Ergänzende Bedingungen Auftragsverarbeitung (ErgB-AV) für die Open Telekom Cloud

Vertragspartner sind die Telekom Deutschland GmbH (im Folgenden Telekom genannt), Landgrabenweg 151, 53227 Bonn, und der Kunde.

1 Allgemeines

Gegenstand der Vereinbarung ist die Regelung der Rechte und Pflichten des Kunden (im Folgenden auch Verantwortlicher genannt) und der Telekom (im Folgenden auch Auftragsverarbeiter genannt), sofern im Rahmen der Leistungserbringung (nach AGB und mitgeltenden Dokumenten der Telekom) eine Verarbeitung personenbezogener Daten durch die Telekom für den Kunden im Sinne des anwendbaren Datenschutzrechts erfolgt.

Mit dieser Vereinbarung soll die Einhaltung von Art. 28 Absätze 3 und 4 der Verordnung (EU) 2016/679 (DSGVO) gewährleistet werden.

Aus den AGB, den sonstigen mitgeltenden Dokumenten, diesen „Ergänzenden Bedingungen Auftragsverarbeitung“ und deren Anhänge („ErgB-AV“) ergeben sich Gegenstand und Dauer sowie Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte des Verantwortlichen und Auftragsverarbeiters.

Zu diesem Zweck vereinbaren die Parteien die von der Europäischen Kommission (EU-Kommission) gemäß Art. 28 Absatz 7 DSGVO veröffentlichten Standardvertragsklauseln EU gemäß Durchführungsbeschluss (EU) 2021/915 vom 4. Juni 2021 (im folgenden „Klauseln“). Diese Klauseln sind in Ziffer 2 mit der jeweils ausgewählten Option im Originaltext aufgeführt.

Weitere Regelungen im Sinne von Klausel 2 Buchstabe b vereinbaren die Parteien in den Ziffern 3, 4 und 5 dieser ErgB-AV. Die Regelungen tragen insbesondere dem Umstand Rechnung, dass es sich bei der Leistung der Telekom um ein standardisiertes AGB-Produkt handelt. Die Parteien sind sich einig, dass diese Regelungen nicht im Widerspruch zu den Klauseln stehen.

2 Standardvertragsklauseln EU („Klauseln“)

ABSCHNITT I

Klausel 1 [Zweck und Anwendungsbereich]

a) Mit diesen Standardvertragsklauseln EU (im Folgenden „Klauseln“) soll die Einhaltung von Artikel 28 Absätze 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 freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) sichergestellt werden [OPTION 1].

b) Die in Anhang I aufgeführten Verantwortlichen und Auftragsverarbeiter haben diesen Klauseln zugestimmt, um die Einhaltung von Artikel 28 Absätze 3 und 4 der Verordnung (EU) 2016/679 und/oder Artikel 29 Absätze 3 und 4 der Verordnung (EU) 2018/1725 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 gemäß der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 unterliegt.

f) Diese Klauseln stellen für sich allein genommen nicht sicher, dass die Verpflichtungen im Zusammenhang mit internationalen Datenübermittlungen gemäß Kapitel V der Verordnung (EU) 2016/679 erfüllt werden.

Klausel 2 [Unabänderbarkeit der Klauseln]

a) Die Parteien verpflichten sich, die Klauseln nicht zu ändern, es sei denn, zur Ergänzung oder Aktualisierung der in den Anhängen angegebenen Informationen.

b) Dies hindert die Parteien nicht daran die in diesen Klauseln festgelegten Standardvertragsklauseln EU 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.

Klausel 3 [Auslegung]

a) Werden in diesen Klauseln die in der Verordnung (EU) 2016/679 definierten Begriffe verwendet, so haben diese Begriffe dieselbe Bedeutung wie in der betreffenden Verordnung.

b) Diese Klauseln sind im Lichte der Bestimmungen der Verordnung (EU) 2016/679 auszulegen.

c) Diese Klauseln dürfen nicht in einer Weise ausgelegt werden, die den in der Verordnung (EU) 2016/679 vorgesehenen Rechten und Pflichten zuwiderläuft oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneidet.

Klausel 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.

Klausel 5 [Kopplungsklausel]

a) Eine Einrichtung, die nicht Partei dieser Klauseln ist, kann diesen Klauseln mit Zustimmung aller Parteien jederzeit als Verantwortlicher oder als Auftragsverarbeiter beitreten, indem sie die Anhänge ausfüllt und Anhang I unterzeichnet.

b) Nach Ausfüllen und Unterzeichnen der unter Buchstabe a genannten Anhänge wird die beitretende Einrichtung als Partei dieser Klauseln behandelt und hat die Rechte und Pflichten eines Verantwortlichen oder eines Auftragsverarbeiters entsprechend ihrer Bezeichnung in Anhang I.

c) Für die beitretende Einrichtung gelten für den Zeitraum vor ihrem Beitritt als Partei keine aus diesen Klauseln resultierenden Rechte oder Pflichten.

ABSCHNITT II

Pflichten der Parteien

Klausel 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.

Klausel 7 [Pflichten der Parteien]

7.1 Weisungen

a) Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur auf dokumentierte Weisung 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.

b) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass vom Verantwortlichen erteilte Weisungen gegen die Verordnung (EU) 2016/679 oder geltende Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstoßen.

7.2 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.

7.3 Dauer der Verarbeitung personenbezogener Daten

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

7.4 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.

7.5 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. Gleiches gilt für Sozialdaten nach §§ 67 Abs. 2 SGB X, 35 Abs. 4 SGB I.

7.6 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 Verordnung (EU) 2016/679 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.

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.

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

7.7 Einsatz von Unterauftragsverarbeitern

a) ALLGEMEINE SCHRIFTLICHE GENEHMIGUNG: Der Auftragsverarbeiter besitzt die allgemeine Genehmigung des Verantwortlichen für die Beauftragung von Unterauftragsverarbeitern, die in einer vereinbarten Liste aufgeführt sind. Der Auftragsverarbeiter unterrichtet den Verantwortlichen mindestens vier Wochen im Voraus ausdrücklich in schriftlicher Form 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. [OPTION 2]

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 im Wesentlichen 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 Verordnung (EU) 2016/679 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.

