eggheads

# Auftragsverarbeitungsvertrag/ Data Processing Agreement

**gemäß Art. 28 Abs. 3 Datenschutz-Grundverordnung/ pursuant to Art. 28 Par. 3 General Data Protection Regulation**

# Vertragspartner/ Contract partner

| | | | |
|---|---|---|---|
| **Auftragnehmer/ Contractor:** | **eggheads GmbH** | **Auftraggeber/ Client:** | |
| **Adresse/ Address:** | Alte Wittener Str. 50, 44803 Bochum | **Adresse/ Address:** | |
| **Land/ Country:** | Deutschland/ Germany | **Land/ Country:** | |
| - Auftragsverarbeiter nachfolgend als „Auftragnehmer“ bezeichnet/ hereinafter referred to as „contractor“ - | | - Verantwortlicher nachfolgend als „Auftraggeber“ bezeichnet/ Controller hereinafter referred to as „client“ - | |
| - gemeinschaftlich als „Vertragsparteien“ bezeichnet/ collectively referred to as the „contractual parties“ - | | | |

| | |
|---|---|
| **Präambel**<br>Dieser Vertrag konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus der in ihren Einzelheiten beschriebenen Auftragsverarbeitung ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit dem Vertrag in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte personenbezogene Daten („Daten“) des Auftraggebers verarbeiten. | **Preamble**<br>This agreement explicates the obligations of the contractual parties concerning data protection which follow from the commission processing that is here described in detail. It shall apply to all actions related to this contract and actions where employees of the contractor or persons commissioned by the contractor process personal data (“data”) of the client. |
| **1. Gegenstand und Dauer des Auftrags**<br>(1) Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer:<br>Dienstleistungen (Services) im Rahmen der Bereitstellung und Nutzung der von EGGHEADS entwickelten Product Information Management (PIM) Software, gemäß den Regelungen des Hauptvertrages.<br>(2) Die Dauer dieses Auftrages (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung. | **1. Object and Period of Commission**<br>(1) The object of the commission for data processing is the performance of the following tasks by the contractor:<br>Services in connection with the implementation and utilization of the Product Information Management (PIM) software developed by EGGHEADS, in accordance with the regulations of the main contract.<br>(2) The duration of this commission (period) is equal to the period of the service agreement. |
| **2. Spezifizierung der Auftragsverarbeitung**<br>**Art und Zweck der vorgesehenen Verarbeitung von Daten**<br>Nähere Beschreibung des Auftragsgegenstandes im Hinblick auf Art und Zweck der Aufgaben des Auftragnehmers:<br>Dienstleistungen (Services) im Rahmen der Bereitstellung und Nutzung der von EGGHEADS entwickelten Product Information Management (PIM) Software, die Wartung und Pflege der Software sowie Schulungen und Workshops. | **2. Specification of Commission Processing**<br>**Type and Purpose of the Planned Processing of Data**<br>More specific description of the object of commission regarding the type and purpose of the tasks of the contractor:<br>Services in connection with the implementation and use of the Product Information Management (PIM) software developed by EGGHEADS, maintenance and care of the software, as well as trainings and workshops. |
| **Art der Daten**<br>Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/ -kategorien (Aufzählung/ Beschreibung der Datenkategorien):<br>a. Personenstammdaten<br>b. Kommunikationsdaten (z. B. Telefon, E-Mail)<br>c. Zugangsdaten Jira, EGGHEADS Helpcenter, Download Website<br>d. Zugangsdaten und Bearbeitungshistorie der User | **Types of Data**<br>Objects of the processing of personal data are the following data types or categories (enumeration or description of data categories):<br>a. Personal master data<br>b. Communication data (e.g. phone, e-mail)<br>c. Credentials for Jira, EGGHEADS Help Center, website downloads<br>d. Credentials and editing/change history of users |
| **Kategorien betroffener Personen**<br>Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:<br>a. Kunden<br>b. Beschäftigte<br>c. Ansprechpartner | **Categories of Data Subjects**<br>Categories of persons from whom data is processed:<br>a. Customers<br>b. Employees<br>c. Contact persons |

