Auftragsverarbeitungsvertrag

(24. November 2026)

gemäß Artikel 28 Absatz 3 der Datenschutz-Grundverordnung (DSGVO)

zwischen

_____

(Name und Anschrift des Unternehmens)

Der Verantwortliche gemäß Art. 24 DSGVO (im Folgenden **Auftraggeber** genannt)

und

DEON GmbH & Co. KG

Ella-Kay-Str. 22c

10405 Berlin

Der Auftragsverarbeiter (im Folgenden **Auftragnehmer** genannt)

Ansprechpartner Datenschutz des Auftragnehmers

Ansprechpartner für alle Fragen des Datenschutzes und der Verarbeitung personenbezogener Daten im Rahmen dieses Vertrages ist die Geschäftsführung des Auftragnehmers. Ein Datenschutzbeauftragter ist nicht benannt, da hierzu keine Pflicht nach Artikel 37 DSGVO oder § 38 BDSG besteht.

Auftragnehmer (DEON GmbH & Co. KG):

Ella-Kay-Str. 22c, 10405 Berlin, Deutschland

E-Mail: datenschutz@deon.de

1 Gegenstand und Dauer des Auftrags

1.1 Gegenstand

Gegenstand des Auftrags über die Datenverarbeitung ist die Bereitstellung einer Software-Plattform für visuelle Arbeit und Kollaboration (im Folgenden **Nutzungsbedingungen**, https://deon.de/terms-of-service/ genannt).

Der Auftragnehmer darf die Daten des Auftraggebers im Rahmen des Datenschutzrechts für eigene Zwecke in eigener Verantwortung verarbeiten und nutzen. Dies ist der Fall, wenn der Auftragnehmer die Daten des Auftraggebers anonym und in anonymisierter Form für eigene Zwecke verarbeitet und nutzt.

1.2 Dauer

Die Dauer dieses Auftrags entspricht der in den Nutzungsbedingungen festgelegten Dauer.

2 Spezifizierung der Auftragsdetails

2.1 Art und Zweck der beabsichtigten Datenverarbeitung

Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind in den Nutzungsbedingungen genau definiert.

2.2 Art der verwendeten personenbezogenen Daten

Folgende Datenkategorien und betroffene Personengruppen unterliegen der Erhebung und/oder Verarbeitung und/oder Nutzung:

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien:

- Name (erforderlich)
- E-Mail (erforderlich)
- Weitere Daten: alle Daten, die vom Auftraggeber in den „Arbeitsbereich“ eingegeben werden.

Kategorien betroffener Personen

Die Kategorien betroffener Personen umfassen:

- Kunden des Auftraggebers
- Mitarbeiter des Auftraggebers

2.3 Angemessenes Schutzniveau

Die Durchführung der vertraglich vereinbarten Datenverarbeitung erfolgt in einem Mitgliedstaat der Europäischen Union (EU) oder in einem Mitgliedstaat des Europäischen Wirtschaftsraums (EWR). Das gilt auch für den Versand von System-E-Mails über Mailgun, der in der EU-Region von Mailgun erfolgt. Eine Übermittlung von Daten in einen Staat, der weder Mitglied der EU noch des EWR ist, erfolgt ausschließlich bei Nutzung der optionalen KI-Funktionen (DAIA), und zwar an den vom Nutzer gewählten, in Ziffer 6.2 genannten KI-Anbieter. Grundlage sind geeignete Garantien nach Artikel 46 DSGVO, insbesondere die Standardvertragsklauseln der EU-Kommission. Jede weitere Übermittlung in einen solchen Staat bedarf der vorherigen Zustimmung des Auftraggebers und erfolgt nur, wenn die spezifischen Bedingungen des Artikels 44 ff. DSGVO erfüllt sind.

Das angemessene Schutzniveau (z. B. Land, Gebiet oder bestimmte Sektoren innerhalb eines Landes):

- wurde von der Europäischen Kommission beschlossen (Artikel 45 Absatz 3 DSGVO) oder
- ergibt sich aus verbindlichen internen Datenschutzvorschriften (Artikel 46 Absatz 2 Buchstabe b in Verbindung mit Artikel 47 DSGVO) oder
- ergibt sich aus Standarddatenschutzklauseln (Artikel 46 Absatz 2 Buchstaben c und d DSGVO) oder
- ergibt sich aus genehmigten Verhaltensregeln (Artikel 46 Absatz 2 Buchstabe e in Verbindung mit Artikel 40 DSGVO) oder
- ergibt sich aus einem genehmigten Zertifizierungsverfahren (Artikel 46 Absatz 2 Buchstabe f in Verbindung mit Artikel 42 DSGVO) oder
- wird auf andere Weise hergestellt (Artikel 46 Absatz 2 Buchstabe a, Absatz 3 Buchstaben a und b DSGVO).

