Vereinbarung zur Auftragsverarbeitung nach Art. 28 Datenschutzgrundverordnung und § 17 Nds. Datenschutzgesetz

zwischen
der **Region Hannover**, Team 12.02, Hildesheimer Straße 20, 30169 Hannover,
vertreten durch den Regionspräsidenten

- nachstehend „**Verantwortliche**“ genannt -

und dem/der

- nachstehend „**Auftragsverarbeiter**“ genannt -

- nachstehend gemeinsam „**Parteien**“ genannt -

§ 1 Gegenstand der Vereinbarung

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten im Auftrag der Verantwortlichen.

(2) Der Gegenstand des Auftrages sind die im zwischen der Verantwortlichen und dem Auftragsverarbeiter geschlossenen Vertrag über Servicevertrag Miete von Kuvertiermaschine und Software (Vergabe-Nr. 30.02-2024/0390) vereinbarten Pflichten des Auftragsverarbeiters.

(3) Die Dauer des Auftrages entspricht der Dauer des Vertrages über 48 Monate).

(4) Die Art der vorgesehenen Verarbeitung von Daten (gem. der Definition in Art. 4 Nr. 2 DSGVO) und die Verarbeitungskategorien (gem. der Definition in Art. 4 Nr. 1 DSGVO) sowie der Verarbeitungszweck sind in der Anlage 2 zu diesem Vertrag dokumentiert.

(5) 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.

(6) Schutzbedarf der verarbeiteten personenbezogenen Daten aus Sicht der Informationssicherheit – niedrig/mittel/hoch (siehe § 6 dieses Vertrages):

- Vertraulichkeit:
- Verfügbarkeit:
- Integrität:

Datenschutzrechtlicher Schutzbedarf gemäß des Schutzstufenkonzepts der Landesbeauftragten für den Datenschutz Niedersachsen:

☒ Schutzstufe A
☒ Schutzstufe B
☐ Schutzstufe C
☐ Schutzstufe D
☐ Schutzstufe E

§ 2 Pflichten der Verantwortlichen

(1) Für die Beurteilung der Zulässigkeit der Datenverarbeitung gemäß Art. 6 DSGVO sowie für die Wahrung der Rechte der Betroffenen nach Art. 12 bis 22 DSGVO ist allein die Verantwortliche verantwortlich. Gleichwohl ist der Auftragsverarbeiter verpflichtet, alle solche Anfragen, sofern sie erkennbar ausschließlich an die Verantwortliche gerichtet sind, unverzüglich an diesen weiterzuleiten.

(2) Die Verantwortliche erteilt alle Aufträge oder Teilaufträge schriftlich. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen und schriftlich festzuhalten.

(3) Die Verantwortliche hat das Recht, Weisungen über Art, Umfang und Verfahren der Datenverarbeitung zu erteilen. Die Weisungsbefugnis der weisungsberechtigten Personen der Verantwortlichen und der Weisungsempfänger bei dem Auftragsverarbeiter sind in der Anlage 3 zu diesem Vertrag dokumentiert.

Mündliche Weisungen sind unverzüglich schriftlich zu bestätigen.

Bei einem Wechsel oder einer längerfristigen Verhinderung der Kontaktperson ist der Verantwortlichen bzw. dem Auftragsverarbeiter unverzüglich schriftlich die Nachfolge- bzw. die Vertretungsregelung mitzuteilen und die Anlage 3 zu diesem Vertrag zu aktualisieren.

Der Auftragsverarbeiter unterrichtet die Verantwortliche unverzüglich, wenn eine von der Verantwortlichen erteilte Weisung nach seiner Meinung zu einem Verstoß gegen gesetzliche Vorschriften führen kann.

(4) Die Verantwortliche ist berechtigt, sich vor Beginn der Datenverarbeitung und sodann regelmäßig bei dem Auftragsverarbeiter von der Einhaltung der bei ihm getroffenen technischen und organisatorischen Maßnahmen zu überzeugen (s. § 6 dieses Vertrages). Die Verantwortliche kann diese Kontrolle auch durch einen Dritten durchführen lassen.

