Vertrag über die Auftragsverarbeitung

Inhaltsverzeichnis

1. Vertragsgegenstand 3
2. Anwendung der EU Standardvertragsklauseln 3
3. Ergänzungen zu den EU Standardvertragsklauseln 3
4. Gegenstand des Auftrags 3
5. Dauer des Auftrags 4

Anlagenverzeichnis 4

For English version please see after page 33

Lime Connect (Userlike) GmbH
(nachfolgend "**Lime Connect**" bezeichnet)

Kölnturm, Im Mediapark 8

50670 Köln

verpflichtet sich als Auftragnehmer gegenüber dem Kunden (nachfolgend entweder als „**Kunde**" oder „**Auftraggeber**" bezeichnet)

nach Maßgabe der folgenden Bestimmungen:

1. Vertragsgegenstand

Dieser Vertrag zur Auftragsverarbeitung gemäß Art 28 DSGVO (nachfolgend **„Vertrag“**) konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, welche sich aus den zwischen den Parteien bereits bestehenden oder künftig abzuschließenden Verträgen (nachfolgend **„Hauptvertrag/AGB“**) ergeben, unter denen es zu einer Verarbeitung personenbezogener Daten durch Lime Connect für den Auftraggeber kommt. Er findet Anwendung auf alle Tätigkeiten, die mit dem Gegenstand des Auftrags (Ziffer 4) in Zusammenhang stehen und bei denen Beschäftigte von Lime Connect (Userlike) GmbH oder durch Lime Connect (Userlike) GmbH Beauftragte, personenbezogene Daten des Verantwortlichen verarbeiten.

2. Anwendung der EU-Standardvertragsklauseln

2.1 Die Parteien legen diesem Vertrag in **Anlage 1** die „Standardvertragsklauseln für Verantwortliche und Auftragsverarbeiter in der EU / im EWR“ gemäß Durchführungsbeschluss der Kommission über Standardvertragsklauseln zwischen Verantwortlichen und Auftragsverarbeitern gemäß Artikel 28 (7) DSGVO und Artikel 29 (7) der Verordnung (EU) 2018/1725 vom 4. Juni 2021 (nachfolgend **„EU-Standardvertragsklauseln“**) zugrunde.

3. Ergänzungen zu den EU-Standardvertragsklauseln

Die Parteien vereinbaren in **Anlage 5** Ergänzungen und Aktualisierungen zu den EU-Standardvertragsklauseln im Sinne der Klausel 2 der EU-Standardvertragsklauseln.

4. Gegenstand des Auftrags

Gegenstand der Verarbeitung ist die Bereitstellung der im Hauptvertrag/**AGB** bezeichneten Lime Connect Services durch den Auftragnehmer für den Auftraggeber.

Lime Connect bietet eine Messenger Funktion für den Web- und Mobilsupport. Die softwarebasierte Lösung zur Chat-Kommunikation bietet einen Kundensupport in Echtzeit und asynchroner Kommunikation, und hilft den Kundenservice auszubauen.

5. Dauer des Auftrags

Die Laufzeit und Kündigung dieses Vertrags richten sich nach den Bestimmungen zur Laufzeit und Kündigung des Hauptvertrags/**AGB.** Eine Kündigung des Hauptvertrags/**AGB** bewirkt automatisch auch eine Kündigung dieses Vertrags. Eine isolierte Kündigung dieses Vertrags ist ausgeschlossen.

Anlagenverzeichnis:

- **Anlage 1:** EU-Standardvertragsklauseln (Standardvertragsklauseln für Verantwortliche und Auftragsverarbeiter in der EU / im EWR – Stand: 4. Juni 2021, Sprache: deutsch)
- **Anlage 2:** Zweck, Art und Umfang der Datenverarbeitung, Art der Daten und Kategorien der betroffenen Personen
- **Anlage 3:** Unterauftragsverarbeiter
- **Anlage 4:** Technische und organisatorische Maßnahmen gem. Art 32 DSGVO
- **Anlage 5:** Ergänzungen zu den EU-Standardvertragsklauseln

Anlage 1: EU-Standardvertragsklauseln (Stand 4. Juni 2021)

Abschnitt I

Klausel 1 - Zweck und Anwendungsbereich

a) Mit diesen Standardvertragsklauseln (im Folgenden „Klauseln“) soll die Einhaltung von Artikel 28 Absätze 3 und 4 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)] sichergestellt werden.
b) Die aufgeführten Verantwortlichen und Auftragsverarbeiter haben diesen Klauseln zugestimmt, um die Einhaltung von Artikel 28 Absätze 3 und 4 der Verordnung (EU) 2016/679 und/oder Artikel 29 Absätze 3 und 4 der Verordnung (EU) 2018/1725 zu gewährleisten.
c) Diese Klauseln gelten für die Verarbeitung personenbezogener Daten gemäß Anlage 2.
d) Die Anhänge 2 bis 5 sind Bestandteil der Klauseln.
e) Diese Klauseln gelten unbeschadet der Verpflichtungen, denen der Verantwortliche gemäß der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 unterliegt.
f) Diese Klauseln stellen für sich allein genommen nicht sicher, dass die Verpflichtungen im Zusammenhang mit internationalen Datenübermittlungen gemäß Kapitel V der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 erfüllt werden.

Klausel 2 – Unabänderbarkeit der Klauseln

a) Die Parteien verpflichten sich, die Klauseln nicht zu ändern, es sei denn, zur Ergänzung oder Aktualisierung der in den Anhängen angegebenen Informationen.
b) Dies hindert die Parteien nicht daran die in diesen Klauseln festgelegten Standardvertragsklauseln in einen umfangreicheren Vertrag aufzunehmen und weitere Klauseln oder zusätzliche Garantien hinzuzufügen, sofern diese weder unmittelbar noch mittelbar im Widerspruch zu den Klauseln stehen oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneiden.

Klausel 3 – Auslegung

a) Werden in diesen Klauseln die in der Verordnung (EU) 2016/679 bzw. der Verordnung (EU) 2018/1725 definierten Begriffe verwendet, so haben diese Begriffe dieselbe Bedeutung wie in der betreffenden Verordnung.
b) Diese Klauseln sind im Lichte der Bestimmungen der Verordnung (EU) 2016/679 bzw. der Verordnung (EU) 2018/1725 auszulegen.
c) Diese Klauseln dürfen nicht in einer Weise ausgelegt werden, die den in der Verordnung (EU) 2016/679 oder der Verordnung (EU) 2018/1725 vorgesehenen Rechten und Pflichten zuwiderläuft oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneidet.

Klausel 4 – Vorrang

Im Falle eines Widerspruchs zwischen diesen Klauseln und den Bestimmungen damit zusammenhängender Vereinbarungen, die zwischen den Parteien bestehen oder später eingegangen oder geschlossen werden, haben diese Klauseln Vorrang.

Klausel 5 – fakultative Kopplungsklausel

a) Eine Einrichtung, die nicht Partei dieser Klauseln ist, kann diesen Klauseln mit Zustimmung aller Parteien jederzeit als Verantwortlicher oder als Auftragsverarbeiter beitreten, indem sie die Anhänge ausfüllt und Anhang I unterzeichnet.
b) Nach Ausfüllen und Unterzeichnen der unter Buchstabe a genannten Anhänge wird die beitretende Einrichtung als Partei dieser Klauseln behandelt und hat die Rechte und Pflichten eines Verantwortlichen oder eines Auftragsverarbeiters entsprechend ihrer Bezeichnung in Anhang I.
c) Für die beitretende Einrichtung gelten für den Zeitraum vor ihrem Beitritt als Partei keine aus diesen Klauseln resultierenden Rechte oder Pflichten.

Abschnitt II

Klausel 6 – Beschreibung der Verarbeitung

Die Einzelheiten der Verarbeitungsvorgänge, insbesondere die Kategorien personenbezogener Daten und die Zwecke, für die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden, sind in Anlage 2 aufgeführt.

Klausel 7 – Pflichten der Parteien

7.1 Weisungen

a) Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen, es sei denn, er ist nach Unionsrecht oder nach dem Recht eines Mitgliedstaats, dem er unterliegt, zur Verarbeitung verpflichtet. In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet. Der Verantwortliche kann während der gesamten Dauer der Verarbeitung personenbezogener Daten weitere Weisungen erteilen. Diese Weisungen sind stets zu dokumentieren.
b) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass vom Verantwortlichen erteilte Weisungen gegen die Verordnung (EU) 2016/679, die Verordnung (EU) 2018/1725 oder geltende Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstoßen.

7.2 Zweckbindung

Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten nur für den/die in Anlage 2 genannten spezifischen Zweck(e), sofern er keine weiteren Weisungen des Verantwortlichen erhält.

7.3 Dauer der Verarbeitung personenbezogener Daten

Die Daten werden vom Auftragsverarbeiter nur für den in den **AGB** vereinbartem Leistungszeitraum verarbeitet.

7.4 Sicherheit der Verarbeitung

a) Der Auftragsverarbeiter ergreift mindestens die in Anlage 4 aufgeführten technischen und organisatorischen Maßnahmen, um die Sicherheit der personenbezogenen Daten zu gewährleisten. Dies umfasst den Schutz der Daten vor einer Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu den Daten führt (im Folgenden „Verletzung des Schutzes personenbezogener Daten“). Bei der Beurteilung des angemessenen Schutzniveaus tragen die Parteien dem Stand der Technik, den Implementierungskosten, der Art, dem Umfang, den Umständen und den Zwecken der Verarbeitung sowie den für die betroffenen Personen verbundenen Risiken gebührend Rechnung.
b) Der Auftragsverarbeiter gewährt seinem Personal nur insoweit Zugang zu den personenbezogenen Daten, die Gegenstand der Verarbeitung sind, als dies für die

Durchführung, Verwaltung und Überwachung des Vertrags unbedingt erforderlich ist. Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung der erhaltenen personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

7.5 Sensible Daten

Falls die Verarbeitung personenbezogene Daten betrifft, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, oder die genetische Daten oder biometrische Daten zum Zweck der eindeutigen Identifizierung einer natürlichen Person, Daten über die Gesundheit, das Sexualleben oder die sexuelle Ausrichtung einer Person oder Daten über strafrechtliche Verurteilungen und Straftaten enthalten (im Folgenden „sensible Daten“), wendet der Auftragsverarbeiter spezielle Beschränkungen und/oder zusätzlichen Garantien an, soweit dies möglich ist.

7.6 Dokumentation und Einhaltung der Klauseln

a) Die Parteien müssen die Einhaltung dieser Klauseln nachweisen können.
b) Der Auftragsverarbeiter bearbeitet Anfragen des Verantwortlichen bezüglich der Verarbeitung von Daten gemäß diesen Klauseln umgehend und in angemessener Weise.
c) Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, die für den Nachweis der Einhaltung der in diesen Klauseln festgelegten und unmittelbar aus der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 hervorgehenden Pflichten erforderlich sind. Auf Verlangen des Verantwortlichen gestattet der Auftragsverarbeiter ebenfalls die Prüfung der unter diese Klauseln fallenden Verarbeitungstätigkeiten in angemessenen Abständen oder bei Anzeichen für eine Nichteinhaltung und trägt zu einer solchen Prüfung bei. Bei der Entscheidung über eine Überprüfung oder Prüfung kann der Verantwortliche einschlägige Zertifizierungen des Auftragsverarbeiters berücksichtigen.
d) Der Verantwortliche kann die Prüfung selbst durchführen oder einen unabhängigen Prüfer beauftragen. Die Prüfungen können auch Inspektionen in den Räumlichkeiten oder physischen Einrichtungen des Auftragsverarbeiters umfassen und werden gegebenenfalls mit angemessener Vorankündigung durchgeführt.
e) Die Parteien stellen der/den zuständigen Aufsichtsbehörde(n) die in dieser Klausel genannten Informationen, einschließlich der Ergebnisse von Prüfungen, auf Anfrage zur Verfügung.

7.7 Einsatz von Unterauftragsverarbeitern

a) ALLGEMEINE SCHRIFTLICHE GENEHMIGUNG: Der Auftragsverarbeiter besitzt die allgemeine Genehmigung des Verantwortlichen für die Beauftragung von Unterauftragsverarbeitern, die in einer vereinbarten Liste aufgeführt sind. Der Auftragsverarbeiter unterrichtet den Verantwortlichen mindestens 30 Tage (siehe Anlage 5 Ziffer 2) im Voraus ausdrücklich in schriftlicher Form über alle beabsichtigten Änderungen dieser Liste durch Hinzufügen oder Ersetzen von Unterauftragsverarbeitern und räumt dem Verantwortlichen damit ausreichend Zeit ein, um vor der Beauftragung des/der betreffenden Unterauftragsverarbeiter/s Einwände gegen diese Änderungen erheben zu können. Der Auftragsverarbeiter stellt dem Verantwortlichen die erforderlichen Informationen zur Verfügung, damit dieser sein Widerspruchsrecht ausüben kann.

b) Beauftragt der Auftragsverarbeiter einen Unterauftragsverarbeiter mit der Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen), so muss diese Beauftragung im Wege eines Vertrags erfolgen, der dem Unterauftragsverarbeiter im Wesentlichen dieselben Datenschutzpflichten auferlegt wie diejenigen, die für den Auftragsverarbeiter gemäß diesen Klauseln gelten. Der Auftragsverarbeiter stellt sicher, dass der Unterauftragsverarbeiter die Pflichten erfüllt, denen der Auftragsverarbeiter entsprechend diesen Klauseln und gemäß der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 unterliegt.

c) Der Auftragsverarbeiter stellt dem Verantwortlichen auf dessen Verlangen eine Kopie einer solchen Untervergabevereinbarung und etwaiger späterer Änderungen zur Verfügung. Soweit es zum Schutz von Geschäftsgeheimnissen oder anderen vertraulichen Informationen, einschließlich personenbezogener Daten notwendig ist, kann der Auftragsverarbeiter den Wortlaut der Vereinbarung vor der Weitergabe einer Kopie unkenntlich machen.

d) Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen in vollem Umfang dafür, dass der Unterauftragsverarbeiter seinen Pflichten gemäß dem mit dem Auftragsverarbeiter geschlossenen Vertrag nachkommt. Der Auftragsverarbeiter benachrichtigt den Verantwortlichen, wenn der Unterauftragsverarbeiter seine vertraglichen Pflichten nicht erfüllt.

e) Der Auftragsverarbeiter vereinbart mit dem Unterauftragsverarbeiter eine Drittbegünstigtenklausel, wonach der Verantwortliche – im Falle, dass der Auftragsverarbeiter faktisch oder rechtlich nicht mehr besteht oder zahlungsunfähig ist – das Recht hat, den Untervergabevertrag zu kündigen und den Unterauftragsverarbeiter anzuweisen, die personenbezogenen Daten zu löschen oder zurückzugeben.

