

FIT-Connect-AVV



Auftragsverarbeitungsvertrag für die Nutzung von FIT-Connect

Zwischen

_____, nachfolgend „Verantwortlicher“

und

FITKO (Föderale IT-Kooperation) AöR, nachfolgend „Auftragsverarbeiter“

wird der folgende Auftragsverarbeitungsvertrag
geschlossen.

Präambel

Der vorliegende Auftragsverarbeitungsvertrag (nachfolgend nur: Auftragsverarbeitungsvertrag, Vertrag oder auch Klauseln)¹ begründet die datenschutzrechtlichen Rechte und Pflichten gem. Art. 28 DSGVO. Die nachfolgenden Klauseln beschreiben den rechtlichen Rahmen der Datenverarbeitung. Kontaktdaten, Details der Datenverarbeitung, technisch-organisatorische Maßnahmen und Unterauftragsverarbeiter sind detailliert in den Anhängen I-IV beschrieben.

Vertragsgegenstand ist die Anbindung an FIT-Connect zur sicheren und vertraulichen Übermittlung von Antragsdaten im Kontext der Online-Antragstellung. Die Anzahl der durch die Verantwortliche angebotenen Systeme ist nicht beschränkt, die Datenübermittlung ist in beide Richtungen möglich.

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.

¹ Der vorliegende Auftragsverarbeitungsvertrag beruht in seinen wesentlichen Teilen auf den Standardvertragsklauseln der Europäischen Kommission, veröffentlicht im Amtsblatt der Europäischen Union von 7.6.2021, L 199/18, [EUR-Lex - 32021D0915 - EN - EUR-Lex \(europa.eu\)](#). 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. Inhaltliche Modifikationen und Ergänzungen wurden insbesondere in der Präambel, Klausel 5 und in Klausel 7 vorgenommen. Die Absätze der Klausel 7 wurden in eigene Paragraphen überführt. Inhaltliche Änderungen in § 2,7 a) c), § 11 am Ende, § 12 d) e), § 13, § 14, § 15 (Vertraulichkeit, neu).

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 diesen Klauseln stehen oder die Grundrechte oder Grundfreiheiten der betroffenen Personen verletzen. 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 [Kopplungsklausel entfernt]

§ 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 Daten werden vom Auftragsverarbeiter nur für die in Anhang II angegebene Dauer verarbeitet.

§ 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 personenbezogener 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 Auftragsverarbeiter 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 der rechtliche Rahmen für die Auftragsverarbeitung, etwa ein Dienstvertrag, eine Verwaltungsvereinbarung, ein Beschluss oder die Ausstattung mit Haushaltsmitteln, nicht mehr besteht, etwa durch Kündigung, Nichtigkeit, Unwirksamkeit, Aufhebung, Streichung oder aus sonstigen Gründen. 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 –Auftragsverarbeitungsvertrag für die Nutzung von FIT-Connect

Liste der Parteien

FITKO (Föderale IT-Kooperation) AöR, als Auftragsverarbeiter:in

Zum Gottschalkhof 3 | 60594 Frankfurt am Main

Vertreten durch die Präsidentin, Dr. Annette Schmidt

Kontaktperson und Weisungsadressat:in:

Marco Holz

Föderales IT-Architekturmanagement

FITKO (Föderale IT-Kooperation)

Zum Gottschalkhof 3 | 60594 Frankfurt am Main

Tel.: +49 (69) 401270 139

marco.holz@fitko.de

Dr. Hauke Traulsen

Produktmanagement FIT-Connect

FITKO (Föderale IT-Kooperation)

Zum Gottschalkhof 3 | 60594 Frankfurt am Main

Tel.: +49 (69) 401270 136

hauke.traulsen@fitko.de

Datenschutzbeauftragte:r

Björn Canders

Datenschutzbeauftragte:r

Zum Gottschalkhof 3 | 60594 Frankfurt am Main

FITKO (Föderale IT-Kooperation)

Tel.: +49 (69) 401270 131

bjoern.canders@fitko.de

Ort, Datum

Name, Unterschrift (FITKO)

Name der/des Verantwortlichen:

Anschrift:

Weisungsbefugte Kontaktperson:

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

Vertretung Weisungsbefugte Kontaktperson:

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

Datenschutzbeauftragte:r:

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

Ort, Datum

Name, Unterschrift (Betreiber:in Onlinedienst)

ANHANG II: Beschreibung der Datenverarbeitung in FIT-Connect

Beschreibung der Verarbeitung

FIT-Connect wurde zur Unterstützung bei der Umsetzung von Online-Antragsprozessen nach dem Onlinezugangsgesetz entwickelt.

FIT-Connect besteht aus drei Kernkomponenten:

1. Antragsübermittlungsdienst (auch Zustelldienst),
2. Self-Service-Portal,
3. Routingdienst.

Der Antragsübermittlungsdienst realisiert dabei die technische Implementierung der interoperablen Datenübermittlung von sendenden Systemen, in denen Anträge gestellt werden können, (z.B. Online-Antragsdienste oder Fachverfahren eines Unternehmens) an empfangende Systeme (antragsbearbeitende Fachverfahren der zuständigen Fachbehörde). FIT-Connect erlaubt auch eine maschinenlesbare Rückkanal-Kommunikation vom empfangenden zum sendenden System.

FIT-Connect bietet dazu eine einheitliche Schnittstelle zur Anbindung von Onlinediensten an die zuständigen Fachverfahren aller föderalen Ebenen und bietet Lösungsverantwortlichen eine einfache Möglichkeit, ihre Software schnell und wirtschaftlich in länder- und ebenenübergreifende Antragsprozesse zu integrieren.

Das Self-Service-Portal von FIT-Connect erlaubt es Bund, Ländern, Kommunen oder interessierten IT-Dienstleistern über eine grafische Oberfläche die für eine Anbindung an FIT-Connect erforderlichen OAuth-API-Clients anzulegen. Behörden können im Self-Service-Portal Zustellpunkte zum Empfang von Antragsdaten für ihre bereits bestehenden Fachverfahren und Verwaltungsleistungen registrieren.

Der Routingdienst macht im Self-Service-Portal registrierte Zustellpunkte sowie deren technische Parameter für andere Onlinedienste über seine Schnittstelle auffindbar. Er erlaubt eine Filterung anhand geografischer Informationen oder der angefragten Verwaltungsleistung, um die für eine Anfrage zuständige Fachbehörde zu identifizieren.

Für eine ausführlichere Beschreibung der Verarbeitungen wird auf das Verzeichnis von Verarbeitungstätigkeiten verwiesen.

Eine detaillierte Beschreibung der Anwendungsfälle von FIT-Connect findet sich unter <https://docs.fitko.de/fit-connect/>.

Kategorien betroffener Personen, deren personenbezogene Daten verarbeitet werden und Kategorien personenbezogener Daten

FIT-Connect kann grundsätzlich personenbezogene Daten aller Menschen verarbeiten, die als Bürger:innen oder Beschäftigte oder Vertreter:innen von juristischen Personen Verwaltungsangelegenheiten besorgen. Dies erfasst die Zustellung an die Behörde, aber ggf. auch Rückantworten.

Die nachfolgende Tabelle orientiert sich am Verarbeitungsverzeichnis. Bei den Nummern 2, 3 und 6 ist der Personenbezug lediglich rein theoretisch vorstellbar, dürfte aber in der Praxis nicht vorkommen.

Nr.	Datenarten	Betroffene Personengruppen
1	Der Antragsübermittlungsdienst verarbeitet ende-zu-ende-verschlüsselte Antragsdaten, inkl. Art. 9 und 10-Daten, in Textform und ggf. auch als Scans und Bilddateien. Eine Entschlüsselung ist technisch für die Betreiber von FIT-Connect nicht möglich.	Der Antragsübermittlungsdienst kann grundsätzlich personenbezogene Daten aller Menschen verarbeiten, die Anträge über an FIT-Connect angeschlossene Online-Dienste stellen.
2	Protokollierung von Events (technische Protokolldaten) bei der Übermittlung von Antragsdaten mit dem Ziel, beteiligten Parteien den aktuellen Status der Übermittlung transparent zu machen sowie die Integrität der übermittelten Daten überprüfen zu können.	Antragsteller:innen
3	Zur Aufrechterhaltung des laufenden Betriebs von FIT-Connect, der Behebung von auftretenden Fehlern und der Unterstützung bei der Bearbeitung von Supportanfragen werden IP-Adressen der an FIT-Connect angebundenen Systeme und weitere technische Daten von Einreichungen erhoben.	Antragsteller:innen
4	Kontakt- und Adressdaten von Verfahrensbetreibern werden für die Erstellung eines Benutzerkontos im Self-Service-Portal zur Verwaltung von technischen Benutzern in FIT-Connect benötigt.	Verfahrensbetreiber und deren Mitarbeiter:innen
5	Um einen Zustellpunkt im Self-Service-Portal anlegen zu können, müssen Kontaktdaten von für einen Zustellpunkt zuständigen Personen hinterlegt werden, sofern keine juristische Person verwendet werden kann.	Verfahrensbetreiber und deren Mitarbeiter:innen
6	Indirekte Geodaten (PLZ, Ortsname, Amtlicher Regionalschlüssel) zur Identifikation der zuständigen Fachbehörde durch den Routingdienst. Die Daten werden ausschließlich zur Beantwortung der Anfrage genutzt und werden nicht gespeichert oder weiter verarbeitet.	Antragsteller:innen

Verarbeitete sensible Daten gem. Art. 9, 10 DSGVO

- ☒ Daten über rassische oder ethnische Herkunft
- ☒ politische Meinungen
- ☒ Daten über religiöse oder weltanschauliche Überzeugungen
- ☒ Daten über Gewerkschaftszugehörigkeit
- ☒ Genetische Daten
- ☒ Biometrische Daten zur Identifizierung einer natürlichen Person
- ☒ Daten über das Sexualleben oder die sexuelle Orientierung
- ☒ Daten über strafrechtliche Verurteilungen und Straftaten nach Art. 10 DSGVO

Die Kategorien der personenbezogenen Daten im Sinne der Art. 9, 10 DSGVO ergeben sich aus den Kategorien der durch die angebundenen Systeme übermittelten Daten. Es ist daher grundsätzlich in der Hand des Verantwortlichen, welche Daten über FIT-Connect Ende-zu-Ende-verschlüsselt übermittelt werden. Dies erlaubt die Nutzung von FIT-Connect im Rahmen dieses Vertrages für mehrere angebundene Systeme (z. B. Online-Dienste oder Fachverfahren). Es berücksichtigt so auch die Möglichkeit, dass besondere Kategorien personenbezogener Daten planwidrig in ein angebundenes System eingebracht werden.

Eine Verarbeitung der übertragenen Fachdaten über die für die Übermittlung (Zustellung und ggf. Rückkanal) notwendigen technischen Schritte hinaus findet nicht statt. Insbesondere erfolgt die Übermittlung dieser Daten jederzeit Ende-zu-Ende-Verschlüsselt, sodass die Auftragsverarbeiterin zu keinem Zeitpunkt Zugriff auf diese übertragenen Daten im Klartext erhalten.

Art der Verarbeitung

Wie unter Beschreibung der Verarbeitung ausgeführt handelt es sich um die Ende-zu-Ende-verschlüsselte Übermittlung von Antragsdaten.

Zweck(e), für den/die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden

Der Zweck der Datenverarbeitung durch den FIT-Connect Antragsübermittlungsdienst besteht ausschließlich in der sicheren Übermittlung der Antragsdaten (Fachdaten, Metadaten und Anhänge) zwischen dem Online-Dienst und dem Fachverfahren. Eine Entschlüsselung der Antragsdaten ist nicht Zweck der Verarbeitung und wird technisch durch eine Ende-zu-Ende Verschlüsselung ausgeschlossen. Das gewährleistet, dass Betreiber der FIT-Connect-Infrastruktur zu keinem Zeitpunkt Zugriff auf die übertragenen Antragsdaten im Klartext erhalten.

Eine Verarbeitung der übertragenen Fachdaten über die für die Übermittlung notwendigen technischen Schritte hinaus findet nicht statt. Zu statistischen Zwecken werden Daten zur Fachlichkeit und zu genutzten technischen Parametern erfasst und ausgewertet, die jedoch keinen Personenbezug aufweisen.

Die Verarbeitung von technischen Metadaten, bei denen ein Personenbezug grundsätzlich ohnehin nicht besteht, erfolgt lediglich zur Gewährleistung einer stabilen Leistungserbringung und eines zuverlässigen Antragsroutings.

Zur Sicherstellung einer erfolgreichen Datenübermittlung und zur Umsetzung von Empfangsbestätigungen werden technische Parameter sowie der Übermittlungsstatus in einem Ereignisprotokoll aufgezeichnet und den angebundenen Systemen zur Verfügung gestellt.

Der Zweck der Datenverarbeitung durch das FIT-Connect Self-Serviceportal besteht in der Verwaltung von technischen Benutzern (API-Clients) und Zustellpunkten. Dafür müssen Benutzerkonten angelegt werden, denen die Rechte zur Verwaltung zugeordnet sind. Die dafür erhobenen Kontaktdaten der Betreiber von angebundenen Systemen werden zum Zwecke der Wartung & Fehlerbeseitigung verarbeitet.

Der Routingdienst verarbeitet Daten ausschließlich zum genannten Zweck, um die korrekte Zustellung eines Antrags gewährleisten zu können.

Dauer der Verarbeitung

Die Lösch- und Speicherfristen ergeben sich aus den Nutzungsbedingungen und dem Verarbeitungsverzeichnis. Die Antrags- und Metadaten werden nicht länger als unbedingt notwendig gespeichert.

Der Vertrag wird unbefristet geschlossen.

ANHANG III: Liste der Unterauftragsverarbeiter für FIT-Connect

Liste der Unterauftragsverarbeiter

Der Verantwortliche hat die Inanspruchnahme folgender Unterauftragsverarbeiter genehmigt:

- IT.Niedersachsen (Antragsübermittlungsdienst)
- TSA Public Service GmbH (Routingdienst)
- FJD Information Technologies AG (Self-Service-Portal)
- creoline GmbH (Logging)

ANHANG IV.1 – Technische und organisatorische Maßnahmen

Die folgenden technischen und organisatorischen Maßnahmen werden durch die Kernkomponenten von FIT-Connect selbst realisiert. Weitere technische und organisatorische Maßnahmen entnehmen Sie bitte den TOM-Listen der für den Betrieb der Komponenten zuständigen Dienstleister, vgl. hier Anhang 4.2, 4.3 etc.

Verschlüsselung

Einreichungen setzen sich aus 4 Kategorien von Daten zusammen:

Technische Daten, Metadaten, Fachdaten und Anlagen.

Metadaten, Fachdaten und Anlagen werden bereits auf Seiten der sendenden Stelle vor Übermittlung an den FIT-Connect Antragübermittlungsdienst Ende-zu-Ende verschlüsselt.

Die zur Verschlüsselung benötigten Schlüssel der empfangenden Stelle werden durch den FIT-Connect Antragübermittlungsdienst (Zustelldienst), auf Anfrage durch den Sender via API, bereitgestellt.

Die Herkunft/Identität der verwendeten Schlüssel wird durch Zertifikate aus der V-PKI gewährleistet.

Rückverfolgbarkeit (Protokollierung)

Antragsübermittlungsdienst (Zustelldienst)

Relevante Ereignisse der Einreichungsübermittlung werden im Ereignisprotokoll des FIT-Connect Zustelldiensts mithilfe von Security Event Tokens gemäß <https://tools.ietf.org/html/rfc8417> protokolliert. Diese bleiben bis zum Ablauf der Aufbewahrungsfristen bestehen und können ausschließlich durch an der Transaktion beteiligte Parteien gelesen und geschrieben werden.

Eine Übersicht der protokollierten Events ist unter [Ereignisse | FIT-Connect \(fitko.de\)](https://docs.fitko.de/fit-connect/docs/getting-started/event-log/events)² zu finden.

Logging-Server

Zusätzlich findet eine technische Protokollierung statt, mit der Auffälligkeiten identifiziert und im Fehlerfall das Betriebsteam oder der Support unterstützt werden kann. Auf dem zentralen Logging-Server laufen die technischen Logs aller FIT-Connect-Dienste zusammen.

Anonymisierung

Anträge/Einreichungen werden zufällig generierte UUIDs zugeordnet. Es erfolgt keine Identifizierung anhand von personenbezogenen Daten sondern ausschließlich anhand der UUIDs.

² <https://docs.fitko.de/fit-connect/docs/getting-started/event-log/events>

Datentrennung

Antragsübermittlungsdienst (Zustelldienst)

Sämtliche im Zustelldienst von FIT-Connect erfassten Einreichungen können ausschließlich von ihren designierten Empfängern abgerufen werden. Eine Einsicht in Einreichungen anderer Behörden ist nicht möglich und wird technisch ausgeschlossen. Es wird auch sichergestellt, dass jeder Zustelldienst nur Zugriff auf sein eigenes Ereignisprotokoll hat und nicht auf die Ereignisprotokolle von anderen Zustelldiensten zugreifen kann.

Self-Service-Portal

Jeder Anwender hat ausschließlich nur auf die Daten seines eigenen Kontos Zugriff.

Logische Zugriffskontrolle

Antragsübermittlungsdienst

Ein Zugriff auf die API zum Anlegen oder Abrufen von Einreichungen setzt eine erfolgreiche Authentifizierung am OAuth-Server von FIT-Connect mit Client ID und Client Secret der technischen Benutzer voraus. Clients gehören dabei entweder zum Typ Sender oder zum Typ Subscriber. Ein Client kann nicht zeitgleich beide Rollen inne haben.

Subscriber müssen konkreten Zustellpunkten zuordnet werden und haben nur auf diese Zustellpunkte (konkretes Ziel einer Antragssübermittlung) Zugriff.

Der Abruf eines Ereignisprotokolls zu einem Antrag oder das Schreiben von Einträgen im Ereignisprotokoll setzt ebenfalls eine Authentifizierung am OAuth Server von FIT-Connect voraus.

Self-Service-Portal

Ein Zugriff auf das Self-Service-Portal setzt eine Authentifizierung über einen externen Identitätsanbieter (ELSTER) voraus. Bei der Registrierung für ein ELSTER-Organisations-Konto wird die Identität der juristischen Person detailliert überprüft. Ein Zugriff für unberechtigte Anwender wird damit stark erschwert.

Datenminimierung

Antragsübermittlungsdienst

Auf Seiten von FIT-Connect werden nur die technischen Daten erfasst, welche zur sicheren Zustellung einer Einreichung an eine zuständige Behörde erforderlich sind. Darüber hinaus benötigte Inhaltsdaten werden durch die sendende Stelle und nicht durch FIT-Connect erfasst und ausschließlich Ende-zu-Ende-verschlüsselt übertragen.

Routingdienst

Die abgefragten Informationen LEIKA-ID, Postleitzahl und/oder Ortsname sowie der amtliche Regionalschlüssel werden einzig zur Einschränkung des Suchbereichs verwendet. Darüber hinaus werden keine Daten erfasst.

Self-Service-Portal

Es werden nur die bei der Authentifizierung über das ELSTER-Organisations-Konto mitgeschickten Daten erfasst, um ein zur Identität gehörendes Konto zu erstellen.

Logging-Server

Es werden nur die technisch notwendigen Daten in den Logs erfasst. Auf personenbezogene Daten wird abseits der IP-Adressen von mit FIT-Connect verbundenen Systemen verzichtet.

Integritätssicherung

Im Rahmen des Ereignisprotokolls werden zu den übertragenen Daten eines Antrags (Metadaten, Fachdaten und Anhänge) AuthenticationTags erfasst, mit denen die Unverändertheit der Daten vor Entschlüsseln überprüft werden kann. Zusätzlich enthalten die verschlüsselten Metadaten Hashwerte der Fachdaten und Anhänge, so dass diese nach Entschlüsseln auf ihre Unverändertheit überprüft werden können.

Einträge in das Ereignisprotokoll werden von ihren Erzeugern digital signiert. So lässt sich die Integrität und Authentizität der Einträge durch berechtigte lesende Stellen überprüfen.

Schutz des Internetauftritts

Sämtliche Endpunkte von FIT-Connect und beteiligter Stellen(Sender/Subscriber) werden durch TLS-Zertifikate abgesichert. Damit wird auf sämtlichen Kommunikationsverbindungen mit und innerhalb von FIT-Connect eine Transportwegeverschlüsselung realisiert.

Keine persistente Speicherung von personenbezogenen Daten

Die Verarbeitung der Anfragen an den Routingdienst erfolgt ausschließlich im Arbeitsspeicher. Es werden keine Daten persistent gespeichert.