Auftragsverarbeitungsvertrag für die Nutzung von FIT-Connect

zwischen

nachfolgend „Verantwortliche:r"

und

FITKO (Föderale IT-Kooperation) AöR

nachfolgend „Auftragsverarbeiterin"

wird der folgende Auftragsverarbeitungsvertrag geschlossen.

Präambel

Der vorliegende Auftragsverarbeitungsvertrag (nachfolgend nur: Auftragsverarbeitungsvertrag, Vertrag oder auch Klauseln)[1] begründet die datenschutzrechtlichen Rechte und Pflichten gemäß Art. 28 DSGVO. Die nachfolgenden Klauseln beschreiben den rechtlichen Rahmen der Datenverarbeitung. Die Kontaktdaten, die Details der Datenverarbeitung, die Unterauftragsverhältnisse und die technisch-organisatorischen Maßnahmen (TOMs) 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 den Verantwortlichen angebundenen Systeme ist nicht beschränkt, die Datenübermittlung ist in beide Richtungen möglich.

Teil 1: Allgemeine Regelungen

§ 1 Zweck und Anwendungsbereich

(1) Mit diesem Auftragsverarbeitungsvertrag soll die Einhaltung von Art. 28 Abs. 3 und 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

[1] Der vorliegende Auftragsverarbeitungsvertrag beruht in seinen wesentlichen Teilen auf den Standardvertragsklauseln der Europäischen Kommission, veröffentlicht im Amtsblatt der Europäischen Union vom 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 Vertrags.

freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (DSGVO) sichergestellt werden.

(2) Die:Der in Anhang I aufgeführte Verantwortliche und die Auftragsverarbeiterin haben diesen Klauseln zugestimmt, um die Einhaltung von Art. 28 Abs. 3 und 4 DSGVO zu gewährleisten.

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

(4) Die Anhänge I bis IV sind Bestandteil der Klauseln.

(5) Diese Klauseln gelten unbeschadet der Verpflichtungen, denen die:der Verantwortliche und die Auftragsverarbeiterin gemäß der DSGVO unterliegen.

§ 2 Änderungen des Vertrags

(1) Wir behalten uns vor den Auftragsverarbeitungsvertrag zu ändern. Änderungen, die erforderlich sind, um gesetzlichen Anforderungen zu genügen und Änderungen, durch die die:der Verantwortliche nicht schlechter gestellt wird, werden 30 Tage nach Zugang der Änderungsmitteilung in Textform wirksam und gelten auch für laufende Nutzungen von FIT-Connect. Dies gilt entsprechend für andere Änderungen, soweit die:der Verantwortliche den Änderungen nicht binnen dort genannter Frist ebenfalls in Textform widerspricht; auf diese Folge werden die Verantwortlichen mit der Änderungsmitteilung hingewiesen.

(2) 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

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

(2) Diese Klauseln sind im Lichte der Bestimmungen der DSGVO auszulegen.

(3) 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 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

§ 6 Weisungen

(1) Die Auftragsverarbeiterin verarbeitet personenbezogene Daten nur auf dokumentierte Weisung (Textform) der:des Verantwortlichen, es sei denn, sie ist nach Unionsrecht oder nach dem Recht eines Mitgliedstaats, dem er unterliegt, zur Verarbeitung verpflichtet. In einem solchen Fall teilt die Auftragsverarbeiterin der:dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet. Die: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.

(2) Die Auftragsverarbeiterin informiert die:den Verantwortliche:n unverzüglich, wenn sie der Auffassung ist, dass von der:dem Verantwortlichen erteilte Weisungen gegen die DSGVO oder geltende Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstoßen.

(3) Die:Der Verantwortliche setzt der Auftragsverarbeiterin eine angemessene Frist zur Umsetzung der Weisungen. Sie:Er wird bei der Fristsetzung und Abfassung ihrer:seiner Weisungen berücksichtigen, dass die Auftragsverarbeiterin Weisungen anderer Verantwortlicher unterliegen kann, und anstreben, sich unbeschadet ihrer:seiner gesetzlichen Rechte mit anderen Verantwortlichen abzustimmen.

