



Ergänzende Bedingungen Auftragsverarbeitung (ErgB-AV) für Business GPT for Websites

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 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 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 („Klauseln“)

ABSCHNITT I

Klausel 1 [Zweck und Anwendungsbereich]

a) Mit diesen Standardvertragsklauseln (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 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]
n.a.

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 personenbezogener Daten betrifft, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, oder die genetische Daten oder biometrische Daten zum Zweck der

eindeutigen Identifizierung einer natürlichen Person, Daten über die Gesundheit, das Sexualleben oder die sexuelle Ausrichtung einer Person oder Daten über strafrechtliche Verurteilungen und Straftaten enthalten (im Folgenden „sensible Daten“), wendet der Auftragsverarbeiter spezielle Beschränkungen und/oder zusätzlichen Garantien an.

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

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 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 Kunde darüber hinaus Art und Umfang der Datenverarbeitung durch die Art der Nutzung des Produktes und durch Auswahl etwaig möglicher Varianten bestimmen. Weisungen des Kunden können im vereinbarten Rahmen des Standardproduktes erfolgen. Bei weiteren Weisungen des Kunden, 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 [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.

3.5 [Drittstaatentransfer]

Die Parteien sind sich einig, dass Telekom 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, gewährleisten kann.

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 und Ziffer 3.3.

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 Sonstiges

5.1 [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.

5.2 [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.

5.3 [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.

5.4 [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.

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 Sonstiges

5.1 [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.

5.2 [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.

5.3 [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.

5.4 [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 Business GPT for Websites

Liste der Parteien

Die Vertragsparteien sind die der AGB.

Anhang II Ergänzende Bedingungen Auftragsverarbeitung (ErgB-AV) für Business GPT for Websites

Beschreibung der Verarbeitung

1 Einzelheiten der Datenverarbeitung

a. Art der Verarbeitung

- ☒ SaaS (Software as a Service)

b. Kategorien betroffener Personen

- ☒ Kunden des Verantwortlichen
☒ Mitarbeiter des Verantwortlichen
☒ Partner des Verantwortlichen
☒ Andere Personen des Verantwortlichen

c. Kategorie personenbezogener Daten:

- ☒ Daten zu Referenzkunden des Verantwortlichen
☒ Kontaktdaten der Mitarbeiter des Verantwortlichen
☒ Login-Daten (der Admins), dazu gehören:
E-Mail Adresse, Name
Authentifizierungs- und Autorisierungsdaten (Access-/ID-/Refresh-Token; Session-IDs; pseudonyme Nutzer-IDs wie oid, sub; Rollen und Gruppenmitgliedschaften)
Technische Nutzungsdaten (IP-Adresse, zeitliche Metadaten wie iat/exp/expires_at; anfragebezogene Protokoll-/Geräteinformationen)
☒ alle sonstigen personenbezogene Daten, die der Kunde im Rahmen der Leistung im Auftrag verarbeiten lässt
☒ Abrechnungsdaten, bereitgestellt durch die Abrechnungssysteme des Marketplace
☒ Webseiteninhalte zur Verarbeitung durch die bereitgestellte SaaS API-Anwendung

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):

Für die Tätigkeiten des Auftragsverarbeiters ist die Verarbeitung sensibler Daten nicht vorgesehen. Kenntnis und Zugriff derer kann jedoch, aufgrund der freiwilligen Angaben der Nutzer*innen, nicht ausgeschlossen werden. Die Verantwortung für die Eingabe und Verarbeitung sensibler Daten in Business GPT for Websites obliegt allein dem Kunden.

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:
Die Daten werden über SSL gesicherte Übertragung an Webservice APIs übermittelt.
☒ verschlüsselte Übermittlung mittels: Web-GUI und API über TLS

2 Zweck(e) der Verarbeitung

Telekom stellt dem Verantwortlichen (Kunden) Webservices zur Datenverarbeitung bereit. Der Zugriff erfolgt über den REST-Webschnittstellen bereitgestellt durch den genutzten Marketplace.

