

**Mustervertrag zur
Auftragsverarbeitung
gemäß Art. 28
Datenschutzgrundverordnu
ng (DSGVO)**

Vereinbarung

zwischen dem/der

.....

.....

- Verantwortlicher – nachstehend
Auftraggeber genannt –
und dem/der

.....

.....

Questionmark GmbH

- Auftragsverarbeiter – nachstehend
Auftragnehmer genannt

Hinweis

„Die einzelnen Festlegungen nach Art. 28 Abs. 3 DS-GVO sollten vollständig in die Vereinbarung übernommen und wie eine Checkliste abgearbeitet werden. Die für das konkrete Dienstleistungsverhältnis zutreffenden Alternativen sollten angekreuzt werden. Leerfelder sind ggf. entsprechend des konkreten Auftrags auszufüllen. Vergütungs- und Haftungsregelungen zu den einzelnen

**Processing in accordance
with Article 28 General Data
Protection Regulation
(GDPR)**

Agreement

between

.....

.....

- the Controller – hereinafter
referred to as the Client –
and

.....

.....

Questionmark GmbH

- the Processor – hereinafter
referred to as the Supplier

Please Note

The specific provisions according to Article 28 Paragraph 3 GDPR should be incorporated into the Agreement in their entirety and be used as a Checklist. The alternatives applicable for the specific service relationship should be ticked. Empty fields are to be filled in as applicable to the specific requirements of each individual Order or Contract. Systems of payment and liability

Leistungen des Auftragnehmers sollten im Hauptvertrag vereinbart werden.“

conditions concerning the specific services of the Supplier should be agreed in the main contract.

1. Gegenstand und Dauer des Auftrags

(1) Gegenstand

☒ Der Gegenstand des Auftrags ergibt sich aus der Leistungsvereinbarung vom, auf die hier verwiesen wird (im Folgenden Leistungsvereinbarung).

oder

- ☐ Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer:
.....
..... (Definition der Aufgaben)

(2) Dauer

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

- ☐ Der Auftrag wird zur einmaligen Ausführung erteilt.

oder

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

oder

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

1. Subject matter and duration of the Order or Contract

(1) Subject matter

☒ The Subject matter of the Order or Contract results from the Service Agreement dated, which is referred to here (hereinafter referred to as Service Agreement).

or

- ☐ The Subject matter of the Order or Contract regarding the processing of data is the execution of the following services or tasks by the Supplier
.....
..... (Definition of the services or tasks)

(2) Duration

☒ The duration of this Order or Contract corresponds to the duration of the Service Agreement.

- ☐ The Order or Contract will be authorised for one time execution only.

or

- ☐ The Duration of this Contract is limited to

or

- ☐ The Contract is authorised for an unlimited period and can be cancelled by either Party with a notice period of.....(time period) to(deadline) . This does not prejudice the right to termination of the contract without notice.

2. Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten

☒ Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind konkret beschrieben in der Leistungsvereinbarung vom

oder

- ☐ Nähere Beschreibung des Auftragsgegenstandes im Hinblick auf Art und Zweck der Aufgaben des Auftragnehmers:
.....

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. Der Lieferant wird hiermit ermächtigt, Daten an einen Staat, der kein Mitgliedstaat der EU oder des EWR ist, zur Verarbeitung zu übergeben, sofern ein angemessener Schutz durch einen der folgenden Mechanismen erreicht wird. Das angemessene Schutzniveau in

☒ ist festgestellt durch einen Angemessenheitsbeschluss der Kommission (Art. 45 Abs. 3 DS-GVO);

2. Specification of the Order or Contract Details

(1) Nature and Purpose of the intended Processing of Data

☒ Nature and Purpose of Processing of personal data by the Supplier for the Client are precisely defined in the Service Agreement dated

or

- ☐ Detailed description of the Subject Matter with regard to the Nature and Purpose of the services provided by the

Supplier:

The undertaking of the contractually agreed Processing of Data shall be carried out exclusively within a Member State of the European Union (EU) or within a Member State of the European Economic Area (EEA). Each and every Transfer of Data to a State which is not a Member State of either the EU or the EEA requires the prior agreement of the Client and shall only occur if the specific Conditions of Article 44 et seq. GDPR have been fulfilled. The Supplier is hereby authorized to transfer Data to a State which is not a Member State of the EU or EEA for Processing provided an adequate level of protection is used by means of one of the following mechanisms

