Rahmenvereinbarung

über agile Softwareentwicklungsleistungen für die digitale zdi-Systemlandschaft

mit dem Vertrag zur Auftragsverarbeitung als Anlage – Entwurf, Bestandteil der Vergabeunterlagen

zwischen

matrix Gesellschaft für Beratung in Wirtschaft, Politik und Verwaltung mbH & Co. KG, Düsseldorfer Straße 16, 40699 Erkrath

– als vom Land Nordrhein-Westfalen beauftragte zdi-Landesgeschäftsstelle –

(nachfolgend „Auftraggeberin“)

und

[Name und Anschrift des Auftragnehmers]

(nachfolgend „Auftragnehmer“)

Die Parteien schließen auf Grundlage des Vergabeverfahrens „Rahmenvereinbarung über agile Softwareentwicklungsleistungen für die digitale zdi-Systemlandschaft“ folgende Rahmenvereinbarung:

§ 1 Gegenstand

(1) Gegenstand dieser Rahmenvereinbarung sind agile Softwareentwicklungsleistungen für die digitale zdi-Systemlandschaft, insbesondere Weiterentwicklung, Neuentwicklung, Integration, Migration, Wartung und Support sowie technische Betriebsunterstützung, nach Maßgabe der Leistungsbeschreibung.

(2) Die Rahmenvereinbarung hat überwiegend dienstvertraglichen Charakter. Konkrete Leistungen werden durch Leistungsfreigaben nach § 4 beauftragt. Aus der Rahmenvereinbarung allein entsteht keine Pflicht der Auftraggeberin, Leistungen abzurufen.

§ 2 Vertragsbestandteile und Rangfolge

(1) Vertragsbestandteile sind in folgender Rangfolge:

1. diese Rahmenvereinbarung,

2. der Vertrag zur Auftragsverarbeitung (AVV) in der Anlage, der in Fragen des Datenschutzes allen anderen Bestandteilen vorgeht,
3. die Leistungsbeschreibung mit den Anlagen A und C in der Fassung der Vergabeunterlagen einschließlich der Antworten auf Bieterfragen,
4. das Preisblatt des Auftragnehmers,
5. das Angebot des Auftragnehmers mit Angebotskonzept, Angebotsformular, Referenzen und Profilen des Kernteams.

(2) Leistungsfreigaben konkretisieren die Leistungen im Rahmen dieser Bestandteile. Sie ändern die Rahmenvereinbarung nur, soweit die Leistungsbeschreibung dies vorsieht.

(3) Allgemeine Geschäftsbedingungen des Auftragnehmers gelten nicht, auch wenn er auf sie verweist.

§ 3 Laufzeit und Kündigung

(1) Die Rahmenvereinbarung tritt mit dem Zuschlag in Kraft. Ab diesem Zeitpunkt können Leistungen abgerufen werden (Leistungsbeginn). Leistungen mit Zugriff auf personenbezogene Daten können erst abgerufen werden, wenn das Land Nordrhein-Westfalen dem Einsatz des Auftragnehmers als weiterer Auftragsverarbeiter zugestimmt hat (§ 1 Abs. 3 AVV).

(2) Leistungsfreigaben können bis zum 31. Dezember 2030 erteilt werden, danach nur noch, soweit sie ausschließlich der geordneten Übergabe, der Fehlerbehebung oder der Abwicklung bereits beauftragter Leistungen dienen. Die Rahmenvereinbarung endet mit Ablauf des 28. Februar 2031, ohne dass es einer Kündigung bedarf (Abschnitt 2.2 der Leistungsbeschreibung).

(3) Für die ordentliche und die außerordentliche Kündigung, die Folgen einer Kündigung für erteilte Leistungsfreigaben und die Übergabe bei Vertragsende gelten die Abschnitte 2.3 und 13 der Leistungsbeschreibung. Kündigungen bedürfen der Textform.

(4) Versagt oder widerruft das Land die Zustimmung nach § 1 Abs. 3 AVV, kann jede Partei die Rahmenvereinbarung außerordentlich kündigen.

§ 4 Leistungsfreigaben, Kapazität und Gesamthöchstwert

(1) Die Auftraggeberin beauftragt Leistungen durch Leistungsfreigaben in Textform nach Abschnitt 8.2 und mit den Mindestangaben nach Anlage A der Leistungsbeschreibung; freigabeberechtigt sind die dort genannten

Personen. Eine Freigabe im vereinbarten Projektmanagementsystem genügt der Textform, wenn die freigebende Person und der Zeitpunkt der Freigabe erkennbar und dauerhaft nachvollziehbar sind.