3 Dauer der Verarbeitung

- ☒ Erforderlichkeit zur Leistungserbringung
- ☒ Gesetzliche Aufbewahrungsfristen

Die Speicherung der personenbezogenen Daten erfolgt ausschließlich für die Dauer von 30 Tagen nach Erhebung. Nach Ablauf dieses Zeitraums werden die Daten automatisch und unwiderruflich gelöscht, sofern keine anderweitigen gesetzlichen Aufbewahrungspflichten bestehen.

4 Verarbeitungsorte in Drittländern

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

5 Nachweis durch die Telekom

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

- ☒ aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z. B. Wirtschaftsprüfer, Revision);
- ☒ eine geeignete Zertifizierung (außer Zertifikat gem. Art. 42 DSGVO)
- ☒ Eigenerklärung des Auftragsverarbeiters.

<https://geschaeftskunden.telekom.de/business/hilfe-und-service/zertifikate>

<https://public.t-cloud.com/leistungsbeschreibung>

Anhang III Ergänzende Bedingungen Auftragsverarbeitung (ErgB-AV) für Business GPT for Websites

Technische und organisatorische Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung

Für die beauftragte Erhebung und/ oder Verarbeitung von personenbezogenen Daten werden folgende Maßnahmen vereinbart:

a) Verfügbarkeit

▪ **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.

▪ **Schutz der IT-Systeme und Netze vor äußeren Einflüssen**

Der Auftragsverarbeiter hat Regelungen definiert um IT-Systeme, Netze und Komponenten vor unbefugtem Zugriff, unbefugter Modifikation, Verlust oder Zerstörung zu schützen. 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.

▪ **Belastbarkeit der Systeme und Dienste**

Informationsverarbeitende Systeme und Dienste sind vor Schadsoftware geschützt und die Belastbarkeit durch eine Systemhärtung erhöht.

▪ **Backupkonzept**

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.

▪ **Notfallkonzept zur Wiederherstellung einer Verarbeitungstätigkeit**

Der Auftragsverarbeiter hat ein Notfallkonzept zur Wiederherstellung nach einer Störung der Datenverarbeitung implementiert.

b) Integrität

▪ **Definition, Anwendung und Kontrolle des Sollverhaltens von Prozessen**

Der Auftragsverarbeiter hat Prozesse zur Umsetzung des Datenschutzes und der Informationssicherheit festgelegt. Ziel der Vorgaben ist es, die Verarbeitung von personenbezogenen Daten so umzusetzen, dass ein definiertes Sollverhalten der Prozesse gewährleistet ist. Die Vorgaben werden regelmäßig auf Wirksamkeit, Aktualität und Regelkonformität hin geprüft.

▪ **Berechtigungskonzept**

Der Auftragsverarbeiter nutzt Berechtigungskonzepte die verbindlich vorgeben, wer wann auf welche Systeme, Datenbanken oder Netze Zugriff hat.

▪ **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.

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.

▪ **Kryptokonzept**

Der Auftragsverarbeiter hat für seinen Verantwortungsbereich den Gebrauch kryptografischer Maßnahmen zum Schutz personenbezogener Daten durch Vorgaben definiert. Diese Vorgaben regeln:

- die Nutzung des angewandten Stands der Technik kryptografischer Verfahren,
- die Verwaltung und Anwendung kryptografischer Schlüssel,
- den Schutz kryptografischer Schlüssel über deren gesamten Lebenszyklus (die Erzeugung, Speicherung, Anwendung und Vernichtung).

▪ **Prozesse zur Aufrechterhaltung der Aktualität von Daten**

Der Auftragsverarbeiter hat Prozesse definiert, welche die Aktualität der Daten durch folgende Maßnahmen unterstützen:

- Anfragen zu Berichtigungen, Änderungen und Löschungen erfolgen zeitnah und über alle gespeicherten Datensätze.
- Speicherdauer und Löschfristen sind gemäß den gesetzlichen oder vertraglichen Vorgaben festgelegt und werden umgesetzt.

c) **Vertraulichkeit**

▪ **Verpflichtung der Mitarbeiter**

Die Mitarbeiter wurden auf Vertraulichkeit sowie das Fernmeldegeheimnis verpflichtet.

