Anlage 1:

Auftragsverarbeitung zum Einzelabruf und technisch-organisatorische Maßnahmen

betreffend die OZG-Verwaltungsleistung:

„Grundsicherung im Alter“

Zwischen dem Auftraggeber (Leistungsbezieher) und dem Auftragnehmer (Leistungserbringer, Kommunalvertreter) wird mit Vertragsschluss des Einzelabrufs die folgende Einzel-Auftragsverarbeitungsvereinbarung (nachstehend „**Einzel-AV**“) zum Einzelabruf betreffend die OZG-Verwaltungsleistung „Grundsicherung im Alter“ als Anlage 1 (nachstehend „**Einzelabruf**“) geschlossen.

Präambel
Diese Einzel-AV regelt auf Grundlage der zwischen den Vertragsparteien geschlossenen Rahmenvereinbarung zur Auftragsverarbeitung (nachstehend „**Rahmen-AV**“) die Einzelheiten der Datenverarbeitung im Zusammenhang mit dem Einzelabruf „Grundsicherung im Alter“.

1 OZG-Verwaltungsleistungs-spezifische Zwecke, Betroffene und Datenkategorien

Der Auftragnehmer verarbeitet im Rahmen der OZG-Verwaltungsleistung „Grundsicherung im Alter“ die folgenden personenbezogenen Daten:

I. Zwecke

Erhebung personenbezogener Daten zur Durchführung des Verwaltungsverfahrens zur Entscheidung über den Antrag auf Grundsicherung im Alter gemäß §§ 41 ff SGB XII durch den zuständigen Träger der Sozialhilfe

II. Betroffene

- Antragsteller/-innen, auch z.B. Vertreter/-innen oder Betreuer/-innen
- Leistungsempfänger/-innen
- Haushaltsangehörige des/der Leistungsempfängers/-in
- Weitere Personen mit familiärer oder ähnlicher Beziehung zu dem/der Leistungsempfänger/-in

III. Datenkategorien

- Folgende Sozialdaten gemäß § 67 Abs. 2 SGB X:
  - Stammdaten Betreuungsperson oder Bevollmächtigte: Familienname, Vorname, ggf. Organisation/Verein, ggf. Beziehung zur antragstellenden Person, Anschrift Inland/Ausland

