Sonderbeilage
Amtsblatt Nr.52 vom 23. Dezember 2024
Anlage zur Ziffer 238

Anlage 2

Vereinbarung zur Auftragsverarbeitung

gemäß Art. 28 DSGVO

---

zwischen der

Hansestadt Herford

nachstehend Auftraggeber genannt

und dem

Kreis Herford

nachstehend Auftragnehmer genannt

Inhalt

1. Gegenstand und Dauer des Auftrags

(1) Gegenstand

☐ Der Gegenstand des Auftrags ergibt sich aus der öffentlich-rechtlichen Vereinbarung über die Zusammenarbeit der gemeinsamen Gebührenkalkulation und der Abrechnung der Einsätze des Rettungsdienstes zwischen der Stadt Herford und dem Kreis Herford die dieser Vereinbarung als Anlage beigefügt ist (nachstehend örV genannt).

☒ Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer:
Die Vereinbarungspartner beschließen eine interkommunale Zusammenarbeit bei der Erstellung der Gebührenkalkulation, der Verhandlung der berechneten Gebühren mit den Kostenträgern und der Abrechnung für die Einsätze des Rettungsdienstes.

Die örV sieht vor, dass der Kreis Herford sowohl für den Kreis Herford als auch für die Hansestadt Herford eine gemeinsame, für beide Vereinbarungspartner geltende Gebührenkalkulation, für die anfallenden Gebühren bei Einsätzen des Rettungsdienstes erstellt. Die gemeinsame Gebührenkalkulation hat zum einen den Vorteil, dass es im Gegensatz zur jetzigen Situation nur noch eine einheitliche Rechnung für die Inanspruchnahme von Rettungsdienstleistungen gibt. Zum anderen können durch die gemeinsame Gebührenkalkulation für beide Vereinbarungspartner Synergien genutzt und Kosten eingespart werden.

(2) Dauer

☐ Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der örV.

☐ Der Auftrag wird zur einmaligen Ausführung erteilt.

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

☒ Der Auftrag ist unbefristet erteilt und kann von beiden Parteien mit einer Frist von 12 Monaten zum Jahresende schriftlich gekündigt werden. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt. Bei gesetzlichen Änderungen kann auch eine kürzere Kündigungsfrist nach Abstimmung mit den Vertragsparteien gewählt werden.

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 örV vom _____.

☒ Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind konkret in Ziffer 1. (Gegenstand und Dauer des Auftrags) beschrieben.

(2) Art der Daten

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

☒ Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/ -kategorien:

☒ Vorname
☒ Nachname
☒ Straße
☒ Hausnummer
☒ Postleitzahl
☒ Ort
☒ Geschlecht
☒ Geburtsdatum
☒ Vertragsabrechnungs- und Zahlungsdaten
☒ Auskunftsangaben
☐

(3) Kategorien der betroffenen Personen

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

☒ Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

☐ Kunden
☐ Interessenten
☐ Beschäftigte
☒ Ansprechpartner
☐ Lieferanten
☐ Abonnenten
☒ Andere: Geschädigte

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 Maßnahmen Grundlage des Auftrags (siehe Anlage). Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen und zu dokumentieren.

(2) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DSGVO, insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO, herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DSGVO zu berücksichtigen.

(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. Darüber hinaus beobachtet der Auftragnehmer die technische Entwicklung und schlägt ggf. notwendige Anpassungen der technisch-organisatorischen Maßnahmen vor.

4. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

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

- **a.** Schriftliche Benennung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DSGVO ausübt. Dessen jeweils aktuelle Kontaktdaten sind auf der Homepage des Auftragnehmers leicht zugänglich hinterlegt und sind dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitzuteilen. Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt.
- **b.** Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29,32 Abs. 4 DSGVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich der Weisung entsprechend des Auftraggebers verarbeiten, einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind. Der Auftragnehmer überwacht durch regelmäßige Kontrollen, dass die Verpflichtungen eingehalten werden. Des Weiteren unterrichtet der Auftragnehmer regelmäßig über geltende datenschutzrechtliche Bestimmungen.
- **c.** Der Auftragnehmer verpflichtet sich, die im Rahmen des Auftragsverhältnisses zur Verfügung gestellten oder erarbeiteten Unterlagen und Daten sowie ihm sonst bekannt gewordenen Informationen vertraulich zu behandeln und nur im Rahmen der Tätigkeit für dieses Vertragsverhältnis zu nutzen. Diese Verpflichtung besteht auch nach Ende des Vertragsverhältnisses fort.
- **d.** Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DSGVO (Einzelheiten siehe Anlage).

