Anhang 5: Vereinbarung zur Auftragsdatenverarbeitung gemäß Artikel 28 ff. Datenschutzgrundverordnung

zwischen

dem Land Nordrhein-Westfalen,
vertreten durch

Bezirksregierung Köln, Zeughausstraße 2-8, 50667 Köln
diese vertreten durch den
Regierungspräsidenten Dr. Thomas Wilk

(nachfolgend **Auftraggeber** genannt)

und

……

(nachfolgend **Auftragnehmer** genannt)

Nur zur Information

I. Gegenstand der Vereinbarung

1. Der Auftragnehmer erhebt / verarbeitet / nutzt personenbezogene Daten im Auftrag des Auftraggebers.

2. Der Auftrag umfasst Folgendes:

   2.1 Gegenstand des Auftrages (Definition der Aufgaben):

   Erbringung von Facility-Management-Dienstleistung in Unterbringungseinrichtungen für Flüchtlinge des Landes Nordrhein-Westfalen (siehe Grundvertrag).

   2.2 Dauer des Auftrags: siehe § 14 Grundvertrag

   Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen die Bestimmungen dieses Vertrages vorliegt, insbesondere wenn der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer den Zutritt des Auftraggebers vertragswidrig verweigert. Wird dieser Vertrag wegen eines schweren Verstoßes gekündigt, wird zugleich und mit gleicher Frist der Grundvertrag gekündigt.

   2.3 Umfang, Art und Zweck der Datenerhebung, -verarbeitung oder -nutzung:

   siehe Grundvertrag; insbesondere erhebt, verarbeitet und nutzt der Auftragnehmer Daten von Flüchtlingen im Zusammenhang mit der Organisation der Unterbringungseinrichtung.

2.4 Art der Daten:
siehe Grundvertrag; insbesondere personenbezogene Daten der untergebrachten Flüchtlinge und der eigenen Beschäftigten.

2.5 Kreis der Betroffenen:
siehe Grundvertrag; insbesondere in der Einrichtung untergebrachte Personen und dort für den Auftragnehmer tätige Personen

II. Rechte und Pflichten des Auftraggebers

1. Für die Beurteilung der Zulässigkeit der Datenerhebung / - verarbeitung / -nutzung sowie für die Wahrung der Rechte der Betroffenen ist allein der Auftraggeber verantwortlich.

2. Der Auftraggeber erteilt alle Aufträge oder Teilaufträge schriftlich. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen und schriftlich festzulegen.

3. Der Auftraggeber hat das Recht, in folgendem Umfang Weisungen gegenüber dem Auftragnehmer zu erteilen: Der Auftraggeber ist berechtigt, Weisungen zur Einhaltung dieser Vereinbarung zur Auftragsdatenverarbeitung und der geltenden Datenschutzvorschriften zu erteilen. Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

4. Mündliche Weisungen sind unverzüglich schriftlich zu bestätigen. Die schriftliche Bestätigung der mündlichen Weisungen sollte von Auftraggeber und Auftragnehmer zusammen mit der Vereinbarung so aufbewahrt werden, dass alle maßgeblichen Regelungen jederzeit verfügbar sind.

   Weisungsberechtigte Person des Auftraggebers ist die jeweilige Einrichtungsleitung und/oder die stellvertretende Einrichtungsleitung sowie die Behördenleitung.

   Weisungsempfänger beim Auftragnehmer sind:

   _____
   (Name, Organisationseinheit, Funktion, Telefon)

   Bei einem Wechsel oder einer längerfristigen Verhinderung des Ansprechpartners ist dem Vertragspartner unverzüglich schriftlich der Nachfolger bzw. der Vertreter mitzuteilen. Falls Weisungen die unter Nr. I. 2 dieses Vertrages getroffenen Festlegungen ändern, aufheben oder ergänzen, sind sie nur zulässig, wenn eine entsprechende neue Festlegung erfolgt.

5. Der Auftraggeber ist berechtigt, sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen (s. Nr. IV) zu überzeugen. Der Auftraggeber kann diese Kontrolle auch durch einen Dritten durchführen lassen. Der Auftragnehmer unterstellt sich der Kontrolle des Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (LDI NRW).

6. Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

Nur zur Information

7. Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln.

III. Pflichten des Auftragnehmers

1. Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers. Er hat personenbezogene Daten zu berichtigen, zu löschen und zu sperren, wenn der Auftraggeber dies in der getroffenen Vereinbarung (siehe oben Nr. I. 2.3) oder einer Weisung verlangt.

   Der Auftragnehmer verwendet die zur Datenverarbeitung überlassenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt.

   Der Auftragnehmer übergibt die Daten an den Auftraggeber gemäß dem Grundvertrag samt Anhang (Leistungsbeschreibung). Der Auftraggeber kann vom Auftragnehmer verlangen, dass dieser ohne Mehrkosten geltend zu machen bereits zu einem früheren Zeitpunkt (z.B. halbjährlich) die bis dahin gespeicherten Daten übergibt. Nachdem der Auftraggeber dem Auftragnehmer jeweils den vollständigen Erhalt der Daten schriftlich bestätigt hat, sind diese Daten unverzüglich zu löschen, soweit und solange die Daten für die Auftragsabwicklung durch den Auftragnehmer nicht zwingend erforderlich sind. Hierauf ist der Auftraggeber schriftlich unter Darlegung der Gründe hinzuweisen.

