Anlage 6

Vereinbarung zur Auftragsverarbeitung
gemäß Art. 28 DS-GVO

---

zwischen der

Hansestadt Herford

nachstehend Auftraggeber genannt

und der

Stadt Bielefeld

nachstehend Auftragnehmer genannt

Inhalt

1. Gegenstand und Dauer des Auftrags 12
   (1) Gegenstand 12
   (2) Dauer 12
2. Konkretisierung des Auftragsinhalts 13
   (1) Art und Zweck der vorgesehenen Verarbeitung von Daten 13
   (2) Art der Daten 13
   (3) Kategorien der betroffenen Personen 13
3. Technisch-organisatorische Maßnahmen 14
4. Qualitätssicherung und sonstige Pflichten des Auftragnehmers 14
5. Unterauftragsverhältnisse 15
6. Internationale Datentransfers 16
7. Kontrollrechte des Auftraggebers 17
8. Mitteilung bei Verstößen des Auftragnehmers 18
9. Berichtigung, Einschränkung und Löschung von Daten 18
10. Anfragen betroffener Personen 18
11. Weisungsbefugnis des Auftraggebers 19
12. Löschung und Rückgabe von personenbezogenen Daten nach Beendigung des Vertrags 19
13. Haftung und Schadensersatz 20
14. Außerordentliche Kündigung 20
15. Sonstiges 20

1. Gegenstand und Dauer des Auftrags

(1) Gegenstand

☒ **Der Gegenstand des Auftrags ergibt sich aus der Leistungsvereinbarung dem diese Vereinbarung als Anlage beigefügt ist (nachstehend Leistungsvereinbarung genannt).**

☐ **Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer:**
_____ (ausführliche Beschreibung)

(2) Dauer

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

Falls keine Leistungsvereinbarung zur Dauer besteht:

☐ 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 _____ zum _____ gekündigt werden. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.**

2. Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten

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

☒ 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:

- ☒ Personenstammdaten
- ☒ Kommunikationsdaten
- ☐ Vertragsstammdaten
- ☐ Kundenhistorie
- ☒ Vertragsabrechungs- und Zahlungsdaten
- ☐ Planungs- und Steuerungsdaten
- ☒ Auskunftsangaben
- ☐ Andere: _____

(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: Geschädigten

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

(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 DS-GVO. Insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a. Schriftliche Benennung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DS-GVO 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 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 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 DS-GVO (Einzelheiten siehe Anlage 1).
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 DS-GVO 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 in Anlage 2 aufgeführten Unterauftragnehmern unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zu.

Der Wechsel bestehender Unterauftragnehmer ist zulässig, soweit:

- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab 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 DS-GVO 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 DS-GVO.

☒ 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 2 werden die Maßnahmen zur Gewährleistung eines angemessenen Schutzniveaus aus Art. 44 ff. DS-GVO 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 DS-GVO 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 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 durch

☐ **die Einhaltung genehmigter Verhaltensregeln gem. Art. 40 DS-GVO.**

☐ **die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gem. 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).**

erfolgen.

8. Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-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 Leistungsbeschreibung 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 DS-GVO 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 Leistungsvereinbarung – 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 DS-GVO.

(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 nahe kommen. Entsprechendes gilt im Falle einer Vereinbarungslücke.

Ort, den _____

Hansestadt Herford
Der Bürgermeister
Tim Kähler

_____
Unterschrift

Ort, den _____

Stadt Bielefeld
Der Oberbürgermeister
Pit Clausen

_____
Unterschrift

Anlage 1
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 DS-GVO erfolgt. Diese ergeben sich aus Art. 32 Abs. 1 DS-GVO. Der Auftragnehmer hat nachfolgende Maßnahmen hierzu umgesetzt.

Schutzziele	Maßnahme	Umsetzung der Maßnahme
Vertraulichkeit Art. 32 Abs. 1 lit. b) DS-GVO	**Zutrittskontrolle** Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren.	• Ausgabe von Besucher-/Mitarbeiterausweisen *(Es gilt diese an Gegebenheiten des Auftragsnehmers anzupassen)*
	Zugangskontrolle Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.	• Festlegung befugter Personen *(Es gilt diese an Gegebenheiten des Auftragnehmers anzupassen)*
	Zugriffskontrolle Es ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems 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.	• Aufgabenverteilung *(Es gilt diese an Gegebenheiten des Auftragnehmers anzupassen)*
	Trennungskontrolle Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.	• Funktionstrennung und Verfahrensdokumentation *(Es gilt diese an Gegebenheiten des Auftragnehmers anzupassen)*
Integrität Art. 32 Abs. 1 lit. b) DS-GVO	**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.	• Dokumentation der Abruf- und Übermittlungsprogramme sowie zu den Stellen, an die eine Übermittlung vorgesehen ist *(Es gilt diese an Gegebenheiten des Auftragnehmers anzupassen)*

	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.	• Protokollierung der Eingaben *(Es gilt diese an Gegebenheiten des Auftragnehmers anzupassen)*
Verfügbarkeit und Belastbarkeit Art. 32 Abs. 1 lit. b) DS-GVO	**Verfügbarkeitskontrolle** Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.	• Konzept zur Durchführung von regelmäßigen Datensicherungen *(Es gilt diese an Gegebenheiten des Auftragnehmers anzupassen)*
Wiederherstellbarkeit Art. 32 Abs. 1 lit. c) DS-GVO	**Maßnahmen zur raschen Wiederherstellbarkeit** Bei einem unvorhergesehenen Zwischenfall ist dafür zu sorgen, dass die personenbezogenen Daten „rasch" ihrem Zweck entsprechend wieder genutzt werden können.	• Spiegelung der Daten an zwei Standorten • Konzept zur Sicherung der Datenbestände *(Es gilt diese an Gegebenheiten des Auftragnehmers anzupassen)*
Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung Art. 32 Abs. 1 lit. d) DS-GVO	**Auftragskontrolle** Es ist zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.	• Sorgfältige Auswahl der Auftragnehmer • Dokumentation von kundenbezogenen Anweisungen *(Es gilt diese an Gegebenheiten des Auftragnehmers anzupassen)*
	Datenschutz-Management Zum Schutz personenbezogener Daten ist sicherzustellen, dass eine Datenschutzorganisation etabliert ist und Verantwortlichkeiten festgelegt sind.	• Regelungen zum Datenschutz-Management • Verzeichnisse von Verarbeitungstätigkeiten *(Es gilt diese an Gegebenheiten des Auftragnehmers anzupassen)*
Pseudonymisierung und Verschlüsselung Art. 32 Abs. 1 lit. a) DS-GVO	**Pseudonymisierung** Die Gestaltung der Datenverarbeitung hat eine Minimierung von Risiken betroffener Personen zu gewährleisten.	• Ersetzen von Identifikationsmerkmalen durch Ordnungsziffern oder sonstige Kennzeichen *(Es gilt diese an Gegebenheiten des Auftragnehmers anzupassen)*
	Verschlüsselung Zugang zu den personenbezogenen Daten ist ausschließlich dem befugten Personenkreis zu gewähren.	• Angemessene Verschlüsselung nach Stand der Technik *(Es gilt diese an Gegebenheiten des Auftragnehmers anzupassen)*

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.

Anlage 2
Genehmigte Unterauftragsverhältnisse

Firma Unterauftragnehmer	**Anschrift/Land**	**Leistung**	**Angaben zu geeigneten Garantien bei Datenübermittlungen in ein Drittland** (nur bei Verarbeitung im Drittland)