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

f. 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 Ordnungswidrigkeit- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

g. Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

h. Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person im Hinblick auf Art. 12 - 23 DSGVO gewährleistet wird.

i. Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 6 dieser Vereinbarung.

j. Trennung der Netze der jeweiligen Mandanten im Falle einer Fernwartung.

5. 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 Telekommunikationsdienstleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice 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.

a. ☐ Der Auftragnehmer darf weitere Auftragnehmer (Unterauftragnehmer) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen. Er hat dem Unterauftragnehmer dieselben Regelungen aufzuerlegen, die dem Auftragnehmer nach diesem Vertrag auferlegt wurden.

b. ☐ Der Auftraggeber stimmt der Beauftragung der aufgeführten Unterauftragnehmern unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO zu.

Der Wechsel bestehender Unterauftragnehmer ist zulässig, soweit:

- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab, mindestens 1 Monat im Voraus, schriftlich oder in Textform anzeigt
  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 DSGVO zugrunde gelegt wird.

c. ☒ Eine Unterbeauftragung ist unzulässig.

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

(3) Sämtliche vertragliche Regelungen in der Vertragskette sind auch Unterauftragnehmer aufzuerlegen.

6. Internationale Datentransfers

(1) Jede Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation bedarf einer dokumentierten Weisung des Auftraggebers und bedarf der Einhaltung der Vorgaben zur Übermittlung personenbezogener Daten in Drittländer nach Kapitel V der DSGVO.

☒ 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.

☐ Der Auftraggeber gestattet eine Datenübermittlung in ein Drittland. In der Anlage werden die Maßnahmen zur Gewährleistung eines angemessenen Schutzniveaus aus Art. 44 ff. DSGVO im Rahmen der Unterbeauftragung spezifiziert.

(2) Soweit der Auftraggeber eine Datenübermittlung an Dritte in ein Drittland anweist, ist er für die Einhaltung von Kapitel V der DSGVO verantwortlich.

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. Der Auftragnehmer unterstützt den Auftraggeber bei diesen Prüfungen. Ggf. sorgt er auch dafür, dass der Auftraggeber oder von ihm beauftragte Prüfer Prüfungen auch bei weiteren Auftragnehmern durchführen können und auch diese den Auftraggeber bzw. deren Prüfer unterstützen.

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DSGVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann durch

☐ die Einhaltung genehmigter Verhaltensregeln gem. Art. 40 DSGVO.

☐ die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gem. 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).

erfolgen.

8. Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgenabschätzungen 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 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) Für Unterstützungsleistungen, die nicht in der örV enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

9. 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 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.

10. Anfragen betroffener Personen

Wendet sich eine betroffene Person mit Forderungen zur Berichtigung, Löschung oder Auskunft an den Auftragnehmer, wird der Auftragnehmer die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber nach Angaben der betroffenen Person möglich ist. Der Auftragnehmer informiert den Auftraggeber und leitet den Antrag der betroffenen Person unverzüglich weiter. Er unterstützt den Auftraggeber weiterhin bei der Erfüllung seiner Pflichten nach Kapitel III DSGVO im erforderlichen Umfang. Der Auftragnehmer haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

11. Weisungsbefugnis des Auftraggebers

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers verarbeiten. Der Auftraggeber entscheidet allein über die Zwecke und Mittel der Verarbeitung der personenbezogenen Daten. Eine Verarbeitung für andere Zwecke, insbesondere für eigene Zwecke des Auftragnehmers, ist nicht zulässig. Weisungen werden nur vom Auftraggeber und von keinem Dritten erteilt, auch wenn die Datenverarbeitung im Interesse oder Auftrag Dritter erfolgt und/oder dieser seinerseits Auftraggeber ist.

(2) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich schriftlich (E-Mail ist ausreichend). Diese werden durch den Auftragnehmer dokumentiert.

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

12. Löschung und Rückgabe von personenbezogenen Daten nach Beendigung des Vertrags

(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 örV - hat der Auftragnehmer sämtliche in seinem 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.

13. Haftung und Schadensersatz

(1) Haftung und Schadensersatz nach dieser Vereinbarung zur Auftragsverarbeitung regeln sich nach der Bestimmung des Art. 82 DSGVO.

(2) Weitergehende Haftungsansprüche nach den allgemeinen Gesetzen bleiben unberührt.