(4) Sollte die Auftragsverarbeiterin wider Erwarten eine Weisung der:des Verantwortlichen nicht innerhalb der gesetzten Frist umsetzen können, ist sie verpflichtet, die:den Verantwortlichen unverzüglich hierüber mit Angabe sie:ihn verhindernder Gründe zu informieren.

§ 7 Zweckbindung

Die Auftragsverarbeiterin verarbeitet die personenbezogenen Daten nur für den oder die in Anhang II genannten spezifischen Zweck(e), sofern sie keine weiteren Weisungen des Verantwortlichen erhält.

§ 8 Dauer der Verarbeitung personenbezogener Daten

Die Daten werden von der Auftragsverarbeiterin nur für die in Anhang II angegebene Dauer verarbeitet.

§ 9 Sicherheit der Verarbeitung

(1) Die Auftragsverarbeiterin ergreift mindestens die in Anhang IV 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.

(2) Die Auftragsverarbeiterin gewährt ihrem 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. Die Auftragsverarbeiterin gewährleistet, dass sich die zur Verarbeitung der erhaltenen personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

§ 10 Besondere personenbezogene Daten

Sofern die Verarbeitung personenbezogene Daten betrifft, aus denen bspw. die ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen sowie genetische oder biometrische Daten zum Zweck der eindeutigen Identifizierung einer natürlichen Person, Daten über die Gesundheit, das Sexualleben oder die sexuelle Orientierung einer Person hervorgehen (im Folgenden „besondere personenbezogene Daten"), wendet die Auftragsverarbeiterin zusätzliche angemessene und spezifische Maßnahmen an.

Die zusätzlichen Maßnahmen sind von der Auftragsverarbeiterin gesondert in Anhang IV – Technisch-Organisatorische Maßnahmen – anzugeben.

§ 11 Dokumentation und Einhaltung der Klauseln

(1) Die Parteien müssen die Einhaltung dieser Klauseln nachweisen können.

(2) Die Auftragsverarbeiterin bearbeitet Anfragen der:des Verantwortlichen bezüglich der Verarbeitung von Daten gemäß diesen Klauseln umgehend und in angemessener Weise.

(3) Die Auftragsverarbeiterin stellt der: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 der:des Verantwortlichen gestattet die Auftragsverarbeiterin 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 der Auftragsverarbeiterin berücksichtigen.

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

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

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

c. aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z. B. Wirtschaftsprüfer:innen, Revision, Datenschutzbeauftragte:r, IT-Sicherheitsabteilung, Datenschutzauditor:innen, Qualitätsauditor:innen);

d. eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z. B. nach ISO 27001 oder auf Grundlage von BSI-Grundschutz).

(4) Die:Der Verantwortliche kann die Prüfung selbst durchführen oder eine unabhängige Prüfung beauftragen. Die Prüfungen können auch Inspektionen in den Räumlichkeiten oder physischen Einrichtungen der Auftragsverarbeiterin umfassen und werden gegebenenfalls mit angemessener Vorankündigung durchgeführt. Die:Der Verantwortliche wird ihre:seine Prüftätigkeiten und Inspektionen mit Verantwortlichen gleicher oder vergleichbarer Verarbeitungstätigkeiten mit Unterstützung der Auftragsverarbeiterin abstimmen, um die Belastung für die Geschäftsabläufe der Auftragsverarbeiterin zu begrenzen. Dies kann insbesondere auch die gemeinschaftliche Beauftragung einer unabhängigen Prüfung beinhalten. Die Auftragsverarbeiterin kann zu diesem Zweck den Kontakt zwischen Verantwortlichen herstellen. Die Auftragsverarbeiterin ist berechtigt, Inspektionen mehrerer Verantwortlicher zu einem Termin zusammenzufassen. Die:Der Verantwortliche wird durch die vorstehenden Regelungen nicht in ihren:seinen Kontrollrechten beschränkt. Sie: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 der Auftragsverarbeiterin absehen.

