Anlage Nr. 7

zum Rahmenvertrag für Lieferung und Einbau von Raddauerzählstellen sowie Betrieb einer webbasierten Auswerteplattform

Vergabenummer: OV-L-475-130-26

Auftragnehmer	Auftraggeber
	Landeshauptstadt Potsdam Friedrich-Ebert-Str. 79 / 81 14469 Potsdam

Vereinbarung über die Auftragsverarbeitung gemäß Art. 28 DS-GVO

Anmerkung: Soweit der Platz dieses Formulars nicht ausreicht, fügen Sie bitte zusätzliche Anlagen bei.

Bitte beachten:
Die Türkis hinterlegten Felder ☐ sind durch den Bieter/Auftragnehmer zu ergänzen, sofern eine Vorgabe durch die LHP nicht oder nicht vollständig möglich ist. Nähere Erläuterungen zu den einzelnen Regelungen entnehmen Sie bitte den jeweiligen Fußnoten.

1. Gegenstand und Dauer des Auftrags

(1) Gegenstand

Gegenstand der Verarbeitung ist die Bereitstellung und der Betrieb einer webbasierten Auswerteplattform für Raddauerzählstellen. Im Rahmen der Nutzung werden ausschließlich Benutzerkonten (Login-Daten) der Nutzer der Auftraggeberin verarbeitet.

(2) Dauer

Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung, sofern sich aus den nachfolgenden Bestimmungen nicht darüberhinausgehende Verpflichtungen ergeben.

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.

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.

(2) Art der Daten

Verarbeitet werden ausschließlich:

- Benutzer- und Zugangsdaten (z. B. Benutzername, Passwort, Rollen/Berechtigungen)
- Protokolldaten im Rahmen der Systemnutzung (z. B. Anmeldezeitpunkte, Zugriffe)

(3) Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen sind in der Leistungsvereinbarung konkret beschrieben unter: Beschäftigte der LHP

3. Weisungsbefugnis des Auftraggebers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen des Auftrags und auf dokumentierte Weisungen des Auftraggebers, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragnehmer unterliegt, hierzu verpflichtet ist. In einem solchen Fall teilt der Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

(2) Der Auftragnehmer verwendet die zur Verarbeitung überlassenen Daten für keine anderen, insbesondere nicht für eigene Zwecke.

(3) Der Auftragnehmer darf Daten ausschließlich im Rahmen der Weisungen des Auftraggebers verarbeiten. Eine Weisung ist die auf einen bestimmten Umgang des Auftragnehmers mit Daten gerichtete Anordnung des Auftraggebers.

(4) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

(5) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

(6) Änderungen des Verarbeitungsgegenstandes mit Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren.

4. Berichtigung, Einschränkung und Löschung von Daten

Der Auftragnehmer hat die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) ☐ Schriftliche Bestellung eines Datenschutzbeauftragten[1], der seine Tätigkeit gemäß Art. 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 bestellt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.
- ☐ Dessen jeweils aktuelle Kontaktdaten sind auf der Homepage des Auftragnehmers leicht zugänglich hinterlegt.

☒ Der Auftragnehmer ist nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet. Als Ansprechpartner beim Auftragnehmer wird Herr/Frau [Eintragen: Vorname, Name, Organisationseinheit, Telefon, E-Mail] benannt.

☐ Da der Auftragnehmer seinen Sitz außerhalb der Union hat, benennt er folgenden Vertreter nach Art. 27 Abs. 1 DS-GVO in der Union: [Eintragen: Vorname, Name, Organisationseinheit, Telefon, E-Mail].

b) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

c) Durch den Auftragnehmer erfolgt die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO.

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

e) 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.

f) 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) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen sowie deren Wirksamkeit, 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. Das Ergebnis samt vollständigem Bericht ist dem Auftraggeber mitzuteilen.

[1] Der Auftragnehmer wird in der Regel zur Bestellung eines Datenschutzbeauftragten verpflichtet sein. Anderenfalls hat der Auftragnehmer das Fehlen einer Verpflichtung zu begründen.

h) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 8 dieses Vertrages.

6. Technische und organisatorische Maßnahmen

(1) Der Auftragnehmer garantiert, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen der DS-GVO erfolgt und der Schutz der Rechte der betroffenen Person dadurch gewährleistet wird. Mit seiner Unterschrift unter dieser Vereinbarung erklärt der Auftragnehmer zudem, dass im Einzelnen durch ihn standardmäßig die im Anhang A benannten Maßnahmen umgesetzt werden. Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe im Anhang A dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber nachzuweisen. Zur Nachweisführung wird auf Nr. 8 Abs. 3 verwiesen. Der Anhang A ist Gegenstand dieser Vereinbarung.

