Ergänzende Bedingungen Auftragsverarbeitung (ErgB-AV) für Microsoft Online Dienste (Office 365/Dynamics 365/Azure)

Diese AV bezieht sich auf die Leistungen der Telekom, insbesondere auf Produktbereitstellung, Abrechnung und Support. Die Datenhaltung durch Microsoft ist nicht Teil dieser AV.

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. Zur Klarstellung, obwohl der Kunde in dieser Vereinbarung als Verantwortlicher bezeichnet wird, kann der Kunde entweder als Verantwortlicher oder als Auftragsverarbeiter für Daten agieren, die vom Kunden im Auftrag seiner Kunden verarbeitet werden. In diesem Fall wird die Telekom als Unter-Auftragsverarbeiter des Kunden tätig.

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 die konkreten Vertragspartner, 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. Die Standardvertragsklauseln der EU-Kommission dürfen im Klauseltext der Abschnitte I und II nach den zwingenden Vorgaben der EU-Kommission nicht abgeändert werden und sind unverändert im Originaltext wiederzugeben. Abweichungen sind in Abschnitt III Ziffer 3 ausdrücklich dargelegt. Die Regelung der Kontrollrechte in Ziffer 7.6.b wurde durch Abschnitt III Ziffer 3.2 und Ziffer 7.7.a „Unterauftragnehmer“ wurde durch Abschnitt III Ziffer 3.3 weitergehend modifiziert.

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]

Entfällt

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 und sind vom Auftraggeber zu dokumentieren. 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 Kunde 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.
Vom Kunden mit der Kontrolle betraute Personen oder Dritte sind mit Beauftragung nachweislich zur Wahrung der Vertraulichkeit zu verpflichten. Dritte im Sinne dieses Absatzes dürfen keine Vertreter von Wettbewerbern der Telekom sein.

3.3 [Genehmigte Unterauftragsverarbeiter]

Die Parteien vereinbaren zu Klausel 7.7 Buchstabe a) folgendes: Die Liste der vom Kunde genehmigten Unterauftragsverarbeiter (ALLGEMEINE SCHRIFTLICHE GENEHMIGUNG gem. Klausel 7.7 Buchstabe a) findet sich in Anhang IV.
Die Telekom unterrichtet den Kunden grundsätzlich in Textform über beabsichtigte Änderungen von Unterauftragsverarbeitern. Der Kunde kann binnen zwei Wochen nach Mitteilung schriftlich Einwände gegen diese Änderung erheben. Soweit der Kunde in dieser Zeit keine Einwände erhebt, gilt die Änderung als genehmigt. Der Kunde wird nicht unbillig Einwände erheben. Übt der Kunde sein Recht zum Widerspruch aus und setzt Telekom den Unterauftragsverarbeiter dennoch ein, steht dem Kunden das Recht zu, die betroffenen Leistungen ohne Einhaltung einer Kündigungsfrist zum Zeitpunkt des Wirksamwerdens der Änderungen schriftlich zu kündigen.

3.4 [Drittstaatendatentransfer]

Die Parteien sind sich einig, dass der Auftragsverarbeiter die Einhaltung von Kapitel V der Verordnung (EU) 2016/679 im Sinne der Klauseln 7.8 Buchstabe a auch durch andere, nach Art. 46 DSGVO zugelassene geeignete Garantien, z.B. genehmigte verbindliche interne Datenschutzvorschriften nach Art. 47 DSGVO, sicherstellen kann.

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 Änderungen

Sämtliche Änderungen dieser ErgB-AV sowie Nebenabreden bedürfen der Textform (einschließlich der elektronischen Form). Dies gilt auch für das Abbedingen dieser Schriftformklausel selbst.

Die nachfolgenden Regelungen gelten ausschließlich und abschließend für Änderungen der ErgB-AV. Sie gehen sonstigen z.B. in den AGB getroffenen Regelungen zur Änderung von Leistungen, Preisen oder rechtlichen Bedingungen vor. Für die Änderungen von Unterauftragsverarbeitern gilt Klausel 7.7 Buchstabe a Satz 2.