3 Technische und Organisatorische Maßnahmen

3.1 Vor Beginn der Verarbeitung dokumentiert der Auftragnehmer die Durchführung der notwendigen, vor der Auftragserteilung festgelegten technischen und organisatorischen Maßnahmen, insbesondere im Hinblick auf die detaillierte Vertragsdurchführung, und legt diese dem Auftraggeber zur Prüfung vor. Nach Zustimmung des Auftraggebers werden die dokumentierten Maßnahmen zur Grundlage des Vertrages. Sofern die Prüfung/das Audit durch den Auftraggeber die Notwendigkeit von Änderungen ergibt, werden diese im gegenseitigen Einvernehmen umgesetzt.

3.2 Der Auftragnehmer stellt die Sicherheit gemäß Artikel 28 Absatz 3 Buchstabe c) und Artikel 32 der DSGVO, insbesondere in Verbindung mit Artikel 5 Absatz 1 und Absatz 2 der DSGVO, her. Die zu treffenden Maßnahmen sind Maßnahmen der Datensicherheit und Maßnahmen, die ein dem Risiko angemessenes Schutzniveau hinsichtlich der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme gewährleisten. Dabei sind der Stand der Technik, die Implementierungskosten, die Art, der Umfang, die Umstände und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Artikel 32 Absatz 1 DSGVO zu berücksichtigen [Details in Anhang 1].

3.3 Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Der Auftragnehmer darf unter Beachtung dessen alternative angemessene Maßnahmen implementieren. Das Sicherheitsniveau der festgelegten Maßnahmen darf jedoch nicht reduziert werden. Wesentliche Änderungen müssen dokumentiert werden.

4 Berichtigung, Einschränkung und Löschung von Daten

4.1 Der Auftragnehmer darf Daten, die im Auftrag des Auftraggebers verarbeitet werden, nicht eigenmächtig berichtigen, löschen oder deren Verarbeitung einschränken, sondern nur nach dokumentierter Weisung des Auftraggebers. Wendet sich eine betroffene Person unmittelbar an den Auftragnehmer bezüglich einer Berichtigung, Löschung oder Einschränkung der Verarbeitung, wird der Auftragnehmer das Ersuchen der betroffenen Person unverzüglich an den Auftraggeber weiterleiten.

4.2 Ist es vom Leistungsumfang umfasst, gewährleistet der Auftragnehmer die Löschrichtlinie, das „Recht auf Vergessenwerden“, die Berichtigung, die Datenübertragbarkeit und den Zugriff gemäß den dokumentierten Weisungen des Auftraggebers unverzüglich.

5 Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hält zusätzlich zu der Einhaltung der in diesem Vertrag festgelegten Regelungen die in Artikel 28 bis 33 DSGVO genannten gesetzlichen Anforderungen ein; demgemäß gewährleistet der Auftragnehmer insbesondere die Einhaltung folgender Anforderungen:

