



Pflichtinformationen nach Art. 26, 28, 29 Data Act

WICHTIGE INFORMATIONEN FÜR BUSINESS GPT (NACH ART. 26, 28 UND 29 ABS. 4, 5 DATA ACT)

Gemäß der Verordnung (EU) 2023/2854 des Europäischen Parlaments und des Europäischen Rates vom 13. Dezember 2023 über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung sowie zur Änderung der Verordnung (EU) 2017/2394 und der Richtlinie (EU) 2020/1828 („**Data Act**“) können Kunden von Business GPT zu anderen vergleichbaren Diensten wechseln und ihre Kundeninhalte aus den Business GPT exportieren. Die nachfolgenden Informationen unterstützen unseren Kunden im Falle eines solchen Wechsels oder Datenexports. Daneben steht es dem Kunden anstelle eines Wechsels auch frei, seine Inhalte löschen zu lassen.

VERFÜGBARE WECHSEL- UND ÜBERTRAGUNGSMETHODEN (NACH ART. 26 LIT. A DATA ACT)

- Wir leisten Ihnen und von Ihnen autorisierten Dritten angemessene Unterstützung bei Ihrem Wechsel.
- Um Ihre Kundeninhalte für den Wechsel zu einem anderen Anbieter oder für Ihre eigene IKT-Infrastruktur zu exportieren, stellen wir Ihnen verschiedene Verfahren zur Verfügung:
 - Download aus der Browseranwendung
 - Sie können Ihre **hochgeladenen Dokumente** aus der Browseranwendung von Business GPT herunterladen.
 - Vorgehensweise:
 - Loggen Sie sich unter Ihrem kundenindividuellen Zugang (URL Ihrer Business GPT Umgebung) mit Ihren Business GPT-Zugangsdaten ein.
 - Navigieren Sie in den **Administrationsbereich** und dort in die **Dokumentenübersicht**.
 - Wählen Sie die gewünschten Dokumente einzeln aus und klicken Sie auf „**Herunterladen**“.

Hinweis: Derzeit ist ein **mandantenweiter Download aller Dokumente oder anderer Inhalte über das Webfrontend nicht verfügbar**.

- Export über Support
 - Ein **mandantenweiter Export** aller **Chatverläufe, Assistenten-Konfigurationen, Prompts/Prompt-Bibliothek, Metadaten** und hochgeladener Dokumente kann **über unseren Support angefordert** werden.
 - Die Daten werden in einem **strukturierten, maschinenlesbaren Format** bereitgestellt (z. B. JSON, CSV oder SQL).
 - Enthaltene Inhalte:



- Hochgeladene Dokumente
- Chatverläufe
- Assistenten-Konfigurationen
- Prompt Bibliothek

Nicht exportierbar: technisch abgeleitete Daten wie **Embeddings, interne Indizes oder temporäre Systemdaten**, da diese nur der internen Funktionalität dienen.

- Sofern Sie für Ihre Ausstiegsstrategie für den Cloud-Dienst und den Wechsel weitere Unterstützung benötigen, über die Sie nicht bereits anderweitig verfügen, können Sie sich an unseren Kundendienst wenden:
 - Support Rufnummer: 0800 – 330 44 44
 - Erreichbarkeit: Mo - Fr 08:00 – 20:00 Uhr, Sa 08:00 – 16:00 Uhr
 - Support E-Mail-Adresse: support@cloud.telekom.de

VERFÜGBARE WECHSEL- UND ÜBERTRAGUNGSFORMATE (NACH ART. 26 LIT. A DATA ACT)

Kundenbereitgestellte Inhalte (einschließlich hochgeladener Dokumente) werden in dem jeweiligen **Ursprungsformat** (z. B. PDF, DOCX) bereitgestellt.

Weitere vom Kunden erzeugte oder veranlasste Daten, insbesondere **Chatverläufe und zugehörige Metadaten**, werden in **strukturierten, gängigen und maschinenlesbaren Formaten** (z. B. **JSON oder CSV**) zur Verfügung gestellt.

Technisch abgeleitete interne Datenstrukturen (z. B. Embeddings oder Indizes) sind nicht Bestandteil des Exports.

