

## **Vertrag zur Auftragsverarbeitung gemäß Art. 28 DSGVO**

zwischen

*dem Landkreis Eichsfeld, Friedensplatz 8, 37308 Heilbad Heiligenstadt*  
– nachstehend im Rahmen dieses Vertrags Auftraggeber genannt –

und

...

– nachstehend im Rahmen dieses Vertrags Auftragnehmer genannt –

### **§ 1 Gegenstand und Dauer des Auftrags**

(1) Diese Vereinbarung regelt die Verarbeitung (Art. 4 Nr. 2 DSGVO) personenbezogener Daten (Art. 4 Nr. 1 DSGVO, im Folgenden: Daten) durch den Auftragnehmer im Auftrag des Auftraggebers. Die Art der Daten, Art und Zweck der Datenverarbeitung sowie die Kategorien betroffener Personen sind in der/den Anlage(n) Zusatzvereinbarung zum Vertrag zur Auftragsverarbeitung bestimmt.

(2) 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. Jede Verlagerung der Dienstleistung oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und erfolgt nur, wenn die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

### **§ 2 Verantwortlichkeit**

(1) Der Auftraggeber ist im Rahmen dieses Vertrags für die Einhaltung der datenschutzrechtlichen Bestimmungen, insbesondere auch für die Rechtmäßigkeit der Weitergabe der zu verarbeitenden Daten an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung, allein verantwortlich (Verantwortlicher i.S.d. Art. 4 Nr. 7 DSGVO). Der Auftraggeber ist gemäß Art. 5 Abs. 2 für die Einhaltung der Grundsätze für die Verarbeitung personenbezogener Daten (Art. 5 Abs. 1 DSGVO) verantwortlich.

(2) Auftraggeber und Auftragnehmer unterstützen sich gegenseitig beim Nachweis und der Dokumentation der ihnen obliegenden Rechenschaftspflicht.

(3) Der Auftraggeber ist weiter allein verantwortlich für die Wahrnehmung der Rechte der Betroffenen i.S.v. Art. 12 bis 22 DSGVO.

### **§ 3 Rechte und Pflichten des Auftraggebers**

(1) Der Auftraggeber hat hinsichtlich der Datenverarbeitung ein umfassendes Weisungsrecht. Änderungen des Verarbeitungsgegenstands und Verfahrensänderungen sind zwischen den Parteien abzustimmen und zu dokumentieren. Weisungsberechtigt sind dabei die zeichnungsbefugten Angehörigen der gemäß Geschäftsverteilungsplan zuständigen Organisationseinheit des Auftraggebers. Der Auftraggeber kann jederzeit die Herausgabe, Berichtigung, Anpassung, Löschung und Einschränkung der Verarbeitung der Daten verlangen.

(2) Weisungen werden zunächst durch die Hauptvereinbarung definiert und können von dem Auftraggeber ansonsten durch eine einzelne Weisung geändert, ergänzt oder ersetzt werden. Weisungen werden in schriftlicher Form oder in einem elektronischen Format erteilt, ergänzt oder geändert. Mündliche Weisungen sind unverzüglich schriftlich zu bestätigen.

(3) Weisungsempfänger beim Auftragnehmer sind die jeweils verantwortlichen Beschäftigten in den leistenden Bereichen beim Auftragnehmer. Sofern diese nicht

erreichbar sind, stellt der Auftragnehmer die Aufgabenerledigung sicher.

(4) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen bei der Prüfung der Auftragsergebnisse feststellt.

(5) Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse der Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln.

(6) Der Auftraggeber führt das Verarbeitungsverzeichnis nach Artikel 30 Absatz 1 DSGVO.

#### **§ 4 Rechte und Pflichten des Auftragnehmers**

(1) Der Auftragnehmer verarbeitet die Daten ausschließlich im Rahmen des Auftrags und der Weisungen des Auftraggebers, es sei denn, es liegt ein Fall des Artikel 28 Absatz 3 a) DSGVO vor.

(2) Ist der Auftragnehmer der Auffassung, eine Weisung verstoße gegen geltendes Recht, informiert er den Auftraggeber unverzüglich. In diesem Fall darf der Auftragnehmer die Umsetzung der Weisung solange aussetzen, bis der Auftraggeber die Weisung bestätigt oder abändert.