a) Vertraulichkeit gemäß Artikel 28 Absatz 3 Satz 2 Buchstabe b), Artikel 29 und 32 Absatz 4 DSGVO. Der Auftragnehmer betraut nur solche Mitarbeiter mit der in diesem Vertrag dargelegten Datenverarbeitung, die zur Vertraulichkeit verpflichtet und zuvor mit den für ihre Tätigkeit relevanten Datenschutzbestimmungen vertraut gemacht wurden. Der Auftragnehmer und jede ihm unterstellte Person, die Zugang zu personenbezogenen Daten hat, verarbeitet diese nur auf Weisung des Auftraggebers, wozu auch die in diesem Vertrag gewährten Befugnisse gehören, es sei denn, sie ist gesetzlich dazu verpflichtet.
b) Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Artikel 28 Absatz 3 Satz 2 Buchstabe c), Artikel 32 DSGVO [Details in Anhang 1].
c) Zusammenarbeit bei Anfragen der Aufsichtsbehörde: Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
d) Informationspflicht bei Inspektionen: Der Auftraggeber ist unverzüglich über alle vom Auftragnehmer durchgeführten Inspektionen und Maßnahmen der Aufsichtsbehörde zu informieren, sofern sie sich auf diesen Auftrag beziehen. Dies gilt auch, wenn der Auftragnehmer im Zusammenhang mit der Verarbeitung personenbezogener Daten im Rahmen dieses Auftrags oder Vertrages von einer zuständigen Behörde im Hinblick auf Verstöße gegen zivil- oder strafrechtliche Vorschriften oder Verwaltungsbestimmungen untersucht wird oder an einer solchen Untersuchung beteiligt ist.
e) Unterstützung des Auftraggebers: Wird der Auftraggeber einer Überprüfung durch die Aufsichtsbehörde, einem Verwaltungsverfahren oder strafrechtlichen Verfahren, einem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem sonstigen Anspruch im Zusammenhang mit der Auftragsdatenverarbeitung durch den Auftragnehmer ausgesetzt, wird der Auftragnehmer den Auftraggeber nach besten Kräften unterstützen.
f) Regelmäßige Überprüfung: Der Auftragnehmer überwacht die internen Prozesse und die technischen und organisatorischen Maßnahmen regelmäßig, um sicherzustellen, dass die Verarbeitung in seinem Verantwortungsbereich den Anforderungen des geltenden Datenschutzrechts und dem Schutz der Rechte der betroffenen Person entspricht.
g) Nachweisbarkeit der durchgeführten technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen der in Ziffer 7 dieses Vertrages genannten Kontrollrechte des Auftraggebers.

6 Unterbeauftragung

6.1 Unterbeauftragung im Sinne dieser Vereinbarung sind Dienstleistungen, die in direktem Zusammenhang mit der Erbringung der Hauptleistung stehen. Hiervon ausgenommen sind Nebenleistungen, wie Telekommunikationsdienstleistungen, Post-/Transportdienstleistungen, Wartungs- und Benutzerunterstützungsdienste oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Gewährleistung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen. Der Auftragnehmer ist jedoch verpflichtet, auch bei ausgelagerten Nebenleistungen angemessene und rechtlich verbindliche vertragliche Regelungen zu treffen und angemessene Kontrollmaßnahmen zu ergreifen, um den Datenschutz und die Datensicherheit der Daten des Auftraggebers zu gewährleisten.

6.2 Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher oder dokumentierter Zustimmung des Auftraggebers beauftragen.

Der Auftraggeber stimmt der Beauftragung der folgenden Unterauftragnehmer unter der Bedingung einer vertraglichen Vereinbarung gemäß Artikel 28 Absätze 2–4 DSGVO zu:

Unternehmen Unterauftragnehmer	**Adresse/Land**	**Dienstleistungen**	**Auftragsverarbeitungsvertrag**	**Garantien bei Drittlandübermittlung**
Microsoft Ireland Operations, Ltd.	One Microsoft Place, Dublin, Irland	Hosting (Azure Westeuropa)	Ja	(Keine Drittlandübermittlung, Daten werden innerhalb der EU/des EWR gehostet)
Mailgun Technologies, Inc.	112 E. Pecan St. #1135, San Antonio, TX 78205, USA	Transaktionaler E-Mail-Dienst, Region Europa	Ja	(Keine Drittlandübermittlung, Daten werden innerhalb der EU/des EWR gehostet)
Optional:				
Optional: OpenAI, L.L.C.	3180 18th Street, San Francisco, CA 94110, USA	KI-basierte Generierungs- und Analysedienste (über API)	Ja	Standardvertragsklauseln (SCCs)
Optional: Anthropic	Dublin, Irland; Verarbeitung in	KI-basierte Generierungs-	Ja	Standardvertragsklauseln (SCCs)

Ireland, Limited (Verarbeitung durch Anthropic, PBC, USA)	San Francisco, CA, USA	und Analysedienste (über API, Modelle Claude)		
Optional: Google Cloud EMEA Limited (Verarbeitung auch durch Google LLC, USA)	70 Sir John Rogerson's Quay, Dublin 2, Irland; Verarbeitung auch in den USA	KI-basierte Generierungs- und Analysedienste (über die Gemini API)	Ja	Standardvertragsklauseln (SCCs)
Optional: IONOS SE	Elgendorfer Str. 57, 56410 Montabaur, Deutschland	KI-basierte Generierungs- und Analysedienste (über den IONOS AI Model Hub)	Ja	(Keine Drittlandübermittlung, Verarbeitung in Deutschland)