▪ **Festlegung und Kontrolle der Nutzung zugelassener Ressourcen und Kommunikationskanäle**

Der Auftragsverarbeiter implementiert Maßnahmen so, dass die für die Verarbeitung personenbezogener Daten genutzten Ressourcen und Kommunikationskanäle festgelegt sind und deren Nutzung kontrolliert wird:

- Es sind geeignete Zutrittssteuervorgaben definiert und angewendet, so dass nur berechtigte Personen Zutritt zu Bereichen erhalten, in denen die Verarbeitung erfolgt.
- Eine Zugangssteuerungsrichtlinie ist auf Grundlage der Datenschutzerfordernungen in der Organisation erstellt und umgesetzt. Diese Richtlinie regelt den Zugang zu personenbezogenen Daten auf den zur Aufgabenerfüllung minimalen Umfang (Need-to-know-Prinzip).
- Es existieren Richtlinien, Sicherheitsverfahren und Steuerungsmaßnahmen, um die Übertragung und den Transport von Informationen angemessen zu schützen.

▪ **Sichere Authentisierungsverfahren**

Der Zugang zu Systemen und Anwendungen wird durch ein angemessenes sicheres Authentisierungsverfahren geschützt.

d) **Nichtverkettung**

▪ **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.

▪ **Maßnahmen zur Sicherstellung der Zweckbindung**

Folgende Maßnahmen wurden getroffen, um eine Verkettung von Datensätzen mit unterschiedlicher Zweckbindung zu vermeiden:

- Trennung nach Organisations-/Abteilungsgrenzen
- Trennung der Verarbeitung nach Mandanten

e) **Transparenz**

▪ **Verfahrensverzeichnis**

Der Art. 30 Abs.2 DSGVO wurde beim Auftragsverarbeiter umgesetzt.

▪ **Dokumentation der Datenverarbeitung**

Der Verarbeitungsprozess ist so dokumentiert, dass nachvollziehbar ist, wie die Verarbeitung personenbezogener Daten erfolgt.

▪ **Protokollierung der Datenverarbeitung**

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

▪ **Gewährleistung der Auskunftspflichten**

Der Auftragsverarbeiter hat einen Prozess implementiert, der das Auskunftsrecht eines Betroffenen gem. Art. 15 DSGVO unterstützt.

f) **Intervenierbarkeit**

▪ **Prozessimplementierung zur Umsetzung der Betroffenenrechte**

Der Auftragsverarbeiter hat unterstützende Maßnahmen zur Wahrung von Betroffenenrechten bei der Verarbeitung implementiert. Systeme, Software und Prozesse wurden so implementiert, dass möglichst differenzierte Einwilligungs-, Rücknahme- sowie Widerspruchsmöglichkeiten umgesetzt werden können.

g) **Datenminimierung**

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

- Pseudonymisierungs- und Anonymisierungsverfahren werden angewendet.
- Möglichkeiten der Kenntnisnahme vorhandener Daten (Anzeigeoptionen, Suchfelder, ...) wurden auf das erforderliche Minimum beschränkt.

h) **Besondere Maßnahme zum Schutz sensibler Daten**

Für die Tätigkeiten des Auftragsverarbeiters ist die Verarbeitung sensibler Daten nicht vorgesehen. Kenntnis und Zugriff derer kann jedoch, aufgrund der freiwilligen Angaben der Nutzer*innen, nicht ausgeschlossen werden. In den Nutzungsbedingungen wird darauf hingewiesen, wie mit sensiblen Daten umgegangen werden soll. Den Nutzungsbedingungen muss vor Nutzung des SaaS zugestimmt werden.

