

Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 DS-GVO

1. Vertragsparteien

Die Auftragsverarbeitungsvereinbarung besteht zwischen

Name:

Straße und Hausnummer:

PLZ und Ort:

– Verantwortlicher – (nachfolgend „Auftraggeber“)

und

SYNQONY Leer GmbH

Reimersstraße 41b

26789 Leer

– Auftragsverarbeiter – (nachfolgend „Auftragnehmer“).

2. Gegenstand und Dauer der Verarbeitung

Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers im Rahmen der Bereitstellung und des Betriebs des KI-gestützten Voicebots Qonny. Qonny nimmt eingehende Telefonanrufe automatisiert entgegen, erkennt Anliegen und verarbeitet sie. Personenbezogene Daten werden insbesondere dann verarbeitet, wenn Anrufer sie zur Verfügung stellen und sie zur Bearbeitung der Anfrage weitergegeben werden. Ferner kann es bei Fernwartungen, Fehleranalysen oder Datenübernahmen erforderlich sein, dass personenbezogene Daten eingesehen werden; dies geschieht nur in enger Absprache mit dem Auftraggeber.

Der Auftrag umfasst:

- Bereitstellung und Hosting des KI-Voicebots Qonny (Cloud-basiert)
- Verarbeitung von Sprachdaten (Transkription, Sprachsynthese, KI-gestützte Verarbeitung)
- Anbindung an kundenseitige Systeme (z. B. CRM, Ticketsysteme, Datenbanken) über kundenspezifische Schnittstellen
- Fernwartung
- Fehleranalysen
- Datenübernahmen (nur bei Beauftragung durch den Auftraggeber)

Die Dauer der Verarbeitung entspricht der Laufzeit der jeweiligen Leistungsvereinbarung beziehungsweise der bestehenden Geschäftsbeziehung. Sie beginnt mit deren Wirksamwerden und endet mit deren Beendigung; einer gesonderten Kündigung bedarf es hierfür nicht.

Der Auftraggeber kann diese Vereinbarung jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder gegen die Bestimmungen dieser Vereinbarung vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert. Insbesondere die Nichteinhaltung der in dieser Vereinbarung vereinbarten und aus Art. 28 DS-GVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

Bei Widersprüchen zwischen dieser Vereinbarung und der Leistungsvereinbarung gehen die Regelungen dieser Vereinbarung in datenschutzrechtlicher Hinsicht vor.



3. Art, Zweck und Umfang der Verarbeitung

Art, Zweck, Umfang und Ort der Verarbeitung ergeben sich aus der jeweiligen Leistungsvereinbarung sowie aus Anlage 1 zu dieser Vereinbarung.

Die Kategorien personenbezogener Daten sowie die betroffenen Personengruppen ergeben sich ebenfalls aus Anlage 1. Dort sind auch die Speicher- und Löschregelungen für den laufenden Betrieb ausgewiesen.

Keine automatisierte Entscheidung im Einzelfall

Qonny trifft keine ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidungen, die gegenüber betroffenen Personen rechtliche Wirkung entfalten oder sie in ähnlicher Weise erheblich beeinträchtigen (Art. 22 DS-GVO). Von Qonny angestoßene Aktionen in angebundenen Systemen entfalten entweder keine derartige Wirkung oder unterliegen einer menschlichen Prüfung beim Auftraggeber.

Keine Nutzung zu Trainingszwecken

Die im Auftrag verarbeiteten personenbezogenen Daten werden weder vom Auftragnehmer noch von den in Anlage 3 genannten Unterauftragsverarbeitern zum Training, zur Entwicklung oder zur Verbesserung von KI-Modellen oder sonstigen Diensten genutzt. Der Auftragnehmer stellt dies gegenüber den Unterauftragsverarbeitern vertraglich oder durch entsprechende Konfiguration sicher.

4. Technische und organisatorische Maßnahmen

Der Auftragnehmer trifft geeignete technische und organisatorische Maßnahmen gemäß Art. 32 DS-GVO, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

Diese Maßnahmen sind in Anlage 2 beschrieben und Bestandteil dieser Vereinbarung. Der Auftragnehmer überprüft die Maßnahmen regelmäßig und passt sie an den Stand der Technik an, wobei das vereinbarte Sicherheitsniveau nicht unterschritten wird.

Der Auftragnehmer setzt zudem technische und organisatorische Maßnahmen um, die die in Kapitel III der DS-GVO genannten Rechte der betroffenen Personen wahren (Art. 28 Abs. 3 Satz 2 lit. e DS-GVO).

Der Auftragnehmer führt bei gegebenem Anlass, mindestens aber jährlich, eine Überprüfung, Bewertung und Evaluation der Wirksamkeit der Maßnahmen durch (Art. 32 Abs. 1 lit. d DS-GVO). Das Ergebnis ist zu dokumentieren und dem Auftraggeber auf Verlangen mitzuteilen.

Für die Sicherheit erhebliche Entscheidungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren sind zwischen den Vertragsparteien abzustimmen. Soweit die beim Auftragnehmer getroffenen Maßnahmen den Anforderungen des Auftraggebers nicht genügen, benachrichtigt der Auftragnehmer den Auftraggeber unverzüglich.

Wesentliche Änderungen der Maßnahmen sind mit dem Auftraggeber in dokumentierter Form (schriftlich, elektronisch) abzustimmen. Solche Abstimmungen sind für die Dauer dieser Vereinbarung aufzubewahren.

5. Weisungsbindung des Auftraggebers

Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich auf Weisung des Auftraggebers, auch in Bezug auf eine Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation. Mündliche Weisungen sind unverzüglich schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

Ist der Auftragnehmer der Auffassung, dass eine Weisung des Auftraggebers gegen datenschutzrechtliche Vorschriften verstößt, weist er den Auftraggeber unverzüglich hierauf hin (Art. 28 Abs. 3 Satz 3 DS-GVO). Er



ist berechtigt, die Durchführung der Weisung auszusetzen, bis sie durch den Auftraggeber nach Überprüfung bestätigt oder geändert wird.