Optionale Nutzung von KI-Diensten (OpenAI API und weitere KI-Anbieter)

Wenn der Auftraggeber die optionale KI-Integrationsfunktion innerhalb der DEON-Plattform ausdrücklich aktiviert, darf der Auftragnehmer bestimmte personenbezogene Daten verarbeiten, indem er diese Daten an die OpenAI API übermittelt, die von OpenAI, L.L.C. mit Sitz in den Vereinigten Staaten von Amerika bereitgestellt wird.

Die Verarbeitung durch OpenAI erfolgt auf Grundlage von Standardvertragsklauseln (SCCs) gemäß Art. 46 Abs. 2 lit. c DSGVO, die zwischen dem Auftragnehmer und OpenAI geschlossen wurden. Der Auftraggeber erkennt an und erklärt sich damit einverstanden, dass OpenAI, L.L.C. in diesem Zusammenhang als Unterauftragsverarbeiter agiert.

Für die optionalen KI-Dienste von Anthropic Ireland, Limited (Anthropic API, Verarbeitung durch Anthropic, PBC) und Google Cloud EMEA Limited (Gemini API, Verarbeitung auch durch Google LLC), deren Verarbeitung jeweils auch in den Vereinigten Staaten von Amerika erfolgen kann, gelten der vorstehende und der nachfolgende Absatz entsprechend. Die Verarbeitung erfolgt auf Grundlage der Standardvertragsklauseln, die Bestandteil der jeweiligen Vereinbarung zur Auftragsverarbeitung zwischen dem Auftragnehmer und dem Anbieter sind. Für den IONOS AI Model Hub der IONOS SE erfolgt die Verarbeitung ausschließlich in Deutschland; eine Übermittlung in ein Drittland findet nicht statt. Welchen KI-Anbieter eine Anfrage nutzt, richtet sich nach der Auswahl in der Benutzeroberfläche.

Der Auftragnehmer gewährleistet, dass:

- nur die minimal notwendigen personenbezogenen Daten übermittelt werden;
- Daten von den KI-Anbietern nicht zur Schulung ihrer Modelle oder für andere Zwecke jenseits der angeforderten Dienstleistung verwendet werden;

- angemessene technische und organisatorische Maßnahmen zur Sicherung der Daten während der Übermittlung und Verarbeitung implementiert sind.

Beauftragung von Unterauftragnehmern Die Auslagerung an Unterauftragnehmer oder der Wechsel eines bestehenden Unterauftragnehmers ist zulässig, vorausgesetzt, dass:

a) der Auftragnehmer den Auftraggeber in Textform oder schriftlich angemessen im Voraus über eine solche Auslagerung an Unterauftragnehmer informiert, und
b) der Auftraggeber der beabsichtigten Auslagerung nicht bis zum Zeitpunkt der Datenübermittlung in Textform oder schriftlich gegenüber dem Auftragnehmer widerspricht, und
c) eine vertragliche Vereinbarung gemäß Art. 28 Abs. 3 DSGVO mit einem angemessenen Sicherheitsniveau zugrunde gelegt wird.

6.3 Die Übermittlung personenbezogener Daten vom Auftraggeber an den Unterauftragnehmer und der Beginn der Datenverarbeitung durch den Unterauftragnehmer dürfen erst erfolgen, nachdem alle Anforderungen erfüllt wurden.

6.4 Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR, hat der Auftragnehmer die Einhaltung der EU-Datenschutzbestimmungen durch geeignete Maßnahmen sicherzustellen. Entsprechendes gilt, wenn Dienstleister im Sinne des Absatzes 1 Satz 2 eingesetzt werden sollen.

6.5 Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen Zustimmung des Auftragnehmers (mindestens in Textform).

6.6 Zukünftige KI-Anbieter
DEON kann weitere KI-Dienstleister („KI-Anbieter“) integrieren, um KI-gestützte Funktionen innerhalb der DEON-Plattform anzubieten. Jeder neue KI-Anbieter wird nur als Unterauftragsverarbeiter gemäß Art. 28 DSGVO beauftragt und wird öffentlich unter https://deon.de/ai-providers aufgeführt.

