Logicc

Auftragsverarbeitungsvertrag (AVV)

Stand: 1. Oktober 2026 · erzeugt am 09. November 2026

Präambel

Diese AVV ergänzt den Rahmenvertrag ("Vertrag") zwischen der Logicc GmbH ("Logicc") und dem Kunden, der auf diese AVV Bezug nimmt (Logicc und der Kunde zusammen die "Parteien"). Diese AVV tritt automatisch mit dem Abschluss des Vertrages in Kraft und gilt ab demselben Datum wie der Vertrag.

Im Rahmen der Erfüllung des Vertrages verarbeitet Logicc die vom Kunden bereitgestellten personenbezogenen Daten. Die Parteien vereinbaren, dass Logicc solche personenbezogenen Daten im Auftrag des Kunden verarbeitet, entweder als Auftragsverarbeiter, wenn der Kunde Verantwortlicher ist, oder als Unterauftragsverarbeiter, wenn der Kunde seinerseits ein Auftragsverarbeiter ist. Daher gilt diese AVV, wenn und soweit Logicc bei der Erbringung von Dienstleistungen im Rahmen des Vertrags personenbezogene Daten für den Kunden verarbeitet. Die Parteien vereinbaren, dass diese AVV alle bestehenden Datenschutzbestimmungen ersetzt, die die Parteien zuvor in Verbindung mit den Dienstleistungen abgeschlossen haben.

1. Definitionen

1.1 "Kundendaten" sind alle personenbezogenen Daten, die im Rahmen der Nutzung der Dienstleistungen hochgeladen, aus verbundenen Drittsystemen abgerufen oder beim Auslösen von Aktionen in diesen Systemen im Auftrag des Kunden verarbeitet werden und die Logicc im Rahmen der Erbringung der Dienstleistungen im Auftrag des Kunden verarbeitet.

1.2 "Verantwortlicher" ist die Person oder Gesellschaft, die die Zwecke und Mittel der Verarbeitung personenbezogener Daten festlegt.

1.3 "Auftragsverarbeiter" ist die Person oder Gesellschaft, die personenbezogene Daten im Auftrag eines für die Datenverarbeitung Verantwortlichen verarbeitet.

1.4 "Datenschutzgesetze" sind alle Datenschutzgesetze, die auf die Verarbeitung personenbezogener Daten anwendbar sind. Für die EU und den EWR umfasst dies insbesondere die Datenschutz-Grundverordnung (DSGVO) und die e-Privacy-Richtlinie 2002/58/EG sowie die lokalen Gesetze der Mitgliedstaaten zum Datenschutz.

1.5 "EWR" ist der Europäischen Wirtschaftsraum.

1.6 "EU" ist die Europäische Union.

1.7 "Personenbezogene Daten" sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.

1.8 "Verarbeitung" hat die in der DSGVO festgelegte Bedeutung und umfasst jeden Vorgang oder jede Reihe von Vorgängen, die mit personenbezogenen Daten durchgeführt werden, wie das Erheben, das Erfassen, die Organisation, die Strukturierung, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung oder das

Löschen von personenbezogenen Daten.

1.9 "Sicherheitsvorfall" ist jede unbefugte oder unrechtmäßige Verletzung der Sicherheit, die zur versehentlichen oder unrechtmäßigen Zerstörung, zum Verlust, zur Änderung, zur unbefugten Offenlegung von oder zum Zugriff auf Kundendaten führt.

1.10 "Dienstleistungen" hat die im Vertrag festgelegte Bedeutung.

1.11 "SCC" sind die im Anhang des Durchführungsbeschlusses (EU) 2021/914 der Kommission vom 4. Juni 2021 enthaltenen Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer.

1.12 "Unterauftragsverarbeiter" ist jeder Auftragsverarbeiter, der von Logicc beauftragt wird, um bei der Erbringung der Dienstleistungen zu unterstützen.

2. Gegenstand dieser AVV

2.1 Diese AVV legt die Rechte und Pflichten der Parteien in Bezug auf die Verarbeitung von Kundendaten durch Logicc im Zusammenhang mit der Erbringung der Dienstleistungen fest.

2.2 Zu diesem Zweck beauftragt der Kunde hiermit Logicc als Auftragsverarbeiter, wenn der Kunde als Verantwortlicher handelt, oder als Unterauftragsverarbeiter, wenn der Kunde seinerseits als Auftragsverarbeiter handelt.

2.3 Diese AVV gilt für alle Kundendaten gemäß Spezifikation in Anlage 1, auf die Logicc während der Erbringung der Dienstleistungen Zugriff hat. Dazu gehören Kundendaten, die Logicc vom Kunden für die Erbringung der Dienstleistungen zur Verfügung gestellt werden, Kundendaten, die von Logicc während der Erbringung der Dienstleistungen generiert werden, oder Kundendaten, auf die Logicc auf andere Weise, z. B. direkt von betroffenen Personen, im Rahmen der Erbringung der Dienstleistungen Zugriff erhält. Diese AVV gilt nicht für Daten, die nicht als Kundendaten gelten, einschließlich nicht personenbezogener Daten, die vom Kunden zur Verfügung gestellt werden, oder Daten, die nicht als Teil der Dienstleistungen verarbeitet werden.