4.1 [Änderungen durch Telekom]

Beabsichtigt Telekom die vereinbarten Leistungen oder die Bedingungen der Auftragsverarbeitung zu ändern (z.B. auf Grund von Behördenentscheidungen, Änderungen in Lieferantenbeziehungen, Gesetzesänderungen), wird sie den Kunden mindestens 4 Wochen vor dem Wirksamwerden der Änderungen in Textform (z.B. per Brief oder E-Mail) informieren und soweit möglich Nachteile für den Kunde vermeiden. Die geänderten Bedingungen werden unter den nachfolgenden Voraussetzungen Vertragsbestandteil:

Bei Änderungen steht dem Kunde das Recht zu, die betroffenen Leistungen ohne Einhaltung einer Kündigungsfrist zum Zeitpunkt des Wirksamwerdens der Änderungen in Textform zu kündigen. Auf Inhalt und Zeitpunkt der Vertragsänderung und das Kündigungsrecht wird der Kunde in der Änderungsmitteilung ausdrücklich hingewiesen. Bei Änderungen ausschließlich zugunsten des Kunden, bei rein administrativen Änderungen ohne negative Auswirkungen oder bei unmittelbar durch Unionsrecht oder innerstaatlich geltendes Recht vorgeschriebenen Änderungen steht dem Kunde kein Kündigungsrecht zu.

4.2 [Änderungen durch den Kunden]

Wünscht der Kunde die Anpassung der Leistung oder der Bedingungen der Auftragsverarbeitung, wird er Telekom informieren und seinen Änderungswunsch begründen. Bei umfangreichen Änderungswünschen wird Telekom dem Kunde ein kostenpflichtiges Angebot zur Prüfung derselben übersenden.

Erklärt sich Telekom mit dem Änderungswunsch des Kunden ggf. gegen zusätzliche Vergütung einverstanden, übersendet Telekom diesem die geänderten Unterlagen. Die Änderungen werden zu dem in den Unterlagen genannten Zeitpunkt wirksam, wenn der Kunde binnen 4 Wochen zustimmt. Soweit Telekom den Änderungswunsch des Kunden ablehnt oder nur unter erheblichen Mehrkosten erbringen kann, wird sie diesen hierüber informieren. Der Kunde ist in diesem Fall berechtigt, die betroffene Leistung ohne Einhaltung einer Frist zu kündigen.

Im Falle der Kündigung ist der Kunde verpflichtet, der Telekom einen Ablösebetrag in Höhe von 50% der bis zum Ende der vereinbarten Mindestlaufzeit noch fälligen monatlichen Entgelte zu zahlen. Der Ablösebetrag entfällt oder ist geringer anzusetzen, wenn der Kunde nachweist, dass der Telekom ein wesentlich geringerer oder überhaupt kein Schaden entstanden ist. Der Ablösebetrag entfällt, sofern der Kunde von seiner Aufsichtsbehörde angewiesen wurde, die Datenübermittlung auszusetzen.

4.3 [Fortgeltung der bisherigen Regelungen]

Bis zur Einigung über den Änderungswunsch des Kunden oder Beendigung der betroffenen Leistungen, gelten die bisherigen Bestimmungen unverändert fort und Telekom ist zur Umsetzung etwaiger Änderungen nicht verpflichtet.

4.4 [Aussetzung der Datenverarbeitung]

Der Kunde ist berechtigt, eine Aussetzung der Datenverarbeitung bis zur Einigung über seinen Änderungswunsch oder die Beendigung der betroffenen Leistungen zu verlangen. Er bleibt verpflichtet die vereinbarte Vergütung zu zahlen.

5 Ergänzende Regelung Berufsgeheimnisträger

Verarbeitet die Telekom Daten, die in den Anwendungsbereich von § 203 StGB fallen (im Folgenden „Geheimnisschutzdaten“) und wirkt insoweit an der beruflichen Tätigkeit eines Berufsgeheimnisträgers mit, gilt Folgendes:

Die Telekom verpflichtet sich, über Geheimnisschutzdaten Stillschweigen zu bewahren und sich nur insoweit Kenntnis von diesen Daten zu verschaffen, wie dies zur Erfüllung der ihr zugewiesenen Aufgaben unbedingt erforderlich ist.
Der Kunde weist die Telekom darauf hin, dass Personen, die an der beruflichen Tätigkeit eines Berufsgeheimnisträgers mitwirken, sich nach § 203 Abs. 4 S. 1 StGB strafbar machen, wenn sie unbefugt ein fremdes Geheimnis offenbaren, das ihnen bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt geworden ist.
Zudem macht sich eine mitwirkende Person nach § 203 Abs. 4 S. 2 StGB strafbar, sollte sie sich einer weiteren mitwirkenden Person bedienen, die ihrerseits unbefugt ein fremdes, ihr bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenes Geheimnis offenbart, und nicht dafür Sorge getragen hat, dass diese zur Geheimhaltung verpflichtet wurde.

Die Telekom wird diejenigen ihrer Mitarbeiter, die bestimmungsgemäß mit Geheimnisschutzdaten des Berufsgeheimnisträgers in Berührung kommen oder bei denen dies nicht auszuschließen ist, zur Vertraulichkeit hinsichtlich der Geheimnisschutzdaten verpflichten und über die mögliche Strafbarkeit nach § 203 Abs. 4 StGB belehren.

Die Telekom ist berechtigt, Unterauftragsverarbeiter zur Vertragserfüllung heranzuziehen. Im Ausland dürfen Unterauftragsverarbeiter zur Vertragserfüllung nur dann herangezogen werden, wenn der dort bestehende Schutz der Geheimnisse dem Schutz im Inland vergleichbar ist, es sei denn, dass der Schutz der Geheimnisse dies nicht gebietet.
Die Telekom wird etwaige Unterauftragsverarbeiter sorgfältig auswählen und diese, soweit sie im Rahmen ihrer Tätigkeit Kenntnis von fremden Geheimnissen im Sinne

dieser Vereinbarung erlangen könnten, schriftlich zur Verschwiegenheit verpflichten und über die Folgen einer Pflichtverletzung belehren.

Die Telekom wird ferner etwaige Unterauftragsverarbeiter dazu verpflichten, sämtliche von diesen eingesetzten Personen und etwaige weitere Unterauftragsverarbeiter, die bestimmungsgemäß mit Geheimnisschutzdaten in Berührung kommen oder bei denen dies nicht auszuschließen ist, nach den zuvor genannten Grundsätzen zur Verschwiegenheit zu verpflichten und über die Folgen einer Pflichtverletzung zu belehren. Diese Verpflichtung gilt für sämtliche weitere Unterbeauftragungen (Sub-Unterauftragsverarbeiter).

Die Telekom wird darauf hingewiesen, dass die sich in ihrem Gewahrsam befindenden Geheimnisschutzdaten dem Beschlagnahmeverbot gemäß § 97 Abs. 2 StPO unterliegen. Die Daten werden nicht freiwillig herausgegeben. Im Falle einer Beschlagnahme wird die Telekom diesem widersprechen und unverzüglich den Kunden benachrichtigen, sofern dies rechtlich zulässig ist.

6 Sonstiges

6.1 [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.

6.2 [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.

6.3 [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.

6.4 [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 Microsoft Online Dienste (Office 365/Dynamics 365/Azure)

Liste der Parteien

Die Vertragsparteien sind die der AGB.

Anhang II Ergänzende Bedingungen Auftragsverarbeitung (ErgB-AV) für Microsoft Online Dienste (Office 365/Dynamics 365/Azure)

Beschreibung der Verarbeitung

Eine AVV mit Microsoft gem. Artikel 28 DSGVO wird bei der Produkt-Aktivierung oder der Erneuerung der Produktlizenz abgeschlossen und ist Teil der Software-Nutzungsbestimmungen des Herstellers (Microsoft Customer Agreement MCA, Online Service Terms und die eigentlichen Licensing Terms zum jeweiligen Produkt).

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
☒ Interessenten des Verantwortlichen
☒ Lieferanten des Verantwortlichen
☒ Mitarbeiter von Fremdfirmen

c. Kategorie personenbezogener Daten:

☒ Stammdaten der Kunden des Verantwortlichen
☒ Kontaktdaten der Kunden des Verantwortlichen
☒ Stammdaten der Mitarbeiter des Verantwortlichen
☒ Kontaktdaten der Mitarbeiter des Verantwortlichen
☒ alle sonstigen personenbezogene Daten, die der Kunde im Rahmen der Leistung im Auftrag verarbeiten lässt

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:

☒ Übermittlung durch den Kunden über gesicherte Verbindung:
https:// und VPN-Verbindung zu den Microsoft Online-Diensten.