(2) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO ab Vertragsbeginn zu gewährleisten. 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.

(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 im Anhang A vereinbarten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren und dem Auftraggeber schriftlich oder in Textform bekanntzugeben.

(4) Eine Verarbeitung von Daten außerhalb der Betriebsräume des Auftragnehmers (z.B. Telearbeit, Heimarbeit, mobiles Arbeiten) bedarf der vorherigen ausdrücklichen schriftlichen Zustimmung des Auftraggebers und einer nachgewiesenen Festlegung angemessener technischer und organisatorischer Maßnahmen für diese Art der Verarbeitungstätigkeit.

7. Unterauftragsverhältnisse/Einsatz Dritter

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen, ungeachtet des Rechtsverhältnisses zwischen dem Auftragnehmer und einem Nachunternehmer/Dritten (z. B. Eignungsverleiher, konzernverbundene Unternehmen). 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) sowie Dritte nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen. Die jeweiligen Verantwortlichkeiten sind dabei untereinander klar abzugrenzen. Der Auftragnehmer hat dafür Sorge zu tragen, dass er den Unterauftragnehmer, unter besonderer Berücksichtigung der Eignung der von diesen getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DS-GVO, sorgfältig auswählt. Die relevanten Prüfunterlagen dazu sind dem Auftraggeber auf Anfrage zur Verfügung zu stellen.

a) ☐ Eine Unterbeauftragung ist unzulässig.

b) ☒ Der Auftraggeber stimmt der Einbindung der im Angebot benannten Nachunternehmer/Dritten unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zu.

c) ☒ Die Auslagerung auf Unterauftragnehmer/Dritte oder

☒ der Wechsel des bestehenden Unterauftragnehmers/Dritten nach Vertragsschluss

ist nur zulässig, soweit

- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit (mindestens 2 Monate) vorab schriftlich oder in Textform anzeigt und
- eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde gelegt wird und
- der Auftraggeber nicht bis zum Zeitpunkt der angekündigten Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt.

Zusätzliche bestehende Beschränkungen/Zustimmungsvorbehalte an den Einsatz von Unterauftragnehmern/Dritten aufgrund weitergehender vertraglicher Regelungen, aus § 4 Nr. 4 VOL/B oder nach § 132 GWB bleiben von dieser Regelung unberührt.

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

(4) Erbringt der Unterauftragnehmer/Dritte die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher, Art. 44 ff. DS-GVO. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

(5) Eine weitere Auslagerung durch den Unterauftragnehmer/Dritten

☐ 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/Dritten aufzuerlegen.

8. 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 ohne Störung des Betriebsablaufs zu den üblichen Geschäftszeiten zu überzeugen. Anlassbezogene Überprüfungen können ohne Voranmeldung erfolgen.

(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

- ☐ 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-Grundschutz).

(4) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer keinen separaten Vergütungsanspruch geltend machen. Der Aufwand ist mit dem Vergütungsanspruch für die vertragliche Hauptleistung abgegolten.

9. Unterstützungspflicht 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 vorherigen Konsultationen. Hierzu gehören u.a.

a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen
b) die Verpflichtung, Verletzungen personenbezogener Daten sowie schwerwiegender Störungen des Betriebsablaufs unverzüglich an den Auftraggeber zu melden
c) die Verpflichtung, den 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) Zudem unterstützt der Auftragnehmer den Auftraggeber bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 bis 22 DS-GVO.

(3) Für die genannten Unterstützungsleistungen kann der Auftragnehmer keine separate Vergütung beanspruchen.

10. Auskunft an Betroffene

Soweit sich eine betroffene Person zwecks Geltendmachung eines Betroffenenrechts unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten. Auskünfte an Dritte oder die betroffene Person darf der Auftragnehmer nur nach vorheriger schriftlicher Zustimmung durch den Auftraggeber erteilen.

11. Löschung und Rückgabe von personenbezogenen Daten

(1) Überlassene Datenträger und Datensätze verbleiben im Eigentum des Auftraggebers.

(2) 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.

(3) 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.

(4) 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. Für die nach S.1 aufbewahrten Daten gelten nach Ende der Aufbewahrungsfrist die Pflichten nach Absatz 3.

(5) Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer i. S. d. § 273 BGB hinsichtlich der zu verarbeitenden Daten und der zugehörigen Datenträger ausgeschlossen ist.