14. Außerordentliche Kündigung

Unabhängig von den Regelungen über die oben getroffenen Laufzeiten bzw. die Dauer der Vereinbarung steht dem Auftraggeber ein Recht auf fristlose Kündigung bei schwerwiegenden Vertragsverletzungen des Auftragnehmers zu. Dies kommt insbesondere in Betracht bei Verstoß gegen datenschutzrechtliche Vorschriften, Datenschutz- und Datensicherheitsvereinbarungen, wenn der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer eine Kontrolle des Auftraggebers oder der nordrhein-westfälischen Datenschutzbeauftragten vertragswidrig verweigert.

15. Sonstiges

(1) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als „Verantwortlicher“ im Sinne der EU-Datenschutz-Grundverordnung liegen.

(2) Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(3) Es besteht bei den Vertragsparteien Einigkeit darüber, dass die „Allgemeinen Geschäftsbedingungen“ des Auftragnehmers auf diese Vereinbarung keine Anwendung finden.

(4) Bei etwaigen Widersprüchen gehen Regelungen dieser Vereinbarung zur Auftragsverarbeitung den Regelungen des Vertrages vor. Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht. Unwirksame Bestimmungen sind von den Parteien durch wirksame zu ersetzen, die dem gewollten Zweck möglichst nahekommen. Entsprechendes gilt im Falle einer Vereinbarungslücke.

(5) Gerichtsstand ist, sofern nichts anderes vereinbart ist, Herford.

Herford, den 16.12.2024

Hansestadt Herford
Der Bürgermeister

gez. Tim Kähler

Herford, den 16.12.2024

Kreis Herford
Der Landrat

gez. Jürgen Müller

Anlage
Technische und organisatorische Maßnahmen

Die Anlage beschreibt die technischen und organisatorischen Maßnahmen die sicherstellen und den Nachweis dafür erbringen, dass die Verarbeitung gem. Art. 24 DSGVO erfolgt. Diese ergeben sich aus Art. 32 Abs. 1 DSGVO. Der Auftragnehmer hat nachfolgende Maßnahmen hierzu umgesetzt.

1. Vertraulichkeit gemäß Art. 32 Abs. 1 lit. b DSGVO

1.1 Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

	Technische Maßnahmen		**Organisatorische Maßnahmen**
☒	Alarmanlage	☒	Schlüsselregelung/ -liste
☒	Automatisches Zugangskontrollsystem	☐	Empfang/ Rezeption/ Pförtner
☐	Biometrische Zugangssperren	☐	Personenkontrolle beim Empfang/ Rezeption/ Pförtner
☒	Chipkarten/ Transpondersysteme	☐	Mitarbeiter-/ Besucherausweise
☒	Manuelles Schließsystem	☐	Besucher in Begleitung durch Mitarbeiter
☒	Sicherheitsschlösser	☒	Sorgfältige Auswahl von Reinigungsdienste
☒	Schließsystem mit Codesperre	☐	Sorgfältige Auswahl von Sicherheitspersonal
☐	Absicherung der Gebäudeschächte	☐	
☒	Türen mit Knauf Außenseite	☐	
☐	Klingelanlage mit Kamera	☐	
☐	Videoüberwachung der Eingänge	☐	
☐	Lichtschranken/ Bewegungsmelder	☐	
☐		☐	
☐		☐	

Weitere Maßnahmen bitte hier beschreiben:

1.2 Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

	Technische Maßnahmen		Organisatorische Maßnahmen
☒	Zuordnung von Benutzerrechten	☒	Erstellen von Benutzerprofilen
☒	Passwortvergabe	☐	Authentifikation mit biometrischen Verfahren
☒	Authentifikation mit Benutzername/ Passwort	☒	Zuordnung von Benutzerprofilen zu IT-Systemen
☐	Gehäuseverriegelungen	☐	Einsatz von VPN-Technologie
☒	Sperren von externen Schnittstellen (USB etc.)	☐	Verschlüsselung von mobilen Datenträgern
☐	Einsatz von Intrustion-Detection-Systemen	☐	Verschlüsselung von Datenträgern in Notebooks
☒	Einsatz von Anti-Viren-Software	☐	Verschlüsselung von Smartphone-/ Tablet-Inhalten
☒	Einsatz einer Hardware-Firewall	☐	Einsatz von zentraler Smartphone-/ Tablet-Administrations-Software (z.B. zum externen Löschen von Daten)
☒	Einsatz einer Software-Firewall	☒	Anleitung „Clean Desk Policy“
☐	Sicherheitsrichtlinie IT	☐	Sicherheitsrichtlinie Datenschutz
☐		☐	

Weitere Maßnahmen bitte hier beschreiben:

1.3 Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

	Technische Maßnahmen		Organisatorische Maßnahmen
☒	Erstellen eines Berechtigungskonzeptes	☒	Verwaltung der Rechte durch Systemadministrator
☒	Anzahl der Administratoren auf das „Notwendigste“ beschränkt	☒	Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
☒	Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten	☐	Sichere Aufbewahrung von Datenträgern
☐	physische Löschung von Datenträgern vor Wiederverwendung	☒	ordnungsgemäße Vernichtung von Akten/ Datenträgern (DIN 66399)

☒	Einsatz von Aktenvernichtern bzw. Dienstleistern	☐	Protokollierung der Vernichtung
☐	Verschlüsselung von Datenträgern	☐	
☐		☐	
☐		☐	

Weitere Maßnahmen bitte hier beschreiben:

1.4 Trennungskontrolle

Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

	Technische Maßnahmen		**Organisatorische Maßnahmen**
☐	Trennung von Produktiv- und Testumgebung	☒	Steuerung über Berechtigungskonzept
☒	Physikalische Trennung (Systeme/ Datenbanken/ Datenträger)	☒	Festlegung von Datenbankrechten
☒	Mandantenfähigkeit relevanter Anwendungen	☐	Datensätze sind mit Zweckattributen versehen
☐	Im Falle der Pseudonymisierung: Trennung der Zuordnungsdaten und Aufbewahrung in getrenntem und abgesicherten System (mögl. verschlüsselt)	☐	
☐		☐	

Weitere Maßnahmen bitte hier beschreiben:

1.5 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 spezifischen betroffenen Personen zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorische Maßnahmen unterliegen.

	Technische Maßnahmen		**Organisatorische Maßnahmen**
☐	Im Falle einer Pseudonymisierung: Trennung der Zuordnungsdaten und Aufbewahrung in getrenntem und abgesicherten System (mögl. verschlüsselt)	☒	Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst anonymisieren/ pseudonymisieren
☐		☐	
☐		☐	
☐		☐	

Weitere Maßnahmen bitte hier beschreiben:

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

2.1 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.

	Technische Maßnahmen		**Organisatorische Maßnahmen**
☐	E-Mail-Verschlüsselung	☒	Dokumentation der Datenempfänger sowie der Dauer der geplanten Überlassung bzw. der Löschfristen
☐	Einsatz von VPN	☐	Übersicht regelmäßiger Abruf- und Übermittlungsvorgängen
☐	Protokollierung der Zugriffe und Abrufe	☐	Weitergabe in anonymisierter oder pseudonymisierter Form
☐	Sichere Transportbehälter	☒	Sorgfalt bei der Auswahl von Personal und Fahrzeugen zum Transport
☒	Bereitstellung über verschlüsselte Verbindungen wie sftp, https	☒	Persönliche Übergabe mit Protokoll/ Empfangsbestätigung
☐		☐	
☐		☐	

Weitere Maßnahmen bitte hier beschreiben:

2.2 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.

	Technische Maßnahmen		**Organisatorische Maßnahmen**
☒	Technische Protokollierung der Eingabe, Änderung und Löschung von Daten	☐	Übersicht, mit welchen Programmen welche Daten eingegeben, geändert oder gelöscht werden können
☐		☒	Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
☐		☒	Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzeptes
☐		☒	Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen wurden

☐		☒	Klare Zuständigkeiten für Löschungen (Löschkonzept)
☐		☐	
☐		☐	

Weitere Maßnahmen bitte hier beschreiben:

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

3.1 Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

	Technische Maßnahmen		**Organisatorische Maßnahmen**
☒	Feuer- und Rauchmeldeanlagen	☒	Backup & Recoverykonzept
☒	Feuerlöscher Serverraum	☐	Kontrolle des Sicherungsvorgangs
☒	Serverraumüberwachung: Temperatur und Feuchtigkeit	☐	Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse
☒	Serverraum klimatisiert	☒	Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums
☒	Unterbrechungsfreie Stromversorgung (USV)	☒	Keine sanitären Anschlüsse im oder oberhalb des Serverraums
☒	Schutzsteckdosenleisten im Serverraum	☐	Existenz eines Notfallplans (z.B. BSI IT Grundschutz 100-4)
☐	Datenschutztresor (S60DIS, S120DIS, andere geeignete Normen mit Quelldichtung, etc.)	☒	Getrennte Partitionen für Betriebssysteme und Daten
☒	RAID System/ Festplattenspiegelung	☐	In Hochwassergebieten: Serverräume über der Wassergrenze
☐	Videoüberwachung Serverraum	☐	
☒	Alarmmeldung bei unberechtigtem Zutritt zu Serverraum	☐	
☐		☐	