3. Grundsatz der Verarbeitung im Auftrag des Kunden

3.1 Logicc ergreift geeignete technische und organisatorische Maßnahmen, um sicherzustellen, dass die Verarbeitung von Kundendaten den Anforderungen der geltenden Datenschutzgesetze entspricht und die Rechte der betroffenen Personen gewahrt werden.

3.2 Die Verarbeitung von Kundendaten durch Logicc und ggf. beauftragte Unterauftragsverarbeiter erfolgt grundsätzlich im Gebiet des EWR. Übertragungen von Kundendaten in ein Drittland außerhalb des EWR finden nur statt, wenn Logicc die Einhaltung der Anforderungen der geltenden Datenschutzgesetze sicherstellt und wenn solche Übertragungen durch eine geeignete Rechtsgrundlage gestützt werden, wie z. B. einen Angemessenheitsbeschluss, SCC oder andere geltende Garantien.

3.3 Der Kunde ist für die Rechtmäßigkeit der Verarbeitung der Kundendaten sowie für die Wahrung der Rechte der Betroffenen im Verhältnis der Parteien allein verantwortlich. Sollten Dritte gegen Logicc aufgrund der Verarbeitung von Kundendaten nach Maßgabe dieser AVV Ansprüche geltend machen, wird der Kunde Logicc von solchen Ansprüchen freistellen.

4. Weisungsrecht des Kunden

4.1 Die unter diese AVV fallenden Kundendaten werden nur in Übereinstimmung mit dokumentierten

Weisungen des Kunden verarbeitet, einschließlich Weisungen zur Übermittlung von Kundendaten in ein Drittland. Wenn Logicc nach geltendem Recht verpflichtet ist, Kundendaten ohne solche Weisungen zu verarbeiten, wird Logicc den Kunden vor der Verarbeitung über die gesetzliche Verpflichtung informieren, es sei denn, eine solche Mitteilung ist aus Gründen des öffentlichen Interesses gesetzlich verboten.

4.2 Das Weisungsrecht des Kunden hinsichtlich Art, Umfang und Verfahren der Verarbeitung von Kundendaten ist auf den in dieser AVV und im Vertrag festgelegten Umfang beschränkt. Stimmt Logicc einer darüber hinausgehenden Weisung zu, so hat der Kunde Logicc die damit verbundenen Kosten und Aufwendungen zu ersetzen.

4.3 Der Kunde erteilt seine Anweisungen schriftlich, per E-Mail (in Textform) oder über die Nutzung der Funktionalitäten der Dienstleistungen.

4.4 Logicc darf Kundendaten nicht für andere Zwecke als die Erbringung der Dienstleistungen verwenden. Diese Einschränkung gilt nicht für Sicherungskopien, die zur Sicherstellung einer ordnungsgemäßen Verarbeitung erforderlich sind, oder für Daten, die zur Erfüllung gesetzlicher Aufbewahrungspflichten aufbewahrt werden, oder für anonymisierte oder aggregierte Daten, die nicht wieder identifiziert werden können und ausschließlich für interne Geschäftszwecke, wie z. B. Analysen oder Serviceverbesserungen, verwendet werden. Kundendaten sowie daraus gewonnene anonymisierte oder aggregierte Daten werden nicht zum Training von KI-Modellen verwendet.

5. Unterauftragsverarbeiter

5.1 Logicc wird ohne vorherige schriftliche Zustimmung des Kunden, die entweder als Einzelzustimmung oder als generelle Zustimmung erteilt werden kann, keinen Unterauftragsverarbeiter einschalten.

5.2 Der Kunde erteilt hiermit seine Zustimmung zur Beauftragung der in Anlage 2 aufgeführten Unterauftragsverarbeiter mit Wirkung ab dem Datum dieser AVV.

5.3 Der Kunde erteilt hiermit auch seine allgemeine Zustimmung zur Beauftragung weiterer Unterauftragsverarbeiter. Logicc informiert den Kunden mindestens 15 Tage vor der erstmaligen Verarbeitung durch einen neuen Unterauftragsverarbeiter über alle beabsichtigten Änderungen der Liste der Unterauftragsverarbeiter, einschließlich der Hinzufügung oder des Austauschs eines Unterauftragsverarbeiters, und gibt dem Kunden die Möglichkeit, gegen diese Änderungen Einspruch zu erheben. Der Kunde kann aus angemessenen Gründen innerhalb von 15 Tagen nach der Benachrichtigung schriftlich Einspruch erheben, und die Parteien werden nach Treu und Glauben zusammenarbeiten, um den Einspruch zu lösen.

5.4 Beauftragt Logicc einen Unterauftragsverarbeiter mit der Durchführung bestimmter Verarbeitungstätigkeiten im Auftrag des Kunden, so legt Logicc dem Unterauftragsverarbeiter dieselben Datenschutzverpflichtungen auf, wie sie in dieser AVV festgelegt sind. Dies erfolgt durch einen Vertrag oder ein anderes rechtsverbindliches Instrument gemäß den geltenden Datenschutzgesetzen, wobei sichergestellt wird, dass der Unterauftragsverarbeiter ausreichende Garantien bietet, insbesondere die Umsetzung geeigneter technischer und organisatorischer Maßnahmen zur Einhaltung der Anforderungen der DSGVO und anderer geltender Datenschutzgesetze. Die Vertragsparteien stellen klar, dass es ausreicht, wenn das vom Unterauftragsverarbeiter gebotene Schutzniveau dem Schutzniveau gemäß dieser AVV entspricht.

5.5 Unterliegt die Beauftragung von Unterauftragsverarbeitern durch Logicc den Artikeln 44 ff. DSGVO, schließt Logicc, soweit erforderlich, die anwendbaren SCC und stellt sicher, dass seine

Unterauftragsverarbeiter geeignete technische und organisatorische Maßnahmen ergreifen, um die Einhaltung der geltenden Datenschutzgesetze zu gewährleisten.

5.6 Für den Fall, dass die SCC ungültig werden oder anderweitig nicht mehr als gültiger Datenübermittlungsmechanismus unter der DSGVO oder anderen Datenschutzgesetzen anerkannt sind, kann Logicc auf jede alternative Garantie zurückgreifen, die unter den Datenschutzgesetzen zugelassen ist, wie z. B. verbindliche unternehmensinterne Regeln (BCR) oder andere angemessene Schutzmaßnahmen oder Ausnahmen, die unter Kapitel V der DSGVO oder entsprechenden Datenschutzgesetzen zulässig sind.

5.7 Kommt ein Unterauftragsverarbeiter seinen Datenschutzverpflichtungen nicht nach, ist Logicc dem Kunden gegenüber dafür verantwortlich.

5.8 Die Beauftragung eines Dritten mit der Erbringung von Nebenleistungen (z. B. Telekommunikation, Wartung, Benutzerunterstützung, Reinigung, Prüfung oder Entsorgung von Datenträgern) gilt nicht als Beauftragung eines Unterauftragsverarbeiters. Logicc stellt jedoch sicher, dass geeignete rechtliche Vereinbarungen bestehen und Kontrollmaßnahmen ergriffen werden, um die Sicherheit und Vertraulichkeit der Kundendaten zu schützen, wenn Dritte solche Nebenleistungen erbringen.

5.9 Die Anbindung an vom Kunden autorisierte Drittsysteme über offene Schnittstellen (u.a. Model Context Protocol) erfolgt im Auftrag und mit den Zugangsdaten des Kunden. Datenflüsse zwischen der Plattform und dem verbundenen Drittsystem, einschließlich der dort ausgelösten Aktionen, werden vom Kunden angewiesen. Betreiber solcher Drittsysteme sind, soweit der Kunde eigene Vertragsverhältnisse zu ihnen unterhält, nicht Unterauftragsverarbeiter von Logicc. Der Kunde ist für die Rechtmäßigkeit der Verarbeitung in den Drittsystemen sowie für die datenschutzrechtlichen Grundlagen des Zugriffs verantwortlich.

6. Kontrollrechte des Kunden

6.1 Logicc verpflichtet sich, auf schriftliche Anfrage des Kunden innerhalb eines angemessenen Zeitraums die Informationen zur Verfügung zu stellen, die erforderlich sind, um die Einhaltung der Verpflichtungen aus dieser AVV nachzuweisen.

6.2 Der Kunde oder ein vom Kunden beauftragter Prüfer kann die Einhaltung dieser AVV durch Logicc überprüfen. Die Prüfungen werden während der regulären Geschäftszeiten und in einer Weise durchgeführt, die den Betrieb von Logicc so wenig wie möglich stört.

6.3 Logicc kann zum Nachweis der Einhaltung dieser AVV aktuelle Prüfzeugnisse, Berichte oder Auszüge daraus von unabhängigen Stellen (z.B. Wirtschaftsprüfern, Datenschutzbeauftragten, IT-Sicherheitsabteilungen oder Datenschutzauditoren) oder geeignete Zertifizierungen aus anerkannten IT-Sicherheits- oder Datenschutzaudits vorlegen.

7. Verpflichtung zur Vertraulichkeit

Logicc gewährleistet, dass alle Personen, die zur Verarbeitung von Kundendaten im Rahmen dieser AVV berechtigt sind, zur Vertraulichkeit verpflichtet sind, entweder durch vertragliche Verpflichtungen oder durch gesetzliche Verschwiegenheitspflichten.

8. Technische und organisatorische Maßnahmen

8.1 Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, des Kontexts und der Zwecke der Verarbeitung sowie der unterschiedlichen Wahrscheinlichkeit und Schwere von Risiken für die Rechte und Freiheiten der betroffenen Personen

werden sowohl der Kunde als auch Logicc in ihrem jeweiligen Verantwortungsbereich geeignete technische und organisatorische Maßnahmen ergreifen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten, insbesondere im Hinblick auf Sicherheitsvorfälle.

8.2 Die von Logicc getroffenen technischen und organisatorischen Maßnahmen sind in Anlage 3 aufgeführt. Der Kunde bestätigt, dass diese Maßnahmen die Anforderungen erfüllen und ein angemessenes Schutzniveau für die Verarbeitung von Kundendaten gewährleisten.

8.3 Logicc ist jederzeit berechtigt, die technischen und organisatorischen Maßnahmen durch gleich- oder höherwertige Maßnahmen zu ersetzen, sofern diese den Anforderungen der Ziffer 8 genügen.

