Vertrag über die Verarbeitung von Daten im Auftrag im Rahmen der App satellite

zwischen

KUNDE

Auftraggeber
Im Folgenden: "Kunde"

und

sipgate GmbH, Gladbacher Str. 74, 40219 Düsseldorf, vertreten durch die Geschäftsführer Herrn Tim Mois und Herrn Thilo Salmon, ebenda

Auftragnehmer
Im Folgenden: "sipgate"

Gemeinsam im Folgenden: "Die Parteien"

Die Regelungen zur Auftragsverarbeitung ergänzen die allgemeinen Geschäftsbedingungen der sipgate GmbH. Im Falle eines Widerspruchs zwischen diesen Regelungen und den allgemeinen Geschäftsbedingungen der sipgate GmbH gehen diese Regelungen zur Auftragsverarbeitung vor.

Die Parteien vereinbaren, dass zeitgleich mit Beginn dieser Vereinbarung zur Auftragsverarbeitung etwaige weitere Vereinbarungen zur Auftragsdatenverarbeitung einvernehmlich aufgehoben und durch diese neue Vereinbarung zur Auftragsverarbeitung ersetzt werden.

1. Allgemeines

(1) sipgate verarbeitet personenbezogene Daten im Auftrag des Kunden i.S.d. Art. 4 Nr. 8 und Art. 28 der Verordnung (EU) 2016/679 – Datenschutz-Grundverordnung (DSGVO). Dieser Vertrag regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Verarbeitung von personenbezogenen Daten.
(2) Sofern in diesem Vertrag der Begriff „Datenverarbeitung" oder „Verarbeitung" (von Daten) benutzt wird, wird die Definition der „Verarbeitung" i.S.d. Art. 4 Nr. 2 DSGVO zugrunde gelegt.

(3) Alle in dieser Vereinbarung enthaltenen Verweise auf die DSGVO (Verordnung (EU) 2016/679 des europäischen Parlaments und des Rates vom 27.04.2016 zum Schutz natür-

licher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)) gelten für die DSGVO in ihrer jeweils aktuellen Fassung.

2. Gegenstand des Auftrags

Der Gegenstand der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten und die Kategorien betroffener Personen sind in **Anlage 1** zu diesem Vertrag festgelegt.

3. Rechte und Pflichten des Kunden

(1) Der Kunde ist Verantwortlicher i.S.d. Art. 4 Nr. 7 DSGVO für die Verarbeitung von Daten im Auftrag durch sipgate. sipgate steht nach Ziff. 4 Abs. 5 dieser Vereinbarung das Recht zu, den Kunden darauf hinzuweisen, wenn eine seiner Meinung nach rechtlich unzulässige Datenverarbeitung Gegenstand des Auftrags und/oder einer Weisung ist.

(2) Der Kunde ist als Verantwortlicher für die Wahrung der Betroffenenrechte verantwortlich. sipgate wird den Kunden unverzüglich darüber informieren, wenn Betroffene ihre Betroffenenrechte gegenüber sipgate geltend machen.

(3) Der Kunde hat das Recht, jederzeit ergänzende Weisungen über Art, Umfang und Verfahren der Datenverarbeitung gegenüber sipgate zu erteilen. Weisungen können in Textform (z.B. E-Mail) erfolgen.

(4) Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch ergänzende Weisungen des Kunden bei sipgate entstehen, bleiben unberührt.

(5) Der Kunde informiert sipgate unverzüglich, wenn er Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch sipgate feststellt.

(6) Für den Fall, dass eine Informationspflicht gegenüber Dritten nach Art. 33, 34 DSGVO oder einer sonstigen, für den Kunden geltenden gesetzlichen Meldepflicht besteht, ist der Kunde für deren Einhaltung verantwortlich.

4. Allgemeine Pflichten der sipgate

(1) sipgate verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und/oder unter Einhaltung der ggf. vom Kunden erteilten ergänzenden Wei-

sungen. Ausgenommen hiervon sind gesetzliche Regelungen, die sipgate ggf. zu einer anderweitigen Verarbeitung verpflichten. In einem solchen Fall teilt sipgate dem Kunden diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Zweck, Art und Umfang der Datenverarbeitung richten sich ansonsten ausschließlich nach diesem Vertrag und/oder den Weisungen des Kunden. Eine hiervon abweichende Verarbeitung von Daten ist sipgate untersagt, es sei denn, dass der Kunde dieser schriftlich zugestimmt hat.

