

ERGÄNZUNGSVEREINBARUNG DORA

Nachtrag zu den Nutzungsbedingungen der DeutschlandGPT GmbH für Kunden im Anwendungsbereich der
Verordnung (EU) 2022/2554 · Fassung vom 13. August 2026

Einbezogen über Ziff. 1.4 der Nutzungsbedingungen. Eine gesonderte Unterzeichnung ist nach Art. 30 Abs. 1 der
Verordnung nicht erforderlich.

1. Anwendungsbereich und Vorrang

(1) Diese Ergänzungsvereinbarung („**Nachtrag**“) gilt zwischen der DeutschlandGPT GmbH („**Anbieter**“) und dem Kunden, sofern der Kunde als Finanzunternehmen oder als IKT-Drittdienstleister in den Anwendungsbereich der Verordnung (EU) 2022/2554 über die digitale operationale Resilienz im Finanzsektor („**DORA**“) fällt („**Institut**“). Er tritt mit Abschluss der Nutzungsbedingungen automatisch in Kraft.

(2) Bei Widersprüchen zwischen diesem Nachtrag und den Nutzungsbedingungen oder den Bedingungen zur Auftragsverarbeitung („**AV**“) gehen die Bestimmungen dieses Nachtrags vor. Im Übrigen bleiben beide unberührt.

(3) **Ziffer 13.1 der Nutzungsbedingungen (Änderung durch Zustimmungsfiktion) und Ziffer 13.3 (Abtretung, Übertragung und Novation) finden auf diesen Nachtrag keine Anwendung.** Änderungen dieses Nachtrags bedürfen der Zustimmung beider Parteien in Textform.

(4) Begriffe dieses Nachtrags haben, soweit nicht anders definiert, die Bedeutung der Nutzungsbedingungen bzw. der DORA.

2. Vertragsgegenstand und Einstufung

(1) Der Anbieter stellt dem Institut auf Grundlage der Nutzungsbedingungen die Plattform DeutschlandGPT als Software-as-a-Service bereit („**IKT-Leistungen**“). Art, Umfang und Dienstleistungsgüte richten sich nach den Nutzungsbedingungen und der jeweils gültigen Leistungsbeschreibung.

(2) Das Institut nutzt die IKT-Leistungen nach eigener Einschätzung in einer Weise, bei der diese **keine kritischen oder wichtigen Funktionen** im Sinne des Art. 3 Nr. 22 DORA unterstützen. Der Anbieter ist dementsprechend kein kritischer IKT-Drittdienstleister im Sinne des Art. 31 DORA und unterliegt nicht dem dortigen Überwachungsrahmen.

(3) Die Einstufung nach Absatz 2 obliegt allein dem Institut. Ändert sie sich, teilt das Institut dies dem Anbieter unverzüglich in Textform mit; die Parteien verhandeln sodann eine gesonderte Vereinbarung nach Art. 30 Abs. 3 DORA. Bis zu deren Abschluss gilt dieser Nachtrag fort.

3. Standorte und Datenverarbeitung

(1) Der Anbieter erbringt die IKT-Leistungen in der Europäischen Union. Die Speicherung der Daten des Instituts im Ruhezustand erfolgt in **Deutschland**, auf BSI C5-testierter Infrastruktur der Open Telekom Cloud (T-Systems International GmbH).

(2) Der Ort der Verarbeitung ist **je Unterauftragsverarbeiter** in Anhang IV des AV festgelegt und dort für jeden Dienstleister einzeln ausgewiesen. Diese Angaben stehen dem Institut jederzeit öffentlich zur

Verfügung.

(3) Eine beabsichtigte Änderung der Verarbeitungsstandorte teilt der Anbieter dem Institut mindestens **einen Kalendermonat** im Voraus in Textform mit.

4. Informationsregister

(1) Der Anbieter stellt dem Institut auf Anforderung die Angaben zur Verfügung, die es für die Erstellung und Pflege seines Informationsregisters nach Art. 28 Abs. 3 DORA und der Durchführungsverordnung (EU) 2024/2956 benötigt.