9. Informationspflichten von Logicc

9.1 Logicc wird den Kunden unverzüglich informieren, wenn Logicc Kenntnis von einem Sicherheitsvorfall erhält.

10. Aufgaben zur Unterstützung des Kunden

10.1 Unter Berücksichtigung der Art der Verarbeitung unterstützt Logicc den Kunden mit angemessenen technischen und organisatorischen Maßnahmen bei der Erfüllung der Verpflichtungen des Kunden zur Beantwortung von Anfragen der betroffenen Personen und anderer Verpflichtungen nach den Datenschutzgesetzen.

10.2 Logicc wird den Kunden unverzüglich informieren, wenn Logicc der Auffassung ist, dass eine vom Kunden erteilte Weisung gegen Datenschutzgesetze verstößt.

11. Laufzeit

11.1 Diese AVV tritt automatisch mit dem Abschluss des Vertrages in Kraft und bleibt mindestens für die Dauer des Vertrages in Kraft, sofern nichts anderes bestimmt ist.

11.2 Eine vorzeitige oder anderweitige Beendigung des Vertrages, gleich aus welchem Grund, hat die automatische Beendigung dieser AVV zur Folge. Die Bestimmungen dieser AVV bleiben jedoch insoweit in Kraft, als dies erforderlich ist, um den ordnungsgemäßen Abschluss der Verarbeitung von Kundendaten im Rahmen dieser AVV in Übereinstimmung mit den Datenschutzgesetzen zu gewährleisten, insbesondere in Bezug auf die Löschung oder Rückgabe von Kundendaten. Sobald eine solche Verarbeitung abgeschlossen ist, endet diese AVV ohne weitere Mitteilung.

12. Verpflichtung zur Löschung und Rückgabe nach Beendigung

Nach Beendigung der Dienstleistungen wird Logicc nach Weisung des Kunden alle Kundendaten entweder löschen oder zurückgeben. Der Kunde muss Logicc innerhalb von 30 Tagen nach Beendigung der Dienstleistungen über seine Wahl informieren. Erfolgt innerhalb dieser Frist keine Mitteilung, kann Logicc die Kundendaten löschen, es sei denn, das geltende Recht schreibt eine weitere Speicherung vor. Aufbewahrungs- und Archivierungspflichten nach geltendem Recht bleiben hiervon unberührt. Logicc wird die Löschung oder Rückgabe auf Anfrage des Kunden bestätigen.

13. Datenschutzbeauftragter

Logicc wird einen Datenschutzbeauftragten bestellen, soweit dies nach den Datenschutzgesetzen erforderlich ist, und dem Kunden in diesem Fall die Kontaktdaten des Datenschutzbeauftragten zur Verfügung stellen.

14. Vergütung

14.1 Alle von Logicc im Rahmen dieser AVV erbrachten Leistungen sind vollständig durch die im Vertrag vereinbarte Vergütung abgegolten, sofern in dieser AVV nicht ausdrücklich etwas anderes bestimmt ist.

14.2 Soweit Leistungen im Rahmen dieser AVV als vergütungspflichtig bezeichnet sind, werden diese Leistungen nach Aufwand zu den im Vertrag vereinbarten Sätzen vergütet. Sind keine Vergütungssätze vereinbart, gelten die zum Zeitpunkt der Leistung gültigen Standardsätze von Logicc.

15. Haftung

15.1 Die Haftungsbestimmungen des Vertrages gelten entsprechend für diese AVV.

15.2 Behördliche Strafen oder Bußgelder, die direkt gegen den Kunden verhängt werden, können von Logicc nicht zurückgefordert werden, es sei denn, sie sind auf einen Verstoß von Logicc gegen diese AVV oder Datenschutzgesetze zurückzuführen. In solchen Fällen ist die Haftung von Logicc auf das Mitverschulden beschränkt, das durch eine rechtskräftige Entscheidung eines zuständigen Gerichts oder einer zuständigen Behörde festgestellt wird, und unterliegt den Haftungsbestimmungen des Vertrags.

16. Schlussbestimmungen

16.1 Diese AVV ist integraler Bestandteil des Vertrages. Im Falle eines Widerspruchs zwischen den Bestimmungen des Vertrages und dieser AVV haben die Bestimmungen dieser AVV ausschließlich in Bezug auf die Verarbeitung von Kundendaten Vorrang.

16.2 Logicc behält sich das Recht vor, diese AVV bei Bedarf zu ändern, um Änderungen der geltenden Datenschutzgesetze, regulatorischen Anforderungen oder verbindlichen Entscheidungen der zuständigen Aufsichtsbehörden Rechnung zu tragen. Logicc wird den Kunden mindestens 30 Tage im Voraus schriftlich oder in Textform (z.B. per E-Mail) über solche Änderungen informieren, es sei denn, eine sofortige Änderung ist gesetzlich oder regulatorisch vorgeschrieben. Widerspricht der Kunde solchen Änderungen aus berechtigten Gründen, werden die Parteien nach Treu und Glauben zusammenarbeiten, um eine für beide Seiten akzeptable Lösung zu finden. Widerspricht der Kunde solchen Änderungen und wird innerhalb einer angemessenen Frist keine einvernehmliche Lösung erzielt, kann der Kunde den Vertrag in Bezug auf die betroffenen Verarbeitungstätigkeiten durch schriftliche Mitteilung kündigen.