7.8 Internationale Datenübermittlungen in Drittstaaten ohne Angemessenheitsbeschluss

a) Jede Übermittlung von Daten durch den Auftragsverarbeiter an ein Drittland oder eine internationale Organisation erfolgt ausschließlich auf der Grundlage dokumentierter Weisungen des Verantwortlichen oder zur Einhaltung einer speziellen Bestimmung nach dem Unionsrecht oder dem Recht eines Mitgliedstaats, dem der Auftragsverarbeiter unterliegt, und muss mit Kapitel V der Verordnung (EU) 2016/679 im Einklang stehen.

b) Der Verantwortliche erklärt sich damit einverstanden, dass in Fällen, in denen der Auftragsverarbeiter einen Unterauftragsverarbeiter gemäß Klausel 7.7 für die Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen) in Anspruch nimmt und diese Verarbeitungstätigkeiten eine Übermittlung personenbezogener Daten im Sinne von Kapitel V der Verordnung (EU) 2016/679 beinhalten, der Auftragsverarbeiter und der Unterauftragsverarbeiter die Einhaltung von Kapitel V der Verordnung (EU) 2016/679 sicherstellen können, indem sie Standardvertragsklauseln verwenden, die von der Kommission gemäß Artikel 46 Absatz 2 der Verordnung (EU) 2016/679 erlassen wurden, sofern die Voraussetzungen für die Anwendung dieser Standardvertragsklauseln erfüllt sind.

Klausel 8 [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 Klausel 8 Buchstabe 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 Artikel 32 der Verordnung (EU) 2016/679]. [OPTION 1]

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.

Klausel 9 [Meldung von Verletzungen des Schutzes personenbezogener Daten]

Im Falle einer Verletzung des Schutzes personenbezogener Daten des Verantwortlichen arbeitet der Auftragsverarbeiter mit dem Verantwortlichen zusammen und unterstützt ihn entsprechend, damit der Verantwortliche seinen Verpflichtungen gemäß den Artikeln 33 und 34 der

Verordnung (EU) 2016/679 nachkommen kann, wobei der Auftragsverarbeiter die Art der Verarbeitung und die ihm zur Verfügung stehenden Informationen berücksichtigt.

9.1 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 Artikel 33 Absatz 3 der Verordnung (EU) 2016/679 [OPTION 1] 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 Artikel 34 der Verordnung (EU) 2016/679 [OPTION 1] 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.

9.2. 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 Artikel 33 und 34 der Verordnung (EU) 2016/679 [OPTION 1] zu unterstützen.

ABSCHNITT III

SCHLUSSBESTIMMUNGEN

Klausel 10 [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 Verordnung (EU) 2016/679 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 Verordnung (EU) 2016/679 nicht erfüllt;

3) der Auftragsverarbeiter einer bindenden Entscheidung eines zuständigen Gerichts oder der zuständigen Aufsichtsbehörde(n), die seine Pflichten gemäß diesen Klauseln, der Verordnung (EU) 2016/679 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 Klausel 7.1 Buchstabe 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.

3 Weitere Klauseln im Sinne der Klausel 2 b

3.1 [Weisungen]

Die Parteien sind sich einig, dass als Weisungen im Sinne der Klauseln 7.1 Buchstabe a und 7.2 zunächst die AGB, sonstige mitgeltenden Dokumente sowie diese ErgB-AV zu verstehen sind. Im Rahmen der produktspezifischen Parameter kann der Verantwortliche darüber hinaus Art und Umfang der Datenverarbeitung durch die Art der Nutzung des Produktes und durch Auswahl etwaig ermöglichter Varianten bestimmen. Weisungen des Verantwortlichen können im vereinbarten Rahmen des Standardproduktes erfolgen. Bei weiteren Weisungen des Verantwortlichen, die über den vereinbarten Rahmen hinausgehen, gilt Ziffer 4 dieser ErgB-AV (Änderungen).

3.2 [Ergänzung zu Klausel 7.6]

Die Parteien vereinbaren zu Klausel 7.6, dass der Verantwortliche vorrangig geeignete Zertifizierungen der Telekom und weitere von ihr vorgelegte Dokumente zum Nachweis der Einhaltung der Klauseln sowie den in diesen Klauseln festgelegten und unmittelbar aus der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 hervorgehenden Pflichten verwendet. Er kann darüber hinaus in besonders zu begründenden Ausnahmefällen eine Vor-Ort-Kontrolle durchführen.

3.3 [Genehmigte Unterauftragsverarbeiter]

Die Liste der vom Verantwortlichen genehmigten Unterauftragsverarbeiter (ALLGEMEINE SCHRIFTLICHE GENEHMIGUNG gem. Klausel 7.7 Buchstabe a) findet sich in Anhang IV. Der Auftragsverarbeiter unterrichtet den Verantwortlichen grundsätzlich sechs Wochen im Voraus in Textform über planbare beabsichtigte Änderungen von Unterauftragsverarbeitern, die für den Auftragsverarbeiter Daten des Auftraggebers verarbeiten, und stellt dem Verantwortlichen die erforderlichen Informationen zur Verfügung, um sein Widerspruchsrecht ausüben zu können. Der Verantwortliche wird dem Auftragsverarbeiter hierzu binnen zwei Wochen schriftlich mitteilen, ob er Widerspruch *gegen diese Änderung erhebt* Soweit der Verantwortliche nicht binnen zwei Wochen ab Mitteilung der Änderung Widerspruch *erhebt* gilt die Änderung als genehmigt. Der Verantwortliche wird nicht unbillig Widerspruch einlegen. Legt der Verantwortliche Widerspruch ein und wird dem Auftragsverarbeiter dadurch seine Leistung unmöglich, kann *der Verantwortliche die betroffenen Leistungen ohne Einhaltung einer Frist kündigen.*

3.4 [Internationaler Datentransfer]

Die Ziffer 7.8 wird ersetzt durch:
Eine Übermittlung von Daten durch den Auftragsverarbeiter an ein Drittland ohne Angemessenheitsbeschluss der EU-Kommission nach Art. 45 DSGVO erfolgt nicht.

3.5 [Begriffszuordnung]

Die Parteien sind sich einig, dass die Begriffe “stellt sicher” und “sicherstellen”, soweit sie in den Klauseln verwendet werden, keine Garantie im Rechtssinne darstellen.

3.6 [Ergänzung zu Klausel 10 d) und Art. 28 Abs. 3 g) DSGVO]

Die Parteien sind sich einig, dass Klausel 10 Buchstabe d und Art. 28 Abs. 3 g) DSGVO so auszulegen sind, dass ein Wahlrecht auf Löschung oder Rückgabe nur besteht, wenn die vereinbarte Leistung beide Optionen ermöglicht.

4 Sonstiges

4.1 [Verantwortungsbereich des Kunden]

Für die Beurteilung der Zulässigkeit der Datenverarbeitung ist der Kunde verantwortlich. Der Kunde wird in seinem Verantwortungsbereich dafür Sorge tragen, dass die gesetzlich notwendigen Voraussetzungen (z.B. durch Einholung von Einwilligungserklärungen) geschaffen werden, damit die Telekom die vereinbarten Leistungen insoweit rechtsverletzungsfrei erbringen kann.