Ist der Auftragnehmer aufgrund des Rechts der Europäischen Union oder der Mitgliedstaaten zu einer Verarbeitung verpflichtet, informiert er den Auftraggeber hierüber vor der Verarbeitung, sofern das betreffende Recht eine solche Mitteilung nicht untersagt.

Der Auftragnehmer verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt; hiervon ausgenommen sind Sicherungskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten zur Erfüllung gesetzlicher Aufbewahrungspflichten. Der Auftragnehmer sichert zu, dass die für den Auftraggeber verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.

Der Auftragnehmer berichtigt, löscht oder schränkt die Verarbeitung personenbezogener Daten ein, wenn der Auftraggeber dies mittels einer Weisung verlangt und berechnete Interessen des Auftragnehmers dem nicht entgegenstehen, oder wenn der Weisung ein berechtigter Anspruch der betroffenen Person aus den Art. 16, 17 und 18 DS-GVO zugrunde liegt.

Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder an die betroffene Person erteilt der Auftragnehmer nur nach vorheriger Weisung oder Zustimmung des Auftraggebers.

Weisungsberechtigte des Auftraggebers

Die weisungsberechtigten Personen oder Funktionen des Auftraggebers werden von dem Auftraggeber umgehend nach Abschluss dieser Vereinbarung durch einen Geschäftsführer oder eine vergleichbare Position mitgeteilt. Solange diese Mitteilung nicht erfolgt ist, sieht der Auftragnehmer die Geschäftsführer oder vergleichbare Positionen beim Auftraggeber als weisungsberechtigt an.

Weisungsempfänger beim Auftragnehmer

Der Abteilungsleiter Customer Support oder nach Absprache definierte Personen oder Personenkreise.

Für Weisungen zu nutzende Kommunikationskanäle

- Serviceportal unter <https://service.synqony.com>
- Postalisch an: SYNQONY Leer GmbH, Reimersstraße 41b, 26789 Leer

Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem jeweils anderen Vertragspartner unverzüglich und grundsätzlich schriftlich oder in einem dokumentierten elektronischen Format die Nachfolger beziehungsweise die Vertreter mitzuteilen. Die Weisungen sind für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

Pflichten des Auftraggebers

Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DS-GVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DS-GVO ist allein der Auftraggeber verantwortlich. Gleichwohl ist der Auftragnehmer verpflichtet, alle solche Anfragen, sofern sie erkennbar ausschließlich an den Auftraggeber gerichtet sind, unverzüglich an diesen weiterzuleiten.

Der Auftraggeber stellt sicher, dass die betroffenen Personen in der nach den Art. 12 bis 14 DS-GVO erforderlichen Weise über den Einsatz von Qonny informiert werden, einschließlich der Interaktion mit einem KI-System und einer etwaigen Transkription des Gesprächs. Der Auftragnehmer stellt dem Auftraggeber die hierfür erforderlichen Informationen zur Verfügung.



Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format festzulegen. Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieser Vereinbarung bestehen.

6. Vertraulichkeit

Der Auftragnehmer stellt sicher, dass alle zur Verarbeitung befugten Personen zur Vertraulichkeit verpflichtet sind oder einer gesetzlichen Verschwiegenheitspflicht unterliegen.

Der Auftragnehmer stellt ferner sicher, dass diese Personen nur im Rahmen der Weisungen des Auftraggebers Zugang zu personenbezogenen Daten erhalten (Art. 29, Art. 32 Abs. 4 DS-GVO).

Der Auftragnehmer macht die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut und verpflichtet sie für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigungsverhältnisses in geeigneter Weise zur Verschwiegenheit (Art. 28 Abs. 3 Satz 2 lit. b und Art. 29 DS-GVO). Er überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb.

Die Vertraulichkeitspflicht des Auftragnehmers besteht auch nach Beendigung dieser Vereinbarung fort.

Der Auftragnehmer hat einen Beauftragten für den Datenschutz bestellt. Die Kontaktinformationen sind auf der Homepage des Auftragnehmers veröffentlicht. Ein Wechsel des Datenschutzbeauftragten sowie eine Änderung seiner Kontaktdaten sind dem Auftraggeber unverzüglich mitzuteilen.

Unterliegt der Auftraggeber besonderen Geheimhaltungspflichten, insbesondere dem Berufsgeheimnis nach § 203 StGB, dem Sozialgeheimnis nach § 35 SGB I und § 80 SGB X oder dem Bankgeheimnis, so teilt er dies dem Auftragnehmer mit; der Auftragnehmer beachtet diese Pflichten im Rahmen der Auftragsverarbeitung und verpflichtet die mit der Verarbeitung befassten Personen entsprechend. Soweit der Auftragnehmer bei der Bereitstellung der Telefonieverbindung dem Fernmeldegeheimnis nach § 3 TDDDG unterliegt, wahrt er dieses.

Die Verarbeitung personenbezogener Daten in Privatwohnungen (Telearbeit beziehungsweise Homeoffice von Beschäftigten des Auftragnehmers) ist nur zulässig, wenn die technischen und organisatorischen Maßnahmen nach Art. 32 DS-GVO und nach Anlage 2 auch dort sichergestellt sind und die Möglichkeit zur Kontrolle durch den Auftragnehmer vertraglich gewährleistet ist. Der Auftraggeber erteilt hierzu mit Abschluss dieser Vereinbarung seine Zustimmung; er kann sie aus wichtigem datenschutzbezogenem Grund widerrufen.

