Auftrag gemäß § 80 SGB X

Vereinbarung
zwischen

Senatsverwaltung für Bildung, Jugend und Wissenschaft des Landes Berlin
(Landesjugendamt)
vertreten durch die Abteilungsleiterin III
- nachstehend Auftraggeber genannt –

Und

_____
-nachstehend Auftragnehmer genannt-

Die Vertragsparteien treffen folgende Vereinbarung zur Auftragsdatenverarbeitung hinsichtlich von Daten von unbegleiteten minderjährigen Ausländern, die im Land Berlin zu verarbeiten sind:

1. der Gegenstand und die Dauer des Auftrags,

Gegenstand des Auftrags

Gegenstand des Auftrags zur Verarbeitung von Daten ist die Durchführung folgender Aufgaben durch den Auftragnehmer:

Einsichtnahme in Daten der minderjährigen Ausländer (UmA) im Rahmen des IT-Fachverfahrens ISBJ-UmA zur Dur**chführung der ambulanten Betreuung**

Dauer des Auftrags
Der Auftrag ist unbefristet erteilt und kann von beiden Parteien mit einer Frist von 3 Monate zum Monatsende gekündigt werden. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt. Wird der Vertrag über die Betreuung von UmA beendet, endet auch dieser Vertrag, ohne dass es einer Kündigung bedarf.

2. der Umfang, die Art und der Zweck der vorgesehenen Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen

Nähere Beschreibung des Auftragsgegenstandes im Hinblick auf Umfang, Art und Zweck der Aufgaben des Auftragnehmers:
Der Auftragnehmer übernimmt nach Anweisung des Auftraggebers die **Betreuung von neu eingereisten unbegleiteten ausländischen Kinder und Jugendlichen** im Rahmen der Inobhutnahme nach §§ 42, 42a SGB VIII, **insbesondere kümmert er sich um die Terminplanung im Rahmen des Clearingverfahrens.**
Die Nutzung der Daten findet ausschließlich im Gebiet der Bundesrepublik Deutschland statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers.

die Art der Daten

Gegenstand der Nutzung personenbezogener Daten sind folgende Datenarten / -kategorien (Aufzählung / Beschreibung der
Datenkategorien):

Datenfelder Personenstammdaten, Kommunikationsdaten:

- Personenidentifikationsnummer (PID)
- Name
- Vorname
- Alias
- Geschlecht
- Geburtsdatum
- Staatsangehörigkeit
- Foto

der Kreis der Betroffenen

Personen: Alle ausländischen unbegleiteten Kinder und Jugendlichen, die ohne Sorgeberechtigte/Eltern(-teile) bzw. ohne Personen, die von ihren Eltern bevollmächtigt wurden nach Deutschland eingereist sind und dem Auftragnehmer zur Betreuung zugeteilt wurden.
Beschäftigte: Mitarbeiter des Auftragnehmers

3. die nach § 78a zu treffenden technischen und organisatorischen Maßnahmen

Die zu treffenden technischen und organisatorischen Maßnahmen werden im verfahrensspezifischen Sicherheitskonzept ISBJ dokumentiert. Folgende Maßnahmen nach der Anlage zu § 78a SGB X werden getroffen:

1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen Sozialdaten verarbeitet oder genutzt werden, zu verwehren (**Zutrittskontrolle**),

Im Hochsicherheits-Data-Center (HSDC) des ITDZ Berlin, in dem die Datenverarbeitung von ISBJ erfolgt, ist sichergestellt, dass alle Beteiligten nur über das Zutrittskontrollsystem in Form von Pförtner, Chipkarten, Türsicherungen, Überwachungseinrichtungen und besonders geschützten Sicherheitsbereichen der Datenverarbeitung entsprechend des Standortsicherheitskonzepts des ITDZ Berlin Zutritt erhalten. Für die Standorte, an denen die Endgeräte der Sachbearbeiter stehen, erfolgt die Zutrittskontrolle entsprechend den Standortsicherheitskonzepten.

2. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (**Zugangskontrolle**),

Die Zugangskontrolle erfolgt zweistufig zuerst über eine Authentifizierung mit digitalen Zertifikaten (TLS-Clientzertifikate) und dann über eine benutzerspezifische Anmeldung mit Nutzername und Passwort. Die digitalen Zertifikate werden nur an berechtigte

Nutzende ausgegeben und begrenzen den Zugang auf eine geschlossene Benutzergruppe. Nur nach einer Authentifizierung mit einem gültigen digitalen Zertifikat ist die Anmeldung mit Nutzername und Passwort zugänglich.
Es ist sichergestellt, dass alle beteiligten Organisationen den Kreis der autorisierten Zugriffsberechtigten auf das ISBJ-UmA System ausschließlich zum Zweck der Dienst-Bereitstellung beschränken und dies durch Passwortrichtlinien für Kennwortverfahren (inkl. Sonderzeichen, Mindestlänge, regelmäßiger Wechsel des Kennworts), Zertifikate, automatische Sperrung sowie Verschlüsselung der Datenträger sicherstellen.

3. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass Sozialdaten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (**Zugriffskontrolle**),

Es ist sichergestellt, dass alle beteiligten Organisationen den Zugriff der Kreis der autorisierten Zugriffsberechtigten auf das ISBJ-UmA Moduls durch differenzierte Berechtigungen steuern.
ISBJ verfügt über ein flexibles Berechtigungskonzept und gestattet über detaillierte Berechtigungen den jeweiligen Nutzenden nur die Verarbeitung der für das jeweilige Aufgabengebiet benötigten Daten, insbesondere

- Daten vor nicht autorisierten Zugriffen zu schützen
- die Zugriffsrechte von Mitarbeiterinnen und Mitarbeitern auf bearbeitungserforderliche Daten und Funktionen zu definieren
- Benutzern gezielte Berechtigungen für einzelne Anwendungen zu erteilen und
- die Administration des Berechtigungssystems (Anlegen und Pflegen von Benutzerparametern) zu unterstützen.

Bei der Einrichtung von Berechtigungen wird sichergestellt, dass Anwendende nur auf die zur dienstlichen Aufgabenerledigung notwendigen Daten mit der hierfür erforderlichen Zugriffsberechtigung zugreifen dürfen.

4. zu gewährleisten, dass Sozialdaten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Es ist sichergestellt, dass alle beteiligten Organisationen folgende Schutzmaßnahmen bei Transport, Übertragung und Übermittlung oder Speicherung auf Datenträger (manuell oder elektronisch) sowie bei der nachträglichen Überprüfung vorgesehen haben: Verschlüsslung aller Daten (soweit technisch möglich) und Außenverbindungen, Nutzung von verschlüsselten Verbindungen (TLS, VPN) zum Austausch der Daten, Sicherung durch elektronische Signaturen, sowie Protokollierung aller Datenübermittlungsflüsse. Personenbezogene Daten können nur in der gesicherten IT-Infrastruktur von ISBJ im HSDC des ITDZ webbasiert verarbeitet und gespeichert werden. Innerhalb des HSDC des ITDZ werden die Maßnahmen entsprechend des Standortsicherheitskonzepts des ITDZ Berlin umgesetzt.

5. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem Sozialdaten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (**Eingabekontrolle**),

Es ist sichergestellt, dass alle beteiligten Organisationen die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege gewährleisten. Zur nachträglichen Überprüfung beim ISBJ-JuHi-System, ob und von wem Daten eingegeben, verändert oder gelöscht worden sind werden folgende Maßnahmen gewährleistet: Es wurden über alle relevanten Datenprozesse Protokollierungs- und Auswertungsmechanismen eingerichtet. Zuständig- und Verantwortlichkeiten zum Umgang mit personenbezogenen Daten sind im Rahmen des Berechtigungsmanagements durch die Vergabe eindeutiger Berechtigungen festgelegt. Das System protokolliert die Änderungszeitpunkte und die Personen, die diese Änderungen durchgeführt haben. Die Protokollierung umfasst auch Änderungen der Berechtigungen.

6. zu gewährleisten, dass Sozialdaten, die im Auftrag genutzt werden, nur entsprechend den Weisungen des Auftraggebers genutzt werden können (**Auftragskontrolle**),

Eine Bearbeitung der Daten ist aufgrund eines flexiblen Rollen- und Berechtigungskonzepts nur durch berechtigte Funktionsträger möglich. Eine Veränderung der Daten durch andere als die berechtigten Nutzenden ist ausgeschlossen.
Mitarbeiter des Auftragnehmers werden auf das Datengeheimnis verpflichtet.

7. zu gewährleisten, dass Sozialdaten gegen zufällige Zerstörung oder Verlust geschützt sind (**Verfügbarkeitskontrolle**),

Der Zugriff auf die Daten erfolgt webbasiert über die Applikationsserver des des ITDZ. Die Daten stehen somit zeitgerecht zur Verfügung und können ordnungsgemäß verarbeitet werden. Alle Daten werden nach vollständiger Erfassung im Trägerportal in die interne Datenbank übertragen. Durch eine tägliche Datensicherung ist sichergestellt, dass Daten zeitnah wiederhergestellt werden können. Durch ein redundant ausgelegtes Datenbanksystem (Cluster) werden technische Störungen an Einzelsystemen kompensiert. Alle Maßnahmen zur Verfügbarkeitskontrolle sind entsprechend des Standortsicherheitskonzepts des ITDZ Berlin umgesetzt.

Durch ein passwortgesichertes Zugriffskonzept (Anmeldung mit persönlicher Kennung und einem Passwort) ist sichergestellt, dass nur die entsprechend funktional berechtigten Personen Editor- bzw. Leserrechte haben.

Eine Maßnahme nach Satz 2 Nummer 2 bis 4 ist insbesondere die Verwendung von **dem Stand der Technik entsprechenden Verschlüsselungsverfahren**.

Diese Vorgabe wird durch das etablierte Informationssicherheitsmanagementsystem (ISMS) nach dem BSI-Stand 100-1 des IT-Grundschutz entsprechend dem verfahrensspezifischen Sicherheitskonzept umgesetzt und regelmäßig überprüft.