| | |
|---|---|
| **3. Technisch-organisatorische Maßnahmen**<br>(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.<br>(2) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO 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 DSGVO zu berücksichtigen [Einzelheiten in Anlage TOM].<br>(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. | **3. Technical Organizational Measures**<br>(1) The contractor shall document the performance of the technical and organizational measures agreed upon prior to commission, in particular concerning the concrete performance of the commission, before beginning with the processing, and hand it over to the client for examination. Upon approval by the client, the documented measures shall serve as the basis of the commission. If the examination or audit by the client results in the requirement for amendment, it shall be implemented upon mutual agreement.<br>(2) The contractor shall ensure the security of processing pursuant to Art. 28 Par. 3 Lit. c, 32 GDPR, in particular in relation to Art. 5 Par. 1, Par. 2 GDPR. Altogether, the to-be-performed measures concern data security and guarantee of an appropriate security level adequate to the risks involved, in particular concerning confidentiality, integrity, availability, and system resilience. To this end, the state of the art, implementation costs, and the type, scope, and purpose of processing, as well as the calculated probability and significance of individual risks shall be considered for the rights and freedom of natural persons pursuant to Art. 32 Par. 1 GDPR. [Details provided in the appendix of TOM below.]<br>(3) The technical and organizational measures are subject to technological progress and development. To this extent, the contractor may utilize alternative measures adequate to the agreed-upon measures. Such alternative measures shall not fall short of the security level of defined measures. Essential amendments shall be documented. |
| **4. Berichtigung, Einschränkung und Löschung von Daten**<br>(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.<br>(2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, | **4. Authorization, Restrictions, and Deletion of Data**<br>(1) The contractor shall only correct, delete, or limit the processing of data processed as part of the commission on the basis of documented instructions by the client, instead of doing so on their own authority. If a data subject communicates a request directly to the contractor, the contractor shall immediately communicate this request to the client.<br>(2) To the extent that it is included in the scope of services, the deletion concept, right to be |

| | |
|---|---|
| Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen. | forgotten, authorization, data portability, and right to information on the basis of documented instructions by the client shall be immediately ensured by the contractor. |
| **5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers**<br>Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DSGVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben: | **5. Quality Warranty and Other Obligations by the Contractor**<br>In addition to the regulations concerning the commission, the contractor shall ensure legal obligations pursuant to Art. 28 to 33 GDPR; in particular, the contractor shall comply to the following regulations: |
| a. Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DSGVO ausübt. Dessen Kontaktdaten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt. Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt. | a. Written order of a data protection officer who carries out their activities pursuant to Art. 38 and 39 GDPR. Their contact data shall be provided to the client for the purpose of direct communication. A replacement of the data protection officer shall be communicated to the client immediately. |
| b. Als Datenschutzbeauftragte(r) ist beim Auftragnehmer Herr Jürgen Golda, P2Consult, datenschutzbeauftragter@eggheads.de bestellt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen. | b. As a data protection officer, the contractor has ordered Mr. Jürgen Golda, P2Consult, datenschutzbeauftragter@eggheads.de. A replacement of this data protection officer shall be communicated immediately. |
| c. Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO. 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. | c. Protection of confidentiality pursuant to Art. 28. Par. 3 S. 2. Lit. b, 29, 32 Par. 4 GDPR. The contractor shall only order employees for the performance of labor who comply to the protection of confidentiality and who have been informed about the regulations for data protection relevant to them. The contractor and every person employed by the contractor who is granted access to personal data shall only process such data as instructed by the client, including the permissions granted in this contract, unless they are legally obligated to process such data. |
| d. Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DSGVO [Einzelheiten in Anlage TOM]. | d. The performance and maintenance of all technical and organizational measures required for this contract pursuant to Art. 28 Par. 3 S. 2 Lit. c GDPR. [Details provided in the appendix of TOM below.] |
| e. Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen. | e. The client and contractor shall collaborate to fulfill their tasks upon request by regulating authorities. |
| f. Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, | f. The immediate communication with the client concerning control actions and measures by regulating authorities, to the extent that they concern this commission. This shall also |