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

§ 12 Einsatz von Unterauftragsverarbeiter:innen

(1) Die Auftragsverarbeiterin besitzt die allgemeine Genehmigung der:des Verantwortlichen für die Beauftragung von Unterauftragsverarbeiter:innen, die in Anhang III aufgeführt sind. Die Auftragsverarbeiterin unterrichtet die:den Verantwortliche:n mindestens sechs Wochen im Voraus ausdrücklich in Textform über alle beabsichtigten Änderungen dieser Liste durch Hinzufügen oder Ersetzen von Unterauftragsverarbeiter:innen und räumt der:dem Verantwortlichen damit ausreichend Zeit ein, um vor der Beauftragung der betreffenden Unterauftragsverarbeitung Einwände gegen diese Änderungen erheben zu können. Die Auftragsverarbeiterin stellt der:dem Verantwortlichen die erforderlichen Informationen zur Verfügung, damit dieser ihr:sein Widerspruchsrecht ausüben kann. Beide Parteien müssen jederzeit den Nachweis führen können, welche Unterauftragsverarbeitungen zu welchem Zeitpunkt genehmigt waren.

(2) Beauftragt die Auftragsverarbeiterin eine:n Unterauftragsverarbeiter:in mit der Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag der:des Verantwortlichen), so muss diese Beauftragung im Wege eines Vertrags erfolgen, der der:dem Unterauftragsverarbeiter:in und dessen Unterauftragsverarbeiter:innen dieselben Datenschutzpflichten auferlegt wie diejenigen, die für die Auftragsverarbeiterin gemäß diesen Klauseln gelten. Die Auftragsverarbeiterin stellt sicher, dass die:der Unterauftragsverarbeiter:in die Pflichten erfüllt,

denen die Auftragsverarbeiterin entsprechend diesen Klauseln und gemäß der DSGVO unterliegt.

(3) Die Auftragsverarbeiterin stellt der:dem Verantwortlichen auf ihr: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 die Auftragsverarbeiterin den Wortlaut der Vereinbarung vor der Weitergabe einer Kopie unkenntlich machen.

(4) Die Auftragsverarbeiterin haftet gegenüber der:dem Verantwortlichen in vollem Umfang dafür, dass die:der Unterauftragsverarbeiter:in ihren:seinen Pflichten, gemäß dem mit der Auftragsverarbeiterin geschlossenen Vertrag nachkommt. Die Auftragsverarbeiterin benachrichtigt die:den Verantwortliche:n, wenn die:der Unterauftragsverarbeiter:in ihre:seine vertraglichen Pflichten nicht erfüllt.

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

§ 13 Internationale Datenübermittlungen

Die Auftragsverarbeiterin und ihre Unterauftragsverarbeiter:innen übermitteln keine personenbezogenen Daten, deren Verarbeitung Gegenstand dieses Vertrages ist, in Drittländer.

Teil 3: Schlussbestimmungen

§ 14 Vertraulichkeit geschäftlicher Unterlagen

(1) Die Parteien behandeln Unterlagen und Informationen, die sie im Rahmen des Vertrages erhalten, über § 9 dieses Vertrags hinaus auch dann vertraulich, wenn ihre Verarbeitung nicht Vertragsgegenstand ist oder sie keinen Personenbezug aufweisen.

(2) Diese Verpflichtungen bleiben auch nach Beendigung dieses Vertrages bestehen.

§ 15 Unterstützung des Verantwortlichen

(1) Die Auftragsverarbeiterin unterrichtet die:den Verantwortlichen unverzüglich über jeden Antrag, den sie von der betroffenen Person erhalten hat. Sie beantwortet den Antrag nicht selbst, es sei denn, sie wurde von der:vom Verantwortlichen dazu ermächtigt.

(2) Unter Berücksichtigung der Art der Verarbeitung unterstützt die Auftragsverarbeiterin die:den Verantwortlichen bei der Erfüllung von deren:dessen Pflicht, Anträge betroffener Personen auf Ausübung ihrer Rechte zu beantworten. Bei der Erfüllung ihrer Pflichten befolgt die Auftragsverarbeiterin die Weisungen der:des Verantwortlichen.