2. Zur Sicherstellung einer datenschutzrechtskonformen Auftragsabwicklung sowie zur Wahrung der gesetzlichen Anforderungen trifft der Auftragnehmer geeignete technische und organisatorische Maßnahmen. Diese stellen insbesondere unter Berücksichtigung von Art. 32 DSGVO sicher, dass:
   - Berechtigungs-, Zugangs- und Zugriffskonzepte bestehen,
   - klare Verantwortlichkeiten in der Sphäre des Auftragnehmers bestehen,
   - eine jederzeitige Vollständigkeits- und Authentizitätskontrolle bei der Datenverarbeitung gewährleistet ist,
   - eine jederzeitige Revisionsfähigkeit der zu verarbeitenden Daten sichergestellt ist,
   - der Einsatz von Sicherheitsmaßnahmen einschließlich einer geeigneten Verschlüsselung der online via Internet abrufbaren oder übermittelten Daten nach dem jeweils aktuellen Stand der Technik gewährleistet wird.

   Es müssen ferner Maßnahmen ergriffen werden, um ein unberechtigtes Eindringen in Rechnernetze soweit möglich zu verhindern und Versuche zu erkennen. Technische Komponenten, die in Betracht kommen, sind Firewalls, Intrusion Detection Systeme und insbesondere dem Stand der Technik entsprechende Verschlüsselungsverfahren.

   Zu unterschiedlichen Zwecken erhobene Daten sind getrennt zu verarbeiten.

   Der Auftragnehmer führt Maßnahmen durch, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (regelmäßige Sicherungskopien des Datenbestandes auf einem sicheren Medium; geschützte Aufbewahrung der Sicherungskopien).

   Die zu treffenden technischen und organisatorischen Maßnahmen sind vom Auftragnehmer in einem Datenschutz- und Sicherheitskonzept zusammenzufassen und dem Auftraggeber vor Leistungsaufnahme vorzulegen. Das genehmigte Konzept wird Vertragsbestandteil.

Nur zur Information

3. Die Datenträger, die vom Auftraggeber stammen bzw. für den Auftraggeber genutzt werden, werden besonders gekennzeichnet und unterliegen der laufenden – automatisierten – Verwaltung. Eingang und Ausgang werden dokumentiert.

4. Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu. Er sichert zu, dass die verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.

5. Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt.

6. Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber jederzeit berechtigt ist, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen im erforderlichen Umfang selbst oder durch Dritte zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie sonstige Kontrollen vor Ort. Der Auftragnehmer sichert zu, dass er, soweit erforderlich, bei diesen Kontrollen mitwirkt.

7. Die Verarbeitung von Daten in Privatwohnungen ist nur mit schriftlicher Zustimmung des Auftraggebers im Einzelfall gestattet. Soweit die Daten in einer Privatwohnung verarbeitet werden, ist der Zugang zur Wohnung durch den Auftraggeber vorher mit dem Auftragnehmer abzustimmen. Der Auftragnehmer sichert zu, dass auch die anderen Bewohner dieser Privatwohnung mit dieser Regelung einverstanden sind.

8. Nach Abschluss der vertraglichen Arbeiten hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen. Datensicherungskopien sind nach Abschluss der vertraglichen Arbeiten dem Auftraggeber auszuhändigen.

9. Die Beauftragung von Nachunternehmern ist nur mit vorheriger schriftlicher Zustimmung des Auftraggebers zugelassen. Die Zustimmung kann nur erteilt werden, wenn der Auftragnehmer Namen und Anschrift des Nachunternehmers mitteilt. Außerdem muss der Auftragnehmer versichern, dass er den Nachunternehmer unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig ausgewählt hat. Der Auftragnehmer hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Auftraggeber und Auftragnehmer auch gegenüber Nachunternehmern gelten. Insbesondere muss der Auftraggeber berechtigt sein, Kontrollen vor Ort beim Nachunternehmer durchzuführen oder durch Dritte durchführen zu lassen. Der Auftragnehmer hat die Einhaltung der Pflichten regelmäßig zu überprüfen. Das Ergebnis der Überprüfungen ist zu dokumentieren.

   Erfüllt ein Nachunternehmer die datenschutzrechtlichen Verpflichtungen nicht, so haftet der ihn beauftragende Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten des weiteren Nachunternehmers.

