Angebot auf Abschluss eines Auftragsverarbeitungsvertrages für den Online-Dienst: Einbürgerung (OZG-ID: 10257)

d-NRW AöR, Rheinische Str. 1, 44137 Dortmund (dienstbetreibender IT-Dienstleister des umsetzenden Landes) nachfolgend „Auftragsverarbeiter“

bietet den für die o. g. Leistung den aus dem FIT-Store nutzungsberechtigten Behörden (nachfolgend beide zusammen: die Parteien) verbindlich den Abschluss des nachfolgenden Auftragsverarbeitungsvertrages[[1]](#footnote-1) an.

Präambel

Das vorliegende Angebot auf Abschluss eines privatrechtlichen Auftragsverarbeitungs-vertrages (nachfolgend nur: Auftragsverarbeitungsvertrag, Vertrag oder auch Klauseln) begründet die datenschutzrechtlichen Rechte und Pflichten für den o. g. Online-Dienst gem. Art. 28 DSGVO. Es richtet sich ausschließlich an die Behörden, die direkt oder mittelbar Nutzungsrechte am Online-Dienst über den FIT-Store erworben haben. Diese nachnutzenden Behörden sind datenschutzrechtlich Verantwortliche gem. Art. 4 Nr. 7 DSGVO. Die Details der Datenverarbeitung sind in Anhang II beschrieben.

Der Online-Dienst wird als Einer-für-Alle/Viele-Leistung (EfA) als Software-as-a-Service (SaaS) bereitgestellt. Online-Dienste sind digitale Services, über die Anspruchsberechtigte Antragsformulare ausfüllen und die entsprechenden Daten an die jeweils zuständige Behörde übermitteln können. „EfA“ bedeutet, dass ein Land den Online-Dienst entwickelt und zentral betreibt, und alle anderen Länder den Online-Dienst nachnutzen können.

Die Nutzungsrechte[[2]](#footnote-2) des Verantwortlichen an dem Online-Dienst werden separat über den FIT- Store erworben, was auch für die Vergütung gilt.[[3]](#footnote-3) Bereitsteller und Kunden der FITKO (Föderale IT-Kooperation) AöR verarbeiten im Rahmen der FIT-Store-Verträge keine personenbezogenen Daten des Online-Dienstes und sind weder Vertragsparteien dieses Auftragsverarbeitungsvertrages, noch Verantwortliche gem. Art. 4 Nr. 7 DSGVO.[[4]](#footnote-4) Der Vertrag berechtigt und verpflichtet damit ausschließlich die Vertragsparteien.

Der Auftragsverarbeitungsvertrag ist rechtlich eigenständig gegenüber den Verträgen, die im FIT-Store geschlossen werden. Bei diesen Verträgen handelt es sich um den Vertrag zwischen dem Bereitsteller und der FITKO zur Aufnahme eines Online-Dienstes in den FIT-Store und den Vertrag zwischen der FITKO und dem Kunden, der diesen Online-Dienst mit- oder nachnutzt (begleitende Verträge). Der vorliegende Auftragsverarbeitungsvertrag besteht als Grundlage für die Datenverarbeitung auch dann fort, wenn einer der begleitenden Verträge wegfallen sollte. Die Regelungen, Interessenabwägungen und Anlagen der begleitenden Verträge sind bei der Auslegung dieses Vertrages zu berücksichtigen, wenn und soweit eine Auslegung dieses Vertrages erforderlich werden sollte, oder wenn ausdrücklich auf sie verwiesen wird.

Teil 1: Allgemeine Regelungen

§ 1 Zweck und Anwendungsbereich

a) Mit diesem Auftragsverarbeitungsvertrag soll die Einhaltung von Art. 28 Abs. 3, 4 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (DSGVO) sichergestellt werden.

b) Der in Anhang I aufgeführte Verantwortliche und der Auftragsverarbeiter haben diesen Klauseln zugestimmt, um die Einhaltung von Art. 28 Abs. 3, 4 DSGVO zu gewährleisten.

c) Diese Klauseln gelten für die Verarbeitung personenbezogener Daten gemäß Anhang II.

d) Die Anhänge I bis IV sind Bestandteil der Klauseln.

e) Diese Klauseln gelten unbeschadet der Verpflichtungen, denen der Verantwortliche und der Auftragsverarbeiter gemäß der DSGVO unterliegen.

§ 2 Änderungen des Vertrages

a) Änderungen dieses Vertrages sind nur durch ausdrückliche, übereinstimmende, beweissicher dokumentierte Erklärungen beider Parteien in Textform zulässig. Soweit in diesem Vertrag von Textform die Rede ist, ist Textform gem. § 126b BGB gemeint.

b) Dies hindert die Parteien nicht daran, diesen Vertrag in einen umfangreicheren Vertrag aufzunehmen und weitere Klauseln oder zusätzliche Garantien hinzuzufügen, sofern diese weder unmittelbar noch mittelbar im Widerspruch zu den Klauseln stehen oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneiden. Insoweit sind die Parteien auch nicht daran gehindert, Verträge neben diesem Vertrag zu schließen.

§ 3 Auslegung

a) Werden in diesen Klauseln die in der DSGVO definierten Begriffe verwendet, so haben diese Begriffe dieselbe Bedeutung wie in der betreffenden Verordnung.

b) Diese Klauseln sind im Lichte der Bestimmungen der DSGVO auszulegen.

c) Diese Klauseln dürfen nicht in einer Weise ausgelegt werden, die den in der DSGVO vorgesehenen Rechten und Pflichten zuwiderläuft oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneidet.

§ 4 Vorrang

Im Falle eines Widerspruchs zwischen diesen Klauseln und den Bestimmungen damit zusammenhängender Vereinbarungen, die zwischen den Parteien bestehen oder später eingegangen oder geschlossen werden, haben diese Klauseln Vorrang.

§ 5 Gültigkeit und Annahme des Angebots auf Abschluss eines Auftragsverarbeitungsvertrages

a) Das vorliegende Angebot richtet sich an alle Behörden, denen mittelbar oder unmittelbar über den FIT-Store Nutzungsrechte am Online-Dienst eingeräumt wurden. Annahmeerklärungen durch Verantwortliche außerhalb dieses Kreises von Berechtigten führen nicht zum Abschluss eines Auftragsverarbeitungsvertrages.

b) Das vorliegende Angebot ist so lange gültig, wie es im FIT-Store, auf anderen Vertriebsplattformen oder beim Auftragsverarbeiter verfügbar ist.

c) Die Angebotsannahme erfolgt über die in Anhang I beschriebene Art und Weise. Die Pflichtangaben sind als vertragswesentliche Bestandteile Voraussetzung für einen Vertragsschluss.

§ 6 Beschreibung der Verarbeitung

Die Einzelheiten der Verarbeitungsvorgänge, insbesondere die Kategorien personenbezogener Daten und die Zwecke, für die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden, sind in Anhang II aufgeführt.

Teil 2: Pflichten der Parteien

§ 7 Weisungen

a) Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur auf dokumentierte Weisung (Textform) des Verantwortlichen, es sei denn, er ist nach Unionsrecht oder nach dem Recht eines Mitgliedstaats, dem er unterliegt, zur Verarbeitung verpflichtet. In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet. Der Verantwortliche kann während der gesamten Dauer der Verarbeitung personenbezogener Daten weitere Weisungen erteilen. Diese Weisungen sind stets zu dokumentieren. Die weisungsberechtigten Personen sind in Anhang I anzugeben.

b) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass vom Verantwortlichen erteilte Weisungen gegen die DSGVO oder geltende Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstoßen.

c) Der Verantwortliche setzt dem Auftragsverarbeiter eine angemessene Frist zur Umsetzung der Weisungen. Er wird bei der Fristsetzung und Abfassung seiner Weisungen berücksichtigen, dass der Auftragsverarbeiter Weisungen anderer Verantwortlicher unterliegen kann, und anstreben, sich, unbeschadet seiner gesetzlichen Rechte, mit anderen Verantwortlichen abzustimmen.

d) Sollte der Auftragsverarbeiter wider Erwarten eine Weisung des Verantwortlichen nicht innerhalb der gesetzten Frist umsetzen können, ist er verpflichtet, den Verantwortlichen unverzüglich hierüber mit Angabe ihn verhindernder Gründe zu informieren.

§ 8 Zweckbindung

Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten nur für den/die in Anhang II genannten spezifischen Zweck(e), sofern er keine weiteren Weisungen des Verantwortlichen erhält.

§ 9 Dauer der Verarbeitung personenbezogener Daten

Die Dauer der Auftragsverarbeitung richtet sich nach der Dauer der Nutzung des Onlinedienstes durch die verantwortliche Behörde.

§ 10 Sicherheit der Verarbeitung

a) Der Auftragsverarbeiter ergreift mindestens die in Anhang III aufgeführten technischen und organisatorischen Maßnahmen, um die Sicherheit der personenbezogenen Daten zu gewährleisten. Dies umfasst den Schutz der Daten vor einer Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu den Daten führt (im Folgenden „Verletzung des Schutzes personenbezogener Daten“). Bei der Beurteilung des angemessenen Schutzniveaus tragen die Parteien dem Stand der Technik, den Implementierungskosten, der Art, dem Umfang, den Umständen und den Zwecken der Verarbeitung sowie den für die betroffenen Personen verbundenen Risiken gebührend Rechnung.

b) Der Auftragsverarbeiter gewährt seinem Personal nur insoweit Zugang zu den personenbezogenen Daten, die Gegenstand der Verarbeitung sind, als dies für die Durchführung, Verwaltung und Überwachung des Vertrags unbedingt erforderlich ist. Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung der erhaltenen personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

§ 11 Sensible Daten

Falls die Verarbeitung personenbezogene Daten betrifft, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, oder die genetische Daten oder biometrische Daten zum Zweck der eindeutigen Identifizierung einer natürlichen Person, Daten über die Gesundheit, das Sexualleben oder die sexuelle Ausrichtung einer Person oder Daten über strafrechtliche Verurteilungen und Straftaten enthalten (im Folgenden „sensible Daten“), wendet der Auftragsverarbeiter spezielle Beschränkungen und/oder zusätzlichen Garantien an.

Die speziellen Beschränkungen und/oder zusätzlichen Garantien sind vom Auftragsverarbeiter gesondert in Anhang III – Technisch-Organisatorische Maßnahmen – anzugeben.

§ 12 Dokumentation und Einhaltung der Klauseln

a) Die Parteien müssen die Einhaltung dieser Klauseln nachweisen können.

b) Der Auftragsverarbeiter bearbeitet Anfragen des Verantwortlichen bezüglich der Verarbeitung von Daten gemäß diesen Klauseln umgehend und in angemessener Weise.

c) Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, die für den Nachweis der Einhaltung der in diesen Klauseln festgelegten und unmittelbar aus der DSGVO hervorgehenden Pflichten erforderlich sind. Auf Verlangen des Verantwortlichen gestattet der Auftragsverarbeiter ebenfalls die Prüfung der unter diese Klauseln fallenden Verarbeitungstätigkeiten in angemessenen Abständen oder bei Anzeichen für eine Nichteinhaltung und trägt zu einer solchen Prüfung bei. Bei der Entscheidung über eine Überprüfung oder Prüfung kann der Verantwortliche einschlägige Zertifizierungen des Auftragsverarbeiters berücksichtigen.

Der Nachweis solcher Maßnahmen, die nicht nur den vorliegenden Auftragsverarbeitungsvertrag betreffen, sondern das Datenschutzniveau beim Auftragsverarbeiter im Allgemeinen, kann erfolgen durch

1. die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO;

2. die Zertifizierung nach einem genehmigten Zertifizierungsverfahren, insbesondere solche gemäß Art. 42 DSGVO;

3. aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);

4. eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

d) Der Verantwortliche kann die Prüfung selbst durchführen oder einen unabhängigen Prüfer beauftragen. Die Prüfungen können auch Inspektionen in den Räumlichkeiten oder physischen Einrichtungen des Auftragsverarbeiters umfassen und werden gegebenenfalls mit angemessener Vorankündigung durchgeführt. Der Verantwortliche wird seine Prüftätigkeiten und Inspektionen mit Verantwortlichen gleicher oder vergleichbarer Verarbeitungstätigkeiten mit Unterstützung des Auftragsverarbeiters abstimmen, um die Belastung für die Geschäftsabläufe des Auftragsverarbeiters zu begrenzen. Dies kann insbesondere auch die gemeinschaftliche Beauftragung eines unabhängigen Prüfers beinhalten. Der Auftragverarbeiter kann zu diesem Zweck den Kontakt zwischen Verantwortlichen herstellen. Der Auftragsverarbeiter ist berechtigt, Inspektionen mehrerer Verantwortlicher zu einem Termin zusammenzufassen. Der Verantwortliche wird durch die vorstehenden Regelungen nicht in seinen Kontrollrechten beschränkt. Er kann jederzeit, insbesondere, wenn der Anlass der Kontrolle oder Risiken für betroffene Personen dies erforderlich machen, von einer Abstimmung mit anderen Verantwortlichen oder auch dem Auftragsverarbeiter absehen.

e) Die Parteien stellen den zuständigen Aufsichtsbehörden die in dieser Klausel genannten Informationen, einschließlich der Ergebnisse von Prüfungen, auf Anfrage zur Verfügung.

§ 13 Einsatz von Unterauftragsverarbeitern

a) Der Auftragsverarbeiter besitzt die allgemeine Genehmigung des Verantwortlichen für die Beauftragung von Unterauftragsverarbeitern, die in Anhang IV aufgeführt sind. Der Auftragsverarbeiter unterrichtet den Verantwortlichen mindestens sechs Wochen im Voraus ausdrücklich in Textform über alle beabsichtigten Änderungen dieser Liste durch Hinzufügen oder Ersetzen von Unterauftragsverarbeitern und räumt dem Verantwortlichen damit ausreichend Zeit ein, um vor der Beauftragung des/der betreffenden Unterauftragsverarbeiter/s Einwände gegen diese Änderungen erheben zu können. Der Auftragsverarbeiter stellt dem Verantwortlichen die erforderlichen Informationen zur Verfügung, damit dieser sein Widerspruchsrecht ausüben kann. Beide Parteien müssen jederzeit den Nachweis führen können, welche Unterauftragsverarbeiter zu welchem Zeitpunkt genehmigt waren.

b) Beauftragt der Auftragsverarbeiter einen Unterauftragsverarbeiter mit der Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen), so muss diese Beauftragung im Wege eines Vertrags erfolgen, der dem Unterauftragsverarbeiter und dessen Unterauftragsverarbeitern dieselben Datenschutzpflichten auferlegt wie diejenigen, die für den Auftragsverarbeiter gemäß diesen Klauseln gelten. Der Auftragsverarbeiter stellt sicher, dass der Unterauftragsverarbeiter die Pflichten erfüllt, denen der Auftragsverarbeiter entsprechend diesen Klauseln und gemäß der DSGVO unterliegt.

c) Der Auftragsverarbeiter stellt dem Verantwortlichen auf dessen Verlangen eine Kopie einer solchen Untervergabevereinbarung und etwaiger späterer Änderungen zur Verfügung. Soweit es zum Schutz von Geschäftsgeheimnissen oder anderen vertraulichen Informationen, einschließlich personenbezogener Daten notwendig ist, kann der Auftragsverarbeiter den Wortlaut der Vereinbarung vor der Weitergabe einer Kopie unkenntlich machen.

d) Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen in vollem Umfang dafür, dass der Unterauftragsverarbeiter seinen Pflichten gemäß dem mit dem Auftragsverarbeiter geschlossenen Vertrag nachkommt. Der Auftragsverarbeiter benachrichtigt den Verantwortlichen, wenn der Unterauftragsverarbeiter seine vertraglichen Pflichten nicht erfüllt.

e) Der Auftragsverarbeiter vereinbart mit dem Unterauftragsverarbeiter eine Drittbegünstigtenklausel, wonach der Verantwortliche – im Falle, dass der Auftragsverarbeiter faktisch oder rechtlich nicht mehr besteht oder zahlungsunfähig ist – das Recht hat, den Untervergabevertrag zu kündigen und den Unterauftragsverarbeiter anzuweisen, die personenbezogenen Daten zu löschen oder zurückzugeben.

§ 14 Internationale Datenübermittlungen

Der Auftragsverarbeiter und seine Unterauftragsverarbeiter übermitteln keine personenbezogenen Daten, deren Verarbeitung Gegenstand dieses Vertrages ist, in Drittländer.

Teil 3: Schlussbestimmungen

§ 16 Vertraulichkeit geschäftlicher Unterlagen

a) Die Parteien behandeln Unterlagen und Informationen, die sie im Rahmen des Vertrages erhalten, über § 10 dieses Vertrages hinaus auch dann vertraulich, wenn ihre Verarbeitung nicht Vertragsgegenstand ist oder sie keinen Personenbezug aufweisen.

b) Diese Verpflichtungen bleiben auch nach Beendigung dieses Vertrages bestehen.

§ 17 Unterstützung des Verantwortlichen

a) Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich über jeden Antrag, den er von der betroffenen Person erhalten hat. Er beantwortet den Antrag nicht selbst, es sei denn, er wurde vom Verantwortlichen dazu ermächtigt.

b) Unter Berücksichtigung der Art der Verarbeitung unterstützt der Auftragsverarbeiter den Verantwortlichen bei der Erfüllung von dessen Pflicht, Anträge betroffener Personen auf Ausübung ihrer Rechte zu beantworten. Bei der Erfüllung seiner Pflichten gemäß den Buchstaben a und b befolgt der Auftragsverarbeiter die Weisungen des Verantwortlichen.

c) Abgesehen von der Pflicht des Auftragsverarbeiters, den Verantwortlichen gemäß § 17 lit. b zu unterstützen, unterstützt der Auftragsverarbeiter unter Berücksichtigung der Art der Datenverarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen zudem bei der Einhaltung der folgenden Pflichten:

1. Pflicht zur Durchführung einer Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten (im Folgenden „Datenschutz-Folgenabschätzung“), wenn eine Form der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat;

2. Pflicht zur Konsultation der zuständigen Aufsichtsbehörde(n) vor der Verarbeitung, wenn aus einer Datenschutz-Folgenabschätzung hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft;

3. Pflicht zur Gewährleistung, dass die personenbezogenen Daten sachlich richtig und auf dem neuesten Stand sind, indem der Auftragsverarbeiter den Verantwortlichen unverzüglich unterrichtet, wenn er feststellt, dass die von ihm verarbeiteten personenbezogenen Daten unrichtig oder veraltet sind;

4. Verpflichtungen gemäß Art. 32 DSGVO: Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragsverarbeiter gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen muss der Auftragsverarbeiter mit dem Verantwortlichen in Textform abstimmen. Solche Abstimmungen sind für die Dauer dieses Vertrages aufzubewahren.

d) Die Parteien legen in Anhang III die geeigneten technischen und organisatorischen Maßnahmen zur Unterstützung des Verantwortlichen durch den Auftragsverarbeiter bei der Anwendung dieser Klausel sowie den Anwendungsbereich und den Umfang der erforderlichen Unterstützung fest.

§ 18 Meldung von Verletzungen des Schutzes personenbezogener Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten arbeitet der Auftragsverarbeiter mit dem Verantwortlichen zusammen und unterstützt ihn entsprechend, damit der Verantwortliche seinen Verpflichtungen gemäß den Art. 33, 34 DSGVO nachkommen kann, wobei der Auftragsverarbeiter die Art der Verarbeitung und die ihm zur Verfügung stehenden Informationen berücksichtigt.

(1) Verletzung des Schutzes der vom Verantwortlichen verarbeiteten Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Verantwortlichen verarbeiteten Daten unterstützt der Auftragsverarbeiter den Verantwortlichen wie folgt:

a) bei der unverzüglichen Meldung der Verletzung des Schutzes personenbezogener Daten an die zuständige(n) Aufsichtsbehörde(n), nachdem dem Verantwortlichen die Verletzung bekannt wurde, sofern relevant (es sei denn, die Verletzung des Schutzes personenbezogener Daten führt voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen);

b) bei der Einholung der folgenden Informationen, die gemäß Art. 33 Abs. 3 DSGVO in der Meldung des Verantwortlichen anzugeben sind, wobei diese Informationen mindestens Folgendes umfassen müssen:

1. die Art der personenbezogenen Daten, soweit möglich, mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen sowie der Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;

2. die wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;

3. die vom Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Wenn und soweit nicht alle diese Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt;

c) bei der Einhaltung der Pflicht gemäß Art. 34 DSGVO, die betroffene Person unverzüglich von der Verletzung des Schutzes personenbezogener Daten zu benachrichtigen, wenn diese Verletzung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat.

(2) Verletzung des Schutzes der vom Auftragsverarbeiter verarbeiteten Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Auftragsverarbeiter verarbeiteten Daten meldet der Auftragsverarbeiter diese dem Verantwortlichen unverzüglich, nachdem ihm die Verletzung bekannt wurde. Diese Meldung muss zumindest folgende Informationen enthalten:

a) eine Beschreibung der Art der Verletzung (möglichst unter Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen und der ungefähren Zahl der betroffenen Datensätze);

b) Kontaktdaten einer Anlaufstelle, bei der weitere Informationen über die Verletzung des Schutzes personenbezogener Daten eingeholt werden können;

c) die voraussichtlichen Folgen und die ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten, einschließlich Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Wenn und soweit nicht alle diese Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt.

Die Parteien legen in Anhang III alle sonstigen Angaben fest, die der Auftragsverarbeiter zur Verfügung zu stellen hat, um den Verantwortlichen bei der Erfüllung von dessen Pflichten gemäß Art. 33, 34 DSGVO zu unterstützen.

§ 19 Verstöße gegen die Klauseln und Beendigung des Vertrags

a) Falls der Auftragsverarbeiter seinen Pflichten gemäß diesen Klauseln nicht nachkommt, kann der Verantwortliche – unbeschadet der Bestimmungen der DSGVO – den Auftragsverarbeiter anweisen, die Verarbeitung personenbezogener Daten auszusetzen, bis er diese Klauseln einhält oder der Vertrag beendet ist. Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich, wenn er aus welchen Gründen auch immer nicht in der Lage ist, diese Klauseln einzuhalten.

b) Der Verantwortliche ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn

1. der Verantwortliche die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter gemäß Buchstabe a ausgesetzt hat und die Einhaltung dieser Klauseln nicht innerhalb einer angemessenen Frist, in jedem Fall aber innerhalb eines Monats nach der Aussetzung, wiederhergestellt wurde;

2. der Auftragsverarbeiter in erheblichem Umfang oder fortdauernd gegen diese Klauseln verstößt oder seine Verpflichtungen gemäß der DSGVO nicht erfüllt;

3. der Auftragsverarbeiter einer bindenden Entscheidung eines zuständigen Gerichts oder der zuständigen Aufsichtsbehörde(n), die seine Pflichten gemäß diesen Klauseln oder der DSGVO zum Gegenstand hat, nicht nachkommt.

c) Der Auftragsverarbeiter ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn der Verantwortliche auf der Erfüllung seiner Anweisungen besteht, nachdem er vom Auftragsverarbeiter darüber in Kenntnis gesetzt wurde, dass seine Anweisungen gegen geltende rechtliche Anforderungen gemäß § 7 lit. b verstoßen.

d) Nach Beendigung des Vertrags löscht der Auftragsverarbeiter nach Wahl des Verantwortlichen alle im Auftrag des Verantwortlichen verarbeiteten personenbezogenen Daten und bescheinigt dem Verantwortlichen, dass dies erfolgt ist, oder er gibt alle personenbezogenen Daten an den Verantwortlichen zurück und löscht bestehende Kopien, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Bis zur Löschung oder Rückgabe der Daten gewährleistet der Auftragsverarbeiter weiterhin die Einhaltung dieser Klauseln.

e) Der Vertrag wird auf unbestimmte Zeit geschlossen. Er kann von beiden Vertragsparteien jederzeit in Textform mit einer Frist von vier Monaten zum Ende eines Kalenderjahres beendet werden.

f) Dieser Vertrag besteht auch dann fort, wenn einer der begleitenden Verträge durch Kündigung, Nichtigkeit, Unwirksamkeit oder aus sonstigen Gründen nicht mehr besteht. In diesen Fällen kann der Vertrag jedoch von beiden Parteien mit sofortiger Wirkung gekündigt werden.

g) Sollten einzelne Bestimmungen dieses Vertrages ganz oder teilweise nicht rechtswirksam oder nicht durchführbar sein oder werden, so wird hierdurch die Gültigkeit der jeweils übrigen Bestimmungen nicht berührt.

h) Als Gerichtsstand wird der Sitz des Auftragsverarbeiters bestimmt.

ANHANG I – Annahmeerklärung des Auftragsverarbeitungsvertrages für den Online-Dienst Einbürgerung (OZG-ID: 10257)

Das Angebot von

**d-NRW AöR,**

**Rheinische Str. 1, 44137 Dortmund**

**Kontaktperson und Weisungsadressatin:**Cansu Aktepe

kommunalvertreter@digitales.nrw.de

**Datenschutzbeauftragte:**Astrid Hoppe

Stellv.: André Bruchthal

datenschutz@d-nrw.de

auf Abschluss eines AVV für die Datenverarbeitung im o. g. Online-Dienst wird hiermit von der

**Name der Verantwortlichen**Anschrift

**Weisungsbefugte Kontaktperson:**Name  
Dienstliche Kontaktdaten (Telefon, E-Mail-Adresse, Postanschrift)

**Datenschutzbeauftragte:**Name  
Dienstliche Kontaktdaten (Telefon, E-Mail-Adresse, Postanschrift)

verbindlich angenommen

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Ort, Datum

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Name, Unterschrift

ANHANG II: Beschreibung der Datenverarbeitung für den Online-Dienst Einbürgerung (OZG-ID: 10257)

Beschreibung der Verarbeitung

Kategorien betroffener Personen, deren personenbezogene Daten verarbeitet werden:

* Antragsteller: Ausländerinnen und Ausländer im Sinne des Staatsangehörigkeitsgesetzes (StAG) bzw. Staatenlose als Nutzende des Online-Dienstes (Antragsteller), Personen die als Bevollmächtigte einen Antrag stellen;
* Angehörige der Antragsteller wie Ehepartner oder minderjährige Kinder, falls diese über den gleichen Antrag miteingebürgert werden sollten.

Kategorien der Daten, die immer verarbeitet werden:

Vorname, Familienname, Geburtsdatum, Geburtsort, Geburtsland, Staatsangehörigkeit, Familienstand, Geschlecht, Adressdaten, Zahlungsinformationen.

Folgende Kategorien werden nur bei Bedarf verarbeitet:

Daten zu wirtschaftlichen Verhältnissen, Daten zum ausländerrechtlichen Status, Schulbildung, Sprachkenntnisse, Personendaten von Vorfahren, Ehegatten und Kindern, frühere Personendaten, Volkstum.

Besondere Kategorien personenbezogener Daten („sensible Daten"), Verarbeitung nur falls für das spezielle Verfahren erforderlich:

Daten zur Verurteilung wegen einer Straftat, Daten aus den Ermittlungsergebnissen der angefragten Behörden, Gesundheitsdaten, Daten zur politischen Orientierung soweit sie sich aus der erforderlichen Sicherheits-befragung und/oder der Ausländerakte ergeben.

Der Zweck des Online-Dienstes ist die elektronische Beantragung eines Einbürgerungsantrages.

Der Online-Dienst bildet dabei die folgenden Unterzwecke ab:

1. Vorabauskunft, ob die Beantragung für die Person in Frage kommt,
2. Strukturierte elektronische Erhebung von Antragsdaten, ggf. unter Zuhilfenahme des Nutzerkontos (Übergabe der dort hinterlegten Stamm- und Kontaktdaten),
3. Übermittlung der Antragsdaten zur Weiterbearbeitung im Fachverfahren,

Bei der Verarbeitung durch (Unter-)Auftragsverarbeiter sind auch Gegenstand, Art und Dauer der Verarbeitung anzugeben (siehe Anhang IV).

ANHANG III: Beschreibung der TOM für den Online-Dienst Einbürgerung (OZG-ID: 10257)

Technische und organisatorische Maßnahmen, einschließlich zur Gewährleistung der Sicherheit der Daten

**Technische und Organisatorische Maßnahmen (TOM)** gemäß Art. 32 Abs. 1 DSGVO (unter Einhaltung sonstiger relevanter gesetzlicher Vorschriften und AKDB-interner Compliance-Regelungen) für im AKDB-Rechenzentrum betriebene Verfahren. Als Nachweis des Stands der Technik hält die AKDB ein BSI-Zertifikat vor.

Die regelmäßige Überprüfung der Wirksamkeit der Technischen und Organisatorischen Maßnahmen erfolgt mindestens jährlich im Rahmen der vorhandenen ISO 27001-Zertifizierung auf Basis von BSI IT-Grundschutz.

1. Vertraulichkeit

1.1 Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen zu verwehren, mit denen personenbezogene Daten verarbeitet oder genutzt werden:

* Mehrstufigen Zutrittsschutz
  + Besucherkontrolle am Empfang am Standort des Primärrechenzentrums
  + Gesonderte Zutrittsberechtigung zu allen sicherheitsrelevanten Räumen mittels Chipkarte und zusätzlicher Codeeingabe am Zugangsterminal
* Regelmäßige Überprüfung der Zutrittsberechtigungen
* Kontrollierte Schlüsselvergabe
* Videoüberwachung des Gebäudes einschließlich des Zugangs sowie in den Storage- und CPU-Räumen im Primärrechenzentrum
* Außenhautsicherung des Primärrechenzentrumgebäudes an kritischen Stellen durch einbruchhemmende Spezialfenster und Türen
* Außenhautsicherung des Primärrechenzentrumgebäudes kombiniert mit Einbruchmeldeanlage mit Alarmweiterleitung zur Polizei
* Besucher in Begleitung durch Mitarbeiter

1.2 Zugangskontrolle

Maßnahmen, die geeignet sind, zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können:

* Login mit Benutzername und Passwort
* Detaillierte Passwortregelung
* Erzwungene Passwortkomplexität
* Regelmäßigen technisch vorgegebenen Passwortwechsel
* Sperrung der Benutzerkennung nach mehrmaliger Fehleingabe
* Detaillierte Security-Policies für die Produktionsumgebung und deren regelmäßige Überprüfung
* Einsatz von Firewall-Systemen mit eigener Security-Policy
* Zusätzlicher Einsatz von Intrusion-Prevention-Systemen
* Anti-Viren-Software
* Mobile Device Management
* Verschlüsselung von Notebooks

1.3 Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können:

* Regelmäßige Aktualisierung der Sicherheitskonzepte
* Vergabe differenzierter Berechtigungsstufen innerhalb der Verfahren
* Protokollierung von Veränderungen oder Löschungen der Daten
* Datenträgervernichtung gemäß DIN 66399

1.4 Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

* Trennung von Produktiv- und Testumgebung
* Mandantenfähigkeit relevanter Anwendungen
* Festlegung von Datenbankrechten
* Steuerung über Berechtigungskonzept

2. Integrität

2.1 Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

* Datenübermittlung über gesicherte Datenverbindungen
* Verschlüsselung der Daten beim Transport auf Datenträgern

2.2. Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

* Technische Protokollierung der Eingabe, Änderung und Löschung von Daten
* Keine Modifizierbarkeit der Protokolle
* Kontrolle der Protokolle

3. Verfügbarkeit und Belastbarkeit

3.1 Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

* Hohe Hardwarequalität der Systeme mit abgeschlossenen Wartungsverträgen mit kurzen Reaktionszeiten seitens der Hardwarehersteller
* Redundante Server-Systeme
* Speicherung der Daten auf eigenen Storage-Systemen mit Raid-Technik und Spareplatten, zu großen Teilen in Clustertechnik ausgeführt
* Aufbewahrung von längerfristigen Sicherungsbeständen im Tresor
* Regelmäßig aktualisierten Virenschutz
* Redundante Firewall-Systeme
* Redundante Internetanschlüsse
* Redundanter Behördennetzanschluss (BYBN)
* Mobile Arbeitsplätze mit gesichertem Zugang für Mitarbeiter in den Bereichen Operating, Produktionsdurchführung und Systemadministration zum Zugang auch außerhalb der üblichen Arbeitszeiten
* Gebäudetechnische Maßnahmen (Feuer- Rauchmeldeanlagen, Feuerlöscher, Klimatisierung, USV)
* Regelmäßiges Patchen der Systeme (Funktions- und Sicherheitspatches)
* Regelmäßige Backup- und Recovery-Maßnahmen

Regelmäßige Tests zur Datenwiederherstellung

ANHANG IV: Liste der Unterauftragsverarbeiter für den Online-Dienst Einbürgerung (OZG-ID: 10257)

Liste der Unterauftragsverarbeiter

ERLÄUTERUNG:

Dieser Anhang muss alle bei Vertragsschluss mit der Datenverarbeitung für den Online-Dienst beauftragten Unter-Auftragsverarbeiter enthalten (§§ 13 lit. a), 14).

Der Verantwortliche hat die Inanspruchnahme folgender Unterauftragsverarbeiter genehmigt:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Name des Subunternehmers | Kontaktperson | Anschrift | Leistung |
| 1 | AKDB | Michael Diepold  Martin Senft | Anstalt für Kommunale Datenverarbeitung in Bayern (AKDB)  Hansastraße 12-16  80686 München | Betrieb der virtuellen Container-Infrastruktur für die eigentliche Anwendung und die dazu benötigten Dienste (Anwendungscluster) sowie Betrieb der OK.KOMM-Schnittstelle für den Online-Dienst |

1. Der vorliegende Auftragsverarbeitungsvertrag beruht in seinen wesentlichen Teilen auf den Standardvertragsklauseln der Europäischen Kommission, veröffentlich im Amtsblatt der Europäischen Union von 7.6.2021, L 199/18, [EUR-Lex - 32021D0915 - EN - EUR-Lex (europa.eu)](https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32021D0915). Die Bezeichnung der datenschutzrechtlichen Vorschriften wurde den Gepflogenheiten des inländischen Rechtsverkehrs angepasst, Bezüge auf die Verordnung (EU) 2018/1725 wurden entfernt. Der Begriff der „Klausel“ in dem vorliegenden Vertrag ist nicht mehr im Sinne von Standardvertragsklausel zu verstehen, sondern bezeichnet lediglich die Paragraphen und Abschnitte des vorliegenden Vertrages. Vertragspartner, Vertragsgegenstand, Technisch-Organisatorische Maßnahmen und Unterauftragsverarbeiter sind in den Anhängen I bis IV beschrieben. Inhaltliche Modifikationen und Ergänzungen wurden insbesondere in der Präambel, Klausel 5 und in Klausel 7 vorgenommen. Die Absätze der Klausel 7 wurden in eigene Klauseln überführt. Inhaltliche Änderungen in § 2,7 a) c), § 11 am Ende, § 12 d) e), § 13, § 14, § 15 (Vertraulichkeit, neu). [↑](#footnote-ref-1)
2. Vgl. Ziffer 3.4 SaaS-Einstellungs-AGB und Ziffer 2.4 SaaS-Nachnutzungs-AGB, abrufbar unter <https://www.fitko.de/fit-store>. [↑](#footnote-ref-2)
3. Die Nachnutzung der Online-Dienste per Software as a Service (SaaS) erfolgt auf die Weise, dass ein Bereitsteller an einem von ihm bzw. in Zusammenarbeit mit seinen IT-DL entwickelten Online-Dienst mittels SaaS-Vertrages (SaaS-Einstellungsvertrag) auf Basis der Vertragsbedingungen für den SaaS- Vertrag (SaaS-Einstellungs-AGB) die Nutzungsrechte und das Recht zur Weitergabe dieser Nutzungsrechte der FITKO einräumt. Zur Nachnutzung dieses Online-Dienstes schließt ein Land mit FITKO den SaaS-Nachnutzungsvertrag (SaaS-Nachnutzungsvertrag) auf Basis der Allgemeinen Vertragsbedingungen für den SaaS-Nachnutzungsvertrag (SaaS-Nachnutzungs-AGB). [↑](#footnote-ref-3)
4. Vgl. SaaS-Vertragsleitfaden , Version 1.0 vom 30.08.2021, 3.2 Datenschutzrecht, abrufbar unter <https://www.fitko.de/fit-store>. [↑](#footnote-ref-4)