(5) Die Verantwortliche informiert den Auftragsverarbeiter unverzüglich, wenn Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse festgestellt werden.

(6) Die Verantwortliche ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragsverarbeiters vertraulich zu behandeln.

§ 3 Pflichten des Auftragsverarbeiters

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen der Verantwortlichen. Er verwendet die zur Datenverarbeitung überlassenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate werden ohne Wissen der Verantwortlichen nicht erstellt. Hiervon ausgenommen sind Sicherungskopien zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung.

(2) Der Auftragsverarbeiter sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsmäßige Abwicklung aller vereinbarten Maßnahmen zu. Er sichert zu, dass die überlassenen Daten ausschließlich in der Weise verarbeitet werden, dass diese jederzeit von sonstigen Datenbeständen scharf getrennt und bereitgestellt werden können.

(3) Der Auftragsverarbeiter erklärt sich damit einverstanden, dass die Verantwortliche jederzeit berechtigt ist, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen im erforderlichen Umfang zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme.

(4) An der Eintragung in das Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 DSGVO sowie bei erforderlichen Datenschutz-Folgeabschätzungen des Verantwortlichen hat der Auftragsverarbeiter im notwendigen Umfang mitzuwirken und die Verantwortliche soweit möglich angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. e und f DSGVO). Er hat die erforderlichen Angaben der Verantwortlichen zuzuleiten.

(5) Der Auftragsverarbeiter unterstützt die Verantwortliche bei der Einhaltung der in den Art. 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen

b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an die Verantwortliche zu melden,

c) die Verpflichtung, der Verantwortlichen im Rahmen ihrer Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihr in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen,

d) die Unterstützung der Verantwortlichen für deren Datenschutz-Folgenabschätzung,

e) die Unterstützung der Verantwortlichen im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

(6) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragsverarbeiters zurückzuführen sind, kann der Auftragsverarbeiter eine Vergütung beanspruchen.

(7) Die Verarbeitung von personenbezogenen Daten in Privatwohnungen (Tele- bzw. Heimarbeit von Beschäftigten des Auftragsverarbeiters) sowie das mobile Arbeiten sind nur mit Zustimmung des Verantwortlichen gestattet. Die Maßnahmen nach Art. 32 DSGVO sind auch in diesem Fall durch den Auftragsverarbeiter sicherzustellen.

Das vor Vertragsschluss in diesem Fall durch den Anbieter vorzulegende zusätzliche Datenschutz- und Informationssicherheitskonzept muss mindestens die in der Anlage 4 dieses Vertrages beschriebenen Technischen und organisatorischen Maßnahmen erfüllen

(8) Der Auftragsverarbeiter verpflichtet sich bei einem Cyberangriff[1] unverzüglich die Verantwortliche zu informieren, sowie über einen Verlust und/oder eine ggfls. mögliche Veröffentlichung von Daten der Verantwortlichen Auskunft zu erteilen.

[1] Einwirkung auf ein oder mehrere andere informationstechnische Systeme im oder durch den Cyber-Raum, die zum Ziel hat, deren IT-Sicherheit durch informationstechnische Mittel ganz oder teilweise zu beeinträchtigen

§ 4 Datengeheimnis und Vertraulichkeit

(1) Der Auftragsverarbeiter sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigungsverhältnisses in geeigneter Weise zur Verschwiegenheit verpflichtet (Art. 28 Abs. 3 Satz 2 lit. b und Art. 29 DSGVO). Der Auftragsverarbeiter überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb.

Er verpflichtet sich, die gleichen Geheimnisschutzregeln zu beachten, wie sie der Verantwortlichen obliegen, insbesondere § 203 StGB oder besondere Berufsgeheimnisse.