Anhang IV Ergänzende Bedingungen Auftragsverarbeitung (ErgB-AV) für Business GPT for Websites

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 MMS GmbH,
Riesaer Straße 5, 01129 Dresden
Leistungen: Bereitstellung der SaaS-Lösung Business GPT for Websites, basierend auf skalierender Cloudarchitektur
Verarbeitungsort: Deutschland

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

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

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

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

Deutsche Telekom Geschäftskunden 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 TCMP
Verarbeitungsort: Slowakei

2 Genehmigte Unter-Unterauftragsverarbeiter

T-Systems International GmbH,
Friedrich-Ebert-Allee 140, 53113 Bonn
Leistung: Bereitstellung der Infrastruktur von T Cloud Public.
Weitere Verarbeiter können abgefragt werden unter service@open-telekom-cloud.com
Verarbeitungsort: Deutschland
Eingesetzt von: Deutsche Telekom MMS GmbH

Anhang V Ergänzende Bedingungen Auftragsverarbeitung (ErgB-AV) für Business GPT for Websites

Besondere produktspezifische Bedingungen zur Verarbeitung personenbezogener Daten mittels Business GPT for Websites

In diesem Dokument informieren wir darüber, was auf Seiten des Kunden für die Nutzung von Business GPT for Websites hinsichtlich der Verwendung personenbezogener Daten beachtet werden sollte und welche Verpflichtungen in der Eigenverantwortung des Kunden verbleiben.

1 Wichtige allgemeine Hinweise

Business GPT for Websites ist ein digitaler Dienst (KI-basierter Chat- und Dokumentenverarbeitungsdienst), der von Unternehmen und Organisationen („Kunden“) genutzt werden kann. Die Nutzung kann Beschäftigte des Kunden und ggf. weitere vom Kunden berechnigte Nutzer betreffen.

Die Anwendung Business GPT for Websites wird auf der T Cloud Public der T-Systems International GmbH durch die Deutsche Telekom MMS GmbH (MMS) in Deutschland betrieben.

Wir weisen darauf hin, dass es sich hierbei um ein KI-System handelt, das große Sprachmodelle (LLM) und Funktionen nutzt, die aus der T Cloud Public bereitgestellt werden.

Der Kunde entscheidet eigenverantwortlich, ob und welche personenbezogenen Daten sowie vertraulichen Informationen (Inhaltsdaten) in seinem Unternehmen bzw. seiner Organisation in die LLM-Services eingebracht werden dürfen und stellt seinen Nutzern die Informationen z. B. anhand von unternehmensspezifischen Nutzungsbedingungen eigenständig zur Verfügung.

2 Inhalte im Chat und in den Datenspeichern (RAG / Dokumentenchat)

Business GPT for Websites ist für die Verarbeitung personenbezogener Daten nicht vorgesehen. Eine diesbezügliche Prüfung erfolgt aber seitens der Telekom Deutschland GmbH nicht. Die Verantwortung hinsichtlich der datenschutzkonformen Verarbeitung obliegt dem Kunden.

In der aktuellen Version werden Chatverläufe für die Dauer der Session vorgehalten.

Nach Ablauf der Session werden Chatverläufe automatisch gelöscht.

3 Function Calls und Aufrufe externer Systeme

Business GPT for Websites kann so konfiguriert werden, dass das zugrundeliegende Sprachmodell über „Function Calls“ (Tool Calls) externe Systeme des Kunden aufruft. Dabei können Daten (z. B. Status, Ticket, Stamm oder Prozessdaten) aus diesen Systemen abgerufen und in Antworten des Modells einbezogen werden. Durch Function Calls erfolgt keine zusätzliche Speicherung dieser Daten in Business GPT for Websites über die Session hinaus. Eine Speicherung findet nur in den vom Kunden separat

eingesetzten Speichern (z. B. Chat oder Datenspeicher/RAG) statt, sofern diese unabhängig von den Function Calls konfiguriert wurden.

4 Einsatz spezialisierter KI-Dienste

Für die eigentliche KI-Funktionalität von Business GPT for Websites (z. B. Generierung von Antworten, Zusammenfassungen, Verarbeitung von Prompts und RAG-Kontexten) nutzen wir Dienste spezialisierter KI-Anbieter, die über den T Cloud Serving Service bereitgestellt und in Deutschland gehostet werden: <https://marketplace.otc.t-systems.com/product-offering/g2chzNTJzN5HTInwEkE5z>