EINSCHRÄNKUNGEN UND TECHNISCHE BESCHRÄNKUNGEN (NACH ART. 26 LIT. A DATA ACT)

Bei einem Wechsel des Datenverarbeitungsdienstes oder beim Export von Kundeninhalten können folgende **technisch bedingte Einschränkungen** bestehen:

- **Integritäts- und Vollständigkeitseinschränkungen**, sofern Daten aus unterschiedlichen Quellen stammen oder sich während des Exportvorgangs ändern.
- **Software- und Formatinkompatibilitäten** bei der Weiterverwendung der exportierten Daten in Systemen Dritter.
- **Nichtverfügbarkeit von technisch abgeleiteten internen Datenstrukturen** (z. B. Embeddings, Indizes oder Vektorrepräsentationen).
- **Bandbreiten- und Übertragungsbeschränkungen**, insbesondere bei großen Datenmengen.
- **Größen- und Volumenbeschränkungen**, z. B. bei der gleichzeitigen Übertragung sehr großer Datenbestände.
- **Zeitliche Beschränkungen**, etwa durch erforderliche Wartungs- oder Übertragungsfenster.
- **Sicherheits- und Verschlüsselungsanforderungen**, die den Export oder die Bereitstellung beeinflussen können.



- **Erforderliche manuelle Schritte**, insbesondere bei der Anforderung oder Bereitstellung mandantenweiter Exporte über den Support.

Diese Einschränkungen dienen ausschließlich der technischen Sicherheit und Stabilität des Dienstes und stellen **keine unangemessenen Hindernisse** für einen Anbieterwechsel dar.

ONLINE-REGISTER (NACH ART. 26 LIT. B DATA ACT)

Kunden erhalten unter [Governance - Business GPT - Online Hilfe](#) weitere Einzelheiten zu allen Datenstrukturen und Datenformaten sowie zu den einschlägigen Normen und offenen Interoperabilitätsspezifikationen, in denen die exportierbaren Daten verfügbar sind.

GERICHTSBARKEIT, DER DIE IKT-INFRASTRUKTUR UNTERLIEGT, DIE FÜR BUSINESS GPT ERRICHTET WURDE (NACH ART. 28 ABS. 1 LIT. A DATA ACT)

Die Infrastruktur, die die Telekom für **Business GPT** einsetzt, unterliegt dem Recht der Bundesrepublik Deutschland und einschließlich des unmittelbar geltenden Rechts der Europäischen Union.

MAßNAHMEN GEGEN INTERNATIONALE STAATLICHE ZUGRIFFE AUF NICHT-PERSONENBEZOGENE KUNDENINHALTE (NACH ART. 28 ABS. 1 LIT. B DATA ACT)

Die Telekom bietet ihren Kunden ein Bündel aus technischen, organisatorischen und vertraglichen Maßnahmen, um einen internationalen staatlichen Zugriff auf nicht-personenbezogene Kundeninhalte zu verhindern, einschließlich Übermittlungen von in der EU gespeicherter Kunden an staatliche Institutionen in Drittländern, soweit diese gegen nationales oder EU-Recht verstoßen.

- Technische und organisatorische Maßnahmen
 - Verschlüsselung
 - Hochgeladene Dokumente werden während Speicherung und Übertragung verschlüsselt.
 - Die Telekom hat kryptografische Maßnahmen durch Vorgaben definiert. Diese Vorgaben beinhalten:
 - die Nutzung anerkannter 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).
- Chatverläufe, die in der Datenbank gespeichert werden, werden derzeit **nicht verschlüsselt**, da sie innerhalb des Systems durch Rollen- und Berechtigungskonzepte geschützt werden.
- Technisch abgeleitete Daten, wie Embeddings oder interne Indizes, werden ebenfalls **nicht verschlüsselt**, da sie nicht exportierbar sind.
- Der Zugriff auf exportierbare Kundeninhalte ist auf autorisierte Rollen und Systeme beschränkt.
- Kundenkontrolle und Berechtigungskonzepte

Der Kunde kontrolliert, wo seine Kundeninhalte verarbeitet werden und wer auf sie Zugriff haben soll. Für Zugriff auf Kundeninhalte durch die Telekom gibt es intern definierte Berechtigungen in Form von Rollen auf Basis der geschäftlichen, sicherheitsrelevanten und datenschutzrechtlichen Anforderungen. Das beinhaltet:

- 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.
- Verpflichtung von Mitarbeitern

Die Telekom verpflichtet alle Mitarbeiter, die an der Verarbeitung von Kundeninhalten beteiligt sind, die Daten vertraulich zu behandeln und nicht mit Dritten zu teilen. Die Mitarbeiter werden dafür sensibilisiert, wie sie mit etwaigen Datenoffenlegungsverlangen staatlicher Institutionen umzugehen haben, nach



Maßgabe der vertraglichen Verpflichtungen der Telekom gegenüber ihren Kunden und unter Beachtung der maßgeblichen europäischen Gesetze.