(2) sipgate verpflichtet sich, die Datenverarbeitung im Auftrag nur in Mitgliedsstaaten der Europäischen Union (EU) oder des Europäischen Wirtschaftsraums (EWR) durchzuführen, soweit nicht der Nutzer eine Einwilligung in die Datenverarbeitung außerhalb der EU/des EWR erteilt hat.

(3) sipgate sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsmäßige Abwicklung aller vereinbarten Maßnahmen zu.

(4) sipgate ist verpflichtet, sein Unternehmen und seine Betriebsabläufe so zu gestalten, dass die Daten, die sipgate im Auftrag des Kunden verarbeitet, im jeweils erforderlichen Maß gesichert und vor der unbefugten Kenntnisnahme Dritter geschützt sind. sipgate wird Änderungen in der Organisation der Datenverarbeitung im Auftrag, die für die Sicherheit der Daten erheblich sind, vorab mit dem Kunden abstimmen.

(5) sipgate wird den Kunden unverzüglich darüber informieren, wenn eine vom Kunden erteilte Weisung nach seiner Auffassung gegen gesetzliche Regelungen verstößt. sipgate ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Kunden bestätigt oder geändert wird. Sofern sipgate darlegen kann, dass eine Verarbeitung nach Weisung des Kunden zu einer Haftung der sipgate nach Art. 82 DSGVO führen kann, steht sipgate das Recht frei, die weitere Verarbeitung insoweit bis zu einer Klärung der Haftung zwischen den Parteien auszusetzen.

(6) Die Verarbeitung von Daten im Auftrag des Kunden außerhalb von Betriebsstätten der sipgate oder Subunternehmern ist nur mit Zustimmung des Kunden in Schriftform oder Textform zulässig. Eine Verarbeitung von Daten für den Kunden in Privatwohnungen ist nur mit Zustimmung des Kunden in Schriftform oder Textform im Einzelfall zulässig.

(7) sipgate wird die Daten, die sie im Auftrag für den Kunden verarbeitet, getrennt von anderen Daten verarbeiten. Eine physische Trennung ist nicht zwingend erforderlich.

5. Datenschutzbeauftragter der sipgate

(1) sipgate bestätigt, dass sie einen Datenschutzbeauftragten nach Art. 37 DSGVO benannt hat. sipgate trägt Sorge dafür, dass der Datenschutzbeauftragte über die erforderliche Qualifikation und das erforderliche Fachwissen verfügt. sipgate wird dem Kunden den Namen und die Kontaktdaten seines Datenschutzbeauftragten gesondert in Textform mitteilen.

(2) Die Pflicht zur Benennung eines Datenschutzbeauftragten nach Absatz 1 kann im Ermessen des Kunden entfallen, wenn sipgate nachweisen kann, dass sie gesetzlich nicht

verpflichtet ist, einen Datenschutzbeauftragten zu bestellen und sipgate nachweisen kann, dass betriebliche Regelungen bestehen, die eine Verarbeitung personenbezogener Daten unter Einhaltung der gesetzlichen Vorschriften, der Regelungen dieses Vertrages sowie etwaiger weiterer Weisungen des Kunden gewährleisten.

6. Meldepflichten der sipgate

(1) sipgate ist verpflichtet, dem Kunden jeden Verstoß gegen datenschutzrechtliche Vorschriften oder gegen die getroffenen vertraglichen Vereinbarungen und/oder die erteilten Weisungen des Kunden, der im Zuge der Verarbeitung von Daten durch ihn oder andere mit der Verarbeitung beschäftigten Personen erfolgt ist, unverzüglich mitzuteilen. Gleiches gilt für jede Verletzung des Schutzes personenbezogener Daten, die sipgate im Auftrag des Kunden verarbeitet.

(2) Ferner wird sipgate den Kunden unverzüglich darüber informieren, wenn eine Aufsichtsbehörde nach Art. 58 DSGVO gegenüber sipgate tätig wird und dies auch eine Kontrolle der Verarbeitung, die sipgate im Auftrag des Kunden erbringt, betreffen kann.

(3) sipgate ist bekannt, dass für den Kunden eine Meldepflicht nach Art. 33, 34 DSGVO bestehen kann, die eine Meldung an die Aufsichtsbehörde binnen 72 Stunden nach Bekanntwerden vorsieht. sipgate wird den Kunden bei der Umsetzung der Meldepflichten unterstützen. sipgate wird dem Kunden insbesondere jeden unbefugten Zugriff auf personenbezogene Daten, die im Auftrag des Kunden verarbeitet werden, unverzüglich, spätestens aber binnen 48 Stunden ab Kenntnis des Zugriffs mitteilen. Die Meldung der sipgate an den Kunden muss insbesondere folgende Informationen beinhalten:

- eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
- eine Beschreibung der von sipgate ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

7. Mitwirkungspflichten der sipgate

(1) sipgate unterstützt den Kunden bei seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nach Art. 12-23 DSGVO. Es gelten die Regelungen von Ziff. 11 dieses Vertrages.