(2) Für die Identifikation des Anbieters gilt:

Feld	Angabe
Firma	DeutschlandGPT GmbH
Anschrift	Gabriele-Münter-Straße 3, 82110 Germering, Deutschland
Land	DE
Handelsregister	HRB 282400, Amtsgericht München
Muttergesellschaft	Titanom Group GmbH, Germering (HRB 261817, Amtsgericht München)
Art des Codes	EUID
Identifikationscode	DED2601V.HRB282400

(3) Die Verwendung der EUID anstelle einer LEI ist nach der Durchführungsverordnung (EU) 2024/2956 zulässig; die EBA hat dies für in der Union niedergelassene juristische Personen in ihrer Q&A 2024_7283 zu Feld B_05.01.0020 ausdrücklich klargestellt.

(4) Die Muttergesellschaft firmierte bis 2026 als Titanom Technologies GmbH; unter dieser früheren Firmierung ist sie auf den ISO-Zertifikaten der Gruppe ausgewiesen. Registernummer und juristische Person sind unverändert.

5. Informationssicherheit

(1) Der Anbieter betreibt ein Informationssicherheits-Managementsystem und ist nach **ISO/IEC 27001:2022** zertifiziert. Der Geltungsbereich lautet „Entwicklung, Bereitstellung, Betrieb und das Management von KI-unterstützten Plattform- und Softwarelösungen“. Auf Anforderung stellt der Anbieter das aktuelle Zertifikat sowie den Testatsauszug seines Hosters zur Verfügung.

(2) Der Anbieter trifft angemessene technische und organisatorische Maßnahmen zum Schutz der Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität der IKT-Leistungen und der dabei verarbeiteten Daten des Instituts. Die konkret umgesetzten Maßnahmen ergeben sich aus Anhang III des AV.

(3) Der Anbieter unterhält ein Schwachstellenmanagement. Kritische Schwachstellen behebt der Anbieter unverzüglich.

(4) Der Anbieter verwendet Kundendaten des Instituts nicht zum Training von KI-Modellen und stellt sicher, dass auch die eingesetzten Unterauftragsverarbeiter dies nicht tun.

6. IKT-Vorfälle und Meldepflichten

- (1) Der Anbieter unterrichtet das Institut nach Kenntniserlangung unverzüglich, **spätestens jedoch innerhalb von 48 Stunden**, in Textform über IKT-bezogene Vorfälle, die die vom Anbieter bereitgestellten IKT-Leistungen betreffen und die Sicherheit der Plattform oder der Daten des Instituts erheblich gefährden.
- (2) Der Anbieter stellt dem Institut auf Anforderung die Informationen zur Verfügung, die dieses benötigt, um einen Vorfall einzustufen und die nach Art. 19 DORA erforderlichen Meldungen gegenüber den zuständigen Behörden abzugeben, soweit die Informationen dem Anbieter vorliegen und ihrer Offenlegung keine zwingenden Geheimhaltungspflichten entgegenstehen.
- (3) Bei einem IKT-Vorfall, der mit den vom Anbieter erbrachten IKT-Leistungen in Zusammenhang steht, leistet der Anbieter dem Institut Unterstützung **ohne zusätzliche Kosten**.
- (4) Der Anbieter teilt dem Institut wesentliche Entwicklungen mit, die sich erheblich auf seine Fähigkeit auswirken können, die IKT-Leistungen vertragsgemäß zu erbringen, sobald er hiervon Kenntnis erlangt.
- (5) Die Melde- und Unterstützungspflichten nach dieser Ziffer gelten für die vom Anbieter unmittelbar erbrachten IKT-Leistungen. Für Vorfälle, die **allein in der Infrastruktur eines Anbieters von KI-Modellen** entstehen, leitet der Anbieter alle ihm verfügbaren Informationen an das Institut weiter.

7. Business Continuity und Notfallkonzept

- (1) Der Anbieter unterhält ein Datensicherungs-, Wiederherstellungs- und Notfallkonzept für den Betrieb der Plattform. Es benennt die Sicherungsverfahren, die Wiederanlaufschritte und die Zuständigkeiten im Störfall.
- (2) Der Anbieter überprüft die Wirksamkeit dieses Konzepts **regelmäßig durch Wiederherstellungstests** und dokumentiert die Ergebnisse. Auf Anforderung teilt er dem Institut das Testdatum sowie die dabei erreichten Wiederanlaufkennzahlen mit.