(3) Der Auftragnehmer gewährleistet einen angemessenen Schutz der Daten durch technische und organisatorische Maßnahmen, die den Anforderungen der DSGVO genügen (Datenschutzkonzept). Er hat technische und organisatorische Maßnahmen zu treffen, die insbesondere die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen und welche die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsergebnissen ermöglichen. Die in der Anlage 1 aufgeführten technischen und organisatorischen Maßnahmen sind Grundlage des Auftrags. Soweit eine Prüfung oder ein Audit des Auftraggebers diesbezüglich einen sich aus der DSGVO erforderlichen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen. Die technisch-organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei wird das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten. Wesentliche Änderungen der technischen und organisatorischen Maßnahmen sind zu dokumentieren.

(4) Der Auftragnehmer setzt ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verfahren ein.

(5) Der Auftragnehmer sichert zu, dass die Daten von sonstigen Datenbeständen technisch bzw. logisch getrennt werden. Von diesem Erfordernis ausgenommen sind gemeinsam genutzte Infrastrukturkomponenten (wie Proxy-Server oder Firewalls), die nur dem Transport der Daten dienen.

(6) Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes der personenbezogenen Daten bekannt werden und spricht sich hinsichtlich der insoweit zu treffenden Maßnahmen mit dem Auftraggeber ab. Die Regelungen der Art. 33 und 34 DSGVO bleiben davon unberührt.

(7) Der Auftragnehmer gewährleistet, dass alle von ihm bei der Auftragsverarbeitung eingesetzten Personen nach dem Verpflichtungsgesetz zur Vertraulichkeit und gewissenhaften Erfüllung ihrer Obliegenheiten verpflichtet sind. Die Vertraulichkeitspflicht

besteht auch nach Beendigung des Auftrages fort.

(8) Der Auftragnehmer unterstützt den Auftraggeber bei der Erfüllung von Anfragen und Ansprüchen betroffener Personen. Wendet sich eine betroffene Person unmittelbar an den Auftragnehmer, leitet dieser das Ersuchen unverzüglich an den Auftraggeber weiter und verweist die betroffene Person an den Auftraggeber.

(9) 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.

(10) Der Auftragnehmer unterstützt den Auftraggeber bei der Erstellung des Verarbeitungsverzeichnisses nach Artikel 30 Absatz 1 DSGVO. Er führt das Verarbeitungsverzeichnis nach Artikel 30 Absatz 2 DSGVO.

### **§ 5 Kontrollrechte des Auftraggebers**

(1) Der Auftraggeber ist berechtigt, die Einhaltung der Vorschriften über den Datenschutz selbst oder durch Dritte zu kontrollieren, insbesondere durch die Einholung von Auskünften, durch Einsichtnahme in die gespeicherten Daten und Datenverarbeitungsprogramme sowie durch Kontrollen während der Betriebs- und Geschäftszeiten vor Ort.

(2) Der Auftragnehmer wirkt, soweit erforderlich, an Kontrollen mit. Er 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 kann erfolgen durch

- a. die Einhaltung genehmigter Verhaltensregeln,
- b. die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Artikel 42 DSGVO,
- c. aktuelle Testate oder Berichte unabhängiger Bereiche wie z.B. Revision, Datenschutzbeauftragter, IT-Sicherheitsbeauftragter oder durch
- d. eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit, z.B. nach BSI-Grundschutz.

(4) Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Auftraggebers eine Kontrolle vornehmen, gelten die Absätze 1 bis 3 entsprechend. Der Auftragnehmer informiert den Auftraggeber unverzüglich über Kontrollen und Maßnahmen der Datenschutzaufsichtsbehörde.

### **§ 6 Unterstützung durch den Auftragnehmer**

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 DSGVO genannten Pflichten zum Schutz personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Anfragen. Hierzu gehören insbesondere

- a. die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden,
- b. die Verpflichtung, den Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich bereit zu stellen,
- c. die Unterstützung des Auftraggebers bei dessen Datenschutz-Folgeabschätzung und insbesondere die Zurverfügungstellung aller hierfür erforderlichen Informationen,
- d. die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde und insbesondere die Zurverfügungstellung aller hierfür erforderlichen Informationen,
- e. die Unterstützung hinsichtlich der Rechte der betroffenen Personen, etwa auf Auskunftserteilung, Berichtigung oder Löschung.

## § 7 Unterauftragsverhältnisse

(1) Der Einsatz von Subunternehmern als weitere Auftragsverarbeiter ist nur zulässig, wenn der Auftraggeber zuvor schriftlich zugestimmt hat. Eine zustimmungsbedürftige Beauftragung eines Subunternehmers liegt bereits dann vor, wenn dieser mit der ganzen oder einer Teilleistung der im Vertrag vereinbarten Leistung beauftragt wird.

(2) Der Auftragnehmer hat sicherzustellen, dass in der Vereinbarung mit dem Subunternehmer das Datenschutzniveau diesem Vertrag entspricht und alle Vorgaben dieses Vertrags eingehalten werden können. In dem Vertrag mit dem Subunternehmer sind die Angaben so konkret festzulegen, dass die Verantwortlichen des Auftragnehmers und des Subunternehmers deutlich voneinander abgegrenzt werden.

(3) Der Auftragnehmer hat sicherzustellen, dass der Auftraggeber in der Vereinbarung mit dem Subunternehmer die gleichen Kontrollrechte hat wie nach dem vorliegenden Vertrag.

Die Weiterleitung von Daten an den Subunternehmer ist erst zulässig, wenn dieser die Verpflichtungen nach Artikel 29 und Artikel 32 Absatz 4 DSGVO bezüglich seiner Beschäftigten erfüllt hat. Der Auftragnehmer hat die Einhaltung der Pflichten des Subunternehmers zu überprüfen. Das Ergebnis der Überprüfung ist zu dokumentieren und dem Auftraggeber auf Verlangen zugänglich zu machen.

(4) Der Auftragnehmer haftet gegenüber dem Auftraggeber für die Einhaltung der Pflichten des Subunternehmers.

## § 8 Löschen oder Rückgabe von personenbezogenen Daten

(1) Überlassene Daten(-sätze) und Datenträger verbleiben im Eigentum des Auftraggebers.

(2) 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.

(3) Daten, Datenträger sowie sämtliche sonstigen Materialien sind nach Auftragsende auf Verlangen des Auftraggebers entweder herauszugeben oder datenschutzgerecht zu vernichten. Im Fall von Test- und Ausschussmaterialien ist eine Einzelbeauftragung nicht erforderlich. Das Protokoll der Löschung oder Vernichtung ist dem Auftraggeber mit Datumsangabe schriftlich oder in elektronischer Form auf Anforderung vorzulegen.

## § 9 Schlussbestimmungen

Änderungen oder Ergänzungen dieser Vereinbarung bedürfen der Schriftform. Datenschutzrechtliche Regelungen, die vor Abschluss dieses Vertrags zwischen den Parteien vereinbart worden sind, werden mit Unterzeichnung dieses Vertrages gegenstandslos. Der Auftragnehmer ist verpflichtet, auch über das Ende der Beauftragung hinaus die ihm im Zusammenhang mit der Beauftragung bekannt gewordenen Daten vertraulich zu behandeln. Die vorliegende Zusatzvereinbarung bleibt auch nach Beendigung der Leistung solange gültig, wie der Auftragnehmer über personenbezogene Daten verfügt, die ihm vom Auftraggeber zugeleitet wurden oder die er für diesen erhoben hat.

\_\_\_\_\_  
Ort, Datum, Unterschrift  
Für den Auftraggeber

\_\_\_\_\_  
Ort, Datum, Unterschrift  
Für den Auftragnehmer

## **Anlage 1: Zusatzvereinbarung zum Vertrag zur Auftragsverarbeitung**

zwischen

*dem Landkreis Eichsfeld, Friedensplatz 8, 37308 Heilbad Heiligenstadt*  
– nachstehend im Rahmen dieses Vertrags Auftraggeber genannt –

und

...

– nachstehend im Rahmen dieses Vertrags Auftragnehmer genannt –

Diese Zusatzvereinbarung ist eine Anlage zum Vertrag zur Auftragsverarbeitung gemäß Art. 28 DSGVO.

### **Leistungsbezeichnung:**

Soziale Betreuung und Beratung der Asylbewerber und ausländischen Flüchtlinge im Landkreis Eichsfeld

### **Zu § 1 Gegenstand und Dauer des Auftrags**

Der Gegenstand des Auftrags wird wie folgt konkretisiert:

(1) Zweck der Verarbeitung

Bedarfsgerechte Beratungsleistung für Asylbewerber und Flüchtlinge im Landkreis Eichsfeld

(2) Art der Daten

Gegenstand der Verarbeitung sind folgende personenbezogene Daten:  
Stammdaten, Kontodaten, Dokumente der Akte

(3) Kreis der Betroffenen

Der Kreis der durch den Umgang mit personenbezogenen Daten Betroffenen umfasst:  
Asylbewerber/Flüchtlinge, Vertreter, Bevollmächtigte, Kinder