Der Auftragnehmer informiert den Auftraggeber unverzüglich über den Ausschluss von genehmigten Verhaltensregeln nach Art. 41 Abs. 4 DS-GVO sowie über den Widerruf einer Zertifizierung nach Art. 42 Abs. 7 DS-GVO, soweit einschlägig.

7. Unterauftragsverarbeiter

Der Einsatz von Unterauftragsverarbeitern erfolgt nur mit vorheriger allgemeiner Genehmigung des Auftraggebers (Art. 28 Abs. 2 Satz 2 DS-GVO). Die eingesetzten Unterauftragsverarbeiter sind der Anlage 3 zu entnehmen; mit deren Beauftragung erklärt sich der Auftraggeber einverstanden.

Der Auftragnehmer informiert den Auftraggeber mindestens 14 Kalendertage vor Wirksamwerden über beabsichtigte Änderungen hinsichtlich der Hinzuziehung oder Ersetzung von Unterauftragsverarbeitern unter Angabe von Name, Anschrift, vorgesehener Tätigkeit, Verarbeitungsort und – bei einer Verarbeitung in einem Drittland – der Grundlage der Übermittlung nach Kapitel V DS-GVO. Er räumt dem Auftraggeber die



Möglichkeit zum Widerspruch innerhalb von 14 Kalendertagen ab Mitteilung ein, soweit nachweisbar begründete Bedenken hinsichtlich der technischen und organisatorischen Maßnahmen des Unterauftragsverarbeiters bestehen. In einem solchen Fall steht dem Auftraggeber ein Sonderkündigungsrecht zu.

Der Auftragnehmer stellt sicher, dass die in dieser Auftragsverarbeitungsvereinbarung getroffenen Regelungen einschließlich der Anforderungen aus Anlage 2 auch gegenüber den Unterauftragsverarbeitern gelten und dabei nicht unterschritten werden.

Der Vertrag mit dem Unterauftragsverarbeiter ist schriftlich oder in einem elektronischen Format abzufassen (Art. 28 Abs. 4 und Abs. 9 DS-GVO). In ihm sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten des Auftragnehmers und des Unterauftragsverarbeiters – bei mehreren Unterauftragsverarbeitern auch die Verantwortlichkeiten zwischen diesen – deutlich voneinander abgegrenzt werden.

Der Auftragnehmer wählt Unterauftragsverarbeiter unter besonderer Berücksichtigung der Eignung der von diesen getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DS-GVO sorgfältig aus. Die relevanten Prüfunterlagen stellt er dem Auftraggeber auf Anfrage zur Verfügung.

Der Auftraggeber ist berechtigt, im Bedarfsfall angemessene Überprüfungen und Inspektionen, auch vor Ort, bei Unterauftragsverarbeitern durchzuführen oder durch von ihm beauftragte Dritte durchführen zu lassen. Ziffer 9 gilt entsprechend.

Die Weiterleitung von Daten an einen Unterauftragsverarbeiter ist erst zulässig, wenn dieser die Verpflichtungen nach Art. 29 und Art. 32 Abs. 4 DS-GVO bezüglich seiner Beschäftigten erfüllt hat.

Der Auftragnehmer überprüft die Einhaltung der Pflichten der Unterauftragsverarbeiter mindestens alle zwei Jahre anhand eines Fragenkatalogs sowie durch Prüfung des jeweiligen Datenschutzkonzeptes. Das Ergebnis der Überprüfungen ist zu dokumentieren und dem Auftraggeber auf Verlangen zugänglich zu machen.

Der Auftragnehmer bleibt gegenüber dem Auftraggeber für die Einhaltung der Pflichten aus dieser Vereinbarung verantwortlich und haftet dafür, dass die Unterauftragsverarbeiter den Datenschutzpflichten nachkommen, die ihnen durch den Auftragnehmer vertraglich auferlegt wurden (Art. 28 Abs. 4 Satz 2 DS-GVO).

Leistungen, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung seiner Tätigkeit in Anspruch nimmt (z. B. Telekommunikations-, Post- oder Reinigungsdienstleistungen), stellen kein Unterauftragsverhältnis im Sinne dieser Ziffer dar. Der Auftragnehmer trifft auch in diesen Fällen angemessene Maßnahmen zum Schutz der personenbezogenen Daten.

Verarbeitung in Drittländern

Die Verarbeitung erfolgt an den in Anlage 3 für den jeweiligen Unterauftragsverarbeiter angegebenen Verarbeitungsorten. Sie findet danach nicht ausschließlich innerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums statt; die betroffenen Verarbeitungen und die jeweilige Grundlage der Übermittlung nach Kapitel V DS-GVO sind in Anlage 3 einzeln ausgewiesen.

Jede Verlagerung der Verarbeitung oder von Teilen davon in ein weiteres Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

Beruhet eine Übermittlung auf einem Angemessenheitsbeschluss, insbesondere auf dem EU-US Data Privacy Framework, so überwacht der Auftragnehmer den Fortbestand der jeweiligen Zertifizierung. Entfällt diese oder wird der Angemessenheitsbeschluss aufgehoben, ausgesetzt oder für unwirksam erklärt, so informiert der



Auftragnehmer den Auftraggeber unverzüglich und stellt die Übermittlung unverzüglich auf ein anderes zulässiges Instrument nach Kapitel V DS-GVO um oder beendet sie.

Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn eine Behörde eines Drittlandes die Herausgabe von im Auftrag verarbeiteten personenbezogenen Daten verlangt, sofern das betreffende Recht eine solche Mitteilung nicht verbietet. Er prüft die Rechtmäßigkeit eines solchen Verlangens, beschränkt eine etwaige Herausgabe auf das rechtlich zwingend Erforderliche und dokumentiert das Verlangen sowie seine Reaktion.