4.1 Welche Daten werden an die KI-Dienste übermittelt?

Je nach Nutzung des Dienstes (Chat mit LLM-Wissen, Chat mit Dokumenten/RAG-Inhalten) können insbesondere folgende Daten verarbeitet und an die KI-Dienste übermittelt werden:

Inhalte der Chat-Anfragen („Prompts“), relevante Inhalte aus hochgeladenen Dokumenten und Datenspeichern (z. B. RAG-Chunks), aus angebundenen externen Systemen (externe Datenquellen) in den Prompt einbezogene Inhalte, technische Metadaten, soweit erforderlich (z. B. Request-IDs, Zeitstempel, Fehlermeldungen). Sofern die o. g. Inhaltsdaten auch personenbezogene Daten enthalten, fällt dies in den Verantwortungsbereich des jeweiligen Kunden, da die Telekom Deutschland GmbH keine Kenntnis über die konkreten Inhalte hat.

4.2 Zwecke der Verarbeitung durch die KI-Dienste

- Verarbeitung der Anfragen zur Erzeugung der jeweils gewünschten KI-Ergebnisse, insbesondere:
- Beantwortung von Fragen,
- Zusammenfassung, Strukturierung oder Transformation von Texten,
- Nutzung von Kontext aus RAG-Speichern oder angebundenen Systemen,
- Technische Bereitstellung des KI-Dienstes (z. B. Skalierung, Lastverteilung, Stabilität).

Die Nutzung der Daten durch die KI-Dienste ist vertraglich auf diese Zwecke beschränkt.

5 Abgrenzung der Verantwortlichkeit für die Datenverarbeitung

5.1 Telekom Deutschland GmbH

Für den Schutz der Daten, die im Rahmen der Vertragsanbahnung bzw. Kundenkommunikation und zu

Supportzwecken verwendet werden, ist die Telekom Deutschland GmbH verantwortlich.

5.2 Kunde

Für den rechtmäßigen Einsatz von Business GPT for Websites (inkl. der Frage, welche Daten im Chat und in den Dokumentenspeichern verarbeitet werden) ist grundsätzlich der Kunde Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO.

Die Telekom Deutschland GmbH handelt bei der Bereitstellung von Business GPT for Websites als Auftragsverarbeiter des Kunden gemäß Art. 4 Nr. 8 i. V. m. Art. 28 DSGVO.

6 Verpflichtungen des Kunden

Der Kunde ist insbesondere verantwortlich,

- die Rechtsgrundlage für die Nutzung von Business GPT for Websites einschließlich der Einbindung von Cloud und KI-Diensten in seinem Verantwortungsbereich zu prüfen und festzulegen (z. B. Art. 6 Abs. 1 lit. b oder lit. f DSGVO, ggf. lit. a bei Einwilligung),
- die Zweckmäßigkeit der Verarbeitung sicherzustellen
 - Festlegung der Verarbeitungszwecke,
 - Prüfung der Zweckbindung und Zweckkompatibilität (Art. 5 Abs. 1 lit. b, Art.

6 Abs. 4 DSGVO) bevor Daten in Business GPT for Websites genutzt werden

- Prüfung der Kompatibilität von neuen Zwecken mit ursprünglichen Zwecken (Art. 6 Abs. 4 DSGVO),
- Information der Betroffenen über etwaige Zweckänderungen mittels eigener Datenschutzhinweise,
- Speicherdauer und Löschfristen für Inhalte (Chat-Verläufe) festzulegen und diese im eigenen Verantwortungsbereich umzusetzen. Wir stellen dem Kunden technische Funktionen zur Verfügung, mit denen er diese Pflichten erfüllen kann (z. B. Einstellbarkeit der Speicherdauer, Löschfunktionen),
- Eigene Datenschutzhinweise gemäß Art. 13 DSGVO zur Nutzung von Business GPT for Websites bereitzustellen, inklusive Informationen zum Einsatz von Cloud und KI-Diensten sowie mögliche Datenübermittlungen in Drittländer.
- Für Datenschutzfragen rund um die Nutzung von Business GPT for Websites und verwendete Inhalte muss der Kunde einen eigenen Ansprechpartner benennen und in seinen eigenen Datenschutzhinweisen für die Nutzer aufführen.