(2) Die Verantwortliche verpflichtet sich, dem Auftragsverarbeiter die im Einzelfall zu beachtenden spezialgesetzlichen Datenschutzbestimmungen schriftlich zu benennen. Der Auftragsverarbeiter verpflichtet sich, diese gegen sich gelten zu lassen.

(3) Der Auftragsverarbeiter bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften der DSGVO bekannt sind. Er verpflichtet sich, auch folgende für diesen Auftrag relevanten Geheimnisschutzregeln zu beachten, die der Verantwortlichen obliegen:

- Sozialgeheimnis,
- Steuergeheimnis,
- Fernmeldegeheimnis,
- Berufsgeheimnis

Der Auftragsverarbeiter verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten der Verantwortlichen die Vertraulichkeit zu wahren. Diese besteht auch nach Beendigung des Vertrages fort.

(4) Auskünfte an Dritte oder an Betroffene darf der Auftragsverarbeiter nur nach vorheriger schriftlicher Zustimmung durch die Verantwortliche erteilen.

§ 5 Kontrollrechte der Landesbeauftragten für den Datenschutz (LfD)

Der Auftragsverarbeiter verpflichtet sich, der oder dem jeweils gesetzlich zuständigen Landesbeauftragten für den Datenschutz und den von ihr oder ihm eingesetzten Bediensteten sowie von ihr oder ihm beauftragten Stellen Zugang zu den Arbeitsräumen zu gewähren und unterwirft sich der Kontrolle nach Maßgabe des NDSG in seiner jeweiligen Fassung.

§ 6 Technische und organisatorische Maßnahmen nach Art. 32 Abs. 3, 32 DSGVO; § 17 NDSG

(1) Es wird für die konkrete Auftragsverarbeitung ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Schutzniveau gewährleistet. Dazu werden die Schutzziele von Art. 32 Abs. 1 DSGVO, wie Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und Dienste sowie deren Belastbarkeit in Bezug auf Art, Umfang, Umstände und Zweck der Verarbeitungen derart berücksichtigt, dass durch geeignete technische und organisatorische Abhilfemaßnahmen das Risiko auf Dauer eingedämmt wird.

(2) Für die auftragsgemäße Verarbeitung personenbezogener Daten wird die Methodik des Bundesamtes für Sicherheit in der Informationstechnik (BSI) 200-3 („Risikoanalyse auf Basis von IT-Grundschutz“) zur Risikobewertung verwendet, welche die Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten berücksichtigt.

(3) Die in der Anlage 1 beschriebene technischen und organisatorische Maßnahmen stellen eine Mindestauswahl dar, die passend zum ermittelten Schutzbedarf unter Berücksichtigung der Schutzziele nach dem Stand der Technik detailliert und unter besonderer Berücksichtigung der eingesetzten IT- Systeme und Verarbeitungsprozesse durch Auftragsverarbeiter einzuhalten sind.

(4) Der Auftragsverarbeiter hat bei gegebenem Anlass, mindestens aber einmal jährlich, eine Überprüfung, Bewertung und Evaluation der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung durchzuführen (Art. 32 Abs. 1 lit. d DSGVO). Das Ergebnis ist der Verantwortlichen jährlich mitzuteilen. Die Verantwortliche erhält mindestens alle drei Jahre die Möglichkeit, Einsicht in ggf. erstellte vollständige Auditberichte zu erhalten.

(5) Für die Sicherheit erhebliche Entscheidungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren sind zwischen Auftragsverarbeiter und Verantwortlicher abzustimmen. Soweit die beim Auftragsverarbeiter getroffenen Maßnahmen den Anforderungen der Verantwortlichen nicht genügen, benachrichtigt er die Verantwortliche unverzüglich.

(6) Die Maßnahmen beim Auftragsverarbeiter können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden, dürfen aber die vereinbarten Standards nicht unterschreiten.

(7) Wesentliche Änderungen muss der Auftragsverarbeiter mit der Verantwortlichen in dokumentierter Form (schriftlich, elektronisch) abstimmen. Solche Abstimmungen sind für die Dauer dieses Vertrages aufzubewahren.