(2) sipgate wirkt an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten durch den Kunden mit. Sipgate hat dem Kunden die insoweit jeweils erforderlichen Angaben in geeigneter Weise mitzuteilen.

(3) sipgate unterstützt den Kunden unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in Art. 32-36 DSGVO genannten Pflichten.

(4) sipgate ist berechtigt, für diese Leistungen vom Kunden eine angemessene aufwandsbezogene Vergütung zu verlangen.

8. Kontrollbefugnisse

(1) Der Kunde hat das Recht, die Einhaltung der gesetzlichen Vorschriften zum Datenschutz und/oder die Einhaltung der zwischen den Parteien getroffenen vertraglichen Regelungen und/oder die Einhaltung der Weisungen des Kunden durch sipgate jederzeit im erforderlichen Umfang zu kontrollieren.

Der Nachweis der Einhaltung der einem Auftragsverarbeiter obliegenden Pflichten gemäß der DSGVO soll primär durch unabhängige Prüfberichte und Zertifizierung erbracht werden.

Sofern der Kunde auf Grundlage tatsächlicher Anhaltspunkte berechtigte Zweifel daran geltend macht, dass die Prüfberichte bzw. Zertifizierungen unzureichend oder unzutreffend sind, oder besondere Vorfälle im Sinne von Art. 33 Abs. 1 DSGVO im Zusammenhang mit der Durchführung der Auftragsverarbeitung des Kunden dies rechtfertigen, kann der Kunde Kontrollen nach Ziffer 8. (2) durchführen.

(2) Um dem Kunden eine Auftragskontrolle und insbesondere eine Überprüfung der bei sipgate getroffenen technischen und organisatorischen Maßnahmen vor Beginn und regelmäßig während der Datenverarbeitung zu ermöglichen, wird sipgate die Kontrolle durch einen vom Kunden beauftragten neutralen Dritten (z.B. vereidigter Wirtschaftsprüfer) zulassen. sipgate ist berechtigt, Termine für eine Prüfung nach den betrieblichen Möglichkeiten zu vergeben. Die Prüfung soll innerhalb eines angemessenen Zeitraums nach der Anfrage ermöglicht werden. Alternativ kann sipgate dem Kontrollrecht des Kunden auch dadurch entsprechen, dass sipgate einen von einem unabhängigen, vereidigten Wirtschaftsprüfer im Auftrag der sipgate GmbH erstellten Prüfbericht zur Verfügung stellt. Die Ausübung des Inspektionsrechts darf den Geschäftsbetrieb der sipgate nicht über Gebühr stören oder missbräuchlich sein.

(3) sipgate ist berechtigt, für Kontrollen im Sinne der Ziffer 8. (2) eine angemessene Vergütung vom Kunden zu verlangen.

9. Unterauftragsverhältnisse

(1) Die vertraglich vereinbarten Leistungen bzw. die nachfolgend beschriebenen Teilleistungen werden unter Einschaltung der in **Anlage 2** genannten Unterauftragnehmer durchgeführt. sipgate ist im Rahmen seiner vertraglichen Verpflichtungen zur Begründung von weiteren Unterauftragsverhältnissen mit Unterauftragnehmern befugt. sipgate setzt den Auftraggeber hiervon unverzüglich in Kenntnis. sipgate ist verpflichtet, Unterauftragnehmer sorgfältig nach deren Eignung und Zuverlässigkeit auszuwählen. sipgate hat bei der Einschaltung von Unterauftragnehmern diese entsprechend den Regelungen dieser Vereinbarung zu verpflichten und dabei sicherzustellen, dass der Auftraggeber seine Rechte aus dieser Vereinbarung (insbesondere seine Prüf- und Kontrollrechte) auch direkt gegenüber

den Unterauftragnehmern wahrnehmen kann. Sofern eine Einbeziehung von Unterauftragnehmern in einem Drittland erfolgen soll, hat sipgate sicherzustellen, dass beim jeweiligen Unterauftragnehmer ein angemessenes Datenschutzniveau gewährleistet ist (z.B. durch Abschluss einer Vereinbarung auf Basis der EU-Standarddatenschutzklauseln). sipgate wird dem Auftraggeber auf Verlangen den Abschluss der vorgenannten Vereinbarungen mit seinen Subunternehmern nachweisen.