Alle vertraglichen Bestimmungen in der Vertragskette sind jedem weiteren Unterauftragnehmer mitzuteilen und mit ihm zu vereinbaren.

7 Kontrollrechte des Auftraggebers

7.1 Der Auftraggeber hat nach Absprache mit dem Auftragnehmer das Recht, Inspektionen durchzuführen oder durch einen in jedem Einzelfall zu benennenden Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichproben, die in der Regel vorab anzukündigen sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in seinem Geschäftsbetrieb zu überzeugen.

7.2 Der Auftragnehmer stellt sicher, dass der Auftraggeber die Einhaltung der Pflichten des Auftragnehmers gemäß Artikel 28 DSGVO überprüfen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anfrage die notwendigen Informationen zur Verfügung zu stellen und insbesondere die Durchführung der technischen und organisatorischen Maßnahmen nachzuweisen.

7.3 Der Nachweis solcher Maßnahmen, die sich nicht ausschließlich auf den konkreten Vertrag beziehen, kann durch mindestens eines der folgenden Dokumente erbracht werden:

a) Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO oder
b) Zertifizierung gemäß einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO oder
c) aktuelle Bescheinigungen, Berichte oder Berichtsauszüge von unabhängigen Stellen (z. B. Wirtschaftsprüfern, internen Revisoren, Datenschutzbeauftragten, Informationssicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder
d) eine geeignete Zertifizierung durch ein Informationssicherheits- oder Datenschutzaudit (z. B. nach ISO 27001, PCI DSS, BSI IT-Grundschutz, Europäisches Datenschutzsiegel).

7.4 Der Auftragnehmer kann für die Ermöglichung von Inspektionen des Auftraggebers eine Vergütung verlangen.

8 Kommunikation im Falle von Verstößen durch den Auftragnehmer

8.1 Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der Pflichten zur Sicherheit personenbezogener Daten, den Meldepflichten bei Datenschutzverletzungen, der Datenschutz-Folgenabschätzung und der vorherigen Konsultation, die in den Artikeln 32 bis 36 DSGVO genannt sind. Dazu gehören:

a) Gewährleistung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen unter Berücksichtigung der Umstände und Zwecke der Verarbeitung sowie der voraussichtlichen Wahrscheinlichkeit und Schwere eines möglichen Rechtsverstoßes infolge von Sicherheitslücken und Ermöglichung einer sofortigen Erkennung relevanter Verletzungsereignisse.
b) Die Pflicht zur unverzüglichen Meldung einer Verletzung des Schutzes personenbezogener Daten an den Auftraggeber.
c) Die Pflicht zur Unterstützung des Auftraggebers hinsichtlich seiner Verpflichtung zur Information der betroffenen Person und zur unverzüglichen Bereitstellung aller relevanten Informationen in dieser Hinsicht an den Auftraggeber.
d) Unterstützung des Auftraggebers bei seiner Datenschutz-Folgenabschätzung.
e) Unterstützung des Auftraggebers hinsichtlich der vorherigen Konsultation der

Aufsichtsbehörde.

8.2 Der Auftragnehmer kann eine Vergütung für Unterstützungsleistungen verlangen, die nicht in der Leistungsbeschreibung enthalten sind und nicht auf Versäumnisse des Auftragnehmers zurückzuführen sind.

9 Weisungsbefugnis des Auftraggebers

9.1 Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mindestens in Textform).

9.2 Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen Datenschutzvorschriften verstößt. Der Auftragnehmer ist dann berechtigt, die Ausführung der entsprechenden Weisungen auszusetzen, bis der Auftraggeber sie bestätigt oder ändert.

10 Betroffenenrechte

Wendet sich eine betroffene Person mit Forderungen auf Berichtigung, Löschung oder Auskunft an den Auftragnehmer, wird der Auftragnehmer die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung zum Auftragnehmer nach den Angaben der betroffenen Person möglich ist. Der Auftragnehmer leitet die Anfrage der betroffenen Person unverzüglich an den Auftraggeber weiter. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten auf Weisung, sofern dies vereinbart ist. Der Auftragnehmer haftet nicht, wenn die Anfrage der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht rechtzeitig beantwortet wird.

11 Löschung und Rückgabe personenbezogener Daten

11.1 Kopien oder Duplikate der Daten dürfen ohne Wissen des Auftraggebers niemals erstellt werden, ausgenommen sind Sicherungskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die zur Erfüllung gesetzlicher Aufbewahrungspflichten erforderlich sind.

11.2 Nach Abschluss der vertraglichen Arbeiten oder früher auf Verlangen des Auftraggebers, spätestens jedoch bei Beendigung der Nutzungsbedingungen, übergibt der Auftragnehmer dem Auftraggeber alle in seinen Besitz gelangten, mit dem Vertrag in Zusammenhang stehenden Unterlagen, Verarbeitungs- und Nutzungsergebnisse sowie Datensätze oder vernichtet sie – vorbehaltlich einer vorherigen Zustimmung – auf datenschutzkonforme Weise. Gleiches gilt für sämtliches damit verbundenes Test-, Ausschuss-, Redundanz- und Altmaterial. Das Protokoll der Vernichtung oder Löschung ist auf Anfrage vorzulegen.

11.3 Dokumentationen, die zur Nachweisführung der ordnungsgemäßen Datenverarbeitung gemäß dem Auftrag dienen, bewahrt der Auftragnehmer über die Vertragslaufzeit hinaus entsprechend den jeweiligen Aufbewahrungsfristen auf. Er kann diese Dokumentation am Ende der Vertragslaufzeit dem Auftraggeber übergeben, um den Auftragnehmer von dieser vertraglichen Verpflichtung zu entbinden.

12 Geheimhaltungsvereinbarung

Beide Parteien verpflichten sich, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse über Geschäftsgeheimnisse und Datensicherheitsmaßnahmen der jeweils anderen Partei auch über die Beendigung des Vertrages hinaus vertraulich zu behandeln. Bestehen Zweifel, ob eine Information der Geheimhaltungspflicht unterliegt, ist sie so lange als vertraulich zu behandeln, bis die andere Partei sie schriftlich freigibt.

13 Salvatorische Klausel

Sollten eine oder mehrere Klauseln dieser Vereinbarung ganz oder teilweise unwirksam oder undurchsetzbar sein, so berührt dies die Gültigkeit der übrigen Bestimmungen nicht. Die Parteien werden die unwirksame oder undurchsetzbare Klausel durch eine Regelung ersetzen, die dem Sinn und Zweck der unwirksamen Klausel in zulässiger, wirtschaftlicher und rechtlicher Weise am nächsten kommt. Das Gleiche gilt für etwaige Lücken dieser Vereinbarung.

Einschließlich Anhang 1 „Technische und Organisatorische Maßnahmen“

_____

Datum und Unterschrift des Verantwortlichen (Auftraggeber)

_____

Datum und Unterschrift des Auftragsverarbeiters (Auftragnehmer)

Anhang 1:
Technische und Organisatorische Maßnahmen
gemäß Art. 32 DSGVO

Unternehmen: DEON GmbH & Co. KG
Anschrift: Ella-Kay-Str. 22c, 10405 Berlin
Telefon: +49 30 403 66 77 13
E-Mail: info@deon.de
Internet: https://deon.de

Datum des Inkrafttretens: 01.02.2025

Maßnahme	Zweck	Maßnahmenbeschreibung
Organisatorische Kontrolle	Interne Organisation so strukturieren, dass sie den besonderen Anforderungen des Datenschutzes genügt.	Regelmäßige Verpflichtung der Mitarbeiter auf das Datengeheimnis (mindestens alle zwei Jahre). Regelmäßige Sensibilisierung der Mitarbeiter für Datenschutz am Arbeitsplatz (mindestens einmal jährlich). Vorhandensein eines Datensicherheitskonzepts/Informationssicherheitsmanagements.
Pseudonymisierung (Art. 32 Abs. 1 lit. a) DSGVO)		Personenbezogene Daten mit normalem Schutzbedarf werden in 2 Teile geteilt und somit pseudonymisiert. Personenbezogene Daten mit erhöhtem Schutzbedarf werden in 2 Teile geteilt und somit pseudonymisiert. Verwendung von pseudonymisierten und anonymisierten Daten, wann immer möglich.
Verschlüsselung (Art 32 Abs.1 lit. a) DSGVO)		Verschlüsselung von Festplatten, die personenbezogene Daten enthalten. Verschlüsselung von E-Mails (z. B. PGP).