12. Kündigung

Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DS-GVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

13. Schlussbestimmungen

(1) Sollte das Eigentum oder die zu verarbeitenden Daten des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter gefährdet sein (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.

(2) Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform. Das gilt auch für den Verzicht auf das Formerfordernis.

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

(4) Diese Vereinbarung unterliegt deutschem Recht.

_____	_____
Ort/Datum:	Ort/Datum:
_____	_____
Auftragnehmer	Auftraggeber

Anlagen:

Anhang A – technische und organisatorische Maßnahmen

Anhang A – technische und organisatorische Maßnahmen

Nr.	Maßnahme	Umsetzung der Maßnahme/ Mindestanforderungen wird durch den Auftragnehmer gewährleistet[2]
Art. 32 Abs. 1 lit. a) DS-GVO		
1	**Pseudonymisierung**	
	Es ist zu gewährleisten, dass die Verarbeitung personenbezogener Daten soweit möglich in einer Weise erfolgt, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen unterliegen. ☒ nicht erforderlich *(durch Bedarfsstelle [Auftraggeber] auszufüllen; wenn „nicht erforderlich“, dann ist die Auswahlmöglichkeit in der rechten Spalte zu löschen)*	☐ Ja ☐ Nein ☐ Alternativ, und zwar durch folgende Maßnahmen: (Begründen Sie ggf., warum eine Pseudonymisierung im konkreten Fall nicht möglich / zweckmäßig ist)
2	**Verschlüsselung**	
	Es ist zu gewährleisten, dass personenbezogene Daten vor unbefugtem Zugriff geschützt und vertraulich übermittelt werden. **Mindestanforderungen:** ▪ Verschlüsselung von Datenträgern (ext. Festplatten, Laptops) ▪ Einsatz von Transport-Verschlüsselung, elektronische Signatur oder Virtual Private Networks (VPN). ▪ Verschlüsselung der personenbezogenen Daten bei Transport auf Datenträgern	☒ Ja ☐ Nein ☐ Alternativ, und zwar durch folgende Maßnahmen:
Art. 32 Abs. 1 lit. b) DS-GVO		
3	**Vertraulichkeit**	

[2] Hier ist durch den Bieter/Auftragnehmer zu bestätigen, ob die Maßnahmen/Mindestanforderungen erfüllt werden. In Vergabeverfahren ist die datenschutzrechtliche Zuverlässigkeit des Bieters durch die Bedarfsstelle vor Zuschlagserteilung zu prüfen. Die Maßnahmen werden daher auf ihre Vereinbarkeit mit dem zuvor bestimmten Datenschutzniveau hin überprüft. **Sofern erforderliche Maßnahmen/Mindestanforderungen nicht erfüllt werden, führen diese zum Ausschluss**, soweit keine adäquaten Alternativmaßnahmen durch den Bieter/Auftragnehmer vorgeschlagen werden (Darstellung der Alternativmaßnahmen auch auf einer separaten Anlage möglich).

3.1	**Zutrittskontrolle** Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren. **Mindestanforderungen:** ▪ An den systemkritischen Räumen (wie Serverräumen, Räumen mit technischer Ausstattung) sind Zutrittskontrollfunktionen (z.B. Kartenlesegeräte, elektronische Schlüssel o.ä.) angebracht ▪ Zutritte zu systemkritischen Räumen werden protokolliert. ▪ Besucher werden registriert und erhalten einen Besucherausweis. ▪ Besucher werden nur unter Begleitung durch die Geschäftsräume geführt. ▪ Eine Einbruchs- und Brandmeldeanlage ist installiert und betriebsbereit.	☒ Ja ☐ Nein ☐ Alternativ, und zwar durch folgende Maßnahmen:
3.2	**Zugangskontrolle** Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können. **Mindestanforderungen:** ▪ Nutzung von sicheren Kennwörtern (Passwortrichtlinie o.ä.) ▪ Einsatz automatischer Sperrmechanismen (nach x Versuchen Zugang sperren) ▪ Verschlüsselung von Datenträgern (ext. Festplatten, Laptops) ▪ Zugang zu Server und Clients nur mit persönlicher Authentifizierung (Username und Passwort). ▪ Die Zugriffe werden protokolliert. ▪ Einsatz von Firewalls (Schutz vor externe Angriffe)	☒ Ja ☐ Nein ☐ Alternativ, und zwar durch folgende Maßnahmen:
3.3	**Zugriffskontrolle** Es ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungs-systems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. **Mindestanforderungen:** ▪ Zugriff auf Laptops, Server, Clients erfolgt über eine persönliche Authentifizierung (Username und Passwort) ▪ Sämtliche Zugriffe auf Systeme werden protokolliert. ▪ Es existiert ein dokumentiertes Benutzerkonzept. ▪ Mitarbeiter/Innen werden regelmäßig zu Datenschutz und Datensicherheit geschult	☒ Ja ☐ Nein ☐ Alternativ, und zwar durch folgende Maßnahmen:

3.4	**Trennungskontrolle** Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. **Mindestanforderungen:** ▪ Mandantenfähigkeit bei der Verarbeitung der personenbezogenen Daten. ▪ Ggf. Netzwerksegmentierung. Dies ist separat zu regeln.	☒ Ja ☐ Nein ☐ Alternativ, und zwar durch folgende Maßnahmen:
4	**Integrität**	
4.1	**Weitergabekontrolle** Es ist zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist. **Mindestanforderungen:** ▪ Einsatz von Transport-Verschlüsselung, elektronische Signatur oder Virtual Private Networks (VPN). ▪ Verschlüsselung der personenbezogenen Daten bei Transport auf Datenträgern. ▪ Zwischen AN und AG wird eine Vereinbarung zur Auftragsverarbeitung geschlossen. ▪ Ausschussmaterial, Testausdrucke sowie defekte oder ausgesonderte Speicher-medien werden ausschließlich durch ein zertifiziertes Entsorgungsunternehmen datenschutzgerecht vernichtet. ▪ Mitarbeiter/Innen mit Zugang zu personenbezogenen Daten sind zur Verschwiegenheit verpflichtet.	☒ Ja ☐ Nein ☐ Alternativ, und zwar durch folgende Maßnahmen:
4.2	**Eingabekontrolle** Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. **Mindestanforderungen:** ▪ Es ist zu protokollieren, wer personenbezogene Daten in Datenverarbeitungssystemen eingeben, verändern oder entfernen darf.	☒ Ja ☐ Nein ☐ Alternativ, und zwar durch folgende Maßnahmen:

5	**Verfügbarkeit und Belastbarkeit der Systeme und Dienste**	
5.1	**Verfügbarkeitskontrolle** Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige oder mutwillige Zerstörung oder Verlust geschützt sind. **Mindestanforderungen:** ▪ Backup-Strategie muss vorhanden sein. ▪ Einsatz unterbrechungsfreier Stromversorgung (USV). ▪ Einsatz von Virenschutz, Firewalls, Meldewege und Notfallpläne	☒ Ja ☐ Nein ☐ Alternativ, und zwar durch folgende Maßnahmen:
5.2	**Belastbarkeit der Systeme und Dienste** Es ist zu gewährleisten, dass die zum Einsatz kommenden IT-Systeme und Dienste auch im Fehlerfall, bei Störungen und hoher Beanspruchung widerstandsfähig sind. **Mindestanforderungen:** ▪ Regelmäßige Durchführung von Sicherheitstests (z.B. Belastungs-/Penetrationstests).	☐ Ja ☐ Nein ☐ Alternativ, und zwar durch folgende Maßnahmen:
Art. 32 Abs. 1 lit. c) DS-GVO		
6	**Wiederherstellbarkeit**	
	Es ist zu gewährleisten, dass auf die Daten bei einem physischen oder technischen Zwischenfall rasch wieder zugegriffen werden kann. **Mindestanforderungen:** ▪ Sicherung der Datenbanken und der Dokumente (Backup-Strategie). ▪ Durchführung und Dokumentierung von Wiederherstellungsübungen.	☒ Ja ☐ Nein ☐ Alternativ, und zwar durch folgende Maßnahmen:
Art. 32 Abs. 1 lit. d) DS-GVO		
7	**Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen**	☒ Ja ☐ Nein ☐ Alternativ, und zwar durch folgende Maßnahmen:

Sonstige Maßnahmen		
8	Durch den Auftraggeber werden ☐ folgende sonstige Maßnahmen gefordert (z.B. Maßnahmen zur Gewährleistung der Authentizität, Revisionsfähigkeit): ▪ ▪ ▪ ☐ keine sonstigen Maßnahmen gefordert. *(durch Bedarfsstelle [Auftraggeber] auszufüllen; wenn „keine sonstigen Maßnahmen gefordert“ werden, dann ist die Auswahlmöglichkeit in der rechten Spalte zu löschen)*	☐ Ja ☒ Nein ☐ Alternativ, und zwar durch folgende Maßnahmen: