Anlage 5:

Vereinbarung zur Auftragsverarbeitung zum Einzelabruf und technisch-organisatorische Maßnahmen zur Nutzung der „Zentralen Datenaustausch-Infrastruktur (ZDI)

betreffend die OZG-Verwaltungsleistung:

„Unterhaltsvorschuss“ (10035)

Zwischen dem Leistungsbezieher (Auftraggeber/Kommune) und dem Leistungserbringer (Auftragnehmer/Kommunalvertreter NRW) wird mit Vertragsschluss des Einzelabrufs die folgende Einzel-Auftragsvereinbarung (nachstehend „Einzel-AV“) zum Einzelabruf betreffend die OZG-Verwaltungsleistung „Unterhaltsvorschuss“ als Anlage 5 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 Nutzung der „Zentralen Datenaustausch-Infrastruktur (ZDI) zu dem Einzelabruf „Unterhaltsvorschuss“.

1 OZG-Verwaltungsleistungs-spezifische Datenkategorien, Zwecke, Betroffene Der Auftragnehmer verarbeitet im Rahmen der OZG-Verwaltungsleistung „Unterhaltsvorschuss“ die folgenden personenbezogenen Daten:

I. Zweck

- Verarbeitung erforderlicher Daten zur Antragsbearbeitung

II. Betroffene

- Kind, für das Unterhaltsvorschuss beantragt wird
- Antragsteller:in
- Weitere gemeinsame Kinder
- Anderer familienferne Elternteil

III. Datenkategorien

- Angaben zum Kind, für das UVO beantragt wird: Beispielsweise Meldedaten, Abstammungsdaten, Aufenthalt, Wohnort, Staatsangehörigkeit, Wohnsituation, SGB Leistungen, Erwerbstätigkeiten, Einkünfte, Schul- und Studienbescheinigungen, gesetzliche oder rechtliche Vertreter, Beteiligung von Jugendämtern, inkl. der geforderten Nachweise.
- Angaben zum Antragsteller: Abfrage der persönlichen Daten des Antragstellers, der Bankverbindung, der Anschrift und des Familienstands und der Lebenslage. Bei-

spielsweise Meldedaten, Anspruchsvoraussetzungen, Kontaktdaten, Aufenthalt, Beschäftigung, Einkommen, Bankverbindung, Familienstand und Lebenslage inkl. der geforderten Nachweise.

- Weitere gemeinsame Kinder: Abfrage, ob es weitere gemeinsame Kinder gibt. Wenn ja, dann werden die Daten dieser Kinder abgefragt. Beispielsweise Meldedaten und Wohnort.
- Angaben zum familienfernen Elternteil: Abfrage, ob es Angaben zum anderen Elternteil gibt. Wenn ja, werden diese Angaben abgefragt. Beispielsweise wie bei Angaben zum Antragsteller und Vermögen, Grundbesitz, Kraftfahrzeugen, weiteren Kindern, Berufsausbildung inkl. der geforderten Nachweise.
- Vaterschaft: Angaben zur Vaterschaft, beispielsweise zur Anerkennung und Gerichtsverfahren wie eine Vaterschaftsanfechtungsklage inkl. der geforderten Nachweise.
- Angaben zum Unterhalt: Abfrage der Unterhaltsfestsetzung. Wenn diese erfolgt ist, dann Abfrage der Unterhaltszahlung. Beispielsweise Unterhaltszahlung, Unterhaltsfestsetzung.
- Kopien angehängter Dokumente des Antragstellers: Nachweise zu obigen Datenkategorien
- Authentisierungsdaten des Antragstellers: Authentisierungsdaten des Antragstellers zur Anmeldung an der OSI Plattform

2 Technische und organisatorische Maßnahmen (TOM)

Die technischen und organisatorischen Maßnahmen gestalten sich wie folgt:

- 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 dieser Einzel-AV durch.
- Bremen betreibt den bundesweiten Onlinedienst Unterhaltvorschuss. Bremen 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. Bremen hat jedoch keine Zugriffsmöglichkeit auf auftragsbezogene personenbezogene Daten dieser Einzel-AV und führt bezüglich dieser keinerlei Verarbeitung durch.
- IT.NRW betreibt die gesamte technische Infrastruktur für die Datenverarbeitung im Rahmen dieser Einzel-AV bis zu dem vertraglich vereinbarten Übergabepunkt. IT.NRW trifft für diese Datenverarbeitung die in dieser Einzel-AV festgelegten Technischen und Organisatorischen Maßnahmen.
- Für diese Einzel-AV vereinbaren die Vertragsparteien gemäß Ziffer 6 der Rahmenvereinbarung zur Auftragsverarbeitung die nachfolgend beschriebenen technischen und organisatorischen Maßnahmen.

Im Folgenden werden die technischen und organisatorischen Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit festgelegt, die IT.NRW mindestens einzurichten und laufend aufrecht zu erhalten hat. Ziel ist die Gewährleistung insbesondere die Vertraulichkeit, Integrität und Verfügbarkeit der im Auftrag verarbeiteten Informationen. Für die Bestimmung geeigneter TOM ist zunächst der Schutzbedarf der zu verarbeitenden personenbezogenen Daten festzulegen und hier zu dokumentieren.

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 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. Brandfrüherkennungssysteme
- 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 ISO 27001 auf Basis IT-Grundschutz für die Betriebsinfrastruktur (BIS)
- Regelmäßige Sensibilisierung der Beschäftigten („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	Anschrift	Leistung
1	IT.NRW	Mauerstraße 51 40476 Düsseldorf	Bereitstellung ZDI
2	Seven Principles Solutions & Consulting GmbH	Ettore-BugattiStraße 6-14 51149 Köln	Entwicklung und Support