Maßnahme	Zweck	Maßnahmenbeschreibung
Vertraulichkeit (Art 32 Abs.1 lit. b) DSGVO)		
Zutrittskontrolle	Unbefugten Personen den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, verwehren.	Alle Daten werden in den Rechenzentren von Dienstleistern gespeichert, die eine physische Zutrittskontrolle implementiert haben.
Zugangskontrolle	Verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.	Authentifizierung mit Benutzername und Passwort. Verwaltung von Benutzerberechtigungen. Erstellung von Benutzerprofilen. Einsatz von Anti-Virus-Software. Vergabe von Passwörtern/Passwortregeln. Verwendung von Firewalls. Sofortige Sperrung von Berechtigungen beim Ausscheiden von Mitarbeitern. Sichtschutz für mobile Computer.

Maßnahme	Zweck	Maßnahmenbeschreibung
Zugriffskontrolle	Sicherstellen, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten nur auf die Daten zugreifen können, für die sie eine Berechtigung besitzen, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.	Schriftliches Berechtigungskonzept. Zuweisung von Benutzerrechten/Erstellung von Benutzerprofilen. Rechteverwaltung durch Systemadministrator. Reduzierung der Anzahl der Administratoren auf das lebensnotwendige Minimum. Automatische Sperrung des Arbeitsplatzes. Protokollierung von Softwarezugriffen, insbesondere bei der Eingabe, Änderung und Löschung von Daten. Verwendung von Akten-/Datenträgershreddern. Verschlüsselung von Datenträgern. Ordnungsgemäße Vernichtung von Datenträgern. Löschkonzept für Daten.
Trennungsgebot	Sicherstellen, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.	Konsequente Mandantentrennung (auf Softwareseite). Trennung von Produktions- und Testsystem. Technologie zur Definition von Datenbankrechten. Trennung von Daten verschiedener Auftraggeber.

Maßnahme	Zweck	Maßnahmenbeschreibung
Übertragungskontrolle	Sicherstellen, dass personenbezogene Daten bei der elektronischen Übertragung oder bei ihrem Transport oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Überprüfung und Kontrolle, an welche Stellen personenbezogene Daten durch Datenübertragungseinrichtungen übermittelt werden sollen.	Überwachung des Benutzers und des Zeitpunkts spezifischer Änderungen im System. Organisatorische Vorgaben zur Festlegung der Zuständigkeiten für individuelle Änderungsrechte im System sind dokumentiert. Jeder Mitarbeiter hat den erforderlichen Datenzugriff entsprechend seiner Rolle und zur Erfüllung seines Arbeitsvertrages. Rechte zum Zugriff auf sensible Ressourcen werden umfassend angefordert und von dazu befugten Personen zugewiesen. Es existiert eine Eingabehistorie für alle Benutzer mit Zugriff auf personenbezogene Daten, die überwacht, welche Person welche Aktion zu welchem Zeitpunkt durchgeführt hat, wenn personenbezogene Daten geändert werden.
Integrität (Art 32 Abs.1 lit. b) DSGVO)		
Eingabekontrolle	Sicherstellen, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.	Nachvollziehbarkeit der Eingabe, Änderung und Löschung von Daten durch einzelne Benutzer (nicht Benutzergruppen). Vorhandene Aufbewahrungs-/Löschfrist für Protokolle (Logs).
Dokumentationskontrolle	Sicherstellen, dass die Verfahren zur Verarbeitung personenbezogener Daten so dokumentiert sind, dass sie in zumutbarer Weise reproduzierbar sind.	Implementierung eines Verzeichnisses von Verarbeitungstätigkeiten. Dokumentation der verwendeten IT-Systeme und deren Systemkonfiguration.

Maßnahme	Zweck	Maßnahmenbeschreibung
Kontrolle der Verarbeitung im Auftrag	Sicherstellen, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur gemäß den Weisungen des Auftraggebers verarbeitet werden können.	Vorhandene Verträge zur Verarbeitung im Auftrag. Kontrolle der Vertragsdurchführung. Vernichtung von Daten am Ende des Vertrages. Kontrolle der Wartung (insbesondere Fernwartung). Mitarbeiter mit Zugriffsrechten sind zur Wahrung des Datengeheimnisses verpflichtet. Mitarbeiter haben Arbeitsanweisungen/Richtlinien oder Merkblätter erhalten, die über Maßnahmen zur Einhaltung des Datenschutzes und der IT-Sicherheit informieren. Im Falle von Fehlern bei der Datenverarbeitung oder Verletzung des Datenschutzes wird der Auftraggeber unverzüglich informiert.
Verfügbarkeitskontrolle (Art 32 Abs.1 lit. b) DSGVO)	Sicherstellen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.	Alle Daten werden in den Rechenzentren von Dienstleistern gespeichert, die Maßnahmen zum Schutz gegen zufällige Zerstörung oder Verlust implementiert haben.
Belastbarkeit (Art 32 Abs.1 lit. b) DSGVO)	Sicherstellen, dass die Systeme auch bei unvorhergesehener Überlastung funktionsfähig bleiben.	Speicher-Überreservierung deaktiviert. Festplatten-Überreservierung deaktiviert. Virtuelle Serverumgebung. Automatische Serveralarme an verantwortliche Personen.

Maßnahme	Zweck	Maßnahmenbeschreibung
Wiederherstellbarkeit (Art 32 Abs.1 lit. c) DSGVO)	Sicherstellen, dass personenbezogene Daten nach einem Verstoß wiederhergestellt werden können.	Backup-Konzept. Backups (Beschreibung von Rhythmus, Medium, Speicherdauer und -ort). Vorhandene vollständige Server-Backups. Disaster-Recovery-Konzept. Testen der Datenwiederherstellung. Testen der Server-Wiederherstellung.
Regelmäßiges Testen, Bewerten und Evaluieren (Art 32 Abs.1 lit. d) DSGVO)	Sicherstellen, dass die Verfahren aktuell bleiben und die verwendete technische Ausrüstung dem „Stand der Technik“ entspricht.	Regelmäßige Bewertung der verwendeten Verfahren. Verpflichtung zur Benachrichtigung des Ansprechpartners Datenschutz über neu implementierte Verfahren. Regelmäßige Software-Sicherheitsupdates. Durchführung und Dokumentation von Penetrationstests.

Ergänzende Technische und Organisatorische Maßnahmen für die optionale KI-Integration (OpenAI API, Anthropic API, Gemini API, IONOS AI Model Hub)

(gemäß Art. 28 Abs. 3 lit. c und Art. 32 DSGVO)

Maßnahme	Zweck	Maßnahmenbeschreibung
Datenminimierung (Art. 5 Abs. 1 lit. c DSGVO)	Nur die unbedingt notwendigen personenbezogenen Daten werden übermittelt.	Übermittlung nur der personenbezogenen Daten, die für die spezifische KI-Funktion unbedingt erforderlich sind, an den jeweiligen KI-Anbieter.
Verschlüsselte Übertragung (Art. 32 Abs. 1 lit. a DSGVO)	Schutz der Daten während der Übertragung.	Alle an die KI-Anbieter übermittelten Daten werden über TLS verschlüsselt.
Zugriffskontrolle (Art. 32 Abs. 1 lit. b DSGVO)	Begrenzung der Nutzung auf befugte Personen.	Nur autorisierte Benutzer können auf die KI-Funktionalität zugreifen und diese nutzen. Der Zugriff ist rollenbasiert.
Drittlandgarantien	Sicherstellung eines	Die Datenverarbeitung durch

(Art. 46 Abs. 2 lit. c DSGVO)	angemessenen Schutzniveaus bei Übermittlung in die USA.	OpenAI, L.L.C., Anthropic (Anthropic Ireland, Limited mit Verarbeitung durch Anthropic, PBC) und Google (Google Cloud EMEA Limited mit Verarbeitung auch durch Google LLC), jeweils auch in den USA, basiert auf Standardvertragsklauseln (SCCs), um ein angemessenes Schutzniveau zu gewährleisten. Die IONOS SE verarbeitet die Daten in Deutschland.

Diese Maßnahmen werden regelmäßig überprüft, um die Einhaltung des Stands der Technik, der DSGVO und, soweit relevant, des EU-Gesetzes über künstliche Intelligenz (Verordnung (EU) 2024/1689) sicherzustellen.