Auf Verlangen des Auftraggebers stellt der Auftragnehmer die ihm vorliegenden Informationen bereit, die der Auftraggeber zur Beurteilung der Wirksamkeit der jeweiligen Übermittlungsgrundlage benötigt.

8. Unterstützungspflichten des Auftragnehmers

Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Erfüllung seiner Pflichten, insbesondere im Hinblick auf:

- die Wahrnehmung der Rechte betroffener Personen gemäß Artt. 12 ff. DS-GVO,
- die Einhaltung der Pflichten zur Sicherheit der Verarbeitung gemäß Art. 32 DS-GVO,
- die Meldung von Verletzungen des Schutzes personenbezogener Daten gemäß Art. 33 DS-GVO und die Benachrichtigung betroffener Personen gemäß Art. 34 DS-GVO,
- die Durchführung von Datenschutz-Folgenabschätzungen gemäß Art. 35 DS-GVO,
- die Konsultation von Aufsichtsbehörden gemäß Art. 36 DS-GVO sowie
- die Erstellung und Pflege des Verzeichnisses von Verarbeitungstätigkeiten gemäß Art. 30 DS-GVO.

Die hierfür erforderlichen Angaben leitet der Auftragnehmer unverzüglich an die in Ziffer 5 genannten weisungsberechtigten Personen oder Funktionen des Auftraggebers weiter. Geht beim Auftragnehmer ein Antrag einer betroffenen Person ein, der die Verarbeitung im Auftrag des Auftraggebers betrifft, so beantwortet er diesen nicht selbst, sondern leitet ihn unverzüglich an den Auftraggeber weiter.

Meldung von Verletzungen des Schutzes personenbezogener Daten

Der Auftragnehmer teilt dem Auftraggeber unverzüglich Störungen, Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder gegen die in dieser Vereinbarung getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit.

Eine Verletzung des Schutzes personenbezogener Daten im Sinne von Art. 4 Nr. 12 DS-GVO meldet der Auftragnehmer dem Auftraggeber unverzüglich, spätestens jedoch innerhalb von 48 Stunden nach Kenntniserlangung, über die in Ziffer 5 genannten Kommunikationskanäle. Die Meldung enthält, soweit verfügbar:

- eine Beschreibung der Art der Verletzung sowie der betroffenen Kategorien und der ungefähren Zahl betroffener Personen und Datensätze,
- den Zeitpunkt beziehungsweise Zeitraum des Vorfalls und den Zeitpunkt der Kenntniserlangung,
- eine Beschreibung der wahrscheinlichen Folgen der Verletzung,
- eine Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und zur Abmilderung möglicher nachteiliger Auswirkungen sowie
- den Namen und die Kontaktdaten einer Auskunftsstelle beim Auftragnehmer.

Sind die Informationen nicht vollständig verfügbar, so meldet der Auftragnehmer zunächst die vorliegenden Angaben und ergänzt sie unverzüglich, ohne die Meldung dadurch zu verzögern.

Der Auftragnehmer dokumentiert alle Verletzungen des Schutzes personenbezogener Daten einschließlich der ergriffenen Maßnahmen und stellt die Dokumentation dem Auftraggeber auf Verlangen zur Verfügung.



Meldungen nach Art. 33 DS-GVO an die Aufsichtsbehörde oder Benachrichtigungen nach Art. 34 DS-GVO an betroffene Personen nimmt der Auftragnehmer für den Auftraggeber nur nach vorheriger Weisung gemäß Ziffer 5 vor.

9. Kontrollrechte („Überprüfungen und Inspektionen“)

Der Auftragnehmer stellt dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DS-GVO niedergelegten Pflichten zur Verfügung und verpflichtet sich, den Auftraggeber bei der Überprüfung der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang zu unterstützen. Dazu stellt er dem Auftraggeber auf Nachfrage den aktuellen Auditbericht sowie das Ergebnis der Überprüfung nach Ziffer 4 zur Verfügung.

Überprüfungen – einschließlich Inspektionen – die von Auftraggeberseite darüber hinaus gewünscht sind, sind 30 Kalendertage zuvor anzukündigen und der Aufwand (sowohl für externe Prüfer als auch der insbesondere zeitliche Aufwand auf Auftragnehmerseite) kann dem Auftraggeber in Rechnung gestellt werden. Zum Schutz anderer Kunden kann die Einsichtnahme im erforderlichen Umfang eingeschränkt werden.

Bei Gefahr im Verzug, insbesondere bei einer Verletzung des Schutzes personenbezogener Daten, entfällt die Ankündigungsfrist nach Absatz 2.

Sollte ein durch den Auftraggeber beauftragter Dritter in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht. Beauftragte Dritte müssen durch den Auftraggeber zur Verschwiegenheit verpflichtet werden. Dem Auftragnehmer steht das Recht zu, die Abgabe einer separaten Verschwiegenheitserklärung des beauftragten Dritten zu verlangen.

Der Auftraggeber kann die Einhaltung eines genehmigten Zertifizierungsverfahrens gemäß Art. 42 DS-GVO durch den Auftragnehmer als Faktor heranziehen, um die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen zu beurteilen.

Das Ergebnis von Kontrollen ist zu dokumentieren.

10. Rückgabe oder Löschung von Daten

Nach Beendigung der Verarbeitung löscht oder gibt der Auftragnehmer nach Wahl des Auftraggebers alle personenbezogenen Daten sowie vorhandene Kopien zurück, sofern keine gesetzliche Aufbewahrungspflicht entgegsteht. Dies gilt auch für Daten, die in den Besitz von Unterauftragsverarbeitern gelangt sind.

Die Löschung ist in geeigneter und angemessener Weise durchzuführen und zu dokumentieren. Die Löschung beziehungsweise die Rückgabe ist dem Auftraggeber mit Datumsangabe schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen. Für die Rückgabe kann der Auftragnehmer eine angemessene Aufwandsentschädigung verlangen.

Der Auftraggeber hat das Recht, die vollständige und vertragsgemäße Rückgabe und Löschung der Daten beim Auftragnehmer zu kontrollieren. Dies kann auch durch eine Inaugenscheinnahme der Datenverarbeitungsanlagen in der Betriebsstätte des Auftragnehmers erfolgen; Ziffer 9 gilt entsprechend.

Soweit den Auftragnehmer eine gesetzliche Pflicht zur Aufbewahrung trifft, darf er personenbezogene Daten über die Beendigung dieser Vereinbarung hinaus speichern. In diesen Fällen dürfen die Daten nur für Zwecke der Umsetzung der jeweiligen gesetzlichen Aufbewahrungspflichten verarbeitet werden. Nach Ablauf der Aufbewahrungspflicht sind die Daten unverzüglich zu löschen.

Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der für den Auftraggeber verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.



11. Haftung

Auftraggeber und Auftragnehmer haften gegenüber betroffenen Personen entsprechend der in Art. 82 DSGVO getroffenen Regelungen.

12. Schlussbestimmungen (Salvatorische Klausel)

Im Übrigen gelten die Bestimmungen der Datenschutz-Grundverordnung.

Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Textform.

Vereinbarungen zu den technischen und organisatorischen Maßnahmen sowie Kontroll- und Prüfungsunterlagen – auch zu Unterauftragsverarbeitern – sind von beiden Vertragsparteien für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

Sollte das Eigentum des Auftraggebers oder sollten die für ihn verarbeiteten personenbezogenen Daten beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.

Als Gerichtsstand wird das für den Auftraggeber örtlich zuständige Gericht vereinbart.

Sollten einzelne Bestimmungen dieser Vereinbarung unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.

Anlagen, die Bestandteil dieser Vereinbarung sind

- Anlage 1 – Spezifika
- Anlage 2 – Technische und organisatorische Maßnahmen („Datenschutzkonzept“)
- Anlage 3 – Unterauftragsverarbeiter

Dokumentenversion: 2.0, Stand 11.09.2026

Ort, Datum: _____

Für den Auftraggeber

Name: _____
Position: _____

Unterschrift: _____

Für den Auftragnehmer (SYNQONY Leer GmbH)

Name: _____
Position: _____

Unterschrift: _____



Anlage 1 – Spezifika

1. Gegenstand der Verarbeitung

Gegenstand der Verarbeitung ist die Verarbeitung personenbezogener Daten im Rahmen der Bereitstellung, des Hostings, der Wartung und der Unterstützung des KI-gestützten Voicebots Qonny durch den Auftragnehmer für den Auftraggeber. Eine Verarbeitung der Daten durch den Auftragnehmer zu eigenen Zwecken erfolgt nicht.

2. Art der Verarbeitung

Qonny nimmt eingehende Telefonanrufe automatisiert entgegen, erkennt Anliegen und verarbeitet sie. Dabei werden Sprachdaten in Echtzeit transkribiert, durch ein Sprachmodell (LLM) verarbeitet und Antworten per Sprachsynthese ausgegeben. Je nach Konfiguration kann Qonny Aktionen in angebundenen Kundensystemen auslösen (z. B. Beschwerden erfassen, Termine buchen, Informationen abrufen).

Um den effektiven Einsatz und größtmöglichen Nutzen der Software sicherzustellen, bietet der Auftragnehmer ein breites Spektrum an Dienstleistungen an – von der gründlichen Vorbereitung über die Anpassung des Systems bis zur Schulung der Anwender. Dazu gehört auch die Wartung der Software. Bei diesen Tätigkeiten kann es unausweichlich sein, dass personenbezogene Daten des Auftraggebers, seiner Kunden und seiner Mitarbeiter für den Auftragnehmer sichtbar werden.

Die Verarbeitung erfolgt insbesondere durch:

- Erfassung,
- Speicherung,
- Bearbeitung und Nutzung,
- Weitergabe oder
- Löschung.

3. Umfang der Verarbeitung

Der Umfang der verarbeiteten personenbezogenen Daten ist auf solche Daten beschränkt, die für die ordnungsgemäße Erbringung der Leistungen erforderlich sind oder deren Übermittlung aus technischen Gründen unvermeidbar ist.

Die modular konfigurierbare Architektur von Qonny ermöglicht eine flexible Anpassung an die spezifischen Anforderungen des Auftraggebers. Umfang, Arten und Zwecke der Verarbeitung stehen daher stets in Abhängigkeit von der konkreten Konfiguration, den individuellen Anpassungen und den Workflows, die der Auftraggeber tatsächlich nutzt.

4. Zweck der Verarbeitung

Zweck der Verarbeitung ist die vertraglich geschuldete Leistungserbringung. Folgende Verarbeitungszwecke sind regelmäßig Gegenstand der Verarbeitung:

- Automatisierte Entgegennahme und Bearbeitung eingehender Telefonanrufe
- Echtzeit-Transkription von Sprachdaten
- KI-gestützte Verarbeitung und Beantwortung von Anliegen
- Ausführung von Aktionen in angebundenen Kundensystemen (z. B. Beschwerdeerfassung, Terminbuchung)
- Support des Auftraggebers und seiner Mitarbeiter
- Schulung des Auftraggebers und seiner Mitarbeiter
- Fehleranalyse und Problemanalyse



- Datenübernahme

Der Auftragnehmer empfiehlt, die Software zu den vorstehend aufgeführten Zwecken einzusetzen.