- Stammdaten zur antragstellenden Person: Familienname, Vorname, Geburtsdatum, Geburtsort, Geschlecht, Anschrift Inland/Ausland
- Informationen zum akademischen Grad der antragstellenden Person: Dr., Dr. hc.
- Kontaktdaten: Telefon, E-Mail, Einverständnis Kontaktdaten Person ungleich Mieterin/Mieter
- Allgemeine Daten über Haushaltsmitglieder: Familienname, Vorname, Geschlecht, Geburtsdatum, Familienstand, Staatsangehörigkeit, Aufenthaltsrechtlicher Status, Einreisedatum, voll- oder teilstationäre Unterbringung, Verwandtschaftsverhältnis zur antragstellenden Person
- Finanz- und Versicherungsdaten: Angaben zur Bankverbindung, Nachweise Vermögen, Vorheriger Bezug von Grundsicherungsleistungen, Jahreseinkommen von 100.000 € oder mehr, Angaben zur Krankenversicherung oder zur letzten Krankenversicherung, Einkommen, Angaben zur Rente, Antrag auf Anerkennung nach dem Opferentschädigungsgesetz (OEG), Angaben zur Erwerbstätigkeit im Ausland, andere Einkommensarten, Fahrtkosten, Untervermietung, Leistungen für Kinder, evtl. absetzbare Beträge, Angaben zum Vermögen, Altersvorsorge, KFZ, Ansprüche ggü. Dritten, Immobilien und Grundbesitz, Vermögensübertragungen innerhalb der letzten 10 Jahre, Ermittlung kostenerstattungspflichtigen Trägers, Nachweise Renteneinkommen, Nachweise andere Einkommensarten, Nachweise vom Einkommen eventuell absetzbarer Beträge, Unterhaltsansprüche inkl. Informationen ggü wem (Stammdaten und Einkommen)
- Angaben zum Beruf: Ausgeübte Berufe der Eltern und Kinder
- Daten zur Wohnsituation: Leben in besonderer Wohnform / stationärer Einrichtung, Einrichtung und Anschrift davon, Bedarf für die Unterkunft (Anzahl Haushaltsmitglieder, Wohnfläche, Hauptmieter, Baujahr, Anzahl der Räume, Wohnsituation, Anschrift, Kalt- und Warmmiete), Bedarf für Heiz- und Stromkosten, Zuschläge, Angabe zum Leben im Ausland, geschieden getrennt lebend
- Staatsbürgerschaft- und Aufenthaltsinformationen: Aufenthaltsrechtlicher Status, Einreisedatum, Staatsangehörigkeit, Auslandsaufenthalte in den kommenden 12 Monaten
- Besondere personenbezogene Daten nach Art. 9 DSGVO: Voll oder teilstationäre Unterbringung von Haushaltmitglieder (bspw. Werkstatt für behinderte Menschen) Schwangerschaft, Schwerbehinderung
- Verpflichtungserklärung: Verpflichtungserklärung nach § 68 Aufenthaltsgesetz
- Angaben zu Leistungen zur Teilhabe an Bildung nach § 42b Abs. 3 SGB XII i.V.m. § 112 Abs. 1 S. 1 Nr. 1 und 2 SGB IX
- Mittagsverpflegung: Teilnahme am Mittagessen einer Werkstatt für behinderte Menschen, Anzahl Arbeitstage pro Woche
- Metadaten: Pseudo-User-ID, ProzessID, Erstellungsdatum, letztes Updatedatum, Abschlussdatum, (Client)-Ref-ID, Session-ID, User-ID, User-Object (enthält auch User-ID und Session-ID), Document-UUIDs, Document-Data, Antrags-ID

2 Technische und organisatorische Maßnahmen (TOM)

Die technischen und organisatorischen Maßnahmen (IT.NRW) gestalten sich wie folgt:

I. d-NRW bündelt die Vertragsbeziehungen und die Kommunikation zwischen den weiteren Auftragsverarbeitern gemäß der Liste der genehmigten Subunternehmer in der

nachfolgenden Ziffer 3 und den Leistungsbeziehern, führt jedoch selbst keinerlei Verarbeitung der auftragsbezogenen personenbezogenen Daten gemäß dieses Einzelabrufs durch.

II. Das Ministerium für Arbeit, Gesundheit und Soziales des Landes NRW (MAGS) betreibt die bundesweite Sozialplattform und beauftragt den Landesbetrieb Information und Technik Nordrhein-Westfalen (IT.NRW) mit dem technischen Betrieb der Plattform. Das MAGS ist bezüglich des Betriebs der Webseite der Plattform und der diesbezüglichen Datenverarbeitung (z.B. Verwendung von Cookies) datenschutzrechtlich Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO. Das MAGS hat jedoch keine Zugriffsmöglichkeit auf auftragsbezogene personenbezogene Daten dieses Einzelabrufs und führt bezüglich dieser keinerlei Verarbeitung durch.

III. IT.NRW betreibt die gesamte technische Infrastruktur für die Datenverarbeitung im Rahmen dieses Einzelabrufs bis zu dem vertraglich vereinbarten Übergabepunkt. IT.NRW trifft für diese Datenverarbeitung die in Anlage 2 zu diesem Einzelabruf festgelegten Technischen und Organisatorischen Maßnahmen.

IV. Für diesen Einzelabruf vereinbaren die Vertragsparteien gemäß Ziffer 6 der Rahmenvereinbarung zur Auftragsverarbeitung die nachfolgend beschriebenen Technische und Organisatorische Maßnahmen.

Technische und Organisatorische Maßnahmen bei der Datenverarbeitung bei IT.NRW

Stellen, die selbst oder im Auftrag personenbezogene Daten verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Einhaltung der datenschutzrechtlichen Vorschriften zu gewährleisten. Dabei ist ein angemessenes Verhältnis zwischen erforderlichem Aufwand und angestrebtem Schutzzweck zu wahren.