16.3 Sollte eine Bestimmung dieser AVV ganz oder teilweise unwirksam oder undurchführbar sein oder werden, so wird dadurch die Wirksamkeit der übrigen Bestimmungen dieser AVV nicht berührt. Das Gleiche gilt, wenn und soweit sich eine Lücke in dieser AVV zeigt. Anstelle der unwirksamen oder undurchführbaren Bestimmung oder zur Ausfüllung der Lücke soll eine angemessene Regelung gelten, die, soweit rechtlich möglich, dem am nächsten kommt oder entspricht, was die Parteien wirtschaftlich gewollt haben oder nach dem Sinn und Zweck dieser AVV gewollt hätten, sofern sie diesen Punkt bedacht hätten.

16.4 Im Übrigen gelten die Schlussbestimmungen des Vertrages entsprechend für diese AVV.

Anlage 1: Details der Verarbeitung

1. Kategorien von betroffenen Personen

- Nutzer der Dienstleistungen
- Mitarbeiter des Kunden

- Personen, auf die sich Daten beziehen, die von Nutzern eingegeben, aus verbundenen Drittsystemen abgerufen oder beim Auslösen von Aktionen im Auftrag des Kunden verarbeitet werden

2. Arten von Kundendaten

- Namen, E-Mailadressen von Nutzern und Mitarbeitern des Kunden
- Daten, die von den Nutzern eingegeben werden
- Personenbezogene Daten, die aus vom Kunden autorisierten Drittsystemen abgerufen oder beim Auslösen von Aktionen in diesen Systemen im Auftrag des Kunden verarbeitet werden

3. Umfang und Art der Verarbeitung

- Kommunikationsinhalte mit LLMs
- Dokumente und Informationen, die der Kunde auf der Plattform hochlädt und speichert
- Datenabrufe aus vom Kunden autorisierten Drittsystemen über offene Schnittstellen (u.a. Model Context Protocol)
- Übermittlung und Verarbeitung von Kundendaten beim Auslösen von Aktionen in verbundenen Drittsystemen im Auftrag des Kunden im Rahmen der vom Kunden erteilten Berechtigungen

4. Zweck der Verarbeitung

- Bereitstellung der Dienstleistungen gemäß den Anweisungen des Kunden, einschließlich Datenabrufen aus verbundenen Drittsystemen und Auslösen von Aktionen in diesen Systemen im Auftrag des Kunden

Anlage 2: Unterauftragsverarbeiter

Name: Microsoft Ireland Operations Limited
Adresse: The Atrium Building, Block B, Carmanhall Road, Sandyford Business Estate, Dublin 18, Ireland
Aufgabe: Bereitstellung von Cloud-Infrastruktur und LLM-Modellen via Azure OpenAI Service zur Verarbeitung von Nutzeranfragen (Input) und Generierung von Modellantworten (Output)
Ort der Verarbeitung: EU

Name: Hetzner Online GmbH
Adresse: Industriestr. 25, 91710 Gunzenhausen, Deutschland
Aufgabe: Bereitstellung von Cloud-Infrastruktur für das Hosting der Plattform
Ort der Verarbeitung: Deutschland

Name: Google Ireland Limited
Adresse: Gordon House, Barrow Street, Dublin 4, Irland
Aufgabe: Bereitstellung von Cloud-Infrastruktur zur Verarbeitung von Nutzeranfragen (Input) und Generierung von Modellantworten (Output)
Ort der Verarbeitung: EU

Name: Amazon Web Services EMEA SARL
Adresse: 38 avenue John F. Kennedy, L-1855, Luxemburg
Aufgabe: Bereitstellung von Cloud-Infrastruktur, einschließlich Infrastruktur zur Verarbeitung von Nutzeranfragen (Input) und Generierung von Modellantworten (Output)
Ort der Verarbeitung: EU

Name: Mistral AI SAS
Adresse: 15 rue des Halles, F-75001 Paris

Aufgabe: Bereitstellung von Cloud-Infrastruktur zur Verarbeitung von Nutzeranfragen (Input) und Generierung von Modellantworten (Output)
Ort der Verarbeitung: EU

Name: Cloudflare Inc.
Adresse: 101 Townsend Street, San Francisco, California 94107, United States
Aufgabe: Bereitstellung von DDoS-Schutz, Web Application Firewall (WAF) und Content Delivery Network (CDN)
Ort der Verarbeitung: Ort der Nutzung ist Ort der Verarbeitung
Garantie gemäß Art. 44 ff. DSGVO: Standardvertragsklauseln (SCC) gemäß Art. 46 Abs. 2 lit. c DSGVO sowie ergänzende Schutzmaßnahmen

Name: Stripe Payments Europe, Limited (SPEL)
Adresse: 1 Grand Canal Street Lower, Grand Canal Dock, Dublin, D02 H210, Irland
Aufgabe: Abwicklung und Verwaltung von Zahlungsvorgängen
Ort der Verarbeitung: EU

Name: Clerk, Inc.
Adresse: 660 King Street, Unit 345, San Francisco, CA 94107, USA
Aufgabe: Authentifizierung und Autorisierung von Nutzern der Plattform
Ort der Verarbeitung: Vereinigte Staaten
Garantie gemäß Art. 44 ff. DSGVO: EU-U.S. Data Privacy Framework (DPF) sowie Standardvertragsklauseln (SCC) als Fallback.