- Vertragliche Maßnahmen

Sollte die Telekom eine rechtsverbindliche Anordnung erhalten, Kundeninhalte offenzulegen, wird sie die betreffende staatliche Institution, soweit möglich, direkt an den Kunden verweisen. Außerdem wird die Telekom den Kunden über die Anordnung, soweit rechtlich zulässig, benachrichtigen, um ihm die Möglichkeit zu geben, geeignete Rechtsmittel zu ergreifen. Die Telekom wird die gebotenen Rechtsmittel gegen jede solche Anordnung ergreifen, die gegen anwendbares EU-Recht oder anwendbares Recht eines EU-Mitgliedsstaats verstößt. Sollte die Telekom im Einzelfall dennoch gezwungen sein, entsprechende Kundeninhalte offen zu legen, würde sie nur das absolute Minimum an Kundeninhalten offenlegen, das erforderlich ist, um die Anordnung zu erfüllen.

INFORMATIONEN ÜBER KOMMERZIELLE RAHMENBEDINGUNGEN (NACH ART. 29 ABS. 4 UND 5 DATA ACT)

Die Telekom verlangt keine Entgelte für einen Wechsel. Dies gilt ausdrücklich nur für die vorstehend beschriebenen angemessenen Unterstützungsleistungen und nicht für gesondert vom Kunden bei der Telekom beauftragte Zusatzleistungen, bei denen die Telekom Tätigkeiten aus dem Verantwortungsbereich des Kunden im Zusammenhang mit dem Wechsel in dessen Auftrag übernimmt („Spezielle Unterstützungsleistung“, siehe Ziff.1.4 des Dokuments Regelung zum Data Act).

Der Kunde kann den Vertrag im Zusammenhang mit einem Wechsel zu einem anderen Anbieter, einem Export von Kundeninhalten oder der Löschung von Kundeninhalten kündigen. Die Kündigung kann per Wechselformular oder gesondert in Textform (E-Mail ausreichend) erklärt werden. Die Wechsel-, Export- und Löschungsrechte des Kunden nach den besonderen Bedingungen zum Data Act stehen dem Kunden unabhängig vom gewählten Kündigungsweg zu.

Meistbegünstigung – Kündigungsfristen:

Es gilt das Meistbegünstigungsprinzip: Sowohl die vertragliche Kündigungsfrist als auch die Zwei-Monats-Frist nach den besonderen Bedingungen zum Data Act können genutzt werden; es gilt die jeweils kürzere Frist. Für Paket M / Paket L (12 Monate Mindestvertragslaufzeit) beträgt die vertragliche Kündigungsfrist nach Ablauf der Mindestvertragslaufzeit 30 Tage zum Ende des jeweiligen Verlängerungszeitraums. Für Paket M-1 Monat / Paket L-1 Monat beträgt die vertragliche Kündigungsfrist 20 Tage vor Ablauf der jeweils aktuellen Vertragslaufzeit. Während der Mindestvertragslaufzeit von Paket M / Paket L ist eine ordentliche Kündigung ausgeschlossen; das Kündigungsrecht nach den besonderen Bedingungen zum Data Act kann jedoch auch während der Mindestvertragslaufzeit ausgeübt werden.

Vertragsverlängerung bei Wechselunterstützung:

Nimmt der Kunde den Übergangszeitraum nach den besonderen Bedingungen zum Data Act in Anspruch, wird der Vertrag zu den vereinbarten Konditionen verlängert, jedoch maximal bis



zwei Monate nach Zugang der Kündigungserklärung bei der Telekom (Data-Act-Höchstdauer). Die Wechsel- und Kündigungsrechte des Kunden bleiben hiervon unberührt.