(3) Abgesehen von der Pflicht der Auftragsverarbeiterin, der:den Verantwortlichen gemäß Absatz (2) zu unterstützen, unterstützt die Auftragsverarbeiterin unter Berücksichtigung der

Art der Datenverarbeitung und der ihr zur Verfügung stehenden Informationen die:den Verantwortliche:n zudem bei der Einhaltung der folgenden Pflichten:

a. 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;

b. 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 die:der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft;

c. Pflicht zur Gewährleistung, dass die personenbezogenen Daten sachlich richtig und auf dem neuesten Stand sind, indem die Auftragsverarbeiterin die:den Verantwortliche:n unverzüglich unterrichtet, wenn sie feststellt, dass die von ihr verarbeiteten personenbezogenen Daten unrichtig oder veraltet sind;

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

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

§ 16 Meldung von Verletzungen des Schutzes personenbezogener Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten arbeitet der Auftragsverarbeiterin mit dem Verantwortlichen zusammen und unterstützt ihn entsprechend, damit der Verantwortliche seinen Verpflichtungen gemäß den Art. 33, 34 DSGVO nachkommen kann, wobei der Auftragsverarbeiterin 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 Auftragsverarbeiterin 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:

   - 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;
   - die wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
   - 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 Auftragsverarbeiterin verarbeiteten Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Auftragsverarbeiterin verarbeiteten Daten meldet der Auftragsverarbeiterin 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 IV alle sonstigen Angaben fest, die der Auftragsverarbeiterin zur Verfügung zu stellen hat, um den Verantwortlichen bei der Erfüllung von dessen Pflichten gemäß Art. 33, 34 DSGVO zu unterstützen.

§ 17 Verstöße gegen die Klauseln und Beendigung des Vertrags

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

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

a. der Verantwortliche die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiterin 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;

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

c. der Auftragsverarbeiterin 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.

(3) Die Auftragsverarbeiterin 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 Auftragsverarbeiterin darüber in Kenntnis gesetzt wurde, dass seine Anweisungen gegen geltende rechtliche Anforderungen gemäß § 7 lit. b verstoßen.

(4) Nach Beendigung des Vertrags löscht der Auftragsverarbeiterin 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 Auftragsverarbeiterin weiterhin die Einhaltung dieser Klauseln.

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

(6) 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.

(7) 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.

(8) Als Gerichtsstand wird der Sitz der Auftragsverarbeiterin bestimmt.

Verantwortliche:r:

_____

Ort, Datum

_____

Name, Unterschrift

Für die FITKO als Auftragsverarbeiterin:

_____

Ort, Datum

_____

Name, Unterschrift

ANHANG I –Auftragsverarbeitungsvertrag für die Nutzung von FIT-Connect
Liste der Parteien

FITKO (Föderale IT-Kooperation) AöR, als Auftragsverarbeiterin

Zum Gottschalkhof 3 | 60594 Frankfurt am Main

Vertreten durch den Präsidenten Dr. André Göbel

Kontaktpersonen und Weisungsadressat:innen:

Dr. Hauke Traulsen

Produktmanagement FIT-Connect

FITKO (Föderale IT-Kooperation)

Zum Gottschalkhof 3 | 60594 Frankfurt am Main

fit-connect@fitko.de

Marco Holz

Föderales IT-Architekturmanagement

FITKO (Föderale IT-Kooperation)

Zum Gottschalkhof 3 | 60594 Frankfurt am Main

architekturmanagement@fitko.de

Datenschutzbeauftragte:r

FITKO (Föderale IT-Kooperation) AöR

Zum Gottschalkhof 3 | 60594 Frankfurt am Main

datenschutz@fitko.de

Name der:des Onlinedienste-Anbietenden, **als Verantwortliche**

Adresse

Vertreten durch Name

Kontaktpersonen und Weisungsadressat:innen:

Name

Funktion

Name der:des Onlinedienste-Anbietenden

Adresse

E-Mail-Adresse

Name

Funktion

Name der:des Onlinedienste-Anbietenden

Adresse

E-Mail-Adresse

Datenschutzbeauftragte:r

Name der:des Onlinedienste-Anbietenden

Adresse

E-Mail-Adresse

ANHANG II: Beschreibung der Datenverarbeitung in FIT-Connect

1 Beschreibung der Verarbeitung

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

FIT-Connect besteht aus drei Kernkomponenten:

- Antragsübermittlungsdienst (auch Zustelldienst)
- Self-Service-Portal
- Routingdienst

Der Antragsübermittlungsdienst realisiert dabei die technische Implementierung der interoperablen Datenübermittlung von Onlinediensten, in denen Anträge gestellt werden können, an Verwaltungssysteme. FIT-Connect erlaubt auch eine maschinenlesbare Rückkanal-Kommunikation vom Verwaltungssystem zum Onlinedienst.