(2) Planung, Kapazitätsvorschau, Sprintplanung und die bereitzuhaltenden Kapazitäten (höchstens 120 Stunden je Monat) richten sich nach Abschnitt 8.1 der Leistungsbeschreibung.

(3) Der Gesamthöchstwert beträgt 415.000 Euro netto; eine Mindestabnahme besteht nicht (Abschnitt 2.4 der Leistungsbeschreibung).

§ 5 Vergütung, Rechnungsstellung und Zahlung

(1) Vergütet wird der tatsächlich erbrachte und nachgewiesene Aufwand zu den Stundensätzen des Preisblatts nach Abschnitt 2.5 der Leistungsbeschreibung; dort ist auch geregelt, welche Kosten mit den Sätzen abgegolten sind. Präsenztermine über die dort genannten vier je Kalenderjahr hinaus finden nur nach Vereinbarung in der Leistungsfreigabe statt; Reisezeiten und Reisekosten werden dafür nur vergütet, soweit die Leistungsfreigabe dies ausdrücklich vorsieht.

(2) Der Auftragnehmer rechnet monatlich mit prüffähigen Leistungsnachweisen nach Abschnitt 10.5 der Leistungsbeschreibung ab und ordnet die Stunden der jeweiligen Leistungsfreigabe, Rolle und Tätigkeit zu. Die Budgetobergrenze einer Leistungsfreigabe darf ohne ergänzende Freigabe nicht überschritten werden.

(3) Rechnungen sind innerhalb von 30 Tagen nach Eingang einer prüffähigen Rechnung zur Zahlung fällig. Die Umsatzsteuer wird in der jeweils gesetzlichen Höhe zusätzlich vergütet.

(4) Rechnungen sind als elektronische Rechnung im Sinne des § 14 UStG, etwa im Format XRechnung oder ZUGFeRD, an billing@matrix-gmbh.de, Düsseldorfer Straße 16, 40699 Erkrath, zu übermitteln.

§ 6 Leistungserbringung, Personal und Unterauftragnehmer

(1) Der Auftragnehmer erbringt die Leistungen eigenverantwortlich nach dem Stand der Technik und den Anforderungen der Leistungsbeschreibung, insbesondere den verbindlichen Mindestanforderungen nach Abschnitt 11.1 und dem Technologie-Stack nach Abschnitt 3.4.

(2) Er setzt das mit dem Angebot benannte Kernteam ein. Austausch und Vertretung, einschließlich der Benennung der Vertretungen nach dem Zuschlag, richten sich nach Abschnitt 15.3 der Leistungsbeschreibung.

(3) Gegenüber seinem Personal ist allein der Auftragnehmer weisungsbefugt. Die Auftraggeberin steuert die Leistungen über Leistungsfreigaben, Backlog und Priorisierung, erteilt dem Personal des Auftragnehmers aber keine arbeitsrechtlichen Weisungen. Eine Eingliederung in die Arbeitsorganisation der Auftraggeberin findet nicht statt. Fachliche Abstimmungen laufen über die benannten Ansprechpersonen beider Seiten.

(4) Unterauftragnehmer setzt der Auftragnehmer nur mit vorheriger Zustimmung der Auftraggeberin in Textform ein; die mit dem Angebot benannten Unterauftragnehmer gelten mit dem Zuschlag als genehmigt. Der Auftragnehmer bleibt für deren Leistungen verantwortlich und gibt ihnen die Pflichten aus dieser Rahmenvereinbarung, insbesondere zur Vertraulichkeit (Abschnitt 14 der Leistungsbeschreibung), weiter. Freie Mitarbeiterinnen und Mitarbeiter gelten als Unterauftragnehmer. Unterauftragnehmer erhalten keinen Zugriff auf personenbezogene Daten der Auftraggeberin; weitere Auftragsverarbeiter sind ausgeschlossen (§ 5 AVV).

(5) Beide Parteien benennen eine verantwortliche Ansprechperson und eine Vertretung.

(6) Fehler in Arbeitsergebnissen des Auftragnehmers, die auf einer Verletzung der Anforderungen nach Absatz 1 beruhen und innerhalb von sechs Monaten nach Bereitstellung in der Produktivumgebung gemeldet werden, behebt er ohne gesonderte Vergütung, es sei denn, er hat die Pflichtverletzung nicht zu vertreten.