☒ has been decided by the European Commission (Article 45 Paragraph 3 GDPR);

☒ is the result of Standard Data Protection Clauses (Article 46

☒ wird hergestellt durch Standarddatenschutzklauseln (Art. 46 Abs. 2 litt. c und d DS-GVO);

☒ wird hergestellt durch genehmigte Verhaltensregeln (Artt. 46 Abs. 2 lit. e i.V.m. 40 DS-GVO);

☒ wird hergestellt durch einen genehmigten Zertifizierungsmechanismus (Artt. 46 Abs. 2 lit. f i.V.m. 42 DS-GVO).

Paragraph 2 Points c and d GDPR);

☒ is the result of approved Codes of Conduct (Article 46 Paragraph 2 Point e in conjunction with Article 40 GDPR);

☒ is the result of an approved Certification Mechanism. (Article 46 Paragraph 2 Point f in conjunction with Article 42 GDPR).

(2) Art der Daten

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

Oder

☒ Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien, die unter der alleinigen Kontrolle des Kunden stehen und die die in Artikel 4 DSGVO genannten umfassen (Aufzählung/Beschreibung der Datenkategorien)

- ☐ Personenstammdaten
- ☐ Kommunikationsdaten (z.B. Telefon, E-Mail)
- ☐ Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- ☐ Kundenhistorie
- ☐ Vertragsabrechnungs- und Zahlungsdaten
- ☐ Planungs- und Steuerungsdaten

(2) Type of Data

- ☐ The type of personal data used is precisely defined in the Service Agreement under:.....

or

☒ The Subject Matter of the processing of personal data comprises the following data types/categories, which are within the sole control of Client and include those specified by Article 4 GDPR (List/Description of the Data Categories)

- ☐ Personal Master Data (Key Personal Data)
- ☐ Contact Data
- ☐ Key Contract Data (Contractual/Legal Relationships, Contractual or Product Interest)
- ☐ Customer History
- ☐ Contract Billing and Payments Data
- ☐ Disclosed Information (from third parties, e.g. Credit

- ☐ Auskunftangaben (von Dritten, z.B. Auskunftsteilen, oder aus öffentlichen Verzeichnissen)
- ☐ Sonstige ... (Bitte präzisieren Sie diese hier)

(3) Kategorien betroffener Personen

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

Oder

☒ Die Kategorien der durch die Verarbeitung betroffenen Personen sind in der alleinigen Kontrolle des Kunden und umfassen in der Regel:

- ☐ Kunden
- ☐ Interessenten
- ☒ Abonnenten
- ☒ Beschäftigte
- ☒ Lieferanten
- ☐ Handelsvertreter
- ☐ Ansprechpartner
- ☒ Sonstige: Studenten, Potenzielle Auftragnehmer und andere Bewertungsteilnehmer

Reference Agencies or from Public Directories...

- ☐ Other:... (Please specify)

(3) Categories of Data Subjects

- ☐ The Categories of Data Subjects are precisely defined in the Service Agreement under:.....

or

☒ The Categories of Data Subjects are within the sole control of Client and typically comprise:

- ☐ Customers
- ☐ Potential Customers
- ☒ Subscribers
- ☒ Employees
- ☒ Suppliers
- ☐ Authorised Agents
- ☐ Contact Persons
- ☒ Other:.....students, contractors candidates and other assessment participants (Please specify)

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

3. Technical and Organisational Measures

(1) Before the commencement of processing, the Supplier shall document the execution of the necessary Technical and Organisational Measures, set out in advance of the awarding of the Order or Contract, specifically with regard to the detailed execution of the contract, and shall present these documented measures to the Client for inspection. Upon acceptance by the Client, the

Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen. Die angegebenen Maßnahmen sind in Anlage 1 aufgeführt.

(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

documented measures become the foundation of the contract. Insofar as the inspection/audit by the Client shows the need for amendments, such amendments shall be implemented by mutual agreement. The specified measures are referred to in Appendix 1.

(2) The Supplier shall establish the security in accordance with Article 28 Paragraph 3 Point c, and Article 32 GDPR in particular in conjunction with Article 5 Paragraph 1, and Paragraph 2 GDPR. The measures to be taken are measures of data security and measures that guarantee a protection level appropriate to the risk concerning confidentiality, integrity, availability and resilience of the systems. The state of the art, implementation costs, the nature, scope and purposes of processing as well as the probability of occurrence and the severity of the risk to the rights and freedoms of natural persons within the meaning of Article 32 Paragraph 1 GDPR must be taken into account. [Details in Appendix 1]

(3) The Technical and Organisational Measures are subject to technical progress and further development. In this respect, it is permissible for the Supplier to implement alternative adequate measures. In so doing, the security level of the defined measures must not be reduced. Substantial changes must be documented.

4. Rectification, restriction and erasure of data

(1) The Supplier may not on its own authority rectify, erase or restrict the processing of data that is being processed on behalf of the Client, but only on documented instructions from the Client.

eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

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

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.
 - ☐ Dessen Kontaktdaten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt. Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt.
 - ☐ Als Datenschutzbeauftragte(r) ist beim Auftragnehmer Herr/Frau [Eintragen: Vorname, Name, Organisationseinheit, Telefon, E-Mail]

Insofar as a Data Subject contacts the Supplier directly concerning a rectification, erasure, or restriction of processing, the Supplier will immediately forward the Data Subject's request to the Client.

(2) Insofar as it is included in the scope of services, the erasure policy, 'right to be forgotten', rectification, data portability and access shall be ensured by the Supplier in accordance with documented instructions from the Client without undue delay.

5. Quality assurance and other duties of the Supplier

In addition to complying with the rules set out in this Order or Contract, the Supplier shall comply with the statutory requirements referred to in Articles 28 to 33 GDPR; accordingly, the Supplier ensures, in particular, compliance with the following requirements:

- a) ☒ Appointed Data Protection Officer, who performs his/her duties in compliance with Articles 38 and 39 GDPR.
 - ☐ The Client shall be informed of his/her contact details for the purpose of direct contact. The Client shall be informed immediately of any change of Data Protection Officer.
 - ☐ The Supplier has appointed Mr/Ms [enter: given name, surname, organisational unit, telephone, e-mail] as Data Protection Officer. The Client shall be informed immediately of any

bestellt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

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

- b) ☐ Der Auftragnehmer ist nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet. Als Ansprechpartner beim Auftragnehmer wird Herr/Frau [Eintragen: Vorname, Name, Organisationseinheit, Telefon, E-Mail] benannt.
- c) ☐ Da der Auftragnehmer seinen Sitz außerhalb der Union hat, benennt er folgenden Vertreter nach Art. 27 Abs. 1 DSGVO in der Union: [Eintragen: Vorname, Name, Organisationseinheit, Telefon, E-Mail].
- d) Die Wahrung der Vertraulichkeit gemäß Artt. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 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 und dem Hauptvertrag

change of Data Protection Officer.

☒ His/Her current contact details are always available and easily accessible on the website of the Supplier.

- b) ☐ The Supplier is not obliged to appoint a Data Protection Officer. Mr/Ms [enter: given name, surname, organisational unit, telephone, e-mail] is designated as the Contact Person on behalf of the Supplier.
- c) ☐ As the Supplier is established outside the EU & EEA it designates the following Representative within the Union pursuant to Article 27 Paragraph 1 GDPR: Mr/Ms [enter: given name, surname, organisational unit, telephone, e-mail].
- d) Confidentiality in accordance with Article 28 Paragraph 3 Sentence 2 Point b, Articles 29 and 32 Paragraph 4 GDPR. The Supplier entrusts only such employees with the data processing outlined in this contract who have been bound to confidentiality and have previously been familiarised with the data protection provisions relevant to their work. The Supplier and any person acting under its authority who has access to personal data, shall not process that data unless on instructions from the Client, which includes the powers granted in this contract and the main contract, unless required to do so by law.

- eingewäumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.
- e) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Artt. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO [Einzelheiten in Anlage 1].
 - f) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
 - g) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.
 - h) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.
 - i) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen
- e) Implementation of and compliance with all Technical and Organisational Measures necessary for this Order or Contract in accordance with Article 28 Paragraph 3 Sentence 2 Point c, Article 32 GDPR [details in Appendix 1].
 - f) The Client and the Supplier shall cooperate, on request, with the supervisory authority in performance of its tasks.
 - g) The Client shall be informed immediately of any inspections and measures conducted by the supervisory authority, insofar as they relate to this Order or Contract. This also applies insofar as the Supplier is under investigation or is party to an investigation by a competent authority in connection with infringements to any Civil or Criminal Law, or Administrative Rule or Regulation regarding the processing of personal data in connection with the processing of this Order or Contract.
 - h) Insofar as the Client is subject to an inspection by the supervisory authority, an administrative or summary offence or criminal procedure, a liability claim by a Data Subject or by a third party or any other claim in connection with the Order or Contract data processing by the Supplier, the Supplier shall make every effort to support the Client.
 - i) The Supplier shall periodically monitor the internal processes and the Technical and Organizational Measures to ensure that

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.

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

processing within his area of responsibility is in accordance with the requirements of applicable data protection law and the protection of the rights of the data subject.

- j) Verifiability of the Technical and Organisational Measures conducted by the Client as part of the Client's supervisory powers referred to in item 7 of this contract.

6. Unterauftragsverhältnisse

(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.

(2) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

6. Subcontracting

(1) Subcontracting for the purpose of this Agreement is to be understood as meaning services which relate directly to the provision of the principal service. This does not include ancillary services, such as telecommunication services, postal / transport services, maintenance and user support services or the disposal of data carriers, as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing equipment. The Supplier shall, however, be obliged to make appropriate and legally binding contractual arrangements and take appropriate inspection measures to ensure the data protection and the data security of the Client's data, even in the case of outsourced ancillary services.

(2) The Supplier may commission subcontractors (additional contract processors) only after prior explicit written or documented consent from the Client.

a) ☐ Eine Unterbeauftragung ist unzulässig.

b) ☒ Der Auftraggeber stimmt der Beauftragung der Unterauftragnehmer, die unter www.questionmark.com/go/eu-od-subprocessors (oder eine solche Ersatz-URL, die der Lieferant später schriftlich mitteilen kann) aufgelistet sind zu, unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO:

c) ☐ Die Auslagerung auf Unterauftragnehmer oder

☒ der Wechsel des bestehenden Unterauftragnehmers sind zulässig, soweit:

- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Form einer E-Mail anzeigt, wenn die Liste gemäß (b) oben aktualisiert wird, um sie dem Kunden zur Verfügung zu stellen und
- der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
- eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde gelegt wird.

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

(4) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der

a) ☐ Subcontracting is not permitted.

b) ☒ The Client agrees to the commissioning of the subcontractors listed at www.questionmark.com/go/eu-od-subprocessors (or such replacement URL as Supplier may later advise in writing) in accordance with Article 28 paragraphs 2-4 GDPR:

c) ☐ Outsourcing to subcontractors or

☒ Changing the existing subcontractor are permissible when:

- The Supplier submits such an outsourcing to a subcontractor to the Client in writing or in email form when updating the list referred to in (b) above to provide Client with appropriate advance notice; and
- The Client has not objected to the planned outsourcing in writing or in text form by the date of handing over the data to the Supplier; and
- The subcontracting is based on a contractual agreement in accordance with Article 28 paragraphs 2-4 GDPR.

(3) The transfer of personal data from the Client to the subcontractor and the subcontractors commencement of the data processing shall only be undertaken after compliance with all requirements has been achieved.

(4) If the subcontractor provides the agreed service outside the EU/EEA,

EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

(5) Eine weitere Auslagerung durch den Unterauftragnehmer

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

sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen, gemäß Artikel 28 Absatz 3 DSGVO und gemäß Artikel 28 Absatz 4 DSGVO.

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 erfolgen durch

the Supplier shall ensure compliance with EU Data Protection Regulations by appropriate measures. The same applies if service providers are to be used within the meaning of Paragraph 1 Sentence 2.

(5) Further outsourcing by the subcontractor

- ☐ Is not permitted;
- ☐ Requires the express consent of the main Client (at the minimum in text form);
- ☒ Requires the express consent of the Supplier (at the minimum in text form);

All contractual provisions in the contract chain shall be communicated to and agreed with each and every additional subcontractor in accordance with Article 28(3) GDPR, as required by Article 28(4) GDPR.

7. Supervisory powers of the Client

(1) The Client has the right, after consultation with the Supplier, to carry out inspections or to have them carried out by an auditor to be designated in each individual case. It has the right to convince itself of the compliance with this agreement by the Supplier in his business operations by means of random checks, which are ordinarily to be announced in good time.

(2) The Supplier shall ensure that the Client is able to verify compliance with the obligations of the Supplier in accordance with Article 28 GDPR. The Supplier undertakes to give the Client the necessary information on request and, in particular, to demonstrate the execution of the Technical and Organizational Measures.

(3) Evidence of such measures, which concern not only the specific Order or Contract, may be provided by

- ☒ 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);
- ☒ eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundsatz).

(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

- ☒ Compliance with approved Codes of Conduct pursuant to Article 40 GDPR;
- ☒ Certification according to an approved certification procedure in accordance with Article 42 GDPR;
- ☒ Current auditor's certificates, reports or excerpts from reports provided by independent bodies (e.g. auditor, Data Protection Officer, IT security department, data privacy auditor, quality auditor)
- ☒ A suitable certification by IT security or data protection auditing (e.g. according to BSI-Grundsatz (IT Baseline Protection certification developed by the German Federal Office for Security in Information Technology (BSI)) or ISO/IEC 27001).

(4) The Supplier may claim remuneration for enabling Client inspections.

8. Communication in the case of infringements by the Supplier

(1) The Supplier shall assist the Client in complying with the obligations concerning the security of personal data, reporting requirements for data breaches, data protection impact assessments and prior consultations, referred to in Articles 32 to 36 of the GDPR. These include:

- a) Ensuring an appropriate level of protection through Technical and Organizational Measures that take into account the circumstances and purposes of the processing as well as the projected probability and severity of a possible

Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen

infringement of the law as a result of security vulnerabilities and that enable an immediate detection of relevant infringement events.

- 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,

- b) The obligation to report a personal data breach immediately to the Client
- c) The duty to assist the Client with regard to the Client's obligation to provide information to the Data Subject concerned and to immediately provide the Client with all relevant information in this regard.
- d) Supporting the Client with its data protection impact assessment
- e) Supporting the Client with regard to prior consultation of the supervisory authority

(2) The Supplier may claim compensation for support services which are not included in the description of the services and which are not attributable to failures on the part of the Supplier.

9. Authority of the Client to issue instructions

(1) The Client shall immediately confirm oral instructions (at the minimum in text form).

(2) The Supplier shall inform the Client immediately if he considers that an

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.

instruction violates Data Protection Regulations. The Supplier shall then be entitled to suspend the execution of the relevant instructions until the Client confirms or changes them.

10. Deletion and return of personal data

(1) Copies or duplicates of the data shall never be created without the knowledge of the Client, with the exception of back-up copies as far as they are necessary to ensure orderly data processing, as well as data required to meet regulatory requirements to retain data.

(2) After conclusion of the contracted work, or earlier upon request by the Client, at the latest upon termination of the Service Agreement, the Supplier shall hand over to the Client or – subject to prior consent – destroy all documents, processing and utilization results, and data sets related to the contract that have come into its possession, in a data-protection compliant manner. The same applies to any and all connected test, waste, redundant and discarded material. The log of the destruction or deletion shall be provided on request.

(3) Documentation which is used to demonstrate orderly data processing in accordance with the Order or Contract shall be stored beyond the contract duration by the Supplier in accordance with the respective retention periods. It may hand such documentation over to the Client at the end of the contract duration to relieve the Supplier of this contractual obligation.

Unterschrieben von:

Signed by:

Unterschrieben von:

Signed by:

Anlage 1 – Technisch-organisatorische Maßnahmen

Die Maßnahmen des Auftragnehmer finden sie unter:

www.questionmark.com/go/eu-od-measures

Appendix 1 – Technical and Organisational Measures

The measures of Supplier are found at:

www.questionmark.com/go/eu-od-measures