(2) sipgate hat den Unterauftragnehmer sorgfältig auszuwählen und vor der Beauftragung zu prüfen, dass dieser die zwischen Kunde und sipgate getroffenen Vereinbarungen einhalten kann. sipgate hat insbesondere vorab und regelmäßig während der Vertragsdauer zu kontrollieren, dass der Unterauftragnehmer die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten getroffen hat. Das Ergebnis der Kontrolle ist von sipgate zu dokumentieren und auf Anfrage dem Kunden zu übermitteln.

(3) sipgate ist verpflichtet, sich vom Unterauftragnehmer bestätigen zu lassen, dass dieser einen betrieblichen Datenschutzbeauftragten gemäß Art. 37 DSGVO benannt hat. Für den Fall, dass kein Datenschutzbeauftragter beim Unterauftragnehmer benannt worden ist, hat sipgate den Kunden hierauf hinzuweisen und Informationen dazu beizubringen, aus denen sich ergibt, dass der Unterauftragnehmer gesetzlich nicht verpflichtet ist, einen Datenschutzbeauftragten zu benennen.

(4) Nicht als Unterauftragsverhältnisse i.S.d. Absätze 1 bis 6 sind Dienstleistungen anzusehen, die sipgate bei Dritten als reine Nebenleistung in Anspruch nimmt, um die geschäftliche Tätigkeit auszuüben. Dazu gehören beispielsweise Reinigungsleistungen, reine Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die sipgate für den Kunden erbringt, Post- und Kurierdienste, Transportleistungen, Bewachungsdienste. sipgate ist gleichwohl verpflichtet, auch bei Nebenleistungen, die von Dritten erbracht werden, Sorge dafür zu tragen, dass angemessene Vorkehrungen und technische und organisatorische Maßnahmen getroffen wurden, um den Schutz personenbezogener Daten zu gewährleisten. Die Wartung und Pflege von IT-System oder Applikationen stellt ein zustimmungspflichtiges Unterauftragsverhältnis und Auftragsverarbeitung i.S.d. Art. 28 DSGVO dar, wenn die Wartung und Prüfung solche IT-Systeme betrifft, die auch im Zusammenhang mit der Erbringung von Leistungen für den Kunden genutzt werden und bei der Wartung auf personenbezogenen Daten zugegriffen werden kann, die im Auftrag des Kunden verarbeitet werden.

10. Vertraulichkeitsverpflichtung

(1) sipgate ist bei der Verarbeitung von Daten für den Kunden zur Wahrung der Vertraulichkeit über Daten, die sie im Zusammenhang mit dem Auftrag erhält bzw. zur Kenntnis erlangt, verpflichtet. sipgate verpflichtet sich, die gleichen Geheimnisschutzregeln zu beachten, wie sie dem Kunden obliegen. Der Kunde ist verpflichtet, sipgate etwaige besondere Geheimnisschutzregeln mitzuteilen.

(2) sipgate sichert zu, dass ihm die jeweils geltenden datenschutzrechtlichen Vorschriften bekannt sind und sie mit der Anwendung dieser vertraut ist. sipgate sichert ferner zu, dass sie seine Beschäftigten mit den für sie maßgeblichen Bestimmungen des Datenschutzes vertraut macht und zur Vertraulichkeit verpflichtet hat.

(3) Die Verpflichtung der Beschäftigten nach Absatz 2 sind dem Kunden auf Anfrage nachzuweisen.

11. Wahrung von Betroffenenrechten

(1) Der Kunde ist für die Wahrung der Betroffenenrechte allein verantwortlich. sipgate ist verpflichtet, den Kunden bei seiner Pflicht, Anträge von Betroffenen nach Art. 12-23 DSGVO zu bearbeiten, zu unterstützten. sipgate hat dabei insbesondere Sorge dafür zu tragen, dass die insoweit erforderlichen Informationen unverzüglich an den Kunden erteilt werden, damit dieser insbesondere seinen Pflichten aus Art. 12 Abs. 3 DSGVO nachkommen kann.

(2) Soweit eine Mitwirkung der sipgate für die Wahrung von Betroffenenrechten - insbesondere auf Auskunft, Berichtigung, Sperrung oder Löschung - durch den Kunden erforderlich ist, wird sipgate die jeweils erforderlichen Maßnahmen nach Weisung des Kunden treffen. sipgate wird den Kunden nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nachzukommen. sipgate ist berechtigt, für diese Leistungen eine angemessene Vergütung vom Kunden zu verlangen.