Im Fall der Verarbeitung besonderer Kategorien personenbezogener Daten sind die nach § 17 Abs. 1 NDSG vorgegebenen technischen und organisatorischen Maßnahmen zwingend durch den Auftragsverarbeiter einzuhalten. Insbesondere sind die zusätzlichen in § 17 Abs. 3 NDSG genannten Maßnahmen, soweit erforderlich, wie folgt durch den Auftragsverarbeiter umzusetzen:

☒ Freigabe von personenbezogenen Daten im Vier-Augen-Prinzip

☐ Zugriff nach einer Zwei-Faktor-Authentisierung

☒Übermittlung personenbezogener Daten mit einer Ende-zu-Ende-Verschlüsselung

☐ Speicherung innerhalb vernetzter IT-Systemen nur in verschlüsselter Form

☐ Ausschluss des Datenverlustes durch redundante Auslegung der Systeme, der Energieversorgung und Datenübertragungseinrichtungen

☒ Sicherstellung, dass Daten nicht unbefugt verändert werden und ihre Integrität gewahrt ist.

☐ Schulung der Personen, die Zugang zu den personenbezogenen Daten haben

§ 7 Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftragsverarbeiter darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung der Verantwortlichen berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragsverarbeiter wendet, wird der Auftragsverarbeiter dieses Ersuchen unverzüglich an die Verantwortliche weiterleiten.

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

(3) Der Auftragsverarbeiter informiert die Verantwortliche unverzüglich über geplante Veränderungen in der Organisation der Datenverarbeitung und den angewandten Verfahren, soweit sie für die Auftragsverarbeitung sicherheitsrelevant sind. Entsprechendes gilt in Fällen von schwerwiegenden Betriebsstörungen, bei Verdacht auf Datenschutzverletzungen oder anderen Unregelmäßigkeiten bei der Verarbeitung der Daten der Verantwortlichen.

(4) Die in den o. g. Rechtsvorschriften vorgeschriebenen Regelungen zu technischen und organisatorischen Maßnahmen sind im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung anzupassen. Wesentliche Änderungen sind schriftlich zu vereinbaren.

(5) Soweit die bei dem Auftragsverarbeiter getroffenen Sicherheitsmaßnahmen den Anforderungen der Verantwortlichen nicht mehr genügen, benachrichtigt er die Verantwortliche unverzüglich. Entsprechendes gilt für Störungen sowie bei Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten.

(6) Sollten Sicherheit oder Verfügbarkeit der Daten bzw. Eigentum der Verantwortlichen beim Auftragsverarbeiter durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse möglicherweise gefährdet sein, so hat der Auftragsverarbeiter die Verantwortliche unverzüglich zu unterrichten und der Verantwortlichen alle erforderlichen Auskünfte zur Sicherung der Daten selbst sowie ihrer Verfügbarkeit zu erteilen.

§ 8 Qualitätssicherung und sonstige Pflichten des Auftragsverarbeiters

Der Auftragsverarbeiter hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags, gesetzliche Pflichten gemäß Art. 28 bis 33 DSGVO. Insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DSGVO ausübt.

   Dessen Kontaktdaten werden der Verantwortlichen zum Zweck der direkten Kontaktaufnahme mitgeteilt. Ein Wechsel des Datenschutzbeauftragten wird der Verantwortlichen unverzüglich mitgeteilt.

b) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO. Der Auftragsverarbeiter 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 Auftragsverarbeiter und jede dem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung der Verantwortlichen verarbeiten, einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

c) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DSGVO [Einzelheiten siehe Seite 11 und 12].

d) Die Verantwortliche und der Auftragsverarbeiter arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

e) Die unverzügliche Information der Verantwortlichen 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 Auftragsverarbeiter ermittelt.

f) Soweit die Verantwortliche ihrerseits 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 Auftragsverarbeiter ausgesetzt ist, hat der Auftragsverarbeiter nach besten Kräften zu unterstützen.