| | |
|---|---|
| soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt. | apply to contravention and criminal procedure by relevant authorities in relation to personal data being subject to investigation as part of the commission processing by the contractor. |
| g. 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. | g. To the extent that the client is subject to the control of regulating authorities, a contravention or criminal procedure, the liability claim by a data subject or third party, or another claim in relation to the commission processing by the contractor, the contractor shall support the client to the best of their capacities. |
| h. 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. | h. The contractor controls at regular intervals the internal processes as well as the technical and organizational measures in order to ensure that the processing which falls under their responsibility complies to the requirements of applicable data protection law and that the protection of the rights of the data subject is guaranteed. |
| i. Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages. | i. Proof of performed technical and organizational measures for the client within their supervisory power pursuant to paragraph 7 of this contract. |
| **6. Subunternehmer (weitere Auftragsverarbeiter)** | **6. Subcontractor (Further Commission Processors)** |
| (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-/Transportdienstleistungen, 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. | (1) Sub-contractual relations under the definition of this regulation are services which relate immediately to the performance of the main service. Not included are supplementary services which the contractor performs, for example telecommunication services, mailing and transport services, maintenance and user services, the disposal of data storage devices, and other services to ensure confidentiality, availability, integrity, and system resilience of both hardware and software of data processing systems. However, the contractor is obligated to ensure the data protection and data security of the data by the client with appropriate contractual agreements and control measures conformable to law even when outsourcing supplementary services. |
| (2) Ein Subunternehmerverhältnis liegt vor, wenn der Auftragnehmer weitere Auftragnehmer mit der ganzen oder einer Teilleistung der im Vertrag | (2) A sub-contractual relationship is established when the contractor commissions further subcontractors with all or a part of the services |

| | |
|---|---|
| vereinbarten Leistung beauftragt. Der Auftragnehmer wird mit diesen Dritten im erforderlichen Umfang Vereinbarungen treffen, um angemessene Datenschutz- und Informationssicherheitsmaßnahmen zu gewährleisten. Die Hinzunahme von Subunternehmern wird bei Bedarf vor Vergabe der Tätigkeit angezeigt.<br>(3) Vor der Hinzuziehung weiterer oder der Ersetzung aufgeführter Subunternehmer holt der Auftragnehmer die Zustimmung des Auftraggebers ein, wobei diese nicht ohne wichtigen datenschutzrechtlichen Grund verweigert werden darf.<br><br>(4) Erteilt der Auftragnehmer Aufträge an Subunternehmer, so obliegt es dem Auftragnehmer, seine datenschutzrechtlichen Pflichten aus diesem Vertrag dem Subunternehmer zu übertragen. | agreed upon in this contract. The contractor shall make appropriate agreements with these third parties to the extent required to ensure data protection and information protection measures. If required, the involvement of sub-contractors shall be announced prior to the assignment of activities.<br>(3) Prior to the involvement of further sub-contractors or the replacement of existing sub-contractors, the contractor shall request consent from the client, whereas the client shall not refuse consent without a significant reason regarding the data protection law.<br>(4) If the contractor transfers tasks to sub-contractors, it shall be the obligation of the contractor to also transfer their obligations of data protection concerning this contract to the sub-contractor. |
| **7. Kontrollrechte des Auftraggebers**<br>(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennendem 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.<br>(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DSGVO 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.<br>(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO.<br>(4) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen. | **7. Control Rights of the Client**<br>(1) The client has the right, after consultation with the contractor, to carry out examinations or let examinations be carried out by an examinator designated on an individual basis. They have the right to carry out sample controls which shall be announced ahead of time, so that the client can assure themselves that the contractor complies to this agreement in their business operations.<br>(2) The contractor shall guarantee that the client can assure themselves of the compliance to obligations by the contractor pursuant to Art. 28 GDPR. The contractor is obligated to provide the client with the required information on demand, in particular concerning the performance of technical and organizational measures.<br><br>(3) The proof of such measures which do not only concern the concrete commission may be provided in the form of compliance to agreed-upon rules of conduct pursuant to Art. 40 GDPR.<br>(4) For enabling the control by the client, the contractor shall be entitled to claim remuneration. |
| **8. Mitteilung bei Verstößen des Auftragnehmers**<br>(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzun- | **8. Communication of Breaches by the Contractor**<br>(1) The contractor shall support the client in ensuring the obligations pursuant to Art. 32 to 36 GDPR concerning the security of personal data, obligation to report data breach, data protection impact assessment, and prior business consultations. Among other things, this includes: |

| | |
|---|---|
| gen und vorherige Konsultationen. Hierzu gehören u.a.<br>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<br>b. die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden<br>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<br>d. die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung<br>e. die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde<br>(2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen. | a. The guarantee of an adequate security level through technical and organizational measures, which take into consideration the circumstances and purposes of processing as well as the predicted probability and significance of possible breaches of the law because of security vulnerabilities, and which enable an immediate identification of relevant data breach events.<br>b. The obligation to immediately report a breach of personal data to the client.<br>c. The obligation to support the client in their obligation to inform the data subject and to immediately provide them with all relevant information in this context.<br>d. Support for the client in their data protection impact assessment.<br>e. Support for the client as part of prior consultations with the regulating authorities.<br>(2) For support services not included in the description of services or which are unrelated to misconduct by the contractor, the contractor may request remuneration. |
| **9. Weisungsbefugnis des Auftraggebers**<br>(1) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).<br>(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 so lange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird. | **9. Managerial Authority of the Client**<br>(1) Oral instructions shall be confirmed immediately by the client (at least in written form).<br>(2) The contractor shall immediately inform the client if they hold the opinion that an instruction breaches data protection law. The contractor is entitled to postpone the performance of the instruction for as long as the client does not conform or modify it. |
| **10. Löschung und Rückgabe von personenbezogenen Daten**<br>(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. | **10. Deletion and Return of Personal Data**<br>(1) No copies or duplicates of data shall be created without prior knowledge by the client. This excludes safety copies to the extent that they are required to ensure appropriate data processing, and this also excludes data which is subject to the legal obligation to preserve records. |

| | |
|---|---|
| (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. | (2) After the completion of the contractual tasks, or earlier after request by the client – at the latest after termination of the service agreement – the contractor shall hand over all documents, created processing and usage results, as well as data records related to this commission contract, or delete it upon mutual agreement in a manner that complies to data protection law. The same applies to test and scrap material. The corresponding deletion protocol shall be handed over upon request. |
| (3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend den jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben. | (3) Documentations for the proof of appropriate data processing in compliance to the commission shall be preserved by the contractor for the respective period of the obligation to preserve data after the termination of contract. The contractor may transfer the documentation to the client for the discharge of obligations. |
| **11. Informationspflichten, Schriftformklausel, Rechtswahl** | **11. Information Obligation, Written Form Clause, Choice of Law and Jurisdiction** |
| (1) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als »Verantwortlicher« im Sinne der Datenschutz-Grundverordnung liegen. | (1) If the data of the client stored by the contractor is threatened by seizure related to insolvency or settlement proceedings, or any other event or measure by third parties, the contractor shall immediately inform the client. In this context, the contractor shall immediately inform all persons in response that the power of disposition and ownership of the data are held by the client as the “controller” pursuant to GDPR. |
| (2) Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis. | (2) Modifications and supplements to this appendix and any of its parts – including all warranties by the contractor – require written agreement which may also be provided in electronic form (text form) with an explicit note that it does concern a modification or supplement of these conditions. This also applies to a waiver of this form requirement. |
| (3) Bei etwaigen Widersprüchen gehen Regelungen dieser Anlage zum Datenschutz den Regelungen des Vertrages vor. Sollten einzelne Teile dieser Anlage unwirksam sein, so berührt dies die Wirksamkeit der Anlage im Übrigen nicht. | (3) In the event of contradictions, regulations of this appendix enjoy priority over the regulations of the contract. If individual parts of this appendix are legally void, the remainder of the appendix shall retain its legal effectiveness. |

## Vertragspartner/ Contract partner

| **eggheads GmbH** | | **Auftraggeber/ Client** | |
|---|---|---|---|
| **Name:** | Markus Pichler | **Name:** | |
| **Titel:** | Geschäftsführer/<br>Managing Director | **Titel:** | |
| **Datum/ Date:** | | **Datum/ Date:** | |
| **Ort/ Place:** | Bochum | **Ort/ Place:** | |
| **Unterschrift/**<br>**Signature:** | | **Unterschrift/**<br>**Signature:** | |