Name: Linkup Technologies SAS
Adresse: 28 avenue des Pépinières, 94260 Fresnes, Frankreich
Aufgabe: Bereitstellung einer Web-Suchfunktion für KI-Anwendungen zur Anreicherung von Antworten mit aktuellen Informationen.
Ort der Verarbeitung: EU

Name: OpenAI Ireland Ltd.
Adresse: 1st Floor, The Liffey Trust Centre 117-126 Sheriff Street Upper Dublin 1, D01 YC43 Ireland
Aufgabe: Bereitstellung von LLM-Modellen zur Verarbeitung von Nutzeranfragen (Input) und Generierung von Modellantworten (Output)
Ort der Verarbeitung: EU

Anlage 3: Technische und organisatorische Maßnahmen

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Wahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der betroffenen Personen hat Logicc angemessene technische und organisatorische Sicherheitsmaßnahmen ergriffen und wird diese beibehalten, um die Kundendaten vor Sicherheitsvorfällen zu schützen und die Sicherheit und Vertraulichkeit der Kundendaten zu wahren ("technische und organisatorische Maßnahmen"). Diese Maßnahmen beinhalten folgende Aspekte:

1. Vertraulichkeit

1.1 Zutrittskontrolle

Logicc betreibt keine eigenen Rechenzentren oder Serverräume. Die Anwendung wird auf Cloud-Infrastruktur in ISO/IEC 27001-zertifizierten Rechenzentren betrieben. Die physische Zutrittskontrolle der Rechenzentren wird durch die Hosting-Anbieter gemäß deren vertraglich vereinbarten technischen und organisatorischen Maßnahmen gewährleistet. Für die Geschäftsräume von Logicc gelten folgende Maßnahmen:

- Digitales Zutrittskontrollsystem mit individuellen Zutrittsberechtigungen für Mitarbeiter.
- Authentisierung mittels persönlichem Zugangscode oder biometrischem Faktor.
- Protokollierung von Zutrittsereignissen.
- Vergabe und Entzug von Zutrittsberechtigungen entsprechend der betrieblichen Erforderlichkeit.
- Besucher und externe Dienstleister werden nur durch berechtigte Mitarbeiter eingelassen und dürfen sich in nicht öffentlich zugänglichen Bereichen nicht unbeaufsichtigt aufhalten.

1.2 Zugangskontrolle

Logicc wird angemessene Maßnahmen treffen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

- Technische Maßnahmen:
- Verwendung individueller Benutzerkonten und starker, eindeutiger Authentisierungsmerkmale.
- Einsatz von Multi-Faktor-Authentifizierung oder Passkeys, soweit dies technisch unterstützt wird und insbesondere für privilegierte oder sicherheitsrelevante Zugänge.
- Verwendung eines zentral freigegebenen Passwortmanagements zur Erzeugung und sicheren Speicherung eindeutiger Zugangsdaten.
- Änderung von Zugangsdaten bei bekannt gewordener oder vermuteter Kompromittierung sowie bei sonstigem sicherheitsbezogenem Anlass.
- Automatische Sperrung inaktiver Sitzungen nach einem definierten Zeitraum.
- Zentrale Verwaltung der von Logicc bereitgestellten Endgeräte zur Durchsetzung und Überwachung von Sicherheitskonfigurationen, Betriebssystemaktualisierungen und Gerätekonformität.
- Vollständige Festplattenverschlüsselung der von Logicc bereitgestellten Endgeräte.
- Verwaltung von Benutzerberechtigungen.
- Organisatorische Maßnahmen:
- IT-Sicherheitsrichtlinie, die den sicheren Umgang mit Passwörtern, Zugangsdaten und mobilen Geräten regelt.
- Nutzung von Logicc bereitgestellter und zentral verwalteter Endgeräte durch Mitarbeiter für die Verarbeitung von Kundendaten.
- Vergabe von Benutzerkonten nach dem Prinzip der minimalen Rechtevergabe.
- Regelmäßige Sicherheitsschulungen für Mitarbeiter, um das Bewusstsein für Phishing und andere Bedrohungen zu schärfen.

1.3 Zugriffskontrolle

Logicc wird angemessene Maßnahmen treffen, um sicherzustellen, dass die zur Benutzung der Datenverarbeitungssysteme Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können, und dass Kundendaten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Hierzu trifft Logicc folgende Vorkehrungen:

- Technische Maßnahmen:
- Implementierung eines differenzierten Berechtigungskonzepts, das den Zugriff auf Kundendaten auf das notwendige Minimum beschränkt.
- Einsatz von Netzwerk- und Anwendungsfiltern, einschließlich einer Web Application Firewall für öffentlich erreichbare Anwendungsendpunkte.