Weitere Maßnahmen bitte hier beschreiben:

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

4.1 Datenschutz-Management

	Technische Maßnahmen		Organisatorische Maßnahmen
☒	Software-Lösungen für Datenschutz-Management im Einsatz	☒	Interne(r)/ ~~externe(r)~~ Datenschutzbeauftragte(r) Kontaktdaten: E-Mail: datenschutz@kreis-herford.de Tel.: 05221 131066 Fax: 05221 13171066
☐	Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Beschäftigte nach Bedarf/ Berechtigung	☒	Mitarbeiter geschult (z.B. durch UWEB2000) und auf Vertraulichkeit/ Datengeheimnis verpflichtet
☐	Sicherheitszertifizierung nach ISO 27001, BSI IT-Grundschutz oder ISIS12	☒	Regelmäßige Sensibilisierung der Mitarbeiter/-innen **Mindestens 1 Mal jährlich!**
☐	Alternatives Informationssicherheitskonzept	☒	Interne(r)/ ~~externe(r)~~ IT-Sicherheitsbeauftragte(r) Kontaktdaten: E-Mail: b.waechter@kreis-herford.de Tel.: 05221 131293 Fax: 05221 13171293
☐	Anderweitiges dokumentiertes Sicherheitskonzept	☒	Die Datenschutz-Folgenabschätzung (DSFA - Art. 35 DSGVO) wird bei Bedarf durchgeführt
☐	Eine Überprüfung der technischen Schutzmaßnahmen wird mind. jährlich durchgeführt	☒	Die Organisation kommt den Informationspflichten nach Art. 13, 14 DSGVO nach
☐		☒	Formalisierter Prozess von Auskunftsanfragen seitens Betroffener ist vorhanden
☐		☐	

Weitere Maßnahmen bitte hier beschreiben:

4.2 Incident-Responce-Management

Unterstützung bei der Reaktion auf Sicherheitsverletzungen

	Technische Maßnahmen		Organisatorische Maßnahmen
☒	Einsatz von Firewall und regelmäßige Aktualisierung	☒	Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen/ Datenpannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde)
☒	Einsatz von Spamfilter und regelmäßige Aktualisierung	☒	Einbindung von ☒ DSB und ☒ IT-SiBe in Sicherheitsvorfällen und Datenpannen
☒	Einsatz von Virenscanner und regelmäßige Aktualisierung	☒	Dokumentation von Sicherheitsvorfällen und Datenpannen
☐	Intrusion Detection System (IDS)	☒	Formaler Prozess und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen (Leitfaden Verfahren bei Datenpanne)
☐	Intrusion Prevention System (IPS)	☐	
☐		☐	
☐		☐	
☐		☐	

Weitere Maßnahmen bitte hier beschreiben:

4.3 Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

Privacy by design/ Privacy by default

	Technische Maßnahmen		Organisatorische Maßnahmen
☒	Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind	☐	
☐	Einfache Ausübung des Widerrufrechts des Betroffenen durch technische Maßnahmen	☐	
☐		☐	
☐		☐	

Weitere Maßnahmen bitte hier beschreiben:

4.4 Auftragskontrolle (Outsourcing an Dritte)

Es ist zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Verantwortlichen verarbeitet werden können.

Technische Maßnahmen	Organisatorische Maßnahmen
☐	☒ Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation
☐	☒ Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit)
☐	☒ Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU-Standard-Vertragsklauseln
☐	☒ Schriftliche Weisungen an den Auftragnehmer
☐	☒ Verpflichtung der Mitarbeiter des Auftragnehmers auf Datengeheimnis
☐	☒ Verpflichtung zur Bestellung eines Datenschutzbeauftragten durch den Auftragnehmer bei Vorliegen der Bestellpflicht
☐	☒ Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer
☐	☒ Regelung zum Einsatz weiterer Subunternehmer
☐	☒ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
☐	☒ Bei längerer Zusammenarbeit: Laufende Überprüfung des Auftragnehmers und seines Schutzniveaus
☐	☒ Vertragsstrafen bei Verstößen
☐	☒ Abschluss eines Vertrages über die gemeinsame Verantwortung, sofern erforderlich