4. die bestehenden Pflichten des Auftragnehmers, insbesondere die von ihm vorzunehmenden Kontrollen,

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags nach § 11 Abs. 4 BDSG folgende Pflichten:

- Die Wahrung des Datengeheimnisses entsprechend § 5 BDSG. Alle Personen, die auftragsgemäß auf personenbezogene Daten des Auftraggebers zugreifen können, müssen auf das Datengeheimnis verpflichtet und über die sich aus diesem Auftrag ergebenden besonderen Datenschutzpflichten sowie die bestehende Weisungs- bzw. Zweckbindung belehrt werden.
- Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde nach § 38 BDSG. Dies gilt auch, soweit eine zuständige Behörde nach §§ 43, 44 BDSG beim Auftragnehmer ermittelt.
- Die Durchführung der Auftragskontrolle mittels regelmäßiger Prüfungen durch den Auftragnehmer im Hinblick auf die Vertragsausführung bzw. -erfüllung, insbesondere Einhaltung und ggf. notwendige Anpassung von Regelungen und Maßnahmen zur Durchführung des Auftrags.

5. die Kontrollrechte des Auftraggebers und die entsprechenden Duldungs- und Mitwirkungspflichten des Auftragnehmers,

Der Auftraggeber hat das Recht, die in Nr. 6 der Anlage zu § 9 BDSG vorgesehene Auftragskontrolle im Benehmen mit dem Auftragnehmer 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 verpflichtet sich, dem Auftraggeber auf Anforderung die zur Wahrung seiner Verpflichtung zur Auftragskontrolle erforderlichen Auskünfte zu geben und die entsprechenden Nachweise verfügbar zu machen.
Im Hinblick auf die Kontrollverpflichtungen des Auftraggebers nach § 11 Abs. 2 Satz 4 BDSG vor Beginn der Datenverarbeitung und während der Laufzeit des Auftrags stellt der Auftragnehmer sicher, dass sich der Auftraggeber von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen überzeugen kann. Hierzu weist der Auftragnehmer dem Auftraggeber auf Anfrage die Umsetzung der technischen und organisatorischen Maßnahmen gemäß § 9 BDSG und der Anlage nach. Dabei kann der Nachweis der Umsetzung solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, auch durch Vorlage eines aktuellen Testats, von Berichten oder Berichtsauszügen unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz) erbracht werden.

6. mitzuteilende Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz von Sozialdaten oder gegen die im Auftrag getroffenen Festlegungen,

Der Auftragnehmer erstattet in allen Fällen dem Auftraggeber eine Meldung, wenn durch ihn oder die bei ihm beschäftigten Personen Verstöße gegen Vorschriften zum Schutz personenbezogener Daten des Auftraggebers oder gegen die im Auftrag getroffenen Festlegungen vorgefallen sind.

Es ist bekannt, dass nach § 83a SGB X Informationspflichten im Falle des Abhandenkommens oder der unrechtmäßigen Übermittlung oder Kenntniserlangung von personenbezogenen Daten bestehen können. Deshalb sind solche Vorfälle ohne Ansehen der Verursachung unverzüglich dem Auftraggeber mitzuteilen. Dies gilt auch bei schwerwiegenden Störungen des Betriebsablaufs, bei Verdacht auf sonstige Verletzungen gegen Vorschriften zum Schutz personenbezogener Daten oder anderen Unregelmäßigkeiten beim Umgang mit personenbezogenen Daten des Auftraggebers. Der Auftragnehmer hat im Benehmen mit dem Auftrag-geber angemessene Maßnahmen zur Sicherung der Daten sowie zur Minderung möglicher nachteiliger Folgen für Betroffene zu ergreifen. Soweit den Auftraggeber Pflichten nach § 83a SGB X treffen, hat der Auftragnehmer ihn hierbei zu unterstützen.

7. der Umfang der Weisungsbefugnisse, die sich der Auftraggeber gegenüber dem Auftragnehmer vorbehält,

Der Umgang mit den Daten erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisung des Auftraggebers (vgl. § 80 (2) Satz 2 und 3 SGB X sowie § 11 Abs. 3 Satz 1 BDSG). Der Auftraggeber behält sich im Rahmen der in dieser Vereinbarung getroffenen Auftragsbeschreibung ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung vor, das er durch Einzelweisungen konkretisieren kann. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren. Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger schriftlicher Zustimmung durch den Auftraggeber erteilen.
Mündliche Weisungen wird der Auftraggeber unverzüglich schriftlich oder per E-Mail (in Textform) bestätigen. Der Auftragnehmer verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben. Kopien und Duplikate 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.
Der Auftragnehmer hat den Auftraggeber unverzüglich entsprechend § 11 Abs. 3 Satz 2 BDSG 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 Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.

8. Die Vertragsparteien treffen in Anbetracht der besonderen Dringlichkeit der Aufgabe diese Vereinbarung. Soweit aus datenschutzrechtlichen Gründen eine Ergänzung oder Änderung dieser Vereinbarung erforderlich ist, werden die Vertragsparteien diese unverzüglich vornehmen.

_____ _____

Berlin, den

Senatsverwaltung für Bildung, Jugend und Wissenschaft

Berlin, den

Träger vertreten durch