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

h) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber der Verantwortlichen im Rahmen seiner Kontrollbefugnisse nach § 10 dieses Vertrages.

§ 9 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 Auftragsverarbeiter 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 Auftragsverarbeiter ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten der Verantwortlichen auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Zulässigkeit der Unterbeauftragung

☒ Der Auftragsverarbeiter darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung der Verantwortlichen beauftragen.

☐ Eine Unterbeauftragung ist grundsätzlich unzulässig.

§ 10 Kontrollrechte der Verantwortlichen

(1) Die Verantwortliche hat das Recht, im Benehmen mit dem Auftragsverarbeiter Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Die Verantwortliche hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragsverarbeiter in dessen Geschäftsbetrieb zu überzeugen.

(2) Der Auftragsverarbeiter stellt sicher, dass sich die Verantwortliche von der Einhaltung der Pflichten des Auftragsverarbeiters nach Art. 28 DSGVO überzeugen kann. Der Auftragsverarbeiter verpflichtet sich, der Verantwortlichen 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 DSGVO;
- ☐ die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO;
- ☒ 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).

§ 11 Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen der Verantwortlichen 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 die Verantwortliche – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragsverarbeiter sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, der Verantwortlichen 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 Auftragsverarbeiter entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende der Verantwortlichen übergeben.

Anlage 1 – Technisch-organisatorische Maßnahmen

Hinweis
Hierbei handelt es sich um technisch-organisatorische Maßnahmen, die vom Auftragsverarbeiter mindestens zu erfüllen sind.

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

- Zutrittskontrolle
  - Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, z.B.: Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Werkschutz bzw. Pförtner, Alarmanlagen, Videoanlagen;
- Zugangskontrolle
  - Keine unbefugte Systembenutzung, z.B.: (sichere) Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern;
- Zugriffskontrolle
  - Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen;
- Trennungskontrolle
  - Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B. Mandantenfähigkeit, Sandboxing;
- Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)
  - Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen;

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

- Weitergabekontrolle
  - Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur;
- Eingabekontrolle
  - Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement;

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

- Verfügbarkeitskontrolle
  - Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne;
- Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO)

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

- Datenschutz-Management;
- Incident-Response-Management;
- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO);
- Auftragskontrolle
  - Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DSGVO ohne entsprechende Weisung der Verantwortlichen, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.

Anlage 2

Gegenstand der Vereinbarung – zu § 1 Abs. 4 dieses Vertrages

Übersicht über die Art der vorgesehenen Verarbeitung von Daten (gem. der Definition in Art. 4 Nr. 2 DSGVO) und die Kategorien der vorgesehenen Verarbeitung von Daten (gem. der Definition in Art. 4 Nr. 1 DSGVO)

a) Verarbeitung von personenbezogenen Daten von Betroffenen (bspw. Bürgerinnen und Bürger, EinzelunternehmerInnen, Familienangehörige)

Betroffene Personen	Datenkategorien	Art der Daten	Zweck der Datenverarbeitung
Bürgerinnen und Bürger	Allg. Kontaktdaten	Name, Anschrift, Inhalt des Schreibens	Schreiben versenden

b) Verarbeitung von personenbezogenen von Beschäftigtendaten der Region Hannover

Betroffene Personen	Datenkategorien	Art der Daten	Zweck der Datenverarbeitung
Beschäftigte	Allg. dienstl. Kontaktdaten	Name, Benutzername, Organisationseinheit, behördliche Kontaktdaten	Vertragserfüllung, Durchführung des Dienstverhältnisses,
Beschäftigte	Protokollierungsdaten der EDV-Anwendung	Datum und Uhrzeit von Login und Logout, Bearbeitungshistorie Dokument	Systemsicherheit

Anlage 3 – Weisungsbefugnisse nach § 2 Abs. 3 dieses Vertrages

Weisungsberechtigte Personen der Verantwortlichen sind:

Werden mit Zuschlagserteilung bekannt gegeben

.....