7.8 Internationale Datenübermittlung

a) Jede Übermittlung von Daten durch den Auftragsverarbeiter an ein Drittland oder eine internationale Organisation erfolgt ausschließlich auf der Grundlage

dokumentierter Weisungen des Verantwortlichen oder zur Einhaltung einer speziellen Bestimmung nach dem Unionsrecht oder dem Recht eines Mitgliedstaats, dem der Auftragsverarbeiter unterliegt, und muss mit Kapitel V der Verordnung (EU) 2016/679 oder der Verordnung (EU) 2018/1725 im Einklang stehen.

b) Der Verantwortliche erklärt sich damit einverstanden, dass in Fällen, in denen der Auftragsverarbeiter einen Unterauftragsverarbeiter gemäß Klausel 7.7 für die Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen) in Anspruch nimmt und diese Verarbeitungstätigkeiten eine Übermittlung personenbezogener Daten im Sinne von Kapitel V der Verordnung (EU) 2016/679 beinhalten, der Auftragsverarbeiter und der Unterauftragsverarbeiter die Einhaltung von Kapitel V der Verordnung (EU) 2016/679 sicherstellen können, indem sie Standardvertragsklauseln verwenden, die von der Kommission gemäß Artikel 46 Absatz 2 der Verordnung (EU) 2016/679 erlassen wurden, sofern die Voraussetzungen für die Anwendung dieser Standardvertragsklauseln erfüllt sind.

Klausel 8 – Unterstützung des Verantwortlichen

a) Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich über jeden Antrag, den er von der betroffenen Person erhalten hat. Er beantwortet den Antrag nicht selbst, es sei denn, er wurde vom Verantwortlichen dazu ermächtigt.

b) Unter Berücksichtigung der Art der Verarbeitung unterstützt der Auftragsverarbeiter den Verantwortlichen bei der Erfüllung von dessen Pflicht, Anträge betroffener Personen auf Ausübung ihrer Rechte zu beantworten. Bei der Erfüllung seiner Pflichten gemäß den Buchstaben a und b befolgt der Auftragsverarbeiter die Weisungen des Verantwortlichen.

c) Abgesehen von der Pflicht des Auftragsverarbeiters, den Verantwortlichen gemäß Klausel 8 Buchstabe b zu unterstützen, unterstützt der Auftragsverarbeiter unter Berücksichtigung der Art der Datenverarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen zudem bei der Einhaltung der folgenden Pflichten:

   1) Pflicht zur Durchführung einer Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten (im Folgenden „Datenschutz Folgenabschätzung“), wenn eine Form der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat;
   2) Pflicht zur Konsultation der zuständigen Aufsichtsbehörde(n) vor der Verarbeitung, wenn aus einer Datenschutz- Folgenabschätzung hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft;
   3) Pflicht zur Gewährleistung, dass die personenbezogenen Daten sachlich richtig und auf dem neuesten Stand sind, indem der Auftragsverarbeiter den Verantwortlichen unverzüglich unterrichtet, wenn er feststellt, dass die von ihm verarbeiteten personenbezogenen Daten unrichtig oder veraltet sind;

4) Verpflichtungen gemäß OPTION 1: Artikel 32 der Verordnung (EU) 2016/679].

d) Die Parteien legen in Anlage 4 die geeigneten technischen und organisatorischen Maßnahmen zur Unterstützung des Verantwortlichen durch den Auftragsverarbeiter bei der Anwendung dieser Klausel sowie den Anwendungsbereich und den Umfang der erforderlichen Unterstützung fest.

Klausel 9 – Meldung von Verletzung des Schutzes personenbezogener Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten arbeitet der Auftragsverarbeiter mit dem Verantwortlichen zusammen und unterstützt ihn entsprechend, damit der Verantwortliche seinen Verpflichtungen gemäß den Artikeln 33 und 34 der Verordnung (EU) 2016/679 oder gegebenenfalls den Artikeln 34 und 35 der Verordnung (EU) 2018/1725 nachkommen kann, wobei der Auftragsverarbeiter die Art der Verarbeitung und die ihm zur Verfügung stehenden Informationen berücksichtigt.

9.1 Verletzung des Schutzes der vom Verantwortlichen verarbeiteten Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Verantwortlichen verarbeiteten Daten unterstützt der Auftragsverarbeiter den Verantwortlichen wie folgt:

a) bei der unverzüglichen Meldung der Verletzung des Schutzes personenbezogener Daten an die zuständige(n) Aufsichtsbehörde(n), nachdem dem Verantwortlichen die Verletzung bekannt wurde, sofern relevant (es sei denn, die Verletzung des Schutzes personenbezogener Daten führt voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen);

b) bei der Einholung der folgenden Informationen, die gemäß Artikel 33 Absatz 3 der Verordnung (EU) 2016/679] in der Meldung des Verantwortlichen anzugeben sind, wobei diese Informationen mindestens Folgendes umfassen müssen:

   1) die Art der personenbezogenen Daten, soweit möglich, mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen sowie der Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
   2) die wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
   3) die vom Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Wenn und soweit nicht alle diese Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt;

c) bei der Einhaltung der Pflicht gemäß Artikel 34 der Verordnung (EU) 2016/679], die betroffene Person unverzüglich von der Verletzung des Schutzes personenbezogener Daten zu benachrichtigen, wenn diese Verletzung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat.

9.2 Verletzung des Schutzes der vom Auftragsverarbeiter verarbeiteten Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Auftragsverarbeiter verarbeiteten Daten meldet der Auftragsverarbeiter diese dem Verantwortlichen unverzüglich, nachdem ihm die Verletzung bekannt wurde. Diese Meldung muss zumindest folgende Informationen enthalten:

a) eine Beschreibung der Art der Verletzung (möglichst unter Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen und der ungefähren Zahl der betroffenen Datensätze);
b) Kontaktdaten einer Anlaufstelle, bei der weitere Informationen über die Verletzung des Schutzes personenbezogener Daten eingeholt werden können;
c) die voraussichtlichen Folgen und die ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten, einschließlich Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Wenn und soweit nicht alle diese Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt.

Die Parteien legen Anlage 4 alle sonstigen Angaben fest, die der Auftragsverarbeiter zur Verfügung zu stellen hat, um den Verantwortlichen bei der Erfüllung von dessen Pflichten gemäß Artikel 33 und 34 der Verordnung (EU) 2016/679 zu unterstützen.

Abschnitt III

Klausel 10 – Verstöße gegen die Klauseln und Beendigung des Vertrags

a) Falls der Auftragsverarbeiter seinen Pflichten gemäß diesen Klauseln nicht nachkommt, kann der Verantwortliche – unbeschadet der Bestimmungen der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 – den Auftragsverarbeiter anweisen, die Verarbeitung personenbezogener Daten auszusetzen, bis er diese Klauseln einhält oder der Vertrag beendet ist. Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich, wenn er aus welchen Gründen auch immer nicht in der Lage ist, diese Klauseln einzuhalten.

b) Der Verantwortliche ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn
   1) der Verantwortliche die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter gemäß Buchstabe a ausgesetzt hat und die Einhaltung dieser Klauseln nicht innerhalb einer angemessenen Frist, in jedem Fall aber innerhalb eines Monats nach der Aussetzung, wiederhergestellt wurde;
   2) der Auftragsverarbeiter in erheblichem Umfang oder fortdauernd gegen diese Klauseln verstößt oder seine Verpflichtungen gemäß der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 nicht erfüllt;
   3) der Auftragsverarbeiter einer bindenden Entscheidung eines zuständigen Gerichts oder der zuständigen Aufsichtsbehörde(n), die seine Pflichten gemäß diesen Klauseln, der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 zum Gegenstand hat, nicht nachkommt.

c) Der Auftragsverarbeiter ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn der Verantwortliche auf der Erfüllung seiner Anweisungen besteht, nachdem er vom Auftragsverarbeiter darüber in Kenntnis gesetzt wurde, dass seine Anweisungen gegen geltende rechtliche Anforderungen gemäß Klausel 7.1 Buchstabe b verstoßen.

d) Nach Beendigung des Vertrags löscht der Auftragsverarbeiter nach Wahl des Verantwortlichen alle im Auftrag des Verantwortlichen verarbeiteten personenbezogenen Daten und bescheinigt dem Verantwortlichen, dass dies erfolgt ist, oder er gibt alle personenbezogenen Daten an den Verantwortlichen zurück und löscht bestehende Kopien, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Bis zur Löschung oder Rückgabe der Daten gewährleistet der Auftragsverarbeiter weiterhin die Einhaltung dieser Klauseln.

Anlage 2: Zweck, Art und Umfang der Datenverarbeitung, Art der Daten und Kategorien der betroffenen Personen

1. Zweck der Verarbeitung

Lime Connect bietet eine Messenger Funktion für den Web- und Mobilsupport. Die softwarebasierte Lösung zur Chat-Kommunikation bietet einen Kundensupport in Echtzeit und asynchroner Kommunikation, und hilft den Kundenservice auszubauen.

2. Kategorien von Daten

Die von der Verarbeitung betroffenen Kategorien von Daten hängen von der Nutzung der Lime Connect Services durch den Auftraggeber ab. Als Gegenstand der Verarbeitung in Betracht kommende Kategorien von Daten sind:

Endnutzer

- Chat-Transkript
- E-Mail-Adresse
- Browser
- Betriebssystem
- Endgerät
- Anzahl der Seitenaufrufe
- Anzahl der Seitenbesuche
- Referrer
- URL (wo der Chat gestartet ist)
- Umfrage vor und nach dem Chat (optional)
- Chat-Thema
- Chat-Status (neu, wartend, beendet)
- Chat-Bewertung nach dem Chat
- Dauer des Chats
- Datum des Chats
- Geo-Location (freiwillig, optional)
- Mediale Dateien, die der Kontakt während des Chats mit den Operatoren teilt
- Optionale Datenfelder, die der Auftraggeber an Lime Connect übergibt
- IP-Adresse

Profileinstellungen des Operators

- Username
- Vorname
- Nachname
- Alias-Name
- E-Mail-Adresse
- Sprache
- Zeitzone
- Operator-Gruppe
- Profilfoto
- Chat Transkripte
- Analytics-Kennzahlen zur Chat-Performance
- IP-Adresse

3. Speicherdauer und Löschfristen

Die Löschung personenbezogener Daten erfolgt automatisiert oder auf Veranlassung des Auftraggebers. Sie wird insbesondere ausgelöst durch:

- den Wegfall des Verarbeitungszwecks (z. B. Löschung des Kundenkontos durch den Auftraggeber),
- den Ablauf der nachfolgend festgelegten Speicherfristen,
- den Eingang eines berechtigten Löschersuchens einer betroffenen Person, oder
- den Widerruf einer Einwilligung bzw. einen Widerspruch gegen die Verarbeitung.

Für die nachfolgend genannten Datenkategorien gelten folgende Speicherfristen und Löschmodalitäten:

Datenkategorie	Speicherort	Löschauslöser	Methode	Löschung durch	Protokollierung
Chat-Transkript	Datenbank	Sofort (kundeninitiiert)	Löschung aus der Datenbank	Kundenaktion	Logdatei
Chat-Transkript	Backup (lokal und extern)	Nach 90 Tagen	Entfernung der Backup-Snapshots	Cronjob	Logdatei
Chat-Transkript	Datenbank	Konfigurierbar (1–36 Monate)	Löschung aus der Datenbank	Cronjob (kundenseitig konfigurierbar)	Logdatei
Kundenkontodaten	Datenbank	Sofort (kundeninitiiert)	Löschung aus der Datenbank	Kundenaktion	Logdatei + Auditlog
Kundenkontodaten	Backup (lokal und extern)	Nach 90 Tagen	Entfernung der Backup-Snapshots	Cronjob	Logdatei
Operator-Daten	Datenbank	Sofort (kundeninitiiert)	Löschung aus der Datenbank	Kundenaktion	Logdatei + Auditlog
Operator-Daten	Backup (lokal und extern)	Nach 90 Tagen	Entfernung der Backup-Snapshots	Cronjob	Logdatei

Anwendungs-Logdateien	Dateisystem + Datenbank	Nach 90 Tagen	Anwendung der Aufbewahrungs-richtlinie	Systemseitige Aufbewahrungs-mechanismen	–
System-Logdateien	Dateisystem + Datenbank	Nach 90 Tagen	Anwendung der Aufbewahrungs-richtlinie	Systemseitige Aufbewahrungs-mechanismen	–
LLM-Eingaben/-Ausgaben (Anthropic-Modelle)	AWS Bedrock (EU-Region)	Keine Speicherung (Zero Data Retention, kein Operatorzugriff)	Keine Speicherung	–	–
LLM-Eingaben/-Ausgaben, die als potenziell missbräuchlich markiert wurden (OpenAI-Modelle)	MS Azure OpenAI (EU-Region)	Keine Speicherung (als missbräuchlich markierte Inhalte: Löschung nach max. 30 Tagen)	Markierte Inhalte: automatische Löschung nach Ablauf der Microsoft-Aufbewahrungsfrist	Microsoft-Missbrauchsüberwachung	–

Backups unterliegen unabhängig von einer vorherigen Löschung in der Produktivdatenbank einer gesonderten Aufbewahrungsfrist von 90 Tagen; eine Wiederherstellung aus Backups nach Ablauf dieser Frist ist ausgeschlossen. Sämtliche Löschvorgänge werden protokolliert und regelmäßig durch die zuständigen Compliance-/Security-Verantwortlichen überprüft.

4. Kategorien betroffener Personen

Die von der Verarbeitung betroffenen Kategorien betroffener Personen hängen von der individuellen Nutzung der Lime Connect Services durch den Auftraggeber ab. Als Kategorien betroffener Personen kommen dabei in Betracht:

- Kunden
- Website-Besucher
- Interessenten
- Operatoren des Auftraggebers

Anlage 3: Unterauftragsverarbeiter

Lime Connect setzt für die Verarbeitung folgende Unterauftragsverarbeiter ein:

Dienstleister	**Erläuterung und Zweck**	**Funktion, in deren Rahmen der Einsatz des Unterauftragnehmers stattfindet**	**Serverstandort**	**Rechtsgrundlage für etwaige Drittstaatentransfers**
Hetzner Online GmbH Industriestr. 25 91710 Gunzenhausen Deutschland	*Hosting der Server* *Speicherung der Daten* Verarbeitete Daten: Siehe Anlage 2, Ziffer 2	Systemimmanent	Deutschland	–
Myra Security GmbH Landsberger Str. 187 80687 München Deutschland	*Erweiterter DDoS-Schutz* Verarbeitete Daten: Siehe Anlage 2, Ziffer 2	Systemimmanent	Deutschland	–
Scaleway SAS 8 rue de la Ville l'Evêque, 75008 Paris, Frankreich	*Speicherung verschlüsselter Backups der Daten* Verarbeitete Daten: Siehe Anlage 2, Ziffer 2	Systemimmanent	EU – Frankreich, Niederlande, Polen und Italien	–
	Connect AI. *Hosting AI Model.* Kategorien von Daten: • Unterhaltungen • Kontakt Details	Optional (immanent bei Nutzung von Connect AI)	EU – Frankreich, Niederlande, Polen und Italien	
BunnyWay, informacijske storitve d.o.o. Škofjeloška Cesta 13 1215 Medvode, Slowenien	*Ausspielen der technischen Komponenten* (DNS, Bilder der Webseite, JavaScript Code, Stylesheet-Dateien) • IP-Adresse • Browser • Betriebssystem	Systemimmanent	Regionsabhängig	-

	• Operator Profil-Bilder			
Lime technologies Sweden AB S:t Lars väg 46 SE-222 70 Lund Schweden	*Zugang zu Diensten für interne Verwaltungs- und Betriebszwecke, die den Zugang zum Produkt/Dienst erfordern, d. h. für Entwicklung, Sicherheitsarbeiten, IT-Funktionen* Verarbeitete Daten: Siehe Anlage 2, Ziffer 2	Systemimmanent	Schweden	-
Amazon Web Services EMEA SARL 38 Avenue John F. Kennedy L-1855 Luxemburg	*Ausspielen der technischen Komponenten* (JavaScript Code, Bilder) • IP-Adresse • Browser • Betriebssystem • Operator Profil-Bilder	Systemimmanent	Deutschland	SCC vom 04. Juni 2021 (Art. 46 Abs. 2 lit. c) DSGVO) EU-US Angemessenheits-beschluss
	Angebot des File Uploads. Erweiterung und Verbesserung der Kerndienstleistung. • User File-Uploads • Operator File-Uploads • IP-Adresse • Browser • Betriebssystem	Optional	Deutschland	SCC vom 04. Juni 2021 (Art. 46 Abs. 2 lit. c) DSGVO) EU-US Angemessenheits-beschluss
	Angebot einer Benachrichtigungs-E-Mail über die Antwort des Operators, die dem Endnutzer zugesendet wird, während dieser offline ist, sowie das Senden der Operator-Benachrichtigungen und Chat-Transkripte. Erweiterung	Optional	Irland	SCC vom 04. Juni 2021 (Art. 46 Abs. 2 lit. c) DSGVO) EU-US Angemessenheits-beschluss

	und Verbesserung der Kerndienstleistung. • E-Mail-Adresse • Nutzergenerierter Inhalt • IP-Adresse • Browser • Betriebssystem			
DeepL GmbH Im Mediapark 8a 50670 Köln Deutschland	*Angebot einer maschinellen Übersetzung von Nachrichteninhalten* (verschlüsselt, für die Dauer der Übersetzung). Erweiterung und Verbesserung der Kerndienstleistung. • Nutzergenerierter Inhalt	Optional	Deutschland	–
Mailgun Technologies, Inc. 112 E Pecan St #1135 San Antonio, Texas 78205 USA	*E-Mail-Benachrichtigungen für Endnutzer* Dient als Backup für AWS. Benachrichtigungs-E-Mail (Outbound) über die Antwort des Operators, die dem Endnutzer zugesendet wird, während dieser offline ist, sowie Operator-E-Mails, Chat-Transkripte und Operator-Benachrichtigungen. • E-Mail-Adresse • Kontakt Name • Nutzergenerierter Inhalt *Angebot einer E-Mail-Antwortmöglichkeit des Endnutzers auf eine E-Mail-Benachrichtigung.* Erweiterung und Verbesserung der Kerndienstleistung. • E-Mail-Adresse • Nutzergenerierter Inhalt • IP-Adresse • Browser • Betriebssystem	Optional	EU	SCC vom 04. Juni 2021 (Art. 46 Abs. 2 lit. c) DSGVO)

Twilio Inc. 375 Beale Street, Suite 300, San Francisco, California 94105 USA	*Audio- und Video Chat.* Erweiterung und Verbesserung der Kerndienstleistung. • Nutzergenerierter Inhalt • IP-Adressen • Browser • Betriebssystem	Optional	USA	SCC vom 04. Juni 2021 (Art. 46 Abs. 2 lit. c) DSGVO) EU-US Angemessenheits-beschluss
OMQ GmbH Chausseestraße 22 10115 Berlin Deutschland	*Optionales KI-Software Angebot.* Zugriff nur in Verbindung mit Chatbot API. Möglichkeit, eine KI-basierte Wissensdatenbank zu erstellen, um den Kundenservice zu automatisieren (z. B. über Chatbots oder smart FAQ u.a.) vom Lime Connect Dashboard aus: • Operator IP-Adresse • Operator Name • Operator E-Mail Adresse	Optional	Deutschland	SCC vom 04. Juni 2021 (Art. 46 Abs. 2 lit. c) DSGVO) EU-US Angemessenheits-beschluss
	Optionales Angebot des KI-Software Hostings: *Standard KI:* Der Algorithmus entfernt personenbezogene Daten, bevor diese von der KI gespeichert werden: • Nutzergenerierter Inhalt (KI-Nachrichten und Kontakt Antworten) wird anonymisiert	Optional (immanent bei Nutzung des KI-Software Angebots)	Deutschland	SCC vom 04. Juni 2021 (Art. 46 Abs. 2 lit. c) DSGVO) EU-US Angemessenheits-beschluss
	Optionales Angebot des KI-Software Hostings: *GPT KI-Model:* Durch Microsoft Azure OpenAI Services gehostet.	Optional (immanent bei Nutzung des KI-Software Angebots)	Belgien, Niederlande, Großbritannien	SCC vom 04. Juni 2021 (Art. 46 Abs. 2 lit. c) DSGVO) EU-US Angemessenheits-beschluss

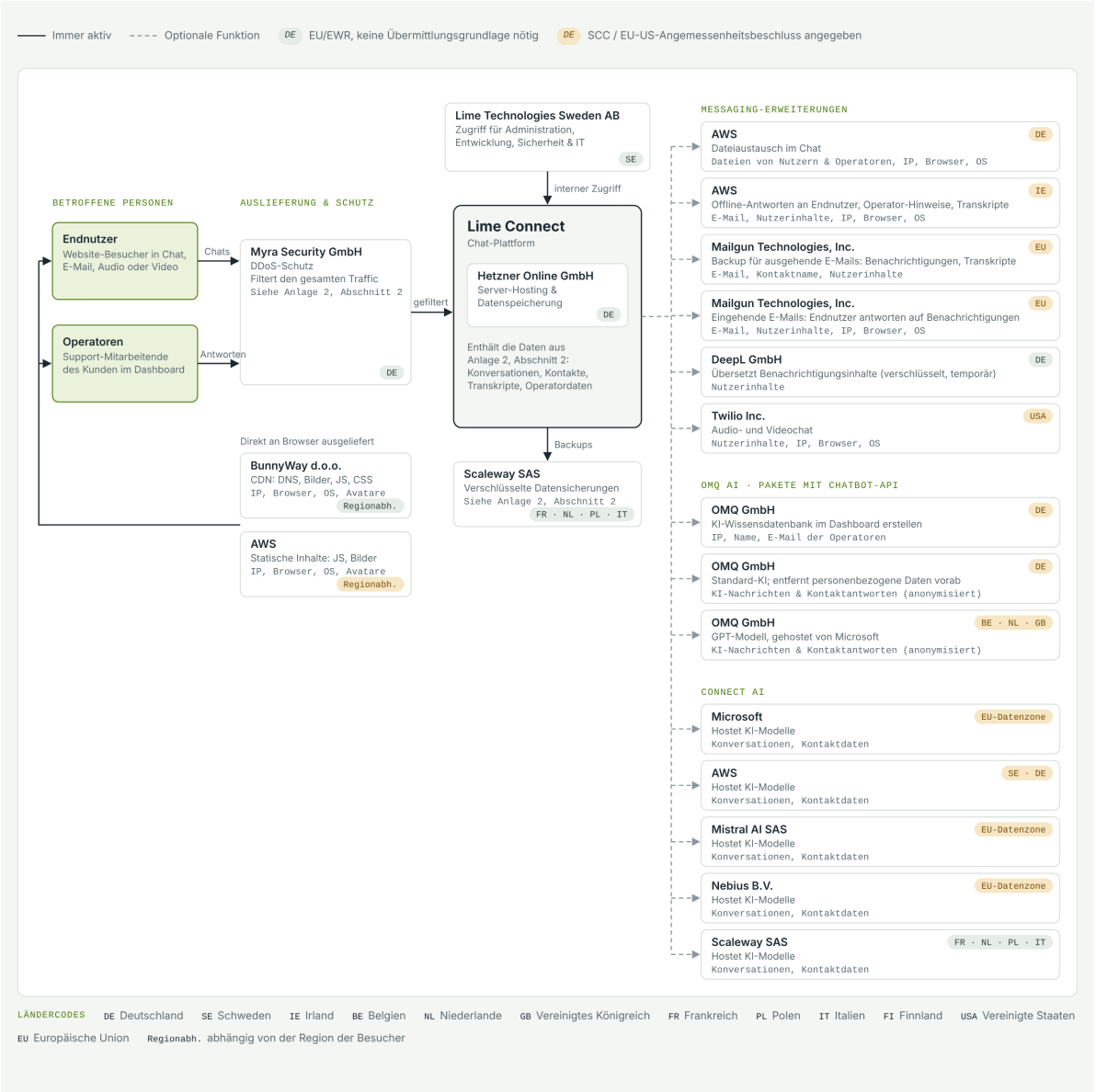
	• Nutzergenerierter Inhalt (KI-Nachrichten und Kontakt Antworten)			
Amazon Web Services EMEA SARL 38 Avenue John F. Kennedy L-1855 Luxemburg	***Connect AI.*** *Hosting der Knowledge base.* Service: S3 Kategorien von Daten: • Knowledge base	Optional (immanent bei Nutzung von Connect AI)	Deutschland	SCC vom 04. Juni 2021 (Art. 46 Abs. 2 lit. c) DSGVO) EU-US Angemessenheits-beschluss
Microsoft Ireland Operations, Ltd. One Microsoft Place South County Business Park Leopardstown Dublin 18, D18 P521 Irland	***Connect AI.*** *Hosting AI Model.* Service: Microsoft Azure OpenAI Services Kategorien von Daten: • Unterhaltungen • Kontakt Details	Optional (immanent bei Nutzung von Connect AI)	EU Daten Zone	SCC vom 04. Juni 2021 (Art. 46 Abs. 2 lit. c) DSGVO) EU-US Angemessenheits-beschluss
Amazon Web Services EMEA SARL 38 Avenue John F. Kennedy L-1855 Luxemburg	***Connect AI.*** *Hosting AI Model.* Service: Bedrock Kategorien von Daten: • Unterhaltungen • Kontakt Details	Optional (immanent bei Nutzung von Connect AI)	EU (Schweden und Deutschland)	SCC vom 04. Juni 2021 (Art. 46 Abs. 2 lit. c) DSGVO) EU-US Angemessenheits-beschluss
Mistral AI SAS 15 rue des Halles, 75001 Paris, Frankreich	***Connect AI.*** *Hosting AI Model.* Kategorien von Daten: • Unterhaltungen • Kontakt Details	Optional (immanent bei Nutzung von Connect AI)	EU (EU Zone)	SCC vom 04. Juni 2021 (Art. 46 Abs. 2 lit. c) DSGVO) EU-US Angemessenheits-beschluss
Nebius B.V. Burgerweeshuispad 101, 1076 ER Amsterdam, Niederlande	***Connect AI.*** *Hosting AI Model.* Kategorien von Daten: • Unterhaltungen • Kontakt Details	Optional (immanent bei Nutzung von Connect AI)	EU (EU Zone)	SCC vom 04. Juni 2021 (Art. 46 Abs. 2 lit. c) DSGVO) EU-US Angemessenheits-beschluss

Anlage 4: Technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO

Zum Zeitpunkt des Vertragsschlusses hat Lime Connect die nachfolgend dargestellten technisch-organisatorischen Maßnahmen implementiert:

1. Datenflussdiagramm

Auf dem nachfolgenden Chart ist der grobe Datenfluss dargestellt:



2. Organisationskontrolle

Sollvorgabe: Das Personal des Auftragnehmers ist auf das Datengeheimnis und die Einhaltung der Verschwiegenheitsvorschriften zu verpflichten. Die Tatsache der Verpflichtung sollte zum Zweck eines jederzeitigen Nachweises in der Personalakte dokumentiert werden.

Entsprechende Unterlagen sind in der Personalakte hinterlegt.

- Textbaustein ist im Standardvertrag für alle Mitarbeiter hinterlegt.
- Mitarbeiter werden nochmals in internen Schulungen darauf hingewiesen.

3. Zutrittskontrolle

Sollvorgabe: Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (wobei der Begriff räumlich zu verstehen ist). Der Auftragnehmer hat zu diesem Zweck ein Zutrittskontrollsystem zu installieren.

Beschreibung der Zutrittskontrollsysteme im Büro (inklusive der physischen Schutzvorkehrungen):

- mechanische Schließanlage Haupteingang sowie Büroeingänge
- elektronische Alarmanlage und Entriegelung mit 24/7 Wachschutz
- Kameras

Beschreibung der Überwachungseinrichtungen:

- Alarmanlage mit Aufschaltung auf Wachschutz
- Videoüberwachung mit 3 Kameras

4. Zugangskontrolle

Sollvorgabe: Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können. Zu diesem Zweck muss der Zugang zu den DV-Anlagen kontrolliert und protokolliert werden (z.B. Anmelden im System, unerlaubtes Hochfahren und Eindringen in das DV-System verhindern).
Das Eindringen Unbefugter in die DV-Systeme ist zu verhindern.

Beschreibung der implementierten Authentifizierungsmechanismen (z.B. Passwortkomplexität, Wechselzyklen, SSH Keys):

- SSH: personalisierte Public Private Keys
- S2S Kommunikation: Mesh VPN: (Curve25519, ChaCha20)
- C2S (Client to Server) Kommunikation: TLS 1.3 und TLS 1.2

Beschreibung der Maßnahmen bei temporärer Inaktivität der Nutzer (z.B. Mitarbeiter verlässt den Arbeitsplatz):

- Beim MacOS X System sind Hot Corners konfiguriert, sodass die Maus in eine Ecke geschoben wird, um den Bildschirm schnell zu sperren. Andernfalls sperrt sich der Monitor nach 5 Minuten.
- Alle MA werden aufgerufen, Bildschirme immer zu sperren.
- Microsoft Defender
- Zentrales Management mit MDM

Beschreibung der technischen Schutzmaßnahmen für Ihre Netzwerkumgebung:

- iptables-Regeln auf externen Schnittstellen
- Dienste lauschen nur auf internen Netzen
- VPN-Kommunikation für Server
- wöchentliche nmap-Scans
- wöchentliche OpenVAS-Scans
- tägliches Monitoring
- tägliches Audit neuer kritischer Fehler
- Anti-DDoS im Datencenter Hetzner online GmbH
- Zusätzliches Anti-DDoS bei Dienst Myra Security GmbH
- Zerotrust Lösung zu internen Diensten (Username + Passwort + 2FA)
- Zentrales Logging der Systeme

5. Zugriffskontrolle

Sollvorgabe: Es ist zu gewährleisten, dass die zur Nutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Personenbezogene Daten müssen bei persistenter Speicherung verschlüsselt werden.

Bedarfsorientierte Ausgestaltung des Berechtigungskonzepts und der Zugriffsrechte sowie deren Überwachung und Protokollierung:

Beschreibung der Verhinderung unerlaubter Tätigkeiten in Datenverarbeitungssystemen außerhalb eingeräumter Berechtigungen (Rollen und Berechtigungen nach dem Need-to-Know Prinzip):

- Rechte- und Rollenmanagement
- Technisches Onboarding und Offboarding von Mitarbeitern
- Zugänge und Rechtevergabe nur nach Erforderlichkeit
- Zugriffe werden monatlich überprüft

Beschreibung der Maßnahmen gegen unzulässige Zugriffe (z. B. Brute Force, SQL Injection, Login Validierung):

- SSH: CrowdSec
- SQL Injections werden durch Nutzung von Query Parameterization bei Datenbankabfragen systematisch ausgeschlossen
- Alle kritischen Endpunkte werden mit Rate Limits gegen Brute Force Angriffe geschützt
- Darüber hinaus werden alle üblichen Django Framework Sicherheitsfeatures (CSRF-Token etc.) genutzt.
- Zugänge für Lime Connect Mitarbeiter sind durch eine 2-Faktor Authentifizierung zusätzlich geschützt.
- Kundenseitig können weitere Sicherheitsfeatures wie eine Login-Validierung per E-Mail aktiviert werden.

Beschreibung der Sicherstellung, dass ausschließlich personifizierte Benutzerkonten für den Zugriff auf die Systeme genutzt werden (ein Konto je Benutzer):

- personalisierter Produkt-/Backend-Account je Nutzer.
- personalisierter Account auf Zero Trust Lösung je Nutzer mit 2FA
- personalisierter Benutzer-Account auf einem Computer

Beschreibung der implementierten Verschlüsselungsmaßnahmen der personenbezogenen Daten:

- Festplattenverschlüsselung mit LUKS2 (cipher: aes-xts-plain64, keysize: 512 bits)
- Transportverschlüsselung mit TLS 1.3 und 1.2
- VPN
- SSH-Sicherungen: GPG

5.1. Weitergabekontrolle

Sollvorgabe: Es ist zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Personenbezogene Daten sind nur verschlüsselt zu übertragen (Transportverschlüsselung).

Beschreibung der Transportverschlüsselung:

- Transportverschlüsselung mit TLS 1.3 und 1.2
- VPN
- SSH

Beschreibung der Protokollierung der Weitergabe von personenbezogenen Daten:

- Nicht anwendbar. Personenbezogene Daten werden nicht von Servern heruntergeladen oder weitergegeben. Ausnahme: Sicherungen. Sicherungen werden protokolliert und verschlüsselt. Täglich manuell geprüft.

Beschreibung der Transportsicherung bei einem physikalischen Transport:

- Nicht anwendbar. Personenbezogene Daten werden nicht von Servern physikalisch transportiert.

5.2. Eingabekontrolle

Sollvorgabe: Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Ein detailliertes Logging System über die Eingabe, Veränderung oder Löschung von personenbezogenen Daten (z. B. Logdateien) ist zu implementieren und regelmäßig auszuwerten.

Beschreibung der Logging / Monitoringsystem zur Überwachung der Zugriffe:

- Dem Kunden steht ein Auditlog zur Verfügung. Das Auditlog ist ein Protokoll, in dem alle Änderungen am Account des Kunden verzeichnet sind.
- Auf der Ebene von Servern werden diverse Protokolle mitgeschrieben, die durch das Anmelden von Mitarbeitern bei Wartungsarbeiten erstellt werden. Diese Protokolle werden stichprobenartig kontrolliert und zentral gespeichert.
- Weiterhin werden diverse Protokolle generiert, die den technischen Zustand des Systems darstellen.

5.3. Verfügbarkeitskontrolle

Sollvorgabe: Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Beschreibung des Datensicherungskonzepts (z.B. Back-Up Verfahren, Redundanzen, USV, Notfallpläne):

- 3 Datacenter (System 3-fach vorhanden)
- 2 verschiedene Standorte/Rechenzentren
- USVs und Dieselgeneratoren an allen Datencenter-Standorten
- gespiegelte Festplatten
- Enterprise-Festplatten
- Automatisiertes Monitoring
- tägliche Backups aller Daten
- Backups an 2 verschiedenen Orten
- mehrere Mitarbeiter, die Prozess beherrschen

5.4. Trennungsgebot

Sollvorgaben: Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können. Der Auftragnehmer sorgt für eine nachweislich logische Trennung der Daten des Mandanten, d.h. Daten verschiedener Auftraggeber sind getrennt zu verarbeiten. Gegenseitiger Zugriff ist auszuschließen. Ebenso werden die Daten nur zweckgebunden verarbeitet.

Beschreibung der Umsetzung zur Mandantenfähigkeit:

- Daten werden zweckgebunden verarbeitet. Daten werden auf Datenbankebene logisch nach Mandanten getrennt (Mandantenfähigkeit).

Beschreibung der Sicherstellung der Trennung von Entwicklung-, Test- und Produktivsystemen:

Physikalische Trennung (verschiedene Server) in 3 Umgebungen:

- Development
- Staging
- Produktion

5.5. Informationssicherheit

Beschreibung des Informationssicherheitsmanagementsystems (ISMS):

- Lime Connect ist ISO 27001 zertifiziert
- Trust Center Ressourcen: https://trust.lime-technologies.com/

- Verantwortung:
  - IT-Security: security@lime-connect.com
  - Datenschutz: privacy@lime-connect.com
- Regelmäßige Schulungen
  - IT Security
  - Datenschutz
  - Feste Prozesse
  - Onboarding
  - Offboarding

5.6. Sonstiges

Beschreibung der Sicherstellung der vertraulichen Aufbewahrung sowie der Löschung oder Vernichtung von Test- und Ausschussmaterialen mit personenbezogenen Daten (z. B. Papier):

- Nicht anwendbar. Da keine Nutzung von Papier. Ausnahme: Buchhaltung, sowie Verträge. Dokumente werden geschreddert.
- Festplatten werden grundsätzlich immer verschlüsselt und vor Abgabe mehrfach überschrieben.

6. Einsatz von Unterauftragnehmern

Die von uns eingesetzten weiteren Auftragsverarbeiter jeweils zum Zeitpunkt des Abschlusses dieser Vereinbarung implementierten technischen und organisatorischen

Maßnahmen sind auf Anfrage zu erhalten. Wir versichern uns in regelmäßigen Abständen von der Angemessenheit und Wirksamkeit der von unseren Unterauftragnehmern getroffenen Maßnahmen.

7. Versicherung des Auftragnehmers

Der Auftragnehmer garantiert, dass alle in diesem Dokument genannten Angaben der Wahrheit entsprechen.