FIT-Connect bietet dazu eine einheitliche Schnittstelle zur Anbindung von Onlinediensten an die zuständigen Verwaltungssysteme 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-Dienstleister:innen 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.

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

2 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 Rück-

antworten. Die nachfolgende Tabelle orientiert sich am Verzeichnis der Verarbeitungstätigkeiten (VVT). 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. Daten gemäß Art. 9 und 10 DSGVO, 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 Onlinedienste 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 Verfahrensbetreiber:innen werden für die Erstellung eines Benutzerkontos im Self-Service-Portal	Verfahrensbetreiber:innen und deren Mitarbeitende

	zur Verwaltung von technischen Benutzer:innen in FIT-Connect benötigt.	
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:innen und deren Mitarbeitende
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 weiterverarbeitet.	Antragsteller:innen

Verarbeitete besondere personenbezogene Daten gemäß 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 und 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 Vertrags für mehrere angebundene Systeme (z. B. Onlinedienste oder Verwaltungssysteme). 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 erhält.

3 Art der Verarbeitung

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

4 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 Onlinedienst und dem Verwaltungssystem. Eine Entschlüsselung der Antragsdaten ist nicht Zweck der Verarbeitung und wird technisch durch eine Ende-zu-Ende-Verschlüsselung ausgeschlossen. Das gewährleistet, dass die Betreiber:innen 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-Service-Portal 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:innen von angebundenen Systemen werden zum Zwecke der Wartung und Fehlerbeseitigung verarbeitet.

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

5 Dauer der Verarbeitung

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

Der Vertrag wird unbefristet geschlossen.

ANHANG III: Liste der Unterauftragsverarbeiter:innen für FIT-Connect Liste der Unterauftragsverarbeitungen

Die:Der Verantwortliche hat die Inanspruchnahme folgender Unterauftragsverarbeiter:innen genehmigt:

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

ANHANG IV – Technische und organisatorische Maßnahmen

Die folgenden technischen und organisatorischen Maßnahmen (TOMs) 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:innen, die wir Ihnen auf Anfrage zur Verfügung stellen.

1 Verschlüsselung

Einreichungen setzen sich aus 4 Kategorien von Daten zusammen:

- Technische Daten
- Metadaten
- Fachdaten
- Anlagen

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

Die zur Verschlüsselung benötigten Schlüssel der Verwaltungssysteme werden durch den FIT-Connect Antragsübermittlungsdienst (Zustelldienst) auf Anfrage durch den Sender via API bereitgestellt.

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

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

3 Anonymisierung

Anträge/ Einreichungen werden zufällig generierten UIDs zugeordnet. Es erfolgt keine Identifizierung anhand von personenbezogenen Daten, sondern ausschließlich anhand der UIDs.

4 Datentrennung

Antragsübermittlungsdienst (Zustelldienst)

Sämtliche im Zustelldienst von FIT-Connect erfassten Einreichungen können ausschließlich von ihren designierten Empfänger:innen 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

Jede:r Anwender:in hat ausschließlich nur auf die Daten ihres:seines eigenen Kontos Zugriff.

5 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 innehaben.

Subscriber müssen konkreten Zustellpunkten zugeordnet werden und haben nur auf diese Zustellpunkte (konkretes Ziel einer Antragsübermittlung) 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.

6 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 den Onlinedienst 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.

7 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, sodass diese nach Entschlüsseln auf ihre Unverändertheit überprüft werden können.

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

8 Schutz des Internetauftritts

Sämtliche Endpunkte von FIT-Connect und beteiligter Stellen (Onlinedienste/ Verwaltungssysteme) werden durch TLS-Zertifikate in der aktuellsten Version abgesichert. Damit wird auf sämtlichen Kommunikationsverbindungen mit und innerhalb von FIT-Connect eine Transportwegeverschlüsselung realisiert.

9 Keine persistente Speicherung von personenbezogenen Daten

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