- Umfassende Protokollierung aller Zugriffe auf Kundendaten in manipulationssicheren Audit-Logs nach festgelegten Aufbewahrungsfristen.
- Gesonderte Protokollierung sicherheitsrelevanter Datenbankzugriffe.
- Administrativer Zugriff auf die Hosting-Infrastruktur ausschließlich über verschlüsselte und zugangsgeschützte Verbindungen.
- Zentrale, verschlüsselte Verwaltung von Produktionsgeheimnissen und kryptografischen Schlüsseln; Zugriffe und Bereitstellung werden auf die jeweils erforderlichen Personen und Dienste beschränkt.
- Verschlüsselung von Kundendaten im Ruhezustand unter Verwendung starker, dem Stand der Technik entsprechender Verschlüsselungsverfahren.
- Organisatorische Maßnahmen:
- Richtlinie zur Vergabe und Entziehung von Zugriffsrechten, die sich am "Need-to-know"-Prinzip orientiert.
- Regelmäßige und anlassbezogene Überprüfung von Zugriffsberechtigungen, insbesondere für privilegierte Zugänge.
- Besondere Autorisierung für den Zugriff auf besonders sensible Datenkategorien.
- Beschränkung privilegierter Zugriffe auf einen kleinen, betrieblich erforderlichen Personenkreis nach dem Prinzip der minimalen Rechtevergabe.
- Mitarbeiter, die bei ihrer Tätigkeit Kenntnis von Kundendaten erlangen können, werden vor dem Zugriff in Textform zur Vertraulichkeit und zur Wahrung fremder Geheimnisse gemäß § 203 StGB verpflichtet.

1.4 Trennungskontrolle

Logicc wird angemessene Maßnahmen treffen, um sicherzustellen, dass zu unterschiedlichen Zwecken erhobene Kundendaten getrennt verarbeitet werden können. Hierzu trifft Logicc folgende Vorkehrungen:

- Technische Maßnahmen:
- Strikte logische Mandantentrennung innerhalb der zentralen Datenbank durch den Einsatz von Row-Level Security (RLS).
- Sicherstellung der Mandantentrennung auf Anwendungsebene, um den Zugriff auf Daten anderer Mandanten zu unterbinden.
- Getrennte Umgebungen für Entwicklung, Tests und Produktion.
- Ein differenziertes Berechtigungskonzept, das den Zugriff regelt.
- Organisatorische Maßnahmen:
- Richtlinie zur Datenklassifizierung und zur getrennten Verarbeitung von Daten verschiedener Mandanten und Zwecke.
- Regelmäßige Kontrolle der technischen und organisatorischen Maßnahmen zur Datentrennung.

2. Integrität

2.1 Weitergabekontrolle

Logicc wird angemessene Maßnahmen treffen, um das Risiko zu reduzieren, dass Kundendaten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger unbefugt gelesen, kopiert, verändert oder entfernt werden können. Hierzu trifft Logicc folgende Vorkehrungen:

- Technische Maßnahmen:

- Konsequente Verschlüsselung sämtlicher Übertragungen von Kundendaten über externe oder öffentliche Netze unter Verwendung von mindestens TLS 1.3.
- Nutzung freigegebener, zugangsgeschützter Übertragungswege und Cloud-Dienste für den Austausch und die Bereitstellung von Kundendaten.
- Organisatorische Maßnahmen:
- Richtlinie zur sicheren Übertragung und Weitergabe von Kundendaten, die die Nutzung unsicherer Kanäle untersagt.
- Sensibilisierung der Mitarbeiter für die Risiken unsicherer Datenübertragung.
- Klare Regelungen zur Nutzung von Cloud-Diensten und zur Übermittlung von Daten an Dritte.
- Dokumentierte Übersicht über regelmäßige Abruf- und Übermittlungsverfahren.

2.2 Eingabekontrolle

Logicc wird angemessene Maßnahmen treffen, um sicherzustellen, dass nachträglich geprüft und festgestellt werden kann, ob und von wem Kundendaten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Hierzu trifft Logicc folgende Vorkehrungen:

- Technische Maßnahmen:
- Umfassende Protokollierung aller Eingaben, Änderungen und Löschungen von Kundendaten in manipulationssicheren Audit-Logs nach festgelegten Aufbewahrungsfristen.
- Gesonderte Protokollierung sicherheitsrelevanter Datenbankzugriffe.
- Plausibilitäts- und Validierungsprüfungen bei der Dateneingabe.
- Nachvollziehbarkeit von Änderungen durch Zeitstempel oder Versionierung, soweit dies für den jeweiligen Verarbeitungsvorgang technisch vorgesehen ist.
- Organisatorische Maßnahmen:
- Klare Zuständigkeiten für die Dateneingabe und -pflege.
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf der Grundlage eines Berechtigungskonzepts.
- Regelmäßige und anlassbezogene Überprüfung sicherheitsrelevanter Protokolle.

3. Verfügbarkeit und Belastbarkeit

Logicc wird angemessene Maßnahmen treffen, um sicherzustellen, dass Kundendaten gegen zufällige Zerstörung oder Verlust geschützt sind. Hierzu trifft Logicc folgende Vorkehrungen:

- Technische Maßnahmen:
- Hosting der Anwendung und Kundendaten in ISO/IEC 27001-zertifizierten Rechenzentren.
- Tägliche Sicherung produktiver Kundendaten sowie der für den sicheren Betrieb erforderlichen Systeme und Konfigurationen.
- Speicherung der Sicherungen innerhalb der Europäischen Union und Verschlüsselung mit AES-256.
- Reguläre Aufbewahrung der Sicherungen für 14 Tage; gelöschte Sicherungen bleiben durch eine Soft-Delete-Funktion für 90 Tage wiederherstellbar.
- Gelöschte Sicherungen werden während der Soft-Delete-Frist ausschließlich für Zwecke der Notfallwiederherstellung vorgehalten, nicht produktiv genutzt und nach Ablauf der Frist automatisch endgültig gelöscht.
- Überwachung der Sicherungsprozesse sowie regelmäßige Kontrolle und Dokumentation der Sicherungsergebnisse.

- Regelmäßige und anlassbezogene Tests der Wiederherstellbarkeit von Sicherungen, mindestens einmal pro Quartal.
- Technische Maßnahmen zur Erkennung und Abwehr von Schadsoftware und sonstigen Sicherheitsbedrohungen.
- Physische Schutz- und Redundanzmaßnahmen der Rechenzentrumsbetreiber, insbesondere für Stromversorgung, Klimatisierung, Brandschutz und Speichersysteme.
- Organisatorische Maßnahmen:
- Dokumentiertes Sicherungs- und Wiederherstellungskonzept, das sich an der Kritikalität der Daten und Systeme orientiert und Verantwortlichkeiten, Eskalationswege sowie automatisierungsunterstützte Wiederherstellungsschritte festlegt.
- Notfallpläne für relevante Ausfallszenarien, die regelmäßig überprüft, aktualisiert und erprobt werden.
- Benannte interne Verantwortliche für Notfälle, technische Sicherheitsvorfälle und erforderliche Wiederherstellungsmaßnahmen.
- Nutzung der vertraglich vereinbarten Standardverfügbarkeiten und Supportleistungen der Hosting-Anbieter.
- Informationssicherheitsrichtlinie mit Vorgaben zur Verfügbarkeit, Wiederherstellung und zum Notfallbetrieb.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Logicc implementiert Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

4.1 Datenschutz-Management

- Es wurde ein externer Datenschutzbeauftragter bestellt. Dieser wird durch den Geschäftsführer und einen dedizierten Mitarbeiter, die als interne Datenschutzkoordinatoren fungieren, bei der Umsetzung der Datenschutzmaßnahmen im Unternehmen unterstützt.
- Implementierung eines Datenschutz-Managementsystems (DSMS) in Anlehnung an bewährte Standards (z.B. ISO 27701, BSI IT-Grundschutz), angepasst an die Größe und Komplexität des Unternehmens.
- Regelmäßige interne Überprüfungen der Datenschutzmaßnahmen und -prozesse, mindestens einmal jährlich.
- Dokumentation und Bearbeitung von Datenschutzvorfällen gemäß einem definierten internen Prozess.
- Regelmäßige Schulungen der Mitarbeiter zum Datenschutz, mindestens einmal jährlich.
- Prozesse bezüglich Informationspflichten gemäß Artikel 13 und 14 DSGVO umgesetzt.
- Formalisiertes Verfahren für Auskunftsersuchen von betroffenen Personen eingerichtet.
- Datenschutz-Checkpoints, soweit möglich und sinnvoll, in die Risikobewertung integriert.
- Datenschutz-Folgenabschätzung (DSFA) wird bei Bedarf für neue Verarbeitungstätigkeiten mit voraussichtlich hohem Risiko durchgeführt.
- Datenschutzaspekte sind Teil des allgemeinen Risikomanagements des Unternehmens.

4.2 Incident-Response-Management

- Einsatz eines auf technische Fehler- und Performanceinformationen beschränkten Monitorings mit Maßnahmen zur Vermeidung der Erfassung von Prompts, Modellantworten, Dokumentinhalten, Authentifizierungstoken und vollständigen Request-Bodies.
- Dokumentierter Incident-Response-Prozess für die Erkennung, Meldung, Analyse, Reaktion und Nachbereitung von Sicherheitsvorfällen und Datenschutzverletzungen, einschließlich der Prüfung gesetzlicher Meldepflichten.
- Benannte interne Incident-Response-Gruppe und Einbindung der technischen Leitung in die Koordination und Bearbeitung von Sicherheitsvorfällen und Datenschutzverletzungen.
- Zentrale Dokumentation und Nachverfolgung von Sicherheitsvorfällen und Datenschutzverletzungen.
- Einsatz einer Web Application Firewall zum Schutz öffentlich erreichbarer Anwendungsendpunkte.
- Nutzung zentraler Spam-, Phishing- und Malware-Schutzmechanismen für die geschäftliche E-Mail-Kommunikation.
- Regelmäßige Schulung der Mitarbeiter im Umgang mit Sicherheitsvorfällen und Phishing-Versuchen.
- Regelmäßige Überprüfung und Weiterentwicklung des Incident-Response-Verfahrens.

4.3 Sichere Softwareentwicklung und Schwachstellenmanagement

- Geschützte Entwicklungszweige sowie geregelte Merge-, Freigabe- und Release-Prozesse für Änderungen am Anwendungscode.
- Prüfung von Änderungen in einer vom Produktivbetrieb getrennten Testumgebung vor der Produktivsetzung.
- In den Entwicklungsprozess integrierte sowie regelmäßig ausgeführte Sicherheits-, Abhängigkeits- und Schwachstellenscans.
- Festgestellte Schwachstellen werden nach Schweregrad und tatsächlicher Betroffenheit priorisiert und zeitnah behoben.