Sanktion bei vorzeitiger Beendigung:

Im Falle einer vorzeitigen Beendigung des Vertrags vor Ablauf der jeweils laufenden Vertragslaufzeit – sei es die Mindestvertragslaufzeit oder ein Verlängerungszeitraum – ist die Telekom berechtigt, einen pauschalierten Schadensersatz in Höhe von 70 % der bis zum Ende der jeweils laufenden Vertragslaufzeit noch ausstehenden Vergütung (netto) zu verlangen. Die Pauschalierung erfolgt unter Berücksichtigung der ersparten Aufwendungen und anderweitigen Verwendungsmöglichkeiten der Telekom. Diese Sanktionsregelung gilt nicht für Kündigungen aus wichtigem Grund gemäß den allgemeinen vertraglichen Bestimmungen.

Abwicklungsfrist:

NACH WIRKSAMWERDEN DER BEENDIGUNG BLEIBT DEM KUNDEN FÜR EINEN ZEITRAUM VON 30 TAGEN ZUGRIFF AUF DIE KUNDENINHALTE AUSSCHLIEßLICH ZUM ZWECKE DES EXPORTS ODER DER LÖSCHUNG; EINE AKTIVE DIENSTLEISTUNG WIRD IN DIESEM ZEITRAUM NICHT ERBRACHT. NACH ABLAUF DIESER 30 TAGE RICHTET SICH DIE LÖSCHUNG BEZIEHUNGSWEISE BEENDIGUNG DES ZUGRIFFS NACH DEN VERTRAGLICHEN UND GESETZLICHEN VORGABEN.

RISIKEN BEI EINEM WECHSEL

Die Telekom weist darauf hin, dass ein Wechsel insbesondere mit folgenden typischen Risiken verbunden ist, die sich aus dem Ausstieg aus Datenverarbeitungsdiensten ergeben und die speziell auf die Datenverarbeitungsdienste zurückgehen:

1. Risiken im Hinblick auf die Datenintegrität und Datenvollständigkeit:

Im Rahmen einer Datenmigration besteht die Möglichkeit, dass gespeicherte Datenbestände nicht vollständig, fehlerhaft oder in veränderter Struktur exportiert/übergeben werden. Insbesondere bei komplexen, KI-bezogenen Datensätzen ist die Wahrung der Datenqualität von besonderer Bedeutung.

2. Einschränkung oder Verlust bestehender Compliance- und Auditierungsnachweise:

Durch den Wechsel können bisher von der Telekom bereitgestellte Nachweise, Zertifizierungen, Audit-Logs oder Dokumentationen, wie sie etwa im Zusammenhang mit Anforderungen des EU AI Act erforderlich sind, entfallen oder für den neuen Anbieter nicht ohne weiteres verfügbar gemacht werden.

3. Störung laufender Geschäftsprozesse und automatisierter Abläufe:

Während der Umstellung kann es zu einer temporären Nichtverfügbarkeit oder zu Einschränkungen bei den von der Telekom betriebenen Datenverarbeitungsdiensten und angebundenen KI-Systemen kommen.



Integrationen mit Drittsystemen, Schnittstellen oder automatisierte Abläufe können hiervon betroffen sein.

4. Probleme bei der Übertragung von spezifischen Zugriffskonzepten und Sicherheitskonfigurationen:

Maßgeschneiderte Zugriffsrechte, Rollenmodelle sowie sicherheitsrelevante Einstellungen, die bei der Telekom etabliert wurden, bedürfen einer sorgfältigen Migration (sofern möglich), um die fortgesetzte Autorisierung und Funktionsfähigkeit sicherzustellen.

5. Erschwerte Übertragbarkeit proprietärer Technologien oder Datenformate:

Die Datenverarbeitungsdienste der Telekom können proprietäre Datenformate, Schnittstellen oder KI-Modelle beinhalten, deren uneingeschränkte Kompatibilität oder Konvertierbarkeit zum System eines anderen Dienstleisters nicht gewährleistet ist.

6. Erhöhte Risiken hinsichtlich Datenschutz und Informationssicherheit:

Im Verlauf der Migration besteht ein erhöhtes Risiko für Datenschutzverletzungen, den Verlust von Vertraulichkeit sowie die Gefährdung der Integrität sensibler Daten im Sinne der Datenschutz-Grundverordnung (DSGVO) und der Vorgaben des EU AI Act.

Es obliegt dem Kunden, sich über die Risiken der Nutzung seiner IKT-Infrastruktur oder der Dienste eines anderen Anbieters, einschließlich einer Migration zu diesem Anbieter, zu informieren.