4.2 [Gültigkeit des Vertrags]

Von der Ungültigkeit einer Bestimmung dieser ErgB-AV bleibt die Gültigkeit der übrigen Bestimmungen unberührt. Sollte sich eine Bestimmung als unwirksam erweisen, werden die Parteien diese durch eine neue ersetzen, die dem von den Parteien Gewollten am nächsten kommt.

4.3 [Gerichtsstand]

Für Streitigkeiten im Zusammenhang mit dieser ErgB-AV ist Gerichtsstand, der in den AGB vereinbarte. Sollten die AGB eine solche Vereinbarung nicht enthalten, gilt als alleiniger Gerichtsstand Bonn. Dies gilt vorbehaltlich eines etwaigen ausschließlich gesetzlichen Gerichtsstandes.

4.4 [Vorrangregelung]

Bei Widersprüchen zwischen den Bestimmungen dieser ErgB-AV und Bestimmungen sonstiger Vereinbarungen, insbesondere der AGB und den mitgeltenden Dokumenten, sind die Bestimmungen dieser ErgB-AV maßgebend. Im Übrigen bleiben die Bestimmungen der AGB und den mitgeltenden Dokumenten unberührt und gelten für diese ErgB-AV entsprechend.

Anhang I Ergänzende Bedingungen Auftragsverarbeitung (ErgB-AV) für die Open Telekom Cloud (OTC)

Liste der Parteien

Parteien der Vereinbarung sind die Vertragspartner des Leistungsvertrages.

Anhang II Ergänzende Bedingungen Auftragsverarbeitung (ErgB-AV) für die Open Telekom Cloud (OTC)

Beschreibung der Verarbeitung

1 Einzelheiten der Datenverarbeitung

a. Art der Leistung

☒ IaaS (Infrastructure as a Service)

☒ PaaS (Platform as a Service)

☒ SaaS (Software as a Service)

b. Kategorien betroffener Personen

☒ Kunden des Verantwortlichen

☒ Mitarbeiter des Verantwortlichen

☒ personenbezogene Daten von Personen, die vom Kunden in der Open Telekom Cloud verarbeitet werden.

c. Kategorie personenbezogener Daten:

☒ Stammdaten der Kunden des Verantwortlichen

☒ Kontaktdaten der Kunden des Verantwortlichen

☒ personenbezogene Daten zur Protollierung (z.B. Benutzerkennung, IP-Adresse)

☒ Alle sonstigen personenbezogene Daten, die in Art. 4 Nr. 1 der DSGVO definiert sind, die vom Kunden im Zuge der Nutzung des Produktes übermittelt oder gespeichert werden und auf die ein Zugriff durch die Systemadministratoren der Telekom nicht vollständig ausgeschlossen werden kann.

d. Sensible personenbezogene Daten

Sensible personenbezogene Daten sowie angewandte Beschränkungen oder Garantien (Art. 9 DSGVO, Art.10 DSGVO), die der Sensibilität der Daten und den damit verbundenen Risiken in vollem Umfang Rechnung tragen (z.B. zusätzliche Sicherheitsmaßnahmen):

Keine.

2 Zugriff auf personenbezogene Daten

Der Kunde stellt der Telekom die personenbezogenen Daten bereit, ermöglicht Zugriff auf die personenbezogenen Daten oder erlaubt personenbezogene Daten zu verarbeiten, und zwar wie nachfolgend beschrieben:
Der Kunde stellt der Telekom die personenbezogenen Daten bereit, ermöglicht ihm Zugriff auf die personenbezogenen Daten oder erlaubt ihm, die personenbezogenen Daten zu erheben, indem der Kunde diese Daten über eine gesicherte Internetverbindung übermittelt. In der Regel hat die Telekom keinen Zugriff auf die personenbezogenen Daten des Kunden. Dieser kann aber in Ausnahmefällen, z.B. Wartung oder Störungsbeseitigung nicht vollständig ausgeschlossen werden und erfolgt nur nach gesonderter Genehmigung durch den Kunden.

3 Zweck der Verarbeitung

Die Art der Leistung sowie der Verarbeitungszweck sind in den Produkt-AGB und der Leistungsbeschreibung abschließend geregelt.

4 Nachweis durch die Telekom

Telekom steht es frei, die Umsetzung der Datenschutzverpflichtungen nach Ziffer 3.2 durch folgende Nachweise zu belegen:

☒ die Einhaltung genehmigter Verhaltensregeln gem. Art. 40 DSGVO;

☒ die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gem. Art. 42 DSGVO;

☒ aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z. B. Wirtschaftsprüfer, Revision);

☒ eine geeignete Zertifizierung (außer Zertifikat gem. Art. 42 DSGVO)

☒ Eigenerklärung des Auftragsverarbeiters.

Anhang III Ergänzende Bedingungen Auftragsverarbeitung (ErgB-AV) für Open Telekom Cloud

Technische und organisatorische Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung

1 Verfügbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

Das Gewährleistungsziel "Verfügbarkeit" bezeichnet die Anforderung, dass der Zugriff auf personenbezogene Daten und ihre Verarbeitung möglich ist und diese so ordnungsgemäß im vorgesehenen Prozess verwendet werden können. Dazu müssen sie im Zugriff von Berechtigten liegen und die vorgesehenen Methoden zu deren Verarbeitung müssen auf sie angewendet werden können.

a. Physischer Schutz vor äußeren Einflüssen

Beim Auftragsverarbeiter sind geeignete Maßnahmen zum Schutz vor internen und externen Bedrohungen konzipiert und umgesetzt. Diese dienen dem Schutz:

- vor Naturkatastrophen, Angriffen oder Unfällen,
- vor Störungen etwa durch Stromausfälle oder anderen Versorgungseinrichtungen,
- der Verkabelung vor Unterbrechung, Störung oder Beschädigung.

Die Maßnahmen zum physischen Schutz werden regelmäßig auf ihre Wirksamkeit getestet. Zudem wird das Schutzkonzept bei Änderungen der Datenverarbeitung angepasst. Entsprechende Prozesse sind beim Auftragsverarbeiter implementiert.

b. Schutz der IT-Systeme und Netze vor äußeren Bedrohungen

Der Auftragsverarbeiter hat Regelungen definiert, die IT-Systeme, Netze und Komponenten (technische Einrichtungen, Versorgungseinrichtungen, etc.) die zur Verarbeitung personenbezogener Daten genutzt werden vor unbefugtem Zugriff, unbefugter Modifikation, Verlust oder Zerstörung oder falscher und gesetzwidriger Nutzung schützen. Diese Regelungen beziehen sich auf den gesamten Lebenszyklus.
Zudem wurden Datenschutz und -sicherheit so in das Business Continuity Management integriert, dass Prozesse, Verfahren und Maßnahmen auch in widrigen Situationen eine vertragsgemäße Auftragsverarbeitung ermöglichen. Der Auftragsverarbeiter überprüft diese regelmäßig auf Wirksamkeit.

c. Systemhärtung

Informationsverarbeitende Systeme sind vor Schadsoftware geschützt und gehärtet. Zum Schutz der Systeme ist geeignete Software (z.B. Virenscanner, IDS) installiert und aktuell. Bei einer Systemhärtung wurden mindestens die folgenden Anforderungen umgesetzt:

- Der Patchstand ist aktuell.
- Bei der Installation eines Systems werden nur solche Software-Komponenten installiert oder aktiviert, die für den Betrieb und die Funktion des Systems notwendig sind.
- Neben Funktionen der Software sind nach der Systeminstallation auch keine Hardware-Funktionen aktiviert, die nicht für den Einsatz des Systems benötigt werden. Solche Funktionen, wie beispielsweise nicht benötigte Schnittstellen, wurden dauerhaft deaktiviert, so dass sie auch nach einem Neustart deaktiviert bleiben.
- Sämtliche auf einem System und den Schnittstellen nicht erforderliche Dienste wurden deaktiviert und bleiben auch nach einem Neustart des Systems weiterhin deaktiviert.
- Die Erreichbarkeit eines Dienstes über die erforderlichen Schnittstellen wurde zudem auf legitime Kommunikationspartner eingeschränkt,
- Nicht benötigte voreingestellte Dienstkonten wurden gelöscht und voreingestellte Passwörter geändert.
- Es ist üblich, dass auf Systemen Authentisierungsmerkmale wie Passwörter und kryptographische Schlüssel durch Hersteller, Entwickler oder Lieferanten vorkonfiguriert werden. Solche Authentisierungsmerkmale wurden in eigene, Dritten nicht bekannte Merkmale geändert.
- Wird das System auf einer Cloud-Plattform betrieben, wurde verhindert, dass das System (bzw. der komplette Mandant/Tenant mit all seinen Diensten und Daten) versehentlich oder durch Unbefugte vollständig gelöscht werden kann.

d. Backup-Konzept

Der Auftragsverarbeiter hat Regelungen definiert, die eine geeignete Backup-Strategie ermöglichen. Diese berücksichtigt insbesondere Anforderungen an die Verfügbarkeit des Systems, die regelmäßige Überprüfung der Wiederherstellbarkeit, sowie gesetzliche Vorgaben an Speicherung oder Löschung.
Ziel dieser Maßnahme ist es, ein konsistentes Abbild der Wirkdaten in Notfall zu gewährleisten. Hier können, abhängig von den Rahmenbedingungen, verschiedene Strategien zur Anwendung kommen. Statt einer „klassischen“ Backuplösung ist auch der Betrieb von Spiegelsystemen in einem anderen Sicherheitsbereich oder eine Kombination aus beiden Strategien möglich.

e. Personalkonzept zur Gewährleistung der Schutzziele

Der Auftragsverarbeiter hat ein Personalkonzept umgesetzt, das den Datenschutz durch die folgenden Maßnahmen unterstützt:

- Es wird nur fachkundiges Personal eingesetzt, das die notwendigen Schulungen und

Verpflichtungen auf Vertraulichkeit und das Fernmeldegeheimnis durchgeführt hat.
- Es gibt für die Verarbeitung personenbezogener Daten einen verantwortlichen Ansprechpartner. Eine Vertreterregelung existiert.
- Beschäftigte und Auftragsverarbeiter geben bei Beendigung des Beschäftigungsverhältnisses, des Vertrags oder der Vereinbarung die in ihrem Besitz befindlichen Werte an die Organisation (Verantwortlicher/Auftragsverarbeiter) zurück, die ihnen zur Erfüllung der Aufgabe überlassen wurden. Zu diesen gehören Zutrittsmittel, Rechner, Speichermedien und mobile Endgeräte.
- Verpflichtung des Personals auf den Geheimnisschutz nach § 203 StGB und das Sozialgeheimnis nach § 35 SGB 1.

f. Erstellung eines Notfallkonzepts zur Wiederherstellung einer Verarbeitungstätigkeit

Der Auftragsverarbeiter hat ein Notfallkonzept zur Wiederherstellung der Datenverarbeitung implementiert. Ziel dieses Konzepts ist die Wiederherstellung der Verfügbarkeit nach einer Störung der Verarbeitung. Das Notfallkonzept genügt dabei den folgenden Anforderungen/Kriterien:
- Es existieren Vorgaben, in denen nach einer Störung die Zeit bis zur Wiederherstellung der geregelten Datenverarbeitung festgelegt ist.
- Die Bereitstellung von Ressourcen zur Wiederherstellung ist erfolgt.
- Die Zuordnung von Verantwortlichkeiten ist erfolgt.
- Die Definition von geprüften Maßnahmen zur Abwehr der Störung und Wiederherstellung des Regelbetriebs ist erfolgt.
- Informations- und Eskalationsketten existieren.
- Definition der Interaktion mit korrespondierenden Prozessen und Regelungen (Backupkonzept, Personalkonzept, ...) ist erfolgt.

2 Integrität (Art. 32 Abs. 1 lit. b DSGVO)

Das Gewährleistungsziel "Integrität" bedeutet, dass die zu verarbeitenden Daten unversehrt, vollständig, richtig und aktuell bleiben.

a. Definition, Anwendung, und Kontrolle des Sollverhaltens von Prozessen

Der Auftragsverarbeiter hat durch seine Leitung oder Geschäftsführung Prozesse zur Umsetzung des Datenschutzes und der Informationssicherheit festgelegt. Diese sind schriftlich fixiert, frei zugänglich, allen internen und externen Beschäftigten bekannt gemacht. Ziel der Vorgaben ist es, die Verarbeitung von personenbezogenen Daten so umzusetzen, dass das definierte Sollverhalten der Prozesse gewährleistet ist. Die Vorgaben werden regelmäßig auf Wirksamkeit, Aktualität und Regelkonformität hin geprüft.

b. Berechtigungskonzept

Der Auftragsverarbeiter nutzt Berechtigungskonzepte, die vorgeben wer wann auf welche Systeme, Datenbanken oder Netze Zugriff hat. Die Berechtigungskonzepte sollen dabei folgenden Eigenschaften genügen:
- Es gibt definierte Berechtigungen in Form von Rollen auf Basis der geschäftlichen, sicherheitsrelevanten und datenschutzrechtlichen Anforderungen.
- Die Rollen sind dokumentiert und aktuell.
- Rollen werden Nutzern oder Maschinen eindeutig zugeordnet.
- Benutzer haben ausschließlich Zugang zu den Netzwerken, Systemen und Daten zu deren Nutzung sie ausdrücklich befugt sind.
- Ein formaler Prozess für die Registrierung und Deregistrierung ist definiert, um die Zuordnung von Zugangsrechten zu ermöglichen.
- Ein formaler Prozess zur Zuteilung von Benutzerzugängen ist definiert, um die Zugangsrechte für alle Benutzerarten zu allen Systemen und Diensten zuzuweisen oder zu entziehen.
- Die Zuteilung und der Gebrauch von privilegierten Zugangsrechten ist eingeschränkt und wird fortlaufend kontrolliert.
- Die Zuteilung von Zugangsrechten unterliegt der Kontrolle, mit dem Ziel eine funktionsübergreifende Rechtezuweisung zu verhindern.

c. Identitätsmanagement

Die Zuteilung einer Berechtigung für den Zugriff auf personenbezogene Daten erfolgt erst nach einer eindeutigen Identifizierung des Benutzers. Benutzer können eindeutig von einem System identifiziert werden. Dies wird dadurch erreicht, dass für jeden Benutzer ein individuelles Benutzerkonto genutzt wird. Sogenannte Gruppenkonten, d.h. die Nutzung eines Benutzerkontos für mehrere Personen werden nicht verwendet.
Eine Ausnahme dieser Anforderung sind die sogenannte Maschinenkonten. Diese werden für Authentifizierung und Autorisierung von Systemen untereinander oder von Anwendungen auf einem System genutzt und können damit nicht einer einzelnen Person zugewiesen werden. Solche Benutzerkonten werden individuell pro System oder pro Anwendung vergeben. Ziel dieser Maßnahme ist, dass eine missbräuchliche Nutzung solcher Benutzerkonten nicht möglich ist.

d. Kryptokonzept

Der Auftragsverarbeiter hat den Gebrauch kryptografischer Maßnahmen zum Schutz personenbezogener Daten durch Vorgaben definiert. Diese Vorgaben beinhalten:
- die Nutzung des angewandten Stands der Technik kryptografischer Verfahren,
- den erforderlichen Schutzbedarf der personenbezogenen Daten auf Basis einer Risikoeinschätzung,
- die Verwaltung und Anwendung kryptografischer Schlüssel,
- den Schutz kryptografischer Schlüssel über deren gesamten Lebenszyklus (die Erzeugung, Speicherung, Anwendung und Vernichtung).

Ziel eines solchen Kryptokonzepts ist es:

- die Integrität schutzbedürftiger Daten zu gewährleisten,
- Prozesse des Identitätsmanagements abzusichern,
- Authorisierungsprozesse zu unterstützen,
- und die Vertraulichkeit schutzbedürftiger Daten zu gewährleisten.

e. Prozesse zur Aufrechterhaltung der Aktualität von Daten

Der Auftragsverarbeiter hat Prozesse definiert, umgesetzt und kommuniziert, die die Aktualität der personenbezogenen Daten unterstützen und den folgenden Anforderungen unterliegen:

- Anfragen zu Berichtigungen, Änderungen und Löschungen durch den Betroffenen erfolgen zeitnah und über alle gespeicherten Datensätze.
- Änderungen oder Löschungen personenbezogener Daten erfolgen automatisiert oder prozessgesteuert über alle gespeicherten Datensätze.
- Erfolgte Änderungen an Daten mit Personenbezug sind über Zeitstempel voneinander unterscheidbar.
- Speicherdauer und Löschfristen sind gemäß den gesetzlichen oder vertraglichen Vorgaben festgelegt.

3 Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

Das Gewährleistungsziel "Vertraulichkeit" bezeichnet die Anforderung, dass keine unbefugte Person personenbezogene Daten zur Kenntnis nehmen oder nutzen kann.

a. Festlegung der Nutzung zugelassener Ressourcen und Kommunikationskanäle

Der Auftragsverarbeiter implementiert die folgenden Maßnahmen so, dass die für die Verarbeitung personenbezogener Daten genutzten Ressourcen und Kommunikationskanäle festgelegt sind:

- Bereiche sind in Abhängigkeit des Schutzbedarfs definiert, die notwendigen Sicherheitsperimeter vorgegeben und umgesetzt. Die Schutzbedarfseinstufung richtet sich nach den in den Bereichen (einschließlich mobiler Arbeitsplätze) befindlichen personenbezogenen Daten oder informationsverarbeitenden Systemen.
- Es sind geeignete Zutrittssteuerungsvorgaben definiert und angewendet, die gewährleisten, dass nur berechtigte Personen Zutritt zu den definierten Bereichen erhalten.
- Eine Zugangssteuerungsrichtlinie ist auf Grundlage der datenschutzrechtlichen und sicherheitsrelevanten Anforderungen in der Organisation erstellt und umgesetzt. Diese Richtlinie regelt den Zugang zu personenbezogenen Daten in Abhängigkeit von deren Schutzbedarf auf den zur Aufgabenerfüllung minimalen Umfang (need to know). Dazu gehört insbesondere der Zugriff auf IT-Systeme, Netzwerke und Datenbanken.
- Verfahren, die die Handhabung von Datenträgern regeln, sind entsprechend dem identifizierten Schutzbedarf umgesetzt.
- Bei Speicherung personenbezogener Daten auf mobilen Datenträgern werden diese wirksam verschlüsselt.
- Es gibt Vorgaben zum Transport von Datenträgern, die sich an dem Schutzbedarf der personenbezogenen Daten orientieren. Soweit personenbezogene Daten nicht verschlüsselt sind, werden angemessene alternative Schutzmaßnahmen ergriffen. Bei hohem Schutzbedarf bestehen besondere Anforderungen an die Zuverlässigkeit des Transportes, die Verpflichtung zur Verschlüsselung von Daten, Dokumentations-, Protokoll- und Nachweispflichten.
- Es existieren Richtlinien, Sicherheitsverfahren und Steuerungsmaßnahmen, um die Übertragung von Informationen für alle Arten von Kommunikationseinrichtungen (einschließlich mobiler Arbeitsplätze) zu schützen.
- Gemessen an den identifizierten Risiken der Nutzung von Mobilgeräten (Laptops, externe Speichermedien, Mobiltelefone) sind geeignete Richtlinien und Maßnahmen zur Gewährleistung der Vertraulichkeit und Integrität in der Organisation umgesetzt. Ziel dieser Regelungen ist es, den Zugriff auf personenbezogene Daten zu minimieren, deren Speicherung und Übertragung zu verschlüsseln und die Nutzung externer Speichermedien auf das Notwendige zu reduzieren.

b. Authentisierungsverfahren

Der Zugang zu Systemen und Anwendungen wird durch ein geeignetes Authentisierungsverfahren umgesetzt. Das Authentisierungsverfahren berücksichtigt den Schutzbedarf der personenbezogenen Daten, auf die nach erfolgreicher Authentisierung zugegriffen werden kann. Bei hohem Schutzbedarf werden Anmeldeverfahren angewendet, die auf Besitz und Wissen (Zwei-Faktor-Authentisierung) basieren. Von hohem Schutzbedarf ist auszugehen, wenn der Zugriff auf Daten ermöglicht wird, die z.B. unter Art. 9 Abs. 1 der DSGVO fallen. Bei geringerem Schutzbedarf ist eine Authentisierung durch Benutzername und Passwort implementiert. Grundsätzlich genügt das gewählte Authentisierungsverfahren den folgenden Kriterien:

- Alle Benutzerkonten des Systems werden vor einer Nutzung durch Unberechtigte geschützt. Hierfür wird das Benutzerkonto mit einem Authentisierungsmerkmal abgesichert, welches eine eindeutige Authentifizierung des zugreifenden Benutzers ermöglicht. Authentisierungsmerkmale sind z.B.: Passwörter, PINs, (Faktor Wissen) /Kryptographische Schlüssel, Token, Smartcards, OTP (Besitz)/oder biometrische Merkmale wie etwa Fingerabdrücke oder die Hand-Geometrie (Inhärenz)
- Die Vorgaben für die Erzeugung/Erstellung von Passwörtern (Länge, Komplexität, Wiederverwendung, etc.) richten sich mindestens nach dem angewandten Stand der Technik

- Beim Einsatz von Passwörtern als Authentisierungsmerkmal ist ein Schutz gegen Online-Angriffe wie Wörterbuch- und Brute-Force-Attacken vorhanden
- Das System bietet Funktionen, die es dem Benutzer ermöglicht das Passwort jederzeit zu ändern.
- Passwörter werden unter Verwendung einer für diesen Zweck geeigneten, nach angewandtem Stand der Technik als sicher eingestuften, kryptografischen Einwegfunktion gespeichert (bekannt als "Password-Hashing" Verfahren)
- Werden Systeme zur Verwaltung und Vergabe von Kennwörtern genutzt, so gewährleisten diese die Verwendung starker Kennwörter. Erfolgt der Zugang durch Hilfsprogramme, automatisiert oder durch Routinen in der Softwareentwicklung, dann wird der Gebrauch dieser auf das notwendige Mindestmaß reduziert und die Anwendung regelmäßig überwacht.
- Benutzer welche über erweiterte Berechtigungen innerhalb eines Systems verfügen, wie etwa einen Zugriff auf personenbezogene Daten mit einem hohen Schutzbedarf, Konfigurationseinstellungen oder Administrationszugänge bekommen, um ein angemessenes Schutzniveau zu erreichen, mindestens zwei voneinander unabhängige Authentisierungs-merkmale. Die verwendeten Authentisierungsmerkmale müssen aus unterschiedlichen Faktoren (Wissen, Besitz, Inhärenz) bestehen. Dieser Ansatz wird allgemein als MFA (Multi-Faktor-Authentisierung) bezeichnet. Eine spezifische Form der MFA ist die 2FA (2-Faktor-Authentisierung), die exakt zwei Authentisierungsmerkmale kombiniert. Eine Kombination von Authentisierungsmerkmalen desselben Faktors (z.B. zwei unterschiedliche Passwörter) ist nicht zulässig.

c. Verpflichtung der Mitarbeiter

Die Telekom wird im Zusammenhang mit der hier vereinbarten Verarbeitung personenbezogener Daten die Vertraulichkeit nach der DSGVO, nach § 3 TTDSG und nach § 203 StGB wahren und die zur Verarbeitung der personenbezogenen Daten befugten Personen entsprechend verpflichten und sensibilisieren. Im Anwendungsbereich der Verarbeitung von Sozialdaten wird die Telekom ergänzend auf die Wahrung des Sozialgeheimnisses nach § 35 SGB I verpflichten. Vereinbarungen in den AGB und den mitgeltenden Dokumenten zur Wahrung der Vertraulichkeit und zum Schutz von nicht personenbezogenen Daten bleiben unberührt. Soweit in den AGB und den mitgeltenden Dokumenten hierzu keine Vereinbarung getroffen wurden, verpflichten sich beide Parteien, alle nicht allgemein offenkundigen Informationen aus dem Bereich der anderen Partei, die ihnen durch die Geschäftsbeziehung bekannt werden, geheim zu halten und nicht für eigene Zwecke außerhalb dieses Vertrages oder Zwecke Dritter zu verwenden.

4 Nichtverkettung

Das Gewährleistungsziel "Nichtverkettung" bezeichnet die Anforderung, dass personenbezogene Daten nicht zusammengeführt, also verkettet, werden. Sie ist insbesondere dann faktisch umzusetzen, wenn die zusammenzuführenden Daten für unterschiedliche Zwecke erhoben wurden.

a. Definition und Festlegung des Verarbeitungszwecks

Der Auftragsverarbeiter setzt geeignete Maßnahmen ein, um die im Auftrag verarbeiteten personenbezogenen Daten nur im Rahmen des vertraglich vereinbarten Zwecks zu verarbeiten. Zu diesen Maßnahmen zählen:

- interne Dokumentation und Kommunikation des Verwendungszwecks in allen Datenverarbeitungsverfahren
- und geregelte Zweckänderungsverfahren.

b. Maßnahmen zur Gewährleistung der Zweckbindung

Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich zu dem vertraglich vereinbarten Zwecken und nur zur Verarbeitung befugte Personen/Instanzen erhalten Zugriff auf die Daten. Neben den definierten Anforderungen zu den Gewährleistungszielen Verfügbarkeit, Integrität und Vertraulichkeit wurden folgende Maßnahmen getroffen, um eine Verkettung von Datensätzen mit unterschiedlicher Zweckbindung zu vermeiden:

- Einschränkung von Verarbeitungs-, Nutzungs- und Übermittlungsrechten auf das zur Verarbeitung zwingend notwendige Maß
- Trennung nach Organisations-/Abteilungsgrenzen
- Trennung von Umgebungen mittels Rollenkonzepten mit abgestuften Zugriffsrechten auf der Basis eines Identitätsmanagements und mittels sicherer Authentifizierungsverfahrens
- Entwicklungs-, Test- und Betriebsumgebungen müssen zumindest logisch getrennt sein. Es wurden geeignete Zugangskontrollen implementiert, um zu gewährleisten, dass der Zugang auf ordnungsgemäß autorisierte Personen beschränkt ist. Innerhalb dieser Umgebungen wurden die personenbezogenen Daten dieser Auftragsverarbeitung von anderen getrennt. Diese Trennung wurde entweder physikalisch oder logisch umgesetzt.
- Wenn Test- oder Entwicklungsnetzwerke oder -geräte den Zugriff auf das betriebliche Netzwerk erfordern, wurden starke Zugriffskontrollen implementiert.
- Die Verarbeitung personenbezogener Daten in Test- und Entwicklungsumgebungen ist ausgeschlossen. Notwendige Ausnahmen sind nur durch eine separate schriftliche Weisung des Auftraggebers möglich.

c. Definition, Einführung und Anwendung von Anonymisierungsverfahren

Der Auftragsverarbeiter organisiert die Datenverarbeitung so, dass personenbezogenen Daten nur unter Berücksichtigung der Zweckbindung verarbeitet werden. Ist eine Zweckbindung nicht gegeben, werden nicht benötigte Daten gelöscht. Sollte eine Löschung nicht möglich sein, werden die entsprechenden Datensätze anonymisiert. Dazu dient der Einsatz von zweckspezifischen Pseudonymen, Anonymisierungsdiensten, anonymen Credentials und die Verarbeitung pseudonymer bzw. anonymisierter Daten sowie die Implementierung von Datenmasken, die Datenfelder unterdrücken, sowie automatischer Sperr- und Löschroutinen, Pseudonymisierungs- und Anonymisierungsverfahren.

5 Transparenz

Das Gewährleistungsziel "Transparenz" bezeichnet die Anforderung, dass in einem unterschiedlichen Maße sowohl Betroffene, als auch die Betreiber von Systemen sowie zuständige Kontrollinstanzen erkennen können, welche Daten wann und für welchen Zweck bei einer Verarbeitungstätigkeit erhoben und verarbeitet werden, welche Systeme und Prozesse dafür genutzt werden, wohin die Daten zu welchem Zweck fließen und wer die rechtliche Verantwortung für die Daten und Systeme in den verschiedenen Phasen einer Datenverarbeitung besitzt.

a. Verfahrensverzeichnis

Die folgende Anforderung aus Art. 30 der DSGVO wurde beim Auftragsverarbeiter umgesetzt:
"Der Auftragsverarbeiter und gegebenenfalls sein Vertreter führen ein Verzeichnis zu allen Kategorien von im Auftrag eines Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung, das Folgendes enthält:

- den Namen und die Kontaktdaten des Auftragsverarbeiters oder der Auftragsverarbeiter und jedes Verantwortlichen, in dessen Auftrag der Auftragsverarbeiter tätig ist, sowie gegebenenfalls des Vertreters des Verantwortlichen oder des Auftragsverarbeiters und eines etwaigen Datenschutzbeauftragten;
- die Kategorien von Verarbeitungen, die im Auftrag jedes Verantwortlichen durchgeführt werden;
- gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Artikel 49 Absatz 1 Unterabsatz 2 DSGVO genannten Datenübermittlungen die Dokumentierung geeigneter Garantien;
- wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1 DSGVO.

Das genannte Verzeichnis ist schriftlich zu führen, was auch in einem elektronischen Format erfolgen kann.
Der Verantwortliche oder der Auftragsverarbeiter sowie gegebenenfalls der Vertreter des Verantwortlichen oder des Auftragsverarbeiters stellen der Aufsichtsbehörde das Verzeichnis auf Anfrage zur Verfügung.
Die in den genannten Pflichten gelten nicht für Unternehmen oder Einrichtungen, die weniger als 250 Mitarbeiter beschäftigen, es sei denn die von ihnen vorgenommene Verarbeitung birgt ein Risiko für die Rechte und Freiheiten der betroffenen Personen, die Verarbeitung erfolgt nicht nur gelegentlich oder es erfolgt eine Verarbeitung besonderer Datenkategorien gemäß Artikel 9 Absatz 1 bzw. die Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten im Sinne des Artikels 10 DSGVO".

b. Dokumentation der Datenverarbeitung

Der Auftragsverarbeiter dokumentiert die Verarbeitung personenbezogener Daten wie folgt:

- Der Verarbeitungsprozess ist so dokumentiert, das nachvollziehbar ist, wie die Verarbeitung personenbezogener Daten umgesetzt ist. Dies bezieht sich auf den gesamten Verarbeitungszyklus von der Übernahme/Erzeugung personenbezogener Daten bis hin zur deren Weitergabe/Löschung.
- Es erfolgt eine Dokumentation im Fall von Störungen, Problembearbeitungen, sowie Änderungen an Verarbeitungstätigkeiten oder den technischen und organisatorischen Maßnahmen.

c. Dokumentation und Speicherung von Verträgen, Vereinbarungen, Weisungen

Der Auftragsverarbeiter legt alle Verträge, Vereinbarungen oder Weisungen so ab, dass diese in angemessener Frist für die Vertragspartner oder Aufsichtsbehörden verfügbar sind.

d. Protokollierung der Datenverarbeitung

Zugriffe von Benutzern und/oder Systemadministratoren auf personenbezogene Daten werden unter Berücksichtigung des Grundsatzes der Datenminimierung und des Schutzbedarfs protokolliert und regelmäßig überprüft.

- Der Zugriff, sowie die Art des Zugriffs (z.B. Lesen, Ändern, Löschen) wird protokolliert.
- Relevante Ereignisse, Ausnahmen, Störungen und Informationssicherheitsvorfälle werden protokolliert und regelmäßig geprüft.
- Die Protokolle werden so abgelegt, dass der Zugriff durch die protokollierten Systemadministratoren oder Benutzer auf die Protokolle nicht möglich ist.

e. Gewährleistung der Auskunftspflichten

Der Auftragsverarbeiter hat einen Prozess implementiert, der das Auskunftsrecht eines Betroffenen gemäß der Vorgaben Art. 15 DSGVO unterstützt. Dieser Prozess wird regelmäßig auf seine Wirksamkeit hin überprüft.