Weitere Maßnahmen bitte hier beschreiben:

5. Ergänzende Gewährleistungsziele nach dem Standard-Datenschutzmodell (SDM) der Datenschutz-Aufsichtsbehörden

a. Datenminimierung

Die Verarbeitung personenbezogener Daten ist auf das dem Zweck angemessene, erhebliche und notwendige Maß zu beschränken.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Design der Informationstechnik durch den Hersteller	☒ Es werden möglichst wenige personenbezogene Daten verarbeitet
☐	☒ Der Grundsatz der Erforderlichkeit wird beachtet (nicht mehr als unbedingt notwendig)
☐	☒ Datenstrom auf Wesentliches und auf ein notwendiges Maß beschränkend (Art. 5 Abs. 1 lit. c DSGVO)
☐	☐
☐	☐

Weitere Maßnahmen bitte hier beschreiben:

5.2 Nichtverkettung

Zu unterschiedlichen Zwecken erhobene personenbezogene Daten dürfen nicht zusammengeführt, d. h. verkettet werden.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Schnittstellen auf Erforderlichkeit prüfen	☒ Abgestuftes Rollen- und Rechtekonzept vorhanden
☐	☒ Trennung nach Organisation- und Abteilungsgrenzen
☐	☒ Einsatz von Pseudonymen, Anonymisierungsdiensten und geregelte Zweckbindungsverfahren

Weitere Maßnahmen bitte hier beschreiben:

5.3 Transparenz

Es muss erkennbar sein, welche Daten wann und für welchen Zweck bei einer Verarbeitungstätigkeit erhoben und verarbeitet werden, welche Systeme und Prozesse dafür genutzt werden, wohin die Daten zu welchem Zweck fließen und wer die rechtliche Verantwortung für die Daten und Systeme in den verschiedenen Phasen einer Datenverarbeitung besitzt.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Schnittstellen auf Erforderlichkeit prüfen	☐ Protokollierungskonzept

☐	Rechteprofile	☒	Abgestuftes Rollen- und Rechtekonzept vorhanden
☐	Zweckbindung hinsichtlich der Nutzung der Protokolldaten	☒	Dokumentation im Sinne einer Inventarisierung aller Verarbeitungstätigkeiten gemäß Art. 30 DSGVO ist vorhanden
☐		☒	Dokumentation von Einwilligungen, deren Widerruf sowie Widersprüche ist vorhanden
☐		☒	Benachrichtigung von Betroffenen bei Datenpannen (siehe Leitfaden Datenschutzvorfall)
☐		☐	

Weitere Maßnahmen bitte hier beschreiben:

5.4 Intervenierbarkeit

Betroffene müssen ihre Rechte an ihren personenbezogenen Daten wahrnehmen können. Konkret bedeutet dies: Die Betroffenen erhalten über ihre gespeicherten Daten Auskunft, sie können Korrekturen vornehmen lassen und sie können ihre personenbezogenen Daten sperren oder löschen lassen. Die Datenverarbeitungsprozesse müssen jeweils so gestaltet sein, dass dies auch möglich ist.

	Technische Maßnahmen		**Organisatorische Maßnahmen**
☐		☒	Konzept zur Gewährleistung der Betroffenenrechte ist vorhanden
☐		☒	Gewährleistung der Nachverfolgbarkeit der Aktivitäten des Verantwortlichen zur Gewährung der Betroffenenrechte
☐		☒	Einsichtsmöglichkeiten der/ des Datenschutzbeauftragten und der Aufsichtsbehörde bestehen
☐		☒	dokumentierte Bearbeitung von Störungen, Problembearbeitungen und Änderungen an Verarbeitungstätigkeiten sowie an den technischen und organisatorischen Maßnahmen
☐		☐	

Weitere Maßnahmen bitte hier beschreiben:

Es handelt sich bei den beschriebenen technischen und organisatorischen Maßnahmen um keine abschließende Auflistung. Diese und **weitere** Maßnahmen dienen der Datensicherheit und der Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der in dieser Anlage beschriebenen Schutzziele. Weiterhin unterliegen die Maßnahmen dem technischen Fortschritt und

der Weiterentwicklung. Dabei wird das tatsächliche Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten.