zugriff auf Daten, die Zugriffsliste wird mittels Prozesse aktuell gehalten.
	Wie lange werden Protokolle aufbewahrt? Wer hat Zugriff auf die Protokolle und wie oft werden sie ausgewertet?	Keine festgelegten Fristen, meist Systemparameter, ausschließlich die Geschäftsführung und ausgewählte Mitarbeiter
1.4	**Trennungskontrolle**	
	Wie wird sichergestellt, dass Daten, die zu unterschiedlichen Zwecken erhoben wurden, getrennt voneinander verarbeitet werden?	n/a
1.5	**Pseudonymisierung**	
	Welche organisatorischen Maßnahmen wurden getroffen, damit die Verarbeitung personenbezogener Daten gesetzeskonform erfolgt?	Alle mit der Verarbeitung von personenbezogenen Daten betrauten Personen wurden entsprechend verpflichtet. Ein Datenschutzkonzept wird im Unternehmen eingesetzt und ist allen Mitarbeitern bekannt gemacht. Das Schulungskonzept beinhaltet sowohl eine Datenschutzunterweisung bei Beginn der Tätigkeit, als auch eine konstante Sensibilisierung durch monatliche Datenschutznewsletter, fachbezogene Webschulungen und persönliche Sensibilisierung durch den externen Datenschutzbeauftragten. Auf die Besonderheiten im Umgang mit pseudonymisierten Daten wurde hingewiesen.
	Welche technischen Maßnahmen oder Hilfsmittel sind bei der Pseudonymisierung von personenbezogenen Daten im Einsatz?	Es ist keine Pseudonymisierung notwendig

2	**Integrität (Art. 32 Abs. 1 lit. b DS-GVO)**	
2.1	**Weitergabekontrolle**	
	Wie gewährleisten Sie die Integrität und Vertraulichkeit bei der Weitergabe von personenbezogenen Daten?	Es werden keine personenbezogenen Daten der Auftragnehmer weitergegeben.
	Werden Verschlüsselungssysteme bei der Weitergabe von personenbezogenen Daten eingesetzt und wenn ja, welche?	Personenbezogene Daten werden mit einer Transportverschlüsselung übertragen
	Wie wird die Weitergabe personenbezogener Daten dokumentiert?	n/a
	Wie wird der unberechtigte Abfluss von personenbezogenen Daten durch technische Maßnahmen beschränkt?	Eine strikte Rechtevergabe sichert die Daten vor unberechtigtem Zugriff.
	Gibt es ein Kontrollsystem, das einen unberechtigten Abfluss von personenbezogenen Daten aufdecken kann?	Unberechtigter Abfluss kann mangels Zugriffsmöglichkeiten Dritter ausgeschlossen werden, siehe Rechtevergabe.
2.2.	**Eingabekontrolle**	
	Welche Maßnahmen werden ergriffen, um nachvollziehen zu können, wer wann und wie lange auf Applikationen zugegriffen hat?	Aufgrund des Rollen-& Rechtekonzepts sind jene Maßnahmen nicht notwendig.
	Wie ist nachvollziehbar, welche Aktivitäten auf den entsprechenden Applikationen durchgeführt wurden?	Rollen-/Rechtekonzepte und diverse Lizenz-modelle mit unterschiedlichen Berechtigungs-konzepten
	Welche Maßnahmen werden ergriffen, damit die Verarbeitung durch die Mitarbeiter nur gemäß der Weisungen des Auftraggebers erfolgen kann?	Zugriffskontrolle anhand des Rollen-/Rechte-konzepts zur ordnungsgemäßen Datenverarbeitung und Speicherung
	Welche Maßnahmen werden getroffen, damit auch Unterauftragnehmer ausschließlich im vereinbarten Umfang personenbezogene Daten des Auftraggebers durchführt?	Sämtliche Unterauftragnehmer unterliegen den gleichen Vorgaben wie der Auftragnehmer. Entsprechende Verträge sind geschlossen. Die Pflichten zur Überprüfung der Unterauftrag-nehmer übernimmt der Datenschutzbeauftrage des Unternehmens. Er ist auch bei der Auswahl der beauftragten Firmen maßgeblich beteiligt.
	Wie wird die Löschung / Sperrung von personenbezogenen Daten am Ende der Aufbewahrungsfrist bei Unterauftragnehmern sichergestellt?	Festlegung durch Vertragsbindung, bei Wegfall des Zweckes ist ebenfalls eine Löschung der Daten indiziert.

3	**Verfügbarkeit und Belastbarkeit**	
3.1.	**Verfügbarkeitskontrolle**	
	Wie wird gewährleistet, dass die Datenträger vor elementaren Einflüssen (Feuer, Wasser, elektromagnetische Abstrahlung etc.) geschützt sind?	Gesicherte Daten sind räumlich getrennt von Produktivdaten
	Welche Schutzmaßnahmen werden zur Bekämpfung von Schadprogrammen eingesetzt und wie wird deren Aktualität gewährleistet?	Ständig aktuelle Virenscanner und Spamfilter finden Einsatz. Die Systeme werden regelmäßig aktualisiert.
	Wie wird sichergestellt, dass nicht mehr benötigte bzw. defekte Datenträger ordnungsgemäß entsorgt werden?	Physische Löschung bei funktionsfähigen Datenträgern und mechanische Zerstörung defekter Datenträger vor der Entsorgung
3.2.	**Wiederherstellbarkeit**	
	Welche organisatorischen und technischen Maßnahmen werden getroffen, um auch im Schadensfall die Verfügbarkeit von Daten und Systemen schnellstmöglich zu gewährleisten? (rasche Wiederherstellbarkeit nach Art. 32 Abs.1 lit.c DS-GVO)	Automatisierte Durchführung relevanter Daten und manuelle Prüfung und Sichtung der Backups
4.	**Verfahren zur regelmäßigen Überprüfung, Bewertung, Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO, Art. 25 Abs. 1 DS-GVO)**	
	Welche Verfahren gibt es zur regelmäßigen Bewertung/Überprüfung, um die Sicherheit der Datenverarbeitung zu gewährleisten (Datenschutz-Management)?	Der externe Datenschutzbeauftragte überprüft regelmäßig und teilweise auch unangekündigt, die Einhaltung der technisch-organisatorischen Maßnahmen.
	Wie wird auf Anfragen bzw. Probleme reagiert (Incident-Response-Management)?	Einsatz eines Ticketsystems (Basis OTRS) zweistufig (1st und 2nd Level); zusätzlich Telefonhotline und automatisierte Überwachung und Alarmierung (Nagios)
	Welche datenschutzfreundlichen Voreinstellungen gibt es (Art. 25 Abs. 2 DS-GVO)?	Keine Vorbelegung durch Haken; bei Anmeldung im System erfolgen keine Vorbelegungen; Benutzer muss die Anmeldeinformationen jeweils eintragen
4.1	**Auftragskontrolle**	
	Welche Vorgänge gibt es zur Weisung bzw. dem Umgang mit der Auftragsdatenverarbeitung (Datenschutz-Management)?	Das Vertragswerk wurde entsprechend den neuen Richtlinien zur Auftragsdatenverarbeitung gestaltet. Der externe Datenschutzbeauftragte nimmt entsprechende Beratungs- und Kontrollpflichten wahr.

Anlage 2 – Unterauftragnehmer

Stand 01.05.2018

Firma Unterauftragnehmer	Anschrift/Land	Leistung
Proact Deutschland GmbH	Südwestpark 43, 90449 Nürnberg	Betreiber Rechenzentrum, Betreuung Server
Hetzner Online GmbH	Industriestr. 25, 91710 Gunzenhausen	Betreiber Rechenzentrum, E-Mail-Providing
OVH GmbH	Dudweiler Landstraße 5, 66123 Saarbrück	Betreiber Rechenzentrum
QualityHosting AG	Uferweg 40-42, 63571 Gelnhausen	E-Mail-Providing

Anlage 3 zum Auftrag gemäß Art. 28 DS-GVO: Konkretisierung des Auftragsinhalts

(1) Gegenstand des Auftrags

- Verarbeitung der personenbezogenen Daten zur Vertragserfüllung
- Verarbeitung der personenbezogenen Daten im Rahmen des Produkts Visavid

(2) Art der Daten

- Personenstammdaten
- Kommunikationsdaten (z.B. Telefon, E-Mail)
- Benutzerkonto: Anrede, Vorname, Nachname, E-Mail, Firma, Passwort, Telefon
- Teilnehmer: Anrede, Vorname, Nachname, E-Mail, Teilnehmernummer

(3) Kategorien betroffener Personen. Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- Teilnehmer
- Inhaber der Benutzerkonten

(4) Art und Zweck der vorgesehenen Verarbeitung von Daten
Nähere Beschreibung des Auftragsgegenstandes in Hinblick auf Art und Zweck der Aufgaben des Auftragnehmers: Wir verarbeiten insbesondere die Daten von Teilnehmern eines Raumes. Bitte beachten Sie, dass diese Teilnehmerdaten automatisiert nach Ablauf von 14 Tagen nach Ende der Veranstaltung gelöscht werden.

Es gelten die jeweils aktuell gültigen Informationen gemäß Artikel 13 DS-GVO: Auctores GmbH für das Produkt Visavid: https://visavid.de/datenschutz/#informationspflicht-visavid.