IT.NRW erfüllt diese Vorgabe durch folgende Maßnahmen:

1. Vertraulichkeit, Art. 32 Abs. 1 DSGVO
1.1 Zutrittskontrolle

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

a. Rechenzentrum

Der Zutritt zum Rechenzentrum ist gemäß der Standards des BSI und der DIN ISO 27001 geregelt unter anderem durch

- Alarmanlage
- Automatisches Zutrittskontrollsystem mit mehreren Faktoren
- Protokollierung des Zugangs
- Videoüberwachung
- Überwachung durch Sicherheitszentrale
- Ausweisregelungen für Mitarbeiter/-innen und Besucher/-innen

b. Büroräume

- Ausweisregelungen für Mitarbeiter/-innen und Besucher/-innen
- Zutrittskontrollsystem in kritischen Bereichen

- Empfang/Pforte

1.2 Zugangskontrolle

Hierzu zählen Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme durch Unbefugte genutzt werden können.

a. Rechenzentrum/Systemadministration

- Technische Maßnahmen zum Schutz von Daten vor Manipulation auf Ebene der Administration
- Sorgfältige Auswahl von Software und Bezugsquellen
- Administrationskennungen mit Passwortsicherung
- Zugang auf Systeme nur über speziell gesicherte Bereiche

b. Büroräume

- Die Authentifizierung gegenüber dem Betriebssystem und den Anwendungen erfolgt über individuelle Benutzerkennung und Kennwort
- Automatische Desktopsperre nach vorgegebener Zeit
- Richtlinie Desktopsperre
- Die Mitarbeiter/-innen sind angewiesen, Kennwörter geheim zu halten und bei dem Verdacht der Kompromittierung diese zu ändern
- An die Kennwörter werden erhöhte Anforderungen gestellt:
  Vorgegebene Mindestlänge, Nutzung von komplexen Kennwörtern (Groß- und Kleinschreibung, Sonderzeichen, Zahlen usw.), regelmäßige erzwungene Änderung der Kennwörter mit Kennworthistorie

c. Fernzugang

- Einsatz von VPN bei Remote-Zugriffen
- BIOS Schutz
- Der Fernzugang zu Systemen ist auf ein absolut notwendiges Minimum reduziert
- Zusätzlich zu den oben dargelegten Maßnahmen erfolgt eine weitere 2-Faktor-Authentifizierung über eine Kombination aus Wissen (z. B. ein Passwort) und Besitz (z. B. ein USB-Dongle oder RSA-Token)

1.3 Zugriffskontrolle

Hierzu zählen Maßnahmen, durch die gewährleistet wird, dass berechtigte Nutzer/-innen ausschließlich im Rahmen ihrer Berechtigung auf Daten zugreifen. Es wird verhindert, dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung unbefugt gelesen, kopiert, verändert oder entfernt werden können.

a. Rechenzentrum

- Berechtigungskonzepte
- Unverzügliche Fehlerbehebung
- Vernichtung von Datenträgern und vertraulichen Dokumenten gemäß DIN 66399
- Aktive Prüfung der Verfügbarkeit und Sicherheit von Infrastruktur, Systemen und Anwendungen
- Unterstützung durch CERT NRW bei Erkennung, Analyse und Behebung von Sicherheitsschwachstellen und IT-Angriffen

b. Büroräume

- Datenspeicherung nur im notwendigen Umfang und auf Servern
- Lokale Speicherung nur auf verschlüsselten Datenträgern
- Arbeitsanweisung für die Vernichtung von Unterlagen in entsprechenden Geräten und Containern

1.4 Trennungskontrolle

Hierzu zählen Maßnahmen, durch die gewährleistet wird, dass zu unterschiedlichen

Zwecken erhobene Daten getrennt verarbeitet werden.