8. Datenschutz und Beendigungsmanagement

- (1) Für den Schutz der personenbezogenen Daten des Instituts, die der Anbieter im Rahmen der IKT-Leistungen verarbeitet, gilt der zwischen den Parteien geschlossene AV.
- (2) Der Anbieter stellt dem Institut auf Anforderung einen **Export der in der Plattform gespeicherten Daten des Instituts in einem gängigen, maschinenlesbaren Format** bereit. Der Export erfolgt innerhalb von 30 Tagen nach Anforderung. Dieser Anspruch besteht während der Vertragslaufzeit sowie für **30 Tage nach Wirksamwerden der Beendigung** — unabhängig vom Grund der Beendigung, einschließlich einer Kündigung aus wichtigem Grund durch eine der Parteien, sowie im Fall der Insolvenz oder der Einstellung des Geschäftsbetriebs des Anbieters.
- (3) Nach Ablauf der Frist nach Absatz 2 löscht der Anbieter die Daten des Instituts nach Maßgabe des AV, soweit keine gesetzliche Aufbewahrungspflicht besteht. Die Löschung bestätigt er dem Institut auf Anfrage.

9. Unterauftragnehmer

- (1) Der Anbieter ist berechtigt, Unterauftragnehmer einzusetzen. Die für die Erbringung der IKT-Leistungen eingesetzten Unterauftragnehmer sind in **Anhang IV des AV** mit Firmierung, Anschrift,

Gegenstand und Art der Verarbeitung sowie **Ort der Verarbeitung** aufgeführt.

(2) Der Einsatz neuer Unterauftragnehmer erfolgt nach Ankündigung gegenüber dem Institut mit einem Vorlauf von mindestens einem Kalendermonat; das Widerspruchsrecht nach dem AV bleibt unberührt.

(3) Auf Anforderung stellt der Anbieter dem Institut weitere Informationen über die eingesetzten Unterauftragnehmer sowie über deren eigene Unterauftragsvergabe zur Verfügung, soweit dies zur Erfüllung aufsichtsrechtlicher Anforderungen des Instituts erforderlich ist und der Offenlegung keine berechtigten Geheimhaltungsinteressen entgegenstehen.

10. Schulungen zu IKT-Sicherheit und digitaler operationaler Resilienz

(1) Der Anbieter betreibt eine eigene Lernplattform und schult seine Mitarbeitenden regelmäßig zu Informationssicherheit und Datenschutz.

(2) Fordert das Institut den Anbieter zur Teilnahme an eigenen Schulungsprogrammen nach Art. 30 Abs. 2 lit. i DORA auf, stimmen die Parteien Umfang und Durchführung einvernehmlich ab. Der Anbieter kann ausreichend vorhandene Schulungsmaßnahmen durch aktuelle Zertifizierungen oder Nachweise belegen, die den jeweiligen Schulungsgegenstand abdecken. Eine vereinbarte Teilnahme ist auf Mitarbeitende beschränkt, die unmittelbar an der Leistungserbringung gegenüber dem Institut beteiligt sind, und erfolgt remote.

11. Prüfungs- und Zugangsrechte

(1) Der Anbieter stellt dem Institut auf Anforderung die bei ihm vorhandenen Informationen zur Verfügung, die erforderlich sind, um die Einhaltung der Pflichten aus diesem Nachtrag gegenüber Aufsichtsbehörden nachzuweisen.

(2) Das Institut sowie von ihm beauftragte Prüfer sind berechtigt, die Einhaltung der Pflichten aus diesem Nachtrag in Bezug auf die vom Anbieter erbrachten IKT-Leistungen in angemessenem Umfang zu prüfen. Der Nachweis erfolgt in der Regel durch Vorlage eines geeigneten, aktuellen Zertifikats, Testats oder Prüfberichts einer unabhängigen Stelle (z. B. ISO/IEC 27001, BSI C5).