5. Kategorien personenbezogener Daten

Folgende Datenarten sind regelmäßig Gegenstand der Verarbeitung:

- Sprachdaten (Audiodateien der Telefonanrufe)
- Transkripte der Gespräche
- Anruferkennung / Telefonnummern
- Adressdaten
- E-Mail-Adressen
- Namen und Kontaktdaten
- Anliegen und Beschwerdeinhalte
- Daten aus angebundenen Kundensystemen (je nach Konfiguration, z. B. Kundennummern, Vertragsdaten, Auftragsdaten)

Die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne der Art. 9 und 10 DS-GVO ist nicht Gegenstand dieses Auftrags und erfolgt im Übrigen nur auf ausdrückliche Weisung des Auftraggebers. Da Anrufer ihre Angaben frei äußern, kann nicht ausgeschlossen werden, dass solche Daten unbeabsichtigt anfallen. Der Auftragnehmer behandelt sie in diesem Fall mit demselben Schutzniveau wie die übrigen Daten des Auftrags; die Speicher- und Löschregelungen nach Ziffer 8 dieser Anlage gelten unverändert.

6. Kategorien betroffener Personen

Von der Verarbeitung können insbesondere betroffen sein:

- Anrufer (Kunden, Bürger, Interessenten des Auftraggebers)
- Mitarbeiter des Auftraggebers
- Sonstige Personen, die den Voicebot kontaktieren

7. Ort der Verarbeitung

Die Verarbeitung personenbezogener Daten erfolgt an den in Anlage 3 für den jeweiligen Unterauftragsverarbeiter angegebenen Verarbeitungsorten. Sie findet nicht ausschließlich innerhalb der Europäischen Union beziehungsweise des Europäischen Wirtschaftsraums statt.

Die Verarbeitungsorte und die jeweilige Grundlage der Übermittlung nach Kapitel V DS-GVO sind in Anlage 3 einzeln ausgewiesen. Im Übrigen gilt Ziffer 7 dieser Vereinbarung.

8. Speicherdauer und Löschung im laufenden Betrieb

Für den laufenden Betrieb von Qonny gelten die folgenden Speicher- und Löschregelungen:

Sprachaufnahmen (Audio)

- Die Anrufe werden ausschließlich in Echtzeit verarbeitet. Eine dauerhafte Speicherung der Audiodaten findet nicht statt.

Spracherkennung (Deepgram)

- Die eingehenden Audiodaten werden ausschließlich in Echtzeit zur Umwandlung in Text verarbeitet. Weder die Audiodaten noch die erzeugten Transkripte werden von Deepgram dauerhaft gespeichert.



Transkripte und Gesprächsdaten

- Transkripte der Gespräche werden für 30 Tage gespeichert und anschließend gelöscht.
- Nach Ablauf dieser Frist werden lediglich Anrufzeitpunkt, Telefonnummer und Anrufrkategorie (z. B. allgemeine Anfrage, Terminprüfung) weiter aufbewahrt. Die Dauer dieser weiteren Aufbewahrung richtet sich nach der im Einzelfall eingesetzten Technik und dem jeweils genutzten Anbieter; sie ist den Angaben des jeweiligen Anbieters zu entnehmen.

KI-Verarbeitung (Azure OpenAI)

- Zur Missbrauchserkennung werden anfallende Daten bis zu 30 Tage gespeichert und anschließend gelöscht. Eine Nutzung der Daten für ein Modelltraining findet nicht statt.

Sprachsynthese (ElevenLabs)

- Die zur Sprachausgabe verarbeiteten Texte werden in der Verlaufshistorie des Anbieters vorgehalten. Die Verlaufsspeicherung ist aktiv; eine feste automatische Speicherfrist ist nicht vorgegeben. Eine Löschung kann bei Bedarf veranlasst werden.

Telefonie-Infrastruktur (Twilio Elastic SIP Trunking)

- Zur technischen Bereitstellung der Telefonieverbindung werden Metadaten der Anrufe (z. B. Anrufernummer, Zielnummer, Zeitpunkt und Dauer) in den Verbindungsprotokollen des Anbieters verarbeitet. Diese Call Logs sind regulär 13 Monate verfügbar und werden dann gelöscht.

Orchestrierung (LiveKit) und Hosting (IONOS)

- Die hierbei anfallenden Verbindungs- und Betriebsdaten unterliegen einer rotierenden Löschung, spätestens nach 13 Monaten.

Allgemeine Metadaten und Protokolldaten

- Es fallen technisch notwendige Protokoll- und Metadaten an. Sie werden nur so lange gespeichert, wie es technisch erforderlich ist, und während des Betriebs fortlaufend rotierend gelöscht beziehungsweise überschrieben, spätestens nach 13 Monaten.

Löschung auf Weisung

- Der Auftraggeber kann jederzeit die Löschung der ihn betreffenden Daten verlangen; der Auftragnehmer setzt dies unverzüglich um und wirkt auf die Löschung bei den Unterauftragsverarbeitern hin. Eine weitergehende Speicherung erfolgt nur bei gesetzlichen Aufbewahrungspflichten.



Anlage 2 – Technische und organisatorische Maßnahmen („Datenschutzkonzept“)

Der Auftragnehmer sichert zu, dass er die nachfolgend beschriebenen technischen und organisatorischen Maßnahmen im Rahmen seines Datenschutzkonzeptes einhält. Die Gliederung folgt den Schutzziele des Art. 32 DS-GVO. Änderungen richten sich nach Ziffer 4 dieser Vereinbarung.