   Die Weiterleitung von Daten ist erst nach vorheriger schriftlicher Zustimmung des Auftraggebers und nur dann zulässig, wenn der Nachunternehmer die Verpflichtung nach der DSGVO und eventuell ergänzender Vorschriften des DSG NRW erfüllt hat. In dem Vertrag mit dem Nachunternehmer werden die Verantwortlichkeiten des Auftragnehmers und des Nachunternehmers deutlich voneinander abgegrenzt. Werden mehrere Nachunternehmer eingesetzt, so gilt dies auch für die Verantwortlichkeiten zwischen diesen Nachunternehmern.

10. Die Verarbeitung und Nutzung der Daten findet ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertrags-

Nur zur Information

staat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der DSGVO und eventuell ergänzender Vorschriften des DSG NRW erfüllt sind.

11. Für die Sicherheit erhebliche Entscheidungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren sind mit dem Auftraggeber abzustimmen.

12. Sofern beim Auftragnehmer ein Beauftragte(r) für den Datenschutz bestellt ist, wird der Auftragnehmer dessen Kontaktdaten dem Auftraggeber unverzüglich nach Vertragsschluss mitteilen. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

13. Der Auftragnehmer verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers das Datengeheimnis zu wahren.

14. Der Auftragnehmer bestätigt, dass ihm die einschlägigen datenschutzrechtlichen Vorschriften des BDSG, der DSGVO und des DSG NRW bekannt sind.

15. Der Auftragnehmer 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 sie auf das Datengeheimnis schriftlich verpflichtet. Der Auftragnehmer überwacht die Einhaltung der hier angegebenen datenschutzrechtlichen Vorschriften**.**

16. Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger schriftlicher Zustimmung durch den Auftraggeber erteilen.

IV. Technische und organisatorische Maßnahmen nach Art. 32 DSGVO

1. Der Auftragnehmer ergreift technische und organisatorische Maßnahmen im Sinne des Art. 32 DSGVO. Auf die Ausführungen unter Ziffer III.2 wird verwiesen.

2. Der Auftragnehmer beachtet die Grundsätze ordnungsgemäßer Datenverarbeitung. Er gewährleistet die vertraglich vereinbarten und gesetzlich vorgeschriebenen Datensicherheitsmaßnahmen.

3. Die technischen und organisatorischen Maßnahmen können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden. Wesentliche Änderungen sind schriftlich zu vereinbaren.

4. Soweit die beim Auftragnehmer getroffenen Sicherheitsmaßnahmen den Anforderungen des Auftraggebers nicht genügen, benachrichtigt er den Auftraggeber unverzüglich.

5. Der Auftragnehmer teilt dem Auftraggeber unverzüglich Störungen, Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit. Dies gilt vor allem auch im Hinblick auf eventuelle Informationspflichten des Auftraggebers nach der DSGVO sowie dem DSG NRW. Der Auftragnehmer sichert zu, den Auftraggeber bei seinen datenschutzrechtlichen Pflichten im Hinblick auf eventuelle Informationspflichten zu unterstützen.

Nur zur Information

V. Verfahrensverzeichnis

Der Auftragnehmer wird ausdrücklich auf seine Verpflichtung nach Art. 30 Abs. 2 Datenschutzgrundverordnung (VO [EU] 679/2016, DSGVO) hingewiesen.

Danach hat der Auftragnehmer als Auftragsdatenverarbeiter ein Verzeichnis über die von ihm vorgenommenen Datenverarbeitungstätigkeiten in Textform zu führen, das auf Verlangen dem Auftraggeber und der Aufsichtsbehörde zur Verfügung zu stellen ist (u.a. Art. 30 Abs. 4 DSGVO).

VI. Vergütung

siehe Grundvertrag

VII. Haftung

1. Der Auftragnehmer haftet dem Auftraggeber für Schäden, die der Auftragnehmer, seine Mitarbeiter bzw. die von ihm mit der Vertragsdurchführung Beauftragten bei der Erbringung der vertraglichen Leistung schuldhaft verursachen.

2. Für den Ersatz von Schäden, die ein Betroffener wegen einer nach der DSGVO oder anderen Vorschriften für den Datenschutz unzulässigen oder unrichtigen Datenverarbeitung im Rahmen des Auftragsverhältnisses erleidet, ist der Auftraggeber gegenüber dem Betroffenen verantwortlich. Soweit der Auftraggeber zum Schadensersatz gegenüber dem Betroffenen verpflichtet ist, bleibt ihm der Rückgriff beim Auftragnehmer vorbehalten.

VIII. Geldbußen

Eine Zuwiderhandlung gegen die Verpflichtungen des DSGVO und des DSG NRW sind nach Art. 83 Abs. 4 lit.a DSGVO mit einer Geldbuße von bis zu 10 000 000 EUR oder bis zu 2 % des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs belegt, je nachdem, was höher ist.

IX. Sonstiges

1. Der Auftragnehmer übereignet dem Auftraggeber zur Sicherung die Datenträger, auf denen sich Dateien befinden, die Daten des Auftraggebers enthalten. Diese Datenträger sind besonders zu kennzeichnen.

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

3. Für Nebenabreden ist die Schriftform erforderlich.

X. Wirksamkeit der Vereinbarung

Nur zur Information

Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

Nur zur Information