§ 7 Mitwirkung der Auftraggeberin

Die Auftraggeberin stellt die Product Ownership (Abschnitt 6.2 der Leistungsbeschreibung), die erforderlichen Informationen sowie Zugänge zu Repositories, Umgebungen und Systemen bereit; Hosting und Infrastruktur verbleiben bei ihr (Abschnitt 6.1). Fehlen Mitwirkungen oder reichen sie nicht aus, zeigt der Auftragnehmer dies unverzüglich in Textform an.

§ 8 Rechte an den Arbeitsergebnissen

(1) Für die Rechte an den Arbeitsergebnissen, den Einsatz von Open-Source- und Drittkomponenten sowie die Übergabe von Quellcode und Dokumentation gilt Abschnitt 12 der Leistungsbeschreibung.

(2) Der Auftragnehmer stellt die Auftraggeberin von Ansprüchen Dritter wegen der Verletzung von Schutzrechten durch die Arbeitsergebnisse einschließlich

der angemessenen Kosten der Rechtsverteidigung frei, soweit er die Verletzung zu vertreten hat.

(3) Für KI-gestützt erstellte Bestandteile gilt Abschnitt 12 der Leistungsbeschreibung entsprechend, auch soweit an ihnen keine Schutzrechte entstehen. Der Auftragnehmer stellt sicher, dass die Nutzungsbedingungen der eingesetzten KI-Dienste dieser Nutzung nicht entgegenstehen.

§ 9 Datenschutz, Vertraulichkeit und KI-Dienste

Für Datenschutz, Vertraulichkeit und die Nutzung von KI-Diensten gilt Abschnitt 14 der Leistungsbeschreibung. Die Parteien schließen mit dieser Rahmenvereinbarung den Vertrag zur Auftragsverarbeitung in der Anlage; er ist Bestandteil dieser Rahmenvereinbarung.

§ 10 Haftung

(1) Die Parteien haften einander nach den gesetzlichen Vorschriften, soweit nachfolgend nichts anderes bestimmt ist.

(2) Bei einfacher Fahrlässigkeit haften die Parteien nur bei Verletzung einer wesentlichen Vertragspflicht, also einer Pflicht, deren Erfüllung die ordnungsgemäße Durchführung des Vertrags überhaupt erst ermöglicht und auf deren Einhaltung die andere Partei regelmäßig vertrauen darf. Die Haftung ist dann auf den vorhersehbaren, vertragstypischen Schaden begrenzt.

(3) Die Beschränkung nach Absatz 2 gilt nicht bei Vorsatz und grober Fahrlässigkeit, für Schäden aus der Verletzung des Lebens, des Körpers oder der Gesundheit, bei Übernahme einer Garantie, nach dem Produkthaftungsgesetz sowie für Ansprüche wegen Verstößen gegen den AVV oder datenschutzrechtliche Pflichten.

§ 11 Haftpflichtversicherung

Der Auftragnehmer unterhält für die Dauer der Rahmenvereinbarung einschließlich des Abwicklungszeitraums eine Berufs- oder Betriebshaftpflichtversicherung mit einer Deckungssumme von mindestens 1.000.000 Euro je Schadensfall für Personen- und Sachschäden sowie für reine Vermögensschäden. Er weist den Versicherungsschutz bis zum Leistungsbeginn und auf Verlangen jederzeit nach. Seine Haftung ist nicht auf die Deckungssumme beschränkt.

§ 12 Mindestlohn und weitere Pflichten

(1) Der Auftragnehmer zahlt seinen Beschäftigten mindestens den gesetzlichen Mindestlohn und verpflichtet seine Unterauftragnehmer entsprechend. Er stellt die Auftraggeberin von Ansprüchen nach § 13 MiLoG frei, die auf Verstößen des Auftragnehmers oder seiner Unterauftragnehmer beruhen.

(2) Werden Erklärungen, die der Auftragnehmer in Teil C des Angebotsformulars abgegeben hat, während der Vertragslaufzeit unzutreffend, teilt er dies unverzüglich in Textform mit. Waren oder werden die Erklärungen zu Ausschlussgründen, zu Art. 5k der Verordnung (EU) Nr. 833/2014 oder zur Schutzklausel (Nummer C.5 des Angebotsformulars) unzutreffend, kann die Auftraggeberin die Rahmenvereinbarung außerordentlich kündigen.

§ 13 Schlussbestimmungen

(1) Änderungen und Ergänzungen dieser Rahmenvereinbarung bedürfen der Textform (§ 126b BGB). Für Leistungsfreigaben gilt § 4.

(2) Es gilt das Recht der Bundesrepublik Deutschland. Gerichtsstand ist, soweit gesetzlich zulässig, der Sitz der Auftraggeberin.

(3) Sollte eine Bestimmung unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.

Für die Auftraggeberin	Für den Auftragnehmer
matrix Gesellschaft für Beratung in Wirtschaft, Politik und Verwaltung mbH & Co. KG	[Firma]
Ort, Datum:	Ort, Datum:
Name, Funktion:	Name, Funktion:

Anlage: Vertrag zur Auftragsverarbeitung nach Art. 28 DSGVO mit Anlage 1 (technische und organisatorische Maßnahmen)

Anlage: Vertrag zur Auftragsverarbeitung nach Art. 28 DSGVO

Dieser Vertrag ist Anlage der vorstehenden Rahmenvereinbarung zwischen der Auftraggeberin und dem Auftragnehmer. Verantwortlicher für die Verarbeitung ist das Land Nordrhein-Westfalen, vertreten durch das Ministerium für Kultur und Wissenschaft (nachfolgend „Land“). Die Auftraggeberin verarbeitet die Daten als Auftragsverarbeiterin des Landes auf Grundlage eines Vertrags zur Auftragsverarbeitung mit dem Land (nachfolgend „Vertrag mit dem Land“). Der Auftragnehmer wird als weiterer Auftragsverarbeiter eingesetzt (Art. 28 Abs. 2 und 4 DSGVO). Dieser Vertrag legt ihm mindestens die Datenschutzpflichten auf, die im Vertrag mit dem Land vereinbart sind.

§ 1 Gegenstand und Dauer

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag der Auftraggeberin im Rahmen der Rahmenvereinbarung. Dieser Vertrag konkretisiert die Pflichten der Parteien nach Art. 28 DSGVO.

(2) Er gilt für die Dauer der Rahmenvereinbarung einschließlich des Abwicklungszeitraums und darüber hinaus, solange der Auftragnehmer personenbezogene Daten der Auftraggeberin verarbeitet. Die Befugnis zur Verarbeitung endet spätestens mit dem Ende des Vertrags mit dem Land oder mit dem Widerruf der Zustimmung des Landes; die Auftraggeberin teilt dies unverzüglich mit, und § 8 gilt.

(3) Der Einsatz des Auftragnehmers als weiterer Auftragsverarbeiter bedarf der vorherigen schriftlichen Zustimmung des Landes (§ 7 Abs. 1 des Vertrags mit dem Land). Die Auftraggeberin holt sie ein und teilt sie dem Auftragnehmer in Textform mit. Bis dahin verarbeitet der Auftragnehmer keine personenbezogenen Daten; Leistungen ohne Zugriff auf solche Daten sind schon vorher möglich.

§ 2 Art, Zweck und Umfang der Verarbeitung

(1) Art der Verarbeitung: Entwicklung, Test, Bereitstellung, Wartung, Fehleranalyse und technische Betriebsunterstützung der in Anlage C der Leistungsbeschreibung beschriebenen Systeme sowie Migration von Daten. Der Auftragnehmer erhält dabei Zugriff auf Produktivsysteme und Datenbanken der Auftraggeberin.

(2) Zweck: Erbringung der Leistungen nach der Rahmenvereinbarung, insbesondere Betrieb und Weiterentwicklung der digitalen zdi-Systemlandschaft für die Arbeit der zdi-Netzwerke und der Landesgeschäftsstelle.

(3) Betroffene Systeme: mein.zdi.nrw, das Data Warehouse mit Airbyte und Apache Superset, Authentik, Open WebUI, Schnittstellen zu bsomint.de, die zdi-Community-Plattform bis zu ihrer Außerbetriebnahme, die öffentliche Website zdi.nrw bei Relaunch und Migration sowie künftige Anwendungen nach Abschnitt 4 und Anlage C.7 der Leistungsbeschreibung, etwa die Kurs- und Angebotsübersicht, die Wettbewerbsplattform und das Befragungstool. Für künftige Anwendungen, neue Datenarten oder weitere Gruppen betroffener Personen erteilt die Auftraggeberin Leistungsfreigaben erst, wenn die Verarbeitung mit dem Land abgestimmt ist.

(4) Arten personenbezogener Daten:

- Kontakt- und Stammdaten, etwa Name, Funktion, Organisation, E-Mail-Adresse und Telefonnummer
- Nutzer- und Kontodaten, etwa Benutzerkennungen, Rollen sowie Gruppen- und Netzwerkzugehörigkeit
- Protokoll- und Nutzungsdaten, etwa Anmeldungen, Zeitstempel und technische Logs
- Monitoring- und Programmdaten mit Personenbezug, etwa Angaben zum Netzwerkpersonal und zu Ansprechpersonen von Partnern und Schulen
- Kurs-, Teilnahme- und Befragungsdaten einschließlich Angaben zu Dozierenden
- Daten von Schüler:innen einschließlich Minderjähriger, etwa Name, Schule, Klasse oder Jahrgangsstufe und Teilnahme
- Eingaben und Verläufe in den KI-Assistenten, soweit sie Personenbezug haben
- Nutzerinhalte und Kommunikationsdaten, etwa Profilangaben, Profilbilder, Beiträge und Nachrichten, insbesondere bei Migration und Außerbetriebnahme der zdi-Community-Plattform
- Buchungs- und Anmeldedaten zu Kursen und Wettbewerben
- Wettbewerbsdaten, etwa Team- und Schulzugehörigkeit, Beiträge, Bewertungen und Platzierungen
- Einwilligungserklärungen und Kontaktdaten von Erziehungsberechtigten

Besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO sind nach derzeitigem Stand nicht Gegenstand der Verarbeitung. Ändert sich das, passen die Parteien diesen Vertrag an.

(5) Kategorien betroffener Personen:

- Beschäftigte der Auftraggeberin und der Landesgeschäftsstelle
- Koordinator:innen und Beschäftigte der zdi-Netzwerke und der zdi-Schüler:innenlabore
- Ansprechpersonen von Partnerorganisationen, Schulen, Hochschulen, Unternehmen und Kommunen

- Lehrkräfte, Dozierende, Coaches und weitere Projektbeteiligte
- Schüler:innen und weitere Teilnehmende einschließlich Minderjähriger
- Nutzer:innen der Plattformen wie z.B. Mitarbeiter:innen des MKW
- Erziehungsberechtigte minderjähriger Teilnehmender
- Besucher:innen der öffentlichen Websites, soweit Formular- oder Protokolldaten verarbeitet werden

(6) Der Auftragnehmer verarbeitet Daten nur im erforderlichen Umfang. Produktivdaten mit Personenbezug übernimmt er nicht in Entwicklungs- oder Testumgebungen, es sei denn, sie sind anonymisiert oder die Auftraggeberin hat im Einzelfall in Textform zugestimmt.

§ 3 Weisungen

(1) Der Auftragnehmer verarbeitet personenbezogene Daten nur auf dokumentierte Weisung der Auftraggeberin, es sei denn, er ist nach dem Recht der Union oder eines Mitgliedstaats zur Verarbeitung verpflichtet (Art. 28 Abs. 3 Buchst. a DSGVO). In einem solchen Fall teilt er der Auftraggeberin diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Weisungen erfolgen in Textform; mündliche Weisungen bestätigt die Auftraggeberin unverzüglich in Textform; die Rahmenvereinbarung, dieser Vertrag und die Leistungsfreigaben gelten als Weisungen.

(2) Hält der Auftragnehmer eine Weisung für rechtswidrig, informiert er die Auftraggeberin unverzüglich. Er kann die Ausführung bis zur Bestätigung durch die Auftraggeberin aussetzen.

(3) Weisungsberechtigt sind die nach Abschnitt 8.2 der Leistungsbeschreibung freigabeberechtigten Personen sowie die Geschäftsführung der Auftraggeberin.

(4) Weisungen des Landes, die die Verarbeitung durch den Auftragnehmer betreffen, gibt die Auftraggeberin als eigene Weisungen weiter. Weisungsempfänger beim Auftragnehmer sind die nach § 6 Abs. 5 der Rahmenvereinbarung benannte Ansprechperson und ihre Vertretung.

(5) Der Auftragnehmer darf Daten nicht eigenmächtig berichtigen, löschen oder ihre Verarbeitung einschränken, sondern nur nach dokumentierter Weisung der Auftraggeberin.

§ 4 Pflichten des Auftragnehmers

(1) Er setzt nur Personen ein, die zur Vertraulichkeit verpflichtet und mit den datenschutzrechtlichen Anforderungen vertraut sind (Art. 28 Abs. 3 Buchst. b,

Art. 29 DSGVO). Er sorgt dafür, dass jede Person, die Zugriff auf personenbezogene Daten der Auftraggeberin erhalten soll, vor dem ersten Zugriff nach dem Verpflichtungsgesetz förmlich verpflichtet wird (§ 4 Abs. 5 des Vertrags mit dem Land); die Verpflichtung nimmt die zuständige Stelle des Landes vor. Die Auftraggeberin vereinbart die Termine, möglichst für mehrere Personen gemeinsam und per Videokonferenz (§ 1 Abs. 2 des Verpflichtungsgesetzes); der Auftragnehmer stellt die Personen dafür bereit. Vorher erhält die Person keinen Zugriff; das gilt auch für Vertretungen und neu eingesetzte Personen. Verzichtet das Land für die Beschäftigten des Auftragnehmers auf die förmliche Verpflichtung, genügt die Verpflichtung auf Vertraulichkeit nach Satz 1, die der Auftragnehmer selbst schriftlich vornimmt.

(2) Er trifft die technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO, die in Anlage 1 beschrieben sind und mindestens die dort genannten Mindestanforderungen erfüllen. Er überprüft sie regelmäßig und passt sie dem Stand der Technik an; das Schutzniveau darf dabei nicht sinken. Die Maßnahmen gewährleisten die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer. Die Daten der Auftraggeberin hält er von seinen sonstigen Datenbeständen technisch oder logisch getrennt; ausgenommen sind gemeinsam genutzte Infrastrukturkomponenten, die nur dem Transport der Daten dienen, etwa Proxy-Server oder Firewalls.

(3) Auf Systeme der Auftraggeberin greift er nur über personengebundene Konten zu, die die Auftraggeberin bereitstellt, und nutzt die Mehr-Faktor-Authentifizierung, soweit das System sie unterstützt. Zugangsdaten gibt er nicht weiter und legt sie nicht in Repositories ab. Nicht mehr benötigte Zugänge meldet er unverzüglich zur Sperrung.

(4) Er unterstützt die Auftraggeberin bei der Erfüllung der Rechte betroffener Personen (Art. 12 bis 22 DSGVO) und bei ihren Pflichten nach Art. 32 bis 36 DSGVO, insbesondere bei der Benachrichtigung betroffener Personen, bei Datenschutz-Folgenabschätzungen und bei der vorherigen Konsultation der Aufsichtsbehörde. Wendet sich eine betroffene Person unmittelbar an ihn, leitet er das Ersuchen unverzüglich an die Auftraggeberin weiter.

(5) Verletzungen des Schutzes personenbezogener Daten meldet er der Auftraggeberin unverzüglich, spätestens 24 Stunden nach Kenntnis, in Textform mit den Angaben nach Art. 33 Abs. 3 DSGVO, soweit sie verfügbar sind. Fehlende Angaben reicht er unverzüglich nach. Er stimmt die zu

treffenden Maßnahmen mit der Auftraggeberin ab und unterstützt sie bei Aufklärung und Behebung.

(6) Er führt ein Verzeichnis nach Art. 30 Abs. 2 DSGVO und benennt eine Ansprechperson für den Datenschutz sowie, soweit gesetzlich vorgeschrieben, seine Datenschutzbeauftragte oder seinen Datenschutzbeauftragten.

(7) Personenbezogene Daten der Auftraggeberin gibt er nicht in KI-Dienste ein, die er für seine eigene Leistungserbringung nutzt, und übermittelt sie nicht an solche Dienste (Abschnitt 14 der Leistungsbeschreibung). Betrieb, Wartung und Test der KI-Assistenten der Auftraggeberin nach einer Leistungsfreigabe bleiben unberührt.

§ 5 Keine weiteren Auftragsverarbeiter

(1) Der Vertrag mit dem Land lässt eine weitere Unterbeauftragung durch den Auftragnehmer nicht zu (§ 7 Abs. 4 dort). Der Auftragnehmer setzt deshalb keine weiteren Auftragsverarbeiter ein. Personenbezogene Daten der Auftraggeberin verarbeiten nur Personen, die ihm unterstellt sind (Art. 29 DSGVO); bei Bietergemeinschaften gilt das für jedes Mitglied.

(2) Unterauftragnehmer nach § 6 Abs. 4 der Rahmenvereinbarung, auch freie Mitarbeiterinnen und Mitarbeiter, sowie Unternehmen, auf deren Kapazitäten sich der Auftragnehmer beruft, erhalten keinen Zugriff auf personenbezogene Daten der Auftraggeberin. Leistungen mit Zugriff auf solche Daten, etwa Wartung, Support, Betriebsunterstützung und Migrationen, erbringen Beschäftigte des Auftragnehmers einschließlich ihm nach dem Arbeitnehmerüberlassungsgesetz überlassener Arbeitnehmerinnen und Arbeitnehmer.

(3) Personenbezogene Daten der Auftraggeberin verarbeitet er nur in den Systemen, die die Auftraggeberin dafür bereitstellt, und nicht in eigenen Diensten Dritter wie Ticket-, Chat- oder Cloud-Speicherdiensten. In Tickets, Fehlerberichten, Repositories und Dokumentation werden solche Daten nur referenziert, etwa über Datensatz-IDs, und nicht kopiert; Screenshots und Exporte mit Produktivdaten gehören nicht dorthin.

(4) Nicht als Unterauftragsverarbeitung gelten Nebenleistungen ohne Zugriff auf Daten der Auftraggeberin, etwa Telekommunikation oder die Wartung der eigenen IT des Auftragnehmers.

(5) Wird § 7 Abs. 4 des Vertrags mit dem Land schriftlich geändert, kann die Auftraggeberin einen weiteren Auftragsverarbeiter im Einzelfall nach

vorheriger schriftlicher Zustimmung des Landes in Textform genehmigen. Der Auftragnehmer legt dem weiteren Auftragsverarbeiter dann vertraglich dieselben Datenschutzpflichten auf (Art. 28 Abs. 4 DSGVO), prüft dessen technische und organisatorische Maßnahmen vor Beginn und haftet für ihn wie für eigenes Handeln.

§ 6 Ort der Verarbeitung

Die Verarbeitung findet ausschließlich in der Europäischen Union oder im Europäischen Wirtschaftsraum statt. Eine Verarbeitung in einem Drittland oder ein Zugriff von dort ist nur mit vorheriger Zustimmung der Auftraggeberin und des Landes in Textform und unter den Voraussetzungen der Art. 44 bis 49 DSGVO zulässig.

§ 7 Kontrollrechte

(1) Die Auftraggeberin kann die Einhaltung dieses Vertrags überprüfen, insbesondere durch Auskünfte, Einsicht in die gespeicherten Daten und die Datenverarbeitungsprogramme und nach rechtzeitiger Ankündigung durch Prüfungen vor Ort während der üblichen Geschäftszeiten. Der Auftragnehmer wirkt mit und stellt die erforderlichen Informationen bereit (Art. 28 Abs. 3 Buchst. h DSGVO). Die Umsetzung der technischen und organisatorischen Maßnahmen kann er auch durch genehmigte Verhaltensregeln, eine Zertifizierung nach Art. 42 DSGVO, aktuelle Testate oder Berichte unabhängiger Stellen, etwa der Revision, des Datenschutzbeauftragten oder des IT-Sicherheitsbeauftragten, oder eine geeignete Zertifizierung durch ein IT-Sicherheits- oder Datenschutzaudit, etwa nach BSI-IT-Grundschutz, nachweisen.

(2) Dieselben Rechte hat das Land; es kann Kontrollen beim Auftragnehmer jederzeit im Umfang dieses Paragrafen selbst durchführen oder durch Dritte durchführen lassen (§ 7 Abs. 7 des Vertrags mit dem Land). Dieselben Rechte haben ferner Prüfer, die die Auftraggeberin beauftragt, sowie Stellen, denen gegenüber die Auftraggeberin zur Ermöglichung solcher Prüfungen verpflichtet ist.

§ 8 Löschung und Rückgabe

Kopien oder Duplikate der Daten erstellt der Auftragnehmer nicht ohne Wissen der Auftraggeberin; ausgenommen sind Sicherheitskopien, soweit sie für eine ordnungsgemäße Verarbeitung erforderlich sind, und Daten, die er zur Erfüllung gesetzlicher Aufbewahrungspflichten benötigt. Erstellte Kopien dokumentiert er nach Zweck, Ort und Löschung; die Auftraggeberin kann die Dokumentation an

das Land weitergeben. Nach Ende der Leistungen oder auf Verlangen gibt der Auftragnehmer alle personenbezogenen Daten der Auftraggeberin sowie Datenträger und sonstige Unterlagen mit solchen Daten nach deren Wahl zurück oder löscht oder vernichtet sie einschließlich aller Kopien, soweit keine gesetzliche Pflicht zur Aufbewahrung besteht (Art. 28 Abs. 3 Buchst. g DSGVO). Test- und Ausschussmaterial vernichtet er ohne gesonderte Weisung. Löschung und Vernichtung bestätigt er mit Datumsangabe in Textform.

§ 9 Haftung

Für die Haftung gilt Art. 82 DSGVO; im Übrigen gilt § 10 der Rahmenvereinbarung.

§ 10 Schlussbestimmungen

(1) Bei Widersprüchen geht dieser Vertrag in Fragen des Datenschutzes den übrigen Vertragsbestandteilen vor.

(2) Änderungen und Ergänzungen bedürfen der Textform. § 13 der Rahmenvereinbarung gilt entsprechend.

(3) Die Auftraggeberin behandelt Kenntnisse über die Datensicherheitsmaßnahmen des Auftragnehmers vertraulich. Sie darf diesen Vertrag, die Rahmenvereinbarung und die Beschreibung der technischen und organisatorischen Maßnahmen dem Land vorlegen (§ 7 Abs. 3 des Vertrags mit dem Land).

(4) Das Land kann die Rechte der Auftraggeberin aus diesem Vertrag, insbesondere Weisungs-, Auskunfts-, Kontroll-, Herausgabe- und Löschungsrechte, auch unmittelbar gegenüber dem Auftragnehmer ausüben (§ 328 BGB). Widersprechen sich Weisungen, gehen die des Landes vor; der Auftragnehmer unterrichtet die Auftraggeberin unverzüglich.

Anlage 1 zum AVV: Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

Mit dem Angebot bestätigt der Bieter, dass er die folgenden Mindestanforderungen erfüllt (Nummer C.7 des Angebotsformulars). Der vorgesehene Zuschlagsempfänger beschreibt vor dem Zuschlag auf Anforderung der Auftraggeberin, wie er sie umsetzt; ein vorhandenes TOM-Dokument kann beigefügt werden, wenn es die Mindestanforderungen abdeckt. Die Beschreibung wird Bestandteil dieses Vertrags. Hosting und Infrastruktur der Systeme stellt die Auftraggeberin; die Maßnahmen betreffen die Organisation und die Arbeitsmittel des Auftragnehmers und seine Zugriffe.

Bereich	Mindestanforderung
Organisation	Verantwortliche Person für Informationssicherheit und Datenschutz; Regeln für den Umgang mit Daten der Auftraggeberin; Verpflichtung der Beschäftigten auf Vertraulichkeit und vor dem ersten Datenzugriff nach dem Verpflichtungsgesetz (§ 4 Abs. 1); regelmäßige Sensibilisierung, mindestens jährlich
Zugang und Zugriff	Personengebundene Konten; Mehr-Faktor-Authentifizierung für Zugriffe auf Systeme der Auftraggeberin und auf eigene Systeme mit Daten oder Code der Auftraggeberin; Rechte nach dem Prinzip der minimalen Berechtigung; sofortiger Entzug bei Ausscheiden oder Rollenwechsel
Trennung	Technische oder logische Trennung der Daten der Auftraggeberin von sonstigen Datenbeständen des Auftragnehmers
Endgeräte	Vollverschlüsselung, aktuelle Sicherheitsupdates, Schutz vor Schadsoftware und automatische Bildschirmsperre; private Geräte nur bei gleichwertiger Absicherung
Übertragung und Speicherung	Zugriffe und Datenübertragungen nur über verschlüsselte Verbindungen (etwa VPN, SSH, TLS); keine Speicherung von Daten der Auftraggeberin in Cloud-Diensten, die die Auftraggeberin nicht freigegeben hat; personenbezogene Daten nur in den dafür bereitgestellten Systemen der Auftraggeberin, in Tickets und Repositories nur als Referenz (§ 5 Abs. 3); für KI-Dienste gilt Abschnitt 14 der Leistungsbeschreibung
Zugangsdaten und Schlüssel	Verwaltung in einem Passwort- oder Secret-Management; keine Ablage in Repositories, Tickets oder Chats

Bereich	Mindestanforderung
Entwicklung und Test	Keine Produktivdaten mit Personenbezug in Entwicklungs- und Testumgebungen, außer anonymisiert oder nach Zustimmung; Code Reviews und Prüfung von Abhängigkeiten nach Abschnitt 11.1 der Leistungsbeschreibung
Verfügbarkeit und Wiederherstellung	Änderungen an Produktivsystemen nur mit aktueller Sicherung und Rückfallplan; Mitwirkung an Sicherung und Wiederherstellung nach Abschnitt 6.1 der Leistungsbeschreibung
Protokollierung	Nachvollziehbarkeit administrativer Zugriffe auf Systeme der Auftraggeberin, soweit die Systeme dies unterstützen
Sicherheitsvorfälle	Verfahren zur Erkennung, Meldung binnen 24 Stunden und Behandlung von Vorfällen
KI-Dienste	Regeln nach Abschnitt 14 der Leistungsbeschreibung; keine personenbezogenen Daten und keine Zugangsdaten in KI-Diensten
Überprüfung	Regelmäßige Überprüfung der Wirksamkeit der Maßnahmen (Art. 32 Abs. 1 Buchst. d DSGVO); Zertifizierungen wie ISO 27001 sind willkommen, aber keine Voraussetzung

Beschreibung des Auftragnehmers: fügt der vorgesehene Zuschlagsempfänger vor dem Zuschlag bei.