(3) Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch Mitwirkungsleistungen im Zusammenhang mit Geltendmachung von Betroffenenrechten gegenüber dem Kunden bei sipgate entstehen, bleiben unberührt.

12. Geheimhaltungspflichten

(1) Beide Parteien verpflichten sich, alle Informationen, die sie im Zusammenhang mit der Durchführung dieses Vertrages erhalten, zeitlich unbegrenzt vertraulich zu behandeln und nur zur Durchführung des Vertrages zu verwenden. Keine Partei ist berechtigt, diese Informationen ganz oder teilweise zu anderen als den soeben genannten Zwecken zu nutzen oder diese Information Dritten zugänglich zu machen.

(2) Die vorstehende Verpflichtung gilt nicht für Informationen, die eine der Parteien nachweisbar von Dritten erhalten hat, ohne zur Geheimhaltung verpflichtet zu sein, oder die öffentlich bekannt sind.

13. Vergütung

Für diesen Vertrag erhält sipgate keine gesonderte Vergütung, soweit dies nicht ausdrücklich erwähnt wird.

14. Technische und organisatorische Maßnahmen zur Datensicherheit

(1) sipgate verpflichtet sich gegenüber dem Kunden zur Einhaltung der technischen und organisatorischen Maßnahmen, die zur Einhaltung der anzuwendenden Datenschutzvorschriften erforderlich sind. Dies beinhaltet insbesondere die Vorgaben aus Art. 32 DSGVO.

(2) Der zum Zeitpunkt des Vertragsschlusses bestehende Stand der technischen und organisatorischen Maßnahmen ist als **Anlage 3** zu diesem Vertrag beigefügt. Die Parteien sind sich darüber einig, dass zur Anpassung an technische und rechtliche Gegebenheiten Änderungen der technischen und organisatorischen Maßnahmen erforderlich werden können. Wesentliche Änderungen, die die Integrität, Vertraulichkeit oder Verfügbarkeit der personenbezogenen Daten beeinträchtigen können, wird sipgate im Voraus mit dem Kunden abstimmen. Maßnahmen, die lediglich geringfügige technische oder organisatorische Änderungen mit sich bringen und die Integrität, Vertraulichkeit und Verfügbarkeit der personenbezogenen Daten nicht negativ beeinträchtigen, können von sipgate ohne Abstimmung mit dem Kunden umgesetzt werden. Der Kunde kann jederzeit eine aktuelle Fassung der von sipgate getroffenen technischen und organisatorischen Maßnahmen anfordern.

(3) sipgate wird die von ihm getroffenen technischen und organisatorischen Maßnahmen regelmäßig und auch anlassbezogen auf ihre Wirksamkeit kontrollieren. Für den Fall, dass es Optimierungs- und/oder Änderungsbedarf gibt, wird sipgate den Kunden informieren.

15. Dauer des Auftrags

(1) Der Vertrag beginnt mit der Beauftragung und wird auf unbestimmte Zeit geschlossen.

(2) Der Vertrag endet bei Kündigung des Hauptvertrages (Telekommunikationsvertrag) ohne dass es einer gesonderten Kündigung bedarf.

Etwaige Lösch- und Rückgabepflichten nach Beendigung dieses Vertrages sind in Ziffer 16. geregelt.

(3) Der Kunde kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß der sipgate gegen die anzuwendenden Datenschutzvorschriften oder gegen Pflichten aus diesem Vertrag vorliegt, sipgate eine Weisung des Kunden nicht ausführen kann oder will oder sipgate den Zutritt des Kunden oder der zuständigen Aufsichtsbehörde vertragswidrig verweigert.

16. Beendigung

(1) Nach Beendigung des Vertrages hat sipgate sämtliche in seinen Besitz gelangten Unterlagen, Daten und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, nach Wahl des Kunden an diesen zurückzugeben

oder zu löschen. Die Löschung ist in geeigneter Weise zu dokumentieren. Etwaige gesetzliche Aufbewahrungspflichten oder sonstige Pflichten zur Speicherung der Daten bleiben unberührt. Für Datenträger gilt, dass diese im Falle einer vom Kunden gewünschten Löschung zu vernichten sind, wobei mindestens die Sicherheitsstufe 3 der DIN 66399 einzuhalten ist; die Vernichtung ist dem Kunden unter Hinweis auf die Sicherheitsstufe gemäß DIN 66399 nachzuweisen.

(2) Der Kunde hat das Recht, die vollständige und vertragsgemäße Rückgabe und Löschung der Daten bei sipgate zu kontrollieren. Dies kann auch durch eine Inaugenscheinnahme der Datenverarbeitungsanlagen in der Betriebsstätte der sipgate erfolgen. Die Vor-Ort-Kontrolle soll mit angemessener Frist durch den Kunden angekündigt werden.

17. Zurückbehaltungsrecht

Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch sipgate i.S.d. § 273 BGB hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen wird.

18. Schlussbestimmungen

(1) Sollte das Eigentum des Kunden bei sipgate durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat sipgate den Kunden unverzüglich zu informieren. sipgate wird die Gläubiger über die Tatsache, dass es sich um Daten handelt, die im Auftrag verarbeitet werden, unverzüglich informieren.

(2) Für Nebenabreden ist die Schriftform erforderlich.

(3) Sollten einzelne Teile dieses Vertrages unwirksam sein, so berührt dies die Wirksamkeit der übrigen Regelungen des Vertrages nicht.

Anlage 1 - Gegenstand des Auftrags

1. Gegenstand und Zweck der Verarbeitung

Der Auftrag des Kunden an sipgate umfasst - vorausgesetzt, der Kunde hat die entsprechenden Funktionen gebucht und aktiviert - folgende Arbeiten und/oder Leistungen:

- Bereitstellung von (in der jeweils geltenden Leistungsbeschreibung näher beschriebenen) Telekommunkationsdienstleistungen, insbesondere die Bereitstellung der Aufbereitung von ein-/ausgehenden Anrufen/Nachrichten/Faxsendungen/Transkriptionen eingegangener Voicemails in der App satellite .

- Bereitstellung der AI-Features der sipgate GmbH: Mittels des Dienstes gpt der OpenAI werden auf Grundlage einer Transkription eines Gespräches verschiedene Produktivitätsfeatures angeboten (automatische Gesprächszusammenfassung mit Verschlagwortung).
  HINWEIS: Diese Features müssen separat aktiviert werden. Hierbei hat der Nutzer seine Einwilligung zu erteilen. Die App ist auch ohne diese Features uneingeschränkt nutzbar.

2. Art(en) der personenbezogenen Daten

Folgende Datenarten sind regelmäßig Gegenstand der Verarbeitung:
Verkehrsdaten, Inhaltsdaten, Kontakt-, Personenstamm- und Kommunikationsdaten (Name, Adresse, Telefonnummer, Faxnummer, Email-Adresse).

3. Kreis betroffener Personen

Kreis der von der Datenverarbeitung betroffenen Personen:
Benutzer Ihres Accounts, anrufende und angerufene Teilnehmer bzw. Sender/Empfänger von SMS/Fax, Beschäftigte, Kunden, Geschäftspartner, Interessenten und Dienstleister des Kunden.

4. Ort der Datenverarbeitung:

Alle Daten werden auf Servern in der EU verarbeitet.

Anlage 2 - Unterauftragnehmer

sipgate nimmt für die Verarbeitung von Daten im Auftrag des Kunden Leistungen von Dritten in Anspruch, die in seinem Auftrag Daten verarbeiten („Unterauftragnehmer“).

Firma, Anschrift	Art der Verarbeitung	Zweck	Art der Daten	Kategorien der betroffenen Personen
Myloc managed IT AG, Am Gatherhof 44 40472 Düsseldorf Deutschland; Interxion Deutschland GmbH, Hanauer Landstraße 298, 60314 Frankfurt am Main, Deutschland	Betreiber RZ	Realisierung der Dienste der sipgate GmbH	Verkehrs-, Inhaltsdaten	Kunden der sipgate GmbH
argon networks UG (haftungsbeschr.), Gladbacher Str. 74, 40219 Düsseldorf	Erbringung von Telekommunikations-Vorleistungen	Realisierung der Dienste der sipgate GmbH	Verkehrs-, Inhalts-, Kontakt-, Personenstammdaten	Kunden der sipgate GmbH
netzquadrat GmbH, Gladbacher Str. 74, 40219 Düsseldorf	Erbringung von Telekommunikations-Vorleistungen	Realisierung der Dienste der sipgate GmbH	Verkehrs-, Inhalts-, Kontakt-, Personenstammdaten	Kunden der sipgate GmbH
sipgate Wireless GmbH, Gladbacher Str. 74, 40219 Düsseldorf	Erbringung von Telekommunikations-Vorleistungen	Realisierung der Dienste der sipgate GmbH	Verkehrs-, Inhalts-, Kontakt-, Personenstammdaten	Kunden der sipgate GmbH
impacx services GmbH (vormals firmierend unter Telinform customer-solutions GmbH), Siemensstr. 32, 47533 Kleve	Call Center-Dienstleistungen	Sicherstellung einer Erreichbarkeit des Kundenservices auch außerhalb der Bürozeiten	Bestands-, Kontakt-, Inhalts-, Vertragsdaten	Kunden, Interessenten und Mitarbeiter der sipgate GmbH

Firma, Anschrift	Art der Verarbeitung	Zweck	Art der Daten	Kategorien der betroffenen Personen
Google Ireland Limited, mit Sitz in Gordon House, Barrow Street, Dublin 4, Irland	Erstellung einer Transkription des Telefonates	Realisierung der AI-Features der sipgate GmbH	Inhaltsdsdaten	Kunden der sipgate GmbH, die die AI-Features nutzen und eine entsprechende Einwilligung erteilt haben; Gesprächspartner dieser Kunden
OpenAI OpCo LLC, 3180 18th St., Suite 100 San Francisco, California 94110, United States	Mittels des Dienstes gpt der OpenAI werden auf Grundlage einer Transkription des Gespräches verschiedene Produktivitätsfeatures (automatische Gesprächszusammenfassung mit Verschlagwortung) realisiert.	Realisierung der AI-Features der sipgate GmbH	Inhaltsdsdaten	Kunden der sipgate GmbH, die die AI-Features nutzen und eine entsprechende Einwilligung erteilt haben; Gesprächspartner dieser Kunden

Anlage 3

Technische und organisatorische Maßnahmen der sipgate

sipgate trifft nachfolgende technische und organisatorische Maßnahmen zur Datensicherheit i.S.d. Art. 32 DSGVO.

1. Vertraulichkeit

Zutrittskontrolle

Um den Zutritt Unbefugter zu den Datenverarbeitungsanlagen, mit denen Daten verarbeitet oder genutzt werden, zu verhindern hat sipgate umfangreiche formale Zutrittskontrollprozesse implementiert.

Der Standort Gladbacher Str. 74 beherbergt neben den Büros der sipgate einen Server und einen Servertechnikraum. Für den Zutritt zum Büro werden an ausgewählte Mitarbeiter elektronische Schlüssel vergeben. Die Schlüssel berechtigen den jeweiligen Mitarbeiter nur zur Öffnung/Schließung einzelner dafür zugelassener Türen. Alle Öffnungs- und Schließvorgänge eines Schlüssels werden gemeinsam mit der eindeutigen ID des Schlüssels elektronisch protokolliert. Für die Verwaltung der Schlüssel sind ausschließlich durch die Geschäftsleitung direkt autorisierte Mitarbeiter zuständig.

Der Serverraum ist jederzeit verschlossen und kann nur von ausgewählten Mitarbeitern betreten werden.

Innerhalb des Gebäudes sind die Zutrittsrechte der Mitarbeiter, auch solcher die über einen Schlüssel verfügen, auf das zur konkreten Aufgabenerfüllung notwendige Maß beschränkt. Innerhalb der Geschäftszeiten wird beim Betreten des Gebäudes am ständig besetzten Empfang des Gebäudes eine Personenkontrolle durchgeführt. Außerhalb der Geschäftszeiten sind alle Zugänge zum Gebäude verschlossen und alarmgesichert. Das Gebäude wird zusätzlich durch einen Wachdienst gesichert. Alle Alarme der Alarmanlage werden direkt an einen Wachdienst gemeldet.

In allen Rechenzentren kommen die standardmäßigen Sicherheitsmaßnahmen zur Anwendung. Diese entsprechen dem Stand der Technik. Es handelt sich unter anderem um elektronische Zugangskontrollsysteme mit Protokollierung, wobei nur autorisierte Personen das Gebäude betreten dürfen, Alarmsysteme, Videoüberwachung Innen/Außen, 24/7 anwesendes Sicherheitspersonal, Alarmanlagen, Sicherung des Gebäudes mit Stacheldraht, Absicherung durch externe Wachdienste, die im Alarmfall über eine dezidierte Alarmleitung automatisch informiert werden.

Die Schlüssel zu den einzelnen Räumen und Cages im Rechenzentrum müssen stets beim Sicherheitspersonal abgeholt werden.

Zugangskontrolle

Um zu gewährleisten, dass Datenverarbeitungssysteme nur durch berechtigte genutzt werden können setzt sipgate zur Verwaltung der Zugangsberechtigungen ein zentrales System ein. Die Zugangsberechtigungen werden durch den technischen Leiter der sipgate vergeben. Die Verwaltung dieser Zugangsberechtigungen erfolgt durch autorisierte Administratoren.