# Anlage TOM – Technisch-organisatorische Maßnahmen/ Appendix TOM – Technical Organizational Measures

| | |
|---|---|
| **1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)**<br>(1) Zutrittskontrolle:<br>Server werden in einem Klasse-3-Rechenzentrum, IDW PS 951 Typ 2 mit ISO-27001-Zertifizierung und TISAX-Zertifikat betrieben. Ein Zugang zu den Servern ist nur in Begleitung des Betreibers möglich.<br>(2) Zugangskontrolle:<br>Keine unbefugte Systembenutzung, z. B.: (sichere) Kennwörter, Einsatz von Firewalls, Einsatz von Mobile Device Management, Verschlüsselung von Datenträgern.<br>(3) Zugriffskontrolle:<br>Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z. B.: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Verschlüsselung von Datenträgern.<br>(4) Trennungskontrolle:<br>Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z. B. Mandantenfähigkeit.<br>(5) Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO):<br>Trennung von Kundenstammdaten und Auftragsdaten. | **1. Confidentiality (Art. 32 Par. 1 Lit. b GDPR)**<br>(1) Entry Control:<br>Servers are operated in a class 3 data centre, IDW PS 951 type 2 with ISO 27001 certification and TISAX certificate. Access to the servers is only possible when accompanied by the operator.<br>(2) Access Control:<br>No unauthorized system use, e.g. secured by passwords, firewalls, mobile device management, encryption of data storage devices.<br>(3) Action Control:<br>No unauthorized reading, writing, modifying, or deletion when utilizing systems, e.g. roles or rights concept, user-based access control, encryption of data storage devices.<br>(4) Separation Control:<br>Processing data utilized for different purposes separately, e.g. multitenancy.<br>(5) Pseudonymization (Art. 32. Par. 1 Lit. a GDPR; Art. 25 Par. 1 GDPR):<br>Separating master data about clients from related commission data. |
| **2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)**<br>(1) Weitergabekontrolle:<br>Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z. B.: Verschlüsselung, Virtual Private Networks (VPN).<br>(2) Eingabekontrolle:<br>Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z. B.: Protokollierung. | **2. Integrity (Art. 32 Par. 1 Lit. b GDPR)**<br>(1) Transfer Control:<br>No unauthorized reading, writing, modifying, or deletion during electronic transfer or transport, e.g. encryption, virtual private networks (VPN).<br>(2) Input Control:<br>Measures for documenting if and who adds, edits, modifies, or deletes personal data in data processing systems, e.g. protocols. |
| **3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)**<br>(1) Verfügbarkeitskontrolle:<br>Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust. Backup wird nach der 3-2-1 Backup-Regel durchgeführt. Virenschutz und Firewall im Einsatz, Meldewege und Notfallpläne ausgearbeitet. | **3. Availability and Resilience (Art. 32 Par. 1 Lit. b GDPR)**<br>(1) Availability Control:<br>Protection against accidental or malicious destruction or loss. Backups are carried out according to the 3-2-1 backup rule. Virus protection and firewall in use, reporting channels and emergency plans developed. |

| | |
|---|---|
| (2) Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO) gegeben.<br><br>**4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)**<br>(1) Durchführung regelmäßiger interner Audits;<br>(2) Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO);<br>(3) Auftragskontrolle. Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DSGVO ohne entsprechende Weisung des Auftraggebers, z. B.: Eindeutige Vertragsgestaltung, separate Anweisungen in Textform, sorgfältige Auswahl von Dienstleistern, Nachkontrollen. | (2) Ensuring quick data recovery (Art. 32 Par. 1 Lit. c GDPR).<br><br>**4. Process for Regular Testing, Assessing, and Evaluation (Art. 32 Par. 1 Lit. d GDPR; Art. 25 Par. 1 GDPR)**<br>(1) Carrying out regular internal audits.<br>(2) Data protection by design and default.<br><br>(3) Commission Control. No commission processing shall be carried out pursuant to Art. 28 GDPR without corresponding instructions by the client, e.g. definite contract design, separate instructions in text form, careful selection of service providers, follow-up controls. |