1. Vertraulichkeit

1.1 Zutrittskontrolle

Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, sichergestellt durch:

- Alarmanlage
- Videoüberwachung der Zufahrt
- Sicherheitsschlösser
- Schlüsselregelung (Schlüsselausgabe an Empfänger dokumentiert, mehrere Schließkreise)
- Personenkontrolle beim Empfang und ständige Aufsicht der Besucher während des Aufenthalts
- Protokollierung der Besucher (Zeitraum des Aufenthalts)
- Sorgfältige Auswahl von Reinigungspersonal
- Tragepflicht von Berechtigungsausweisen (Besucher)

1.2 Zugangskontrolle

Keine unbefugte Systembenutzung, sichergestellt durch:

- Zuordnung von Benutzerrechten
- Erstellen von Benutzerprofilen
- Zuordnung von Benutzerprofilen zu IT-Systemen
- Authentifikation mit Benutzername und Kennwort nach der nachfolgend beschriebenen Kennwortrichtlinie
- Einsatz von VPN-Technologie
- Verschlüsselung von mobilen Datenträgern
- Verschlüsselung von Datenträgern in Laptops und Notebooks
- Einsatz von Anti-Viren-Software
- Einsatz einer Hardware-Firewall
- Einsatz einer Software-Firewall bei allen Arbeitsplätzen

Kennwortrichtlinie (Microsoft Entra Standardrichtlinie)

- Mindestlänge 8 Zeichen, Höchstlänge 256 Zeichen
- Komplexität: drei der vier Kategorien Großbuchstaben, Kleinbuchstaben, Ziffern und Sonderzeichen
- Unicode-Zeichen sind nicht zulässig
- Ein neues Kennwort darf nicht dem aktuellen Kennwort entsprechen
- Abgleich gegen die Sperrliste verbotener Kennwörter (Microsoft Entra Password Protection)
- Es besteht keine Pflicht zum anlasslosen Wechsel des Kennworts; dies entspricht der Empfehlung, Kennwörter nur bei Anhaltspunkten für eine Kompromittierung zu wechseln
- Automatische Kontosperrung (Smart Lockout) nach zehn fehlgeschlagenen Anmeldeversuchen; die Sperrdauer beginnt bei 60 Sekunden und verlängert sich bei weiteren Fehlversuchen

1.3 Zugriffskontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, sichergestellt durch:



- Nutzung eines Berechtigungskonzepts
- Verwaltung der Rechte durch die Systemadministratoren auf Weisung der Geschäftsführung
- Anzahl der Benutzer mit Administratorberechtigungen auf das notwendigste reduziert
- Geltung der Kennwortrichtlinie nach Abschnitt 1.2 auch für den Zugriff auf personenbezogene Daten
- Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
- Sichere Aufbewahrung von Datenträgern
- Ordnungsgemäße Vernichtung von Datenträgern (DIN 66399)
- Einsatz von Aktenvernichtern
- Einsatz von Dienstleistern zur Aktenvernichtung mit Vernichtungsnachweis
- Verschlüsselung von Datenträgern

1.4 Pseudonymisierung

Eine Pseudonymisierung erfolgt, soweit sie technisch möglich und verhältnismäßig umsetzbar ist. Ist der Personenbezug für die Erbringung der beauftragten Leistung erforderlich, unterbleibt sie.

1.5 Trennungskontrolle

Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, sichergestellt durch:

- Getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- Erstellung eines Berechtigungskonzepts
- Versehen der Datensätze mit Zweckattributen und Datenfeldern
- Festlegung von Datenbankrechten
- Trennung von Produktiv- und Testsystem

2. Integrität

2.1 Weitergabekontrolle

Gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung, während ihres Transports oder bei ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, geändert, kopiert oder entfernt werden können, sichergestellt durch:

- Verschlüsselte Datenübertragung über SFTP und FTPS mit Protokollierung
- Verschlüsselte Datenträger werden ausschließlich angenommen
- Dokumentation von Empfängern der Daten
- Dokumentation der Zeitspannen der tatsächlichen Speicherung
- Dokumentation der Spanne der geplanten Überlassung
- Dokumentation des Übertragungsmediums
- Dokumentation des Löschvorgangs
- Automatisierte Warnung bei fehlerhafter Dokumentation
- Zusätzliche manuelle Kontrolle der Dokumentation
- Verschlüsselte Fernwartungsverbindung
- Durch die Fernwartungssoftware generierte sichere Kennwörter
- Protokollierung aller Fernwartungsverbindungen (Benutzer, Zeitraum, Zweck, Verbindungsziel)

2.2 Eingabekontrolle

Nachvollziehbarkeit von Eingabe, Änderung und Löschung personenbezogener Daten, sichergestellt durch:



- Zuordnung von Eingaben, Änderungen und Löschungen zum handelnden Beschäftigten über das persönliche Benutzerkonto in Verbindung mit der Protokollierung; dies ist für die wesentlichen Verarbeitungsschritte sichergestellt
- Protokollierung der Eingabe, Änderung und Löschung von Daten in den Anwendungen (siehe Abschnitt 1.3)
- Bei Datenübernahmen erfolgt keine inhaltliche Änderung der Daten; strukturelle Änderungen sind möglich

2.3 Auftragskontrolle

Gewährleisten, dass die im Auftrag durchgeführten Verarbeitungsvorgänge ausschließlich auf Weisung des Auftraggebers erfolgen, sichergestellt durch:

- Verarbeitung ausschließlich auf Weisung des Auftraggebers nach Ziffer 5 dieser Vereinbarung
- Verpflichtung der mit der Verarbeitung befassten Beschäftigten auf die Vertraulichkeit nach Ziffer 6 dieser Vereinbarung
- Schulung und Unterweisung der mit der Datenverarbeitung befassten Beschäftigten (siehe Abschnitt 4)
- Überprüfung der Unterauftragsverarbeiter nach Ziffer 7 dieser Vereinbarung mindestens alle zwei Jahre
- Dokumentation der Ergebnisse interner Kontrollen

3. Verfügbarkeit und Belastbarkeit

Die Maßnahmen zur Verfügbarkeit und Belastbarkeit der Ausführungsumgebung – insbesondere Datensicherung und Wiederherstellbarkeit, Redundanz, Patch- und Schwachstellenmanagement sowie der physische Schutz der Rechenzentren – werden durch die in Anlage 3 genannten Infrastruktur- und Hosting-Unterauftragsverarbeiter erbracht.

Maßgeblich sind insoweit die jeweils geltenden Dokumentationen und Nachweise dieser Anbieter. Sie sind beim jeweiligen Anbieter einsehbar; der Auftragnehmer stellt dem Auftraggeber die ihm vorliegenden Unterlagen auf Anfrage nach Ziffer 9 dieser Vereinbarung zur Verfügung.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Die Wirksamkeit der Maßnahmen wird durch die folgenden Verfahren überprüft und bewertet:

- Führung eines Verzeichnisses von Verarbeitungstätigkeiten
- Dokumentation der eingesetzten IT-Systeme und der Systemkonfiguration
- Bestellung eines Beauftragten für den Datenschutz
- Mitarbeiter sind über Datensicherheit und Datenschutz geschult
- Mitarbeiter sind per schriftlicher Erklärung dem Datenschutz verpflichtet
- Es existieren verfahrensunabhängige Plausibilitäts- und Sicherheitsprüfungen
- Ein Datensicherheitskonzept beziehungsweise Informationssicherheitsmanagement ist vorhanden
- Eine Datenschutzrichtlinie ist vorhanden
- Überprüfung, Bewertung und Evaluation der Wirksamkeit der Maßnahmen bei gegebenem Anlass, mindestens jährlich, nach Ziffer 4 dieser Vereinbarung
- Durchgängiger Melde- und Bearbeitungsprozess für Verletzungen des Schutzes personenbezogener Daten und für Anfragen betroffener Personen nach Ziffer 8 dieser Vereinbarung

5. Weitere verfahrensspezifische Maßnahmen

Für die Cloud-Ausführungsumgebung von Qonny gelten ergänzend:

- Transportverschlüsselung der Sprach- und Signalisierungsverbindungen über TLS und SRTP
- Verschlüsselte Speicherung der Daten
- Strikte Mandantentrennung



- Zentrale, zugriffsgeschützte Verwaltung und Wechsel der Zugangsschlüssel (API-Keys) zu den eingesetzten KI-Diensten
- Strikte Trennung der Verarbeitungskontexte gegenüber dem Sprachmodell
- Berechtigungssystem nach dem Zero-Trust-Prinzip sowie Protokollierung der Zugriffe für Support und Fernwartung



Anlage 3 – Unterauftragsverarbeiter

Aktuell bestehen die nachfolgenden Unterauftragsverarbeiter im Zusammenhang mit der Auftragsverarbeitung. Für jeden Unterauftragsverarbeiter sind Name, Anschrift, Leistung, Sitz, Verarbeitungsort und – soweit eine Verarbeitung in einem Drittland außerhalb der EU beziehungsweise des EWR erfolgt – die Grundlage der Übermittlung nach Kapitel V DS-GVO angegeben.

1. Twilio Inc.

- Anschrift: 101 Spear Street, 5th Floor, San Francisco, CA 94105, USA
- Leistung: Telefonie und SIP-Trunk (technische Entgegennahme der Anrufe). Der Einsatz erfolgt nur, soweit der Auftraggeber den vom Auftragnehmer bereitgestellten SIP-Trunk nutzt.
- Sitz: San Francisco, Kalifornien, USA
- Verarbeitungsort: USA (Twilio-Region US1)
- Transfergrundlage: EU-US Data Privacy Framework (zertifiziert)

2. LiveKit Inc.

- Anschrift: 369 Sutter Street, San Francisco, CA, USA
- Leistung: Orchestrierung der Echtzeit-Kommunikation
- Sitz: San Francisco, Kalifornien, USA
- Verarbeitungsort: globales LiveKit-Cloud-Netz einschließlich der USA; eine EU-Region ist nicht gepinnt
- Transfergrundlage: EU-US Data Privacy Framework (zertifiziert)

3. Deepgram Inc.

- Anschrift: 548 Market Street, Suite 25104, San Francisco, CA 94104-5401, USA
- Leistung: Echtzeit-Transkription der Sprachdaten (Speech-to-Text)
- Sitz: San Francisco, Kalifornien, USA
- Verarbeitungsort: USA
- Transfergrundlage: Standardvertragsklauseln der Europäischen Kommission (SCC)

4. ElevenLabs Inc.

- Anschrift: 169 Madison Avenue #2484, New York, NY 10016, USA
- Leistung: Sprachsynthese (Text-to-Speech)
- Sitz: New York, USA
- Verarbeitungsort: USA
- Transfergrundlage: EU-US Data Privacy Framework (zertifiziert)

5. Microsoft Ireland Operations Limited

- Anschrift: Leopardstown, Dublin 18, D18 P521, Irland
- Leistung: Bereitstellung des Sprachmodells (LLM) über Azure OpenAI
- Sitz: Dublin, Irland (EU)
- Verarbeitungsort: Deutschland (Azure-Region Germany West Central), EU
- Transfergrundlage: keine Drittlandübermittlung, Verarbeitung innerhalb der EU; eine Nutzung der Daten für ein Modelltraining findet nicht statt

6. 1&1 IONOS Cloud GmbH

- Anschrift: Greifswalder Straße 207, 10405 Berlin, Deutschland
- Leistung: Hosting der Ausführungsumgebung (Rechenzentren in Deutschland)



- Sitz: Berlin, Deutschland (EU)
- Verarbeitungsort: Deutschland, EU
- Transfergrundlage: keine Drittlandübermittlung, Verarbeitung innerhalb der EU

Änderungen dieser Liste richten sich nach Ziffer 7 dieser Vereinbarung.