(Name, Vorname, Funktion, Telefon, E-Mailadresse)

Weisungsberechtigte Personen der Verantwortlichen im Vertretungsfall sind:

Werden mit Zuschlagserteilung bekannt gegeben

.....

(Name, Vorname, Funktion, Telefon, E-Mailadresse)

Weisungsempfänger bei dem Auftragsverarbeiter sind:

.....

(Name, Vorname, Funktion, Telefon, E-Mailadresse)

Weisungsempfänger bei dem Auftragsverarbeiter im Vertretungsfall sind:

.....

(Name, Vorname, Funktion, Telefon, E-Mailadresse)

Anlage 4 - Einzuhaltende TOMs im Homeoffice

- Jegliche private Nutzung mobiler dienstlicher IT-Systeme ist untersagt, hierzu gehört auch die Installation/Anbindung nicht zugelassener und/oder privater Speichermedien und Software (z. B. Apps, USB-Sticks, Festplatten etc.).
- Die Installation spezieller Treiber oder Software zur Nutzung von privaten Geräten ist untersagt.
- Der Zugriff und die Nutzung der mobilen dienstlichen IT-Systeme durch Dritte sind untersagt. Ausgenommen von dieser Regelung sind Dritte, die durch Auftrag oder Einverständnis durch den Auftragsverarbeiter berechtigt sind, auf die mobilen IT-Systeme zuzugreifen (bspw. IT-Dienstleister).
- Bei der Benutzung der mobilen IT-Systeme ist die Einsichtnahme Dritter (z. B. durch Ausrichtung des Monitors nicht in Richtung Fenster und Tür, usw.) zu verhindern.
- Es wird sichergestellt, dass Telefongespräche nicht von unbefugten Dritten mitgehört werden können (z.B. offene Fenster und Türen).
- Alle mobilen dienstlichen IT-Systeme sind nach Beendigung des Dienstgeschäftes sicher und für Dritte unzugänglich aufzubewahren, so dass ein Diebstahl nicht möglich ist (gegebenenfalls Einsatz von Diebstahlsicherungen wie Kensington-Schloss).
- Zugang der Berechtigten zu den sensiblen personenbezogenen Daten nur mit PIN und hardwarebasiertem Vertrauensanker (Zwei-Faktor-Authentifizierung).
- Bei Verlust oder Beschädigung der Geräte ist unverzüglich der IT-Dienstleister und die/der Informationssicherheitsbeauftragte (ISB) des Auftragsverarbeiters zu verständigen. Hier sind Sofortmaßnahmen zu ergreifen: z. B. Remote Wipe (Löschung) bei Smartphones, Sperrung von Hardware-Token.
- Berufliche E-Mails mit datenschutzrechtlich relevanten Inhalten dürfen nicht auf private Postfächer der im Homeoffice Arbeitenden umgeleitet werden.
- Keine Anbindung von Druckern.
- Schutz von USB-Zugängen und anderen Anschlüssen
- Zum Schutz vor unbefugtem Zugriff sind die mobilen IT-Systeme mit den vorhandenen technischen Möglichkeiten zu sperren (sperren des Bildschirmes durch die Tastenkombination „Windows Taste + L“), sobald die Nutzung unterbrochen wird. Es dürfen keine Passwörter auf programmierbaren Funktionstasten von Mäusen oder Tastaturen hinterlegt werden.
- Die Entfernung zugeordneter Rollen und das Umgehen oder Ausschalten von Sicherheitsmaßnahmen ist untersagt.
- Es sind nur vertrauenswürdige und verschlüsselte WLAN zu nutzen.
- Online-Dienste und Sprachassistenten – insbesondere Alexa, Siri, Cortana, Google Assistant und Bixby – sind im häuslichen Umfeld auszuschalten (Abhörgefahr).