☒ Zugriff über einen Secure Data Room:
Bei Batch-Import oder Batch Export von Kundendaten des Kunden in und aus den Microsoft Online Diensten

☒ verschlüsselte Übermittlung mittels:
Standard-SQL Server-Zellenebenen-Verschlüsselung oder HTTPS TLS/SSL (https://learn.microsoft.com/de-de/microsoft-365/compliance/office-365-encryption-in-microsoft-dynamics-365?view=o365-worldwide)

und/oder:

☒ Leistungen der Wartung, Fernwartung oder Fehleranalyse:
Im Einrichtungsfall oder Servicefall: Übermittlung über eine sichere Verbindung, verschlüsselte E-Mail für den Zugang zur Dynamics 365 Plattform und deren Online-Dienste Anwendungen, zur Datenerhebung über eine spezielle Import-Schnittstelle (z. B. per CRM-Import-

Datensatz des Kunden oder manuellen Eintrag durch den Kunden oder durch den Kundensupport selbst).

Die Bereitstellung der Daten an Telekom erfolgt, wie in § 5 Absatz 5.1 e) und h) „Mitwirkungs-leistungen des Kunden“ sowie des § 16 „Datenschutz“ der AGB IT-Leistungen / geregelt.

☒ Software-Prüfung/Wartung per Fernzugriff für folgend(e) Softwareprodukt(e):

Microsoft Dynamics 365 Online-Dienste

Es werden folgende ergänzende Vereinbarungen getroffen:

☒ Prüfungs- und Wartungsarbeiten an Arbeitsplatzsystemen des Kunden werden nach Freigabe durch den jeweiligen Berechtigten / betroffenen Mitarbeiter des Kunden getroffen.

☒ Es erfolgt eine gesonderte Mitteilung (per Mail/telefonisch/schriftlich) über anstehende Prüfungs- und Wartungsarbeiten durch die Telekom an den Kunden vor Beginn der Arbeiten.

☒ Auf Anforderung des Kunden informiert Telekom, welche Arbeiten, wann und von welchen Mitarbeitern der Telekom durchgeführt werden. Telekom informiert wie diese Personen sich dem Kunden gegenüber identifizieren und authentifizieren werden.

☒ Über notwendige Datensicherungsmaßnahmen in den jeweiligen Verantwortungsbereichen der Telekom/des Kunden werden sich die Vertragsparteien bei Bedarf verständigen.

☒ Telekom wird von den ihr eingeräumten Zugriffsrechten, auch in zeitlicher Hinsicht, so Gebrauch machen, als dies für die ordnungsgemäße Durchführung der beauftragten Wartungs- und Prüfungsarbeiten notwendig ist.

3 Dauer der Verarbeitung

☒ Erforderlichkeit zur Leistungserbringung

☒ Gesetzliche Aufbewahrungsfristen

☒ Gesetzliche Löschfristen

4 Zweck der Verarbeitung

Die Leistungen werden detailliert in den Mitwirkungs-leistungen des Kunden im Abschn. 5 und im Abschnitt im Abschnitt 15 „Datenschutz“ der Allgemeinen Geschäfts-bedingungen für IT-Leistungen (mitgeltendes Dokument) beschrieben.

5 Verarbeitungsorte in Drittländern

Sofern eine Auftragsverarbeitung in einem Drittland durchgeführt wird, ist dies in Anhang IV Ergänzende Bedingungen Auftragsverarbeitung (ErgB-AV) aufgeführt.

6 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 Microsoft Online Dienste (Office 365/Dynamics 365/Azure)

Technische und organisatorische Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung

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

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 nach Maßgabe des Herstellers/Lieferanten 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 für seinen Verantwortungsbereich 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.
-

f. Erstellung eines Notfallkonzepts zur Wiederherstellung einer Verarbeitungstätigkeit

Der Auftragsverarbeiter hat in seinem Verantwortungsbereich 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)

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 für seinen Verantwortungsbereich 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 für seinen Verantwortungsbereich Prozesse definiert, umgesetzt und kommuniziert, die die Aktualität der personenbezogenen Daten unterstützen und den folgenden Anforderungen unterliegen:
- Anfragen zu Berichtigungen, Änderungen und Löschungen 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)