Ein Fernzugriff auf Server der sipgate zu administrativen Zwecken, z.B. zur Wartung der Systeme, ist nur über verschlüsselte Verbindungen und nach vorheriger Authentifizierung möglich.

Zugriffskontrolle

Um zu gewährleisten, dass die zur Benutzung eines Systems zur Verarbeitung von Daten Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass gespeicherte oder in Verarbeitung befindliche Daten nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, setzt sipgate ein zentrales System zur Verwaltung der Zugriffsberechtigungen ein. Alle Zugriffe werden lokal und im zentralen Logserver gespeichert. Administrative Rechte sind nur über ein zentrales Verwaltungsprogramm ausführbar.

Der Zugriff auf alle Daten ist bei allen Berechtigten auf das zur konkreten Aufgabenerfüllung notwendige Maß beschränkt. Hierbei werden die gesetzlichen Datenschutzanforderungen, insbesondere solche der Datenschutzgrundverordnung (DSGVO), des Telekommunikation-Telemedien-Datenschutz-Gesetzes (TTDSG) und desTelekommunikationsgesetzes (TKG) eingehalten.

Trennung

sipgate verarbeitet die Daten auf Serversystemen, die durch ein System logischer und physischer Zugriffskontrollen im Netzwerk logisch getrennt sind.

2. Integrität

Eingabekontrolle

Um zu gewährleisten, dass sipgate nachträglich überprüfen und feststellen kann, ob und von wem Daten in den Datenverarbeitungssystemen eingegeben, verändert oder entfernt

worden sind, werden alle Zugriffe auf die gespeicherten Daten des Kunden lokal und im zentralen Logserver protokolliert.

Weitergabekontrolle

Um zu gewährleisten, dass Daten bei der elektronischen Übertragung, während des Transportes oder ihrer Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft werden kann, an welchen Stellen die Übertragung von Daten durch Systeme zur Datenübertragung vorgesehen sind, unterliegt der Zugriff auf sämtliche Systeme, die Kundendaten verarbeiten, wirksamen Zugriffskontrollen. Diese Mechanismen zur Zugriffskontrolle sind bereits oben unter 3. näher beschrieben.

3. Verfügbarkeit und Belastbarkeit

sipgate verwendet in allen Systemen eine Kombination aus redundanten Systemen und BackupLösungen, um die gespeicherten Daten zu schützen und ggf. wiederherstellen zu können. Diese Systeme werden ausschließlich in nach dem aktuellen Stand der Technik gesicherten und ausgestatteten Räumlichkeiten betrieben, die über die notwendige Klimatisierung, Feuer- und Rauchmeldeanlagen verfügen und für die detailierte Notfallpläne bestehen.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Alle nach dieser Anlage getroffenen Maßnahmen werden regelmäßig auf ihre Wirksamkeit hin geprüft und erforderlichenfalls entsprechend dem Stand der Technik fortentwickelt und angepasst.

sipgate hält nach § 166 Telekommunikationsgesetz (TKG) ein (nicht öffentliches) Sicherheitskonzept zum Schutz des Fernmeldegeheimnisses und gegen die Verletzung des Schutzes personenbezogener Daten vor, aktualisiert dieses fortlaufend und wird in dieser Hinsicht regelmäßig durch die zuständige Aufsichtsbehörde geprüft.

Weiterhin werden alle Mitarbeiter regelmäßig zu Themen des Datenschutzes geschult. Diese Schulungen werden komplett inhouse realisiert, sodass eine genaue Abstimmung auf die bei sipgate maßgeblichen Fragen möglich ist. Es werden im Rahmen dieser Schulungen werden auch individuelle Fragen eingehend behandelt.

Alle Mitarbeiter der sipgate, die im Rahmen ihrer Tätigkeit mit der Verarbeitung personenbezogener Daten in Berührung kommen, sind auf den vertraulichen Umgang mit personenbezogenen Daten verpflichtet. Dies geschieht regelmäßig bereits bei der Einstellung neuer Mitarbeiter mittels einer vertraglichen Verpflichtungserklärung, die jeder Mitarbeiter abzugeben hat.

sipgate hat einen Beauftragten für den Datenschutz bestellt.

sipgate unterhält ein Verzeichnis von Verarbeitungstätigkeiten i.S.d. Art. 30 Abs. 1 und 2 DSGVO. Dieses Verarbeitungsverzeichnis ist nicht öffentlich.