- Testrechner werden von Produktivsystemen getrennt und unterliegen separaten Sicherheitsbeschränkungen
- Daten verschiedener Auftraggebenden oder Verfahren bleiben voneinander getrennt

2. Integrität, Art. 32 Abs. 1 b DSGVO
2.1 Weitergabekontrolle

Hierzu zählen Maßnahmen, durch die gewährleistet wird, dass personenbezogene Daten bei der Weitergabe (physisch oder elektronisch) nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Weiterhin kann überprüft und festgestellt werden, an welchen Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen der Datenübertragung vorgesehen ist.

a. Rechenzentrum

- Zugang zu Serversystemen nur über gesicherte Verbindungen
- Einsatz von VPN
- Nutzung von Signaturverfahren

b. Büroräume

- Keine Nutzung von mobilen Datenträgern
- Beschränkung der Laufwerksnutzung an Arbeitsplatzrechnern
- Einsatz verschlüsselter Notebooks

2.2 Eingabekontrolle

Hierzu zählen Maßnahmen, durch die gewährleistet wird, dass auch nachträglich prüf- und feststellbar ist, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

- Zugriffe auf Systeme mit personenbezogenen Daten werden protokolliert
- Schriftliche Verpflichtung auf den Datenschutz und Verschwiegenheit
- Ticketsystem
- Berechtigungskonzept

3. Verfügbarkeit und Belastbarkeit, Art. 32 Abs. 1 b DSGVO

Hierzu zählen Maßnahmen, durch die gewährleistet wird, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

- Backup
- Redundante Klimatisierung in allen Rechnerräumen
- Brandmeldeanlage mit Verbindung zur Feuerwehr, Feuerlöschanlage, teilw. Brandfrühesterkennungssysteme
- Notstromversorgung
- Notfallpläne

4. Auftragskontrolle, Art. 28 Abs. 3 DSGVO

Hierzu zählen Maßnahmen/Regelungen, durch die gewährleistet wird, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen der Auftraggebenden verarbeitet werden:

- Vertrag nach Artikel 28 DSGVO zwischen Auftraggebenden und Auftragnehmenden
- Belehrung über die Pflicht zur Wahrung des Datengeheimnisses für alle Beschäftigten von IT.NRW ist Bestandteil des Arbeitsvertrages und des Dienstverhältnisses
- Bei Einsatz von externem Personal werden diese ebenfalls zur Wahrung des Datengeheimnisses verpflichtet

5. Verfahren der regelmäßigen Überprüfung, Bewertung und Evaluierung, Art. 32 Abs. 1 d, Art. 25 Abs. 1 DSGVO

5.1 Datenschutzmanagement

Hierzu zählen Maßnahmen, die eine systematische Organisation, Steuerung und Überwachung des Datenschutzes gewährleisten:

- Zertifizierung nach DIN ISO 27001 auf Basis IT Grundschutz für die Betriebsinfrastrukturplattform der HSI
- Regelmäßige Sensibilisierung der Mitarbeiter/-in („na sicher“ Kampagne)
- Datenschutzbeauftragte
- Informationssicherheitsbeauftragte

5.2 Incident Response Management

Hierzu zählen Maßnahmen, durch gewährleistet wird, dass eine angemessene Reaktion auf Sicherheitsverletzungen erfolgt.

- Einsatz und Pflege von Firewalls und Virenscanner
- Zusammenarbeit mit dem CERT NRW
- Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen

5.3 Datenschutzfreundliche Voreinstellungen

- Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind
- Umfangreiche, gut auffindbare Datenschutzerklärung der jeweiligen Website

3 Liste der genehmigten Subunternehmer

	Name des Subunternehmers	Kontaktperson	Anschrift	Leistung
1	Ministerium für Arbeit, Gesundheit und Soziales des Landes NRW (MAGS)		Fürstenwall 25, 40219 Düsseldorf	Organisatorische Bündelung weiterer Auftragsverarbeiter (IT.NRW); Keine Verarbeitung der personenbezogenen Daten
2	Landesbetrieb Information und Technik Nordrhein-Westfalen (IT.NRW) (als weiterer Auftragsverarbeiter des MAGS)		Mauerstraße 51, 40476 Düsseldorf	Technischer Betrieb des Online-Dienstes; Betrieb der ZDI;