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 definiert, die die notwendigen Sicherheitsperimeter vorgegeben und umsetzen.
- 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 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 umgesetzt.
- Bei Speicherung personenbezogener Daten auf mobilen Datenträgern werden diese wirksam verschlüsselt.
- 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. 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

Authentisierungsmerkmale. 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

Der Auftragsverarbeiter wird im Zusammenhang mit der hier vereinbarten Verarbeitung personenbezogener Daten die Vertraulichkeit nach der DSGVO, nach § 3 TDDDG wahren und die zur Verarbeitung der personenbezogenen Daten befugten Personen entsprechend verpflichten und sensibilisieren. Im Anwendungsbereich der Verarbeitung von Sozialdaten wird der Auftragsverarbeiter 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

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.

5 Transparenz

a. Verfahrensverzeichnis

Der Art. 30 DSGVO wurde beim Auftragsverarbeiter umgesetzt.

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 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

- **Prozessimplementation zur Umsetzung der Betroffenenrechte**

Der Auftragsverarbeiter hat Maßnahmen zur Wahrung von Betroffenenrechten bei der Verarbeitung implementiert. Systeme, Software und Prozesse wurden so implementiert, dass differenzierte Einwilligungs-, Rücknahme- sowie Widerspruchs-möglichkeiten möglich sind.

.

7 Datenminimierung

Der Auftragsverarbeiter verarbeitet nur personenbezogene Daten, die für den Verarbeitungszweck unbedingt erforderlich sind.

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;

- Auftragskontrolle
- Keine Auftragsverarbeitung 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 Microsoft Online Dienste (Office 365/Dynamics 365/Azure)

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

Deutsche Telekom IT GmbH
Landgrabenweg 149, 53227 Bonn
Leistung: Plattformbetreiber Telekom Cloud Marketplace
Verarbeitungsort: Deutschland

T-Systems International GmbH
Hahnstr. 43d, 60528 Frankfurt am Main
Leistung: Hosting Telekom Cloud Marketplace
Verarbeitungsort: Deutschland

Deutsche Telekom Service GmbH
Friedrich-Ebert-Allee 71-77, 53113 Bonn
Leistungen: 1st und 2nd Level Support
Verarbeitungsort: Deutschland

Deutsche Telekom Individual Solutions & Products GmbH
Friedrich-Ebert-Allee 71-77, D-53113 Bonn
Leistungen: 1st und 2nd Level Support
Verarbeitungsort: Deutschland

Deutsche Telekom Geschäftskunden GmbH
Landgrabenweg 149, 53227 Bonn
Leistung: Vertrieb Geschäftskunden
Verarbeitungsort: Deutschland

Deutsche Telekom Privatkunden GmbH
Landgrabenweg 149, 53227 Bonn
Leistung: Vertrieb Geschäftskunden
Verarbeitungsort: Deutschland

Deutsche Telekom IT & Telecommunications Slovakia s.r.o.
Moldavská cesta 8B, 040 11 Košice, Slovakia
Leistung: Dienstleistungen, Incident Management
Verarbeitungsort: Slowakei

Deutsche Telekom MMS GmbH
Riesaer Straße 5, 01129 Dresden
Leistung: 1st und 2nd Level Support, Dienstleistungen, Service
Verarbeitungsort: Deutschland

LTIMindtree Limited
Eurocentrum Complex,
Gamma Building - 09th Floor
Al. Jerozolimskie 134
02-305 Warsaw, Poland
Leistung: 1st und 2nd Level Support
Verarbeitungsort: Polen

ORBIT Gesellschaft für Applikations- und Informationssysteme mbH
Mildred-Scheel-Str. 1, 53175 Bonn
Leistung: 1st und 2nd Level Support, Dienstleistungen, Service
Verarbeitungsort: Deutschland

2 Genehmigte Unter-Unterauftragsverarbeiter

Deutsche Telekom TSI Hungary Kft.
Könyves Kálmán körút 36.
1097 Budapest, Ungarn
Leistung: 1st und 2nd Level Support
Verarbeitungsort: Ungarn
Eingesetzt durch: Deutsche Telekom MMS GmbH

Bitte beachten Sie, dass ggf. vorhandene Sub-Unter-auftragsverarbeiter der Microsoft, sowie Mircosoft selbst nicht Teil dieser ergänzenden Bedingungen Auftragsverarbeitung zwischen Telekom und Kunde sind.