6 Intervenierbarkeit

Das Gewährleistungsziel "Intervenierbarkeit" bezeichnet die Anforderung, dass den betroffenen Personen die ihnen zustehenden Rechte auf Benachrichtigung, Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit, Widerspruch und Erwirkung des Eingriffs in automatisierte Einzelentscheidungen bei Bestehen der gesetzlichen Voraussetzungen unverzüglich und wirksam gewährt werden.

a. Prozessimplementierung zur Umsetzung der Betroffenenrechte

Der Auftragsverarbeiter hat Maßnahmen zur Wahrung von Betroffenenrechten implementiert. Grundsätzlich sind die im Folgenden genannten Maßnahmen geeignet:

- Sofern nicht bereits durch den Verantwortlichen umgesetzt, hat der Auftragsverarbeiter einen Prozess zur Identifizierung und Authentifizierung der Personen, die Betroffenenrechte wahrnehmen möchten implementiert.
- Verantwortlicher und Auftragsverarbeiter definieren gemeinsam ein Merkmal, mit dem Betroffene eindeutig über Organisationsgrenzen hinweg identifiziert werden kann.
- Der Auftragsverarbeiter hat Systeme, Software und Prozesse so implementiert, dass Maßnahmen für differenzierte Einwilligungs-, Rücknahme- sowie Widerspruchsmöglichkeiten möglich sind.
- Der Auftragnehmer hat die operative Möglichkeit zur Zusammenstellung, konsistenten Berichtigung, Sperrung und Löschung aller zu einer Person gespeicherten Daten implementiert.
- Bevorzugung von automatisierten Verarbeitungsprozessen (nicht Entscheidungsprozessen), die eine Kenntnisnahme verarbeiteter Daten entbehrlich machen und die Einflussnahme begrenzen, gegenüber im Dialog gesteuerten Prozessen.

b. Implementierung von Maßnahmen zur Umsetzung von Betroffenenrechten im Systemdesign (Privacy by Design)

Der Auftragsverarbeiter beachtet beim Systemdesign die Umsetzung der Betroffenenrechte und Anforderungen des Datenschutzes. Die folgenden Maßnahmen werden beim Systemdesign (Prozesse und Software) berücksichtigt:

- Festlegung von Voreinstellungen für betroffene Personen, die die Verarbeitung ihrer Daten auf das für den Verarbeitungszweck erforderliche Maß beschränken.
- Bereitstellen von Optionen für Betroffene, um Programme datenschutzgerecht einstellen zu können
- Deaktivierungsmöglichkeit einzelner Funktionen ohne Mitleidenschaft für das Gesamtsystem.
- Implementierung standardisierter Abfrage- und Dialogschnittstellen für Betroffene zur Geltendmachung und/oder Durchsetzung von Ansprüchen.
- Betreiben einer Schnittstelle für strukturierte, maschinenlesbare Daten zum Abruf durch Betroffene.
- Reduzierung der Verarbeitungsoptionen in Verarbeitungsprozessschritten.
- Schaffung notwendiger Datenfelder z. B. für Sperrkennzeichen, Benachrichtigungen, Einwilligungen, Widersprüche, Gegendarstellungen.
- Entfernen nicht notweniger Datenfelder und Optionen, Reduktion der Ausgabe nach Suchanfragen in Datenbanken, Minimierung von Export- und Druckfunktionen.

7 Datenminimierung

Das Gewährleistungsziel "Datenminimierung" erfasst die grundlegende datenschutzrechtliche Anforderung, die Verarbeitung personenbezogener Daten auf das dem Zweck angemessene, erhebliche und notwendige Maß zu beschränken.

a. Operative Maßnahmen zur Datenminimierung

Der Auftragsverarbeiter ergreift operative Maßnahmen, mit dem Ziel die Verarbeitung personenbezogener Daten zweckgebunden auf ein Minimum zu beschränken. Folgende Maßnahmen sind implementiert:

- Beschränkung der erfassten Attribute der betroffenen Personen auf das erforderliche Minimum
- Bei Weitergabe personenbezogener Daten werden nur solche Attribute weitergegeben, die für den Verarbeitungszweck des nachfolgenden Prozessschritts unbedingt notwendig sind.

b. Technische Maßnahmen zur Datenminimierung

Der Auftragsverarbeiter ergreift technische Maßnahmen, mit dem Ziel die Verarbeitung personenbezogener Daten zweckgebunden auf ein Minimum zu beschränken. Folgende Maßnahmen sind geeignet:

- Beschränkung der Verarbeitungsoptionen in Verarbeitungsprozessschritten.
- Implementierung von Datenmasken, die Datenfelder unterdrücken, sowie automatischer Sperr- und Löschroutinen, Anwendung von Pseudonymisierungs- und Anonymisierungsverfahren.
- Beschränkung von Möglichkeiten der Kenntnisnahme vorhandener Daten (Anzeigeoptionen, Suchfelder, ...) auf das erforderliche Minimum.

c. Definition, Implementation und Kontrolle eines Löschkonzeptes

Der Auftragsverarbeiter erstellt bei Verarbeitung personenbezogener Daten ein Löschkonzept, das Folgendes beinhaltet:

- Nennung der zu löschenden Datenfelder
- Definition von Löschfristen
- Kontrolle und Nachweis der Löschung
- Verantwortliche Personen

8 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

- Datenschutz-Management;
- Incident-Response-Management;
- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO).
- Auftragskontrolle
- Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DSGVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.

Anhang IV Ergänzende Bedingungen Auftragsverarbeitung (ErgB-AV) für Open Telekom Cloud

Liste Unterauftragsverarbeiter (inkl. Unter-Unterauftragsverarbeiter)

Der Kunde hat gem. Ziffer 2 Klausel 7.7 Buchstabe a die Inanspruchnahme folgender Unterauftragsverarbeiter und Unter-Unterauftragsverarbeiter genehmigt:

1 Genehmigte Unterauftragsverarbeiter

Angaben zu Unterauftragsverarbeitern / Leistungen / Verarbeitungsorte

Gesonderte Genehmigung:
Telekom beabsichtigt, die folgenden Unterauftragsverarbeiter für die folgenden Leistungen / an den folgenden Verarbeitungsorten einzusetzen:

T-Systems International GmbH
60528 Frankfurt am Main, Hahnstraße 43d
Service: Cloud Provider
Verarbeitungsort: Deutschland, Niederlande

2 Genehmigte Unter-Unterauftragsverarbeiter

Eingesetzt von: T-Systems International GmbH

Deutsche Telekom IT GmbH
53227 Bonn, Landgrabenweg 151
Service: MyWorkplace
Verarbeitungsort: Deutschland

T-Systems Multimedia Solutions GmbH
01129 Dresden, Riesaer Straße 5
Service: IT-Service Provider
Verarbeitungsort: Deutschland

T-Systems on site services GmbH
13509 Berlin, Holzhauser Str. 4-8
Service: Cloud Provider
Verarbeitungsort: Deutschland

Die Telekom beabsichtigt weitere Unter-Unterauftragsverarbeiter zu beauftragen. Welche dies konkret sind, ist abrufbar bzw. über GDPR@telekom.de zu erfragen .