(3) Soweit (i) das Institut einen konkreten und begründeten Verdacht auf einen Verstoß gegen diesen Nachtrag darlegt, (ii) die Nachweise nach Absatz 2 im Einzelfall keine angemessene Überprüfung ermöglichen oder (iii) ein Audit behördlich oder aufsichtsrechtlich verbindlich angeordnet wurde, sind das Institut sowie von ihm beauftragte Prüfer berechtigt, Audits einschließlich Vor-Ort-Prüfungen durchzuführen. Für die Durchführung gelten die Regelungen des AV über Inspektionen entsprechend.

(4) Die Rechte nach dieser Ziffer stehen in gleichem Umfang den für das Institut zuständigen Aufsichts- und Abwicklungsbehörden zu.

(5) Die Rechte nach dieser Ziffer bestehen für einen Zeitraum von bis zu einem Jahr nach Beendigung der Erbringung der IKT-Leistungen fort, soweit dies zur Erfüllung gesetzlicher oder aufsichtsrechtlicher Pflichten erforderlich ist.

12. Zusammenarbeit mit Behörden

Der Anbieter arbeitet mit den für das Institut zuständigen Aufsichts- und Abwicklungsbehörden sowie den von diesen benannten Personen vollumfänglich zusammen, soweit sich deren Anfragen auf die gegenüber

dem Institut erbrachten IKT-Leistungen beziehen und dem nicht zwingende Geheimhaltungspflichten oder schutzwürdige Vertraulichkeitsinteressen gegenüber anderen Kunden entgegenstehen.

13. Laufzeit und Kündigung

(1) Dieser Nachtrag tritt mit Abschluss der Nutzungsbedingungen in Kraft und endet mit diesen, ohne dass es einer gesonderten Kündigung bedarf.

(2) **Laufzeit, ordentliche Kündigungsfristen und Verlängerung richten sich ausschließlich nach den Nutzungsbedingungen und dem Einzelvertrag.** Dieser Nachtrag ändert sie nicht. Absatz 3 begründet ausschließlich ein zusätzliches außerordentliches Kündigungsrecht für die dort abschließend genannten aufsichtsrechtlichen Fälle.

(3) Das Institut kann die Nutzungsbedingungen und diesen Nachtrag mit einer Frist von 14 Tagen aus wichtigem Grund kündigen, wenn

- (i) der Anbieter erheblich gegen geltende Gesetze, aufsichtsrechtliche Vorgaben oder diesen Nachtrag verstößt,
- (ii) im Rahmen der Überwachung des IKT-Drittparteienrisikos Umstände festgestellt wurden, die die ordnungsgemäße Erbringung der IKT-Leistungen beeinträchtigen,
- (iii) der Anbieter nachweisliche Schwächen in seinem IKT-Risikomanagement aufweist, insbesondere wenn diese die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit der IKT-Leistungen gefährden, oder
- (iv) eine zuständige Aufsichtsbehörde das Institut wegen der Nutzung der IKT-Leistungen nicht mehr wirksam beaufsichtigen kann oder die Beendigung verbindlich anordnet.

In den Fällen (i) bis (iii) ist die Kündigung erst zulässig, wenn der Anbieter den Umstand nicht innerhalb einer angemessenen Frist nach Abmahnung in Textform beseitigt hat. Die Kündigung bedarf der Textform.

(4) Die Rechte des Instituts nach Ziffer 8 Absatz 2 bleiben von einer Kündigung unberührt.

14. Sonstiges

(1) Dieser Nachtrag unterliegt dem Recht der Bundesrepublik Deutschland unter Ausschluss des UN-Kaufrechts und des internationalen Privatrechts.

(2) Gerichtsstand ist der in den Nutzungsbedingungen vereinbarte.

(3) Änderungen und Ergänzungen dieses Nachtrags bedürfen der Textform und der Zustimmung beider Parteien. Mündliche Nebenabreden bestehen nicht.

(4) Sollte eine Bestimmung dieses Nachtrags unwirksam sein oder werden oder eine Lücke enthalten, bleiben die übrigen Bestimmungen unberührt. Die Parteien werden die unwirksame Bestimmung durch eine wirksame ersetzen, die deren Zweck am nächsten kommt und den Anforderungen der DORA genügt.