Anlage 5: Ergänzungen zu den EU-Standardvertragsklauseln

Die Parteien vereinbaren folgende Ergänzungen und Aktualisierungen zu den EU-Standardvertragsklauseln (Anlage 1):

1. Dokumentation und Einhaltung der Klauseln (Klausel 7.6)

Klausel 7.6 der EU-Standardvertragsklauseln wird um die folgenden Regelungen ergänzt:

> Zur Durchführung solcher Inspektionen gem. Klausel 7.6 c) ff. ist der Auftraggeber berechtigt, im Rahmen der üblichen Geschäftszeiten (montags bis freitags von 10 bis 18 Uhr) nach rechtzeitiger Vorankündigung auf eigene Kosten, ohne Störung des Betriebsablaufs und unter strikter Geheimhaltung von Betriebs- und Geschäftsgeheimnissen Lime Connects die Geschäftsräume zu betreten, in denen Auftraggeber Daten verarbeitet werden.

2. Einsatz von Unterauftragsverarbeitern (Klausel 7.7)

Klausel 7.7. a) der EU-Standardvertragsklauseln wird um die folgenden Regelungen ergänzt:

> Lime Connect wird den Auftraggeber über beabsichtigte Änderungen in Bezug auf die Hinzuziehung oder die Ersetzung weiterer Auftragsverarbeiter in elektronischem Format mit einer Frist von 30 Tagen informieren. In Ausnahmefällen, beispielsweise wenn die Hinzuziehung oder die Ersetzung weiterer Auftragsverarbeiter aus Gründen akuter Vorkommnisse im Bereich der IT-Sicherheit geboten erscheint, ist es Lime Connect gestattet, den Auftraggeber über beabsichtigte Änderungen mit einer Frist von 5 Tagen zu informieren. Dem Auftraggeber steht im Einzelfall ein Recht zu, Einspruch gegen die Beauftragung eines potenziellen weiteren Auftragsverarbeiters zu erheben. Ein Einspruch darf vom Auftraggeber nur aus wichtigem, Lime Connect nachzuweisenden Grund erhoben werden. Soweit der Auftraggeber nicht innerhalb von 14 Werktagen nach Zugang der Benachrichtigung Einspruch erhebt, erlischt sein Einspruchsrecht bezüglich der entsprechenden Beauftragung. Erhebt der Auftraggeber Einspruch, ist Lime Connect berechtigt, den Hauptvertrag (**AGB**) und diesen Vertrag zum nach dem Hauptvertrag (**AGB**) nächstmöglichen Zeitpunkt zu kündigen.

3. Internationale Datenübermittlungen (Klausel 7.8)

Klausel 7.8 der EU-Standardvertragsklauseln wird um die folgenden Regelungen ergänzt:

> Es ist Lime Connect gleichwohl gestattet, Auftraggeber-Daten unter Einhaltung der Bestimmungen dieses Vertrags auch außerhalb des EWR zu verarbeiten, wenn er den Auftraggeber vorab über den Ort der Datenverarbeitung informiert und die Voraussetzungen der Art. 44 - 48 DSGVO erfüllt sind oder eine Ausnahme nach Art. 49 DSGVO vorliegt.

4. Umfang der Beauftragung

Die EU-Standardvertragsklauseln werden um die folgenden Regelungen ergänzt:

> Lime Connect bleibt es vorbehalten, Auftraggeber-Daten zu anonymisieren. Die Anonymisierung erfolgt durch Aggregation, sofern eine Identifizierung einzelner betroffener Personen nicht mehr möglich ist. Lime Connect ist berechtigt, derart anonymisierte Daten zum Zweck der bedarfsgerechten Optimierung und Weiterentwicklung sowie zur Erbringung des nach Maßgabe des Hauptvertrags (AGB) vereinbarten Dienstes zu verwenden. Die Parteien stimmen darin überein, dass nach obiger Maßgabe anonymisierte Auftraggeber-Daten nicht mehr als Auftraggeber-Daten im Sinne dieses Vertrags gelten.

5. Sicherheit der Beauftragung (Klausel 7.4)

Klausel 7.4 der EU-Standardvertragsklauseln wird um die folgenden Regelungen ergänzt:

> Lime Connect trifft geeignete technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO, um ein dem Risiko angemessenes Schutzniveau für die Verarbeitung personenbezogener Daten sicherzustellen.
> Lime Connect ist berechtigt, diese technischen und organisatorischen Maßnahmen unter Berücksichtigung des Stands der Technik sowie der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung weiterzuentwickeln oder anzupassen, sofern hierdurch das vereinbarte Schutzniveau nicht unterschritten wird.
> Über wesentliche Änderungen der technischen und organisatorischen Maßnahmen, die Auswirkungen auf die Sicherheit der Verarbeitung haben können, informiert Lime Connect den Auftraggeber in geeigneter Weise.

6. Dauer der Verarbeitung (Klausel 7.3)

Klausel 7.3 der EU-Standardvertragsklauseln wird um die folgenden Regelungen ergänzt:

Die konkreten Speicher- und Löschfristen für die einzelnen Kategorien personenbezogener Daten sowie die jeweiligen Löschauslöser und -verfahren ergeben sich aus Anlage 2

Connect

Data Processing Agreement for Lime Connect

Table of contents

1. Object of agreement 3
2. Implementation of the EU Standard Contractual Clauses 3
3. Additions to the EU Standard Contractual Clauses 4
4. Scope of the contract 4
5. Term of the agreement 4

Schedule of annexes 4

Lime Connect (Userlike) GmbH
(hereinafter referred to as "**Lime Connect**")

Kölnturm, Im Mediapark 8

50670 Cologne

the Processor, undertakes to provide services to the Customer (hereinafter referred to as "**Customer**" or "**Controller**")

in accordance with the following provisions:

1. Object of Agreement

This data processing addendum pursuant to Art. 28 of the GDPR (hereinafter "**Contract**") specifies the obligations of the contracting parties with regard to data protection, which result from the contracts already existing between the parties or to be concluded in the future (hereinafter **"principal contract/Terms and conditions"**), under which personal data is processed by Lime Connect for the Controller. It shall apply to all activities which are related to the scope of the contract (Section 4) and in which employees of Lime Connect (Userlike) GmbH or persons authorized by Lime Connect (Userlike) GmbH process personal data of the Controller.

2. Implementation of the EU Standard Contractual Clauses

2.1 The Parties shall base this Agreement on the "Standard Contractual Clauses for Controllers and Processors in the EU / EEA" pursuant to the Commission Implementing Decision on Standard Contractual Clauses between Controllers and Processors pursuant to Article 28 (7) of the GDPR and Article 29 (7) of Regulation (EU) 2018/1725 of June 4, 2021 (hereinafter "**EU Standard Contractual Clauses**") in **Annex 1**.

3. Additions to the EU Standard Contractual Clauses

The parties agree in **Annex 5** on additions and updates to the EU Standard Contractual Clauses within the terms of clause 2 of the EU Standard Contractual Clauses.

4. Scope of the agreement

Scope of the Processing is the provision of the Lime Connect services designated in the principal contract/Terms and conditions by the Processor for the Controller

Lime Connect offers a messenger function for web and mobile support. The software-based chat communication solution offers customer support in real time and asynchronous communication and helps to develop customer service.

5. Term of the agreement

The term and termination of this Agreement is based on the provisions on term and termination of the principal contract/Terms and conditions. Termination of the principal contract/Terms and conditions automatically results in termination of this Agreement. This Agreement cannot be terminated individually.

Schedule of annexes:

- **Annex 1:** EU Standard Contractual Clauses (Standard contractual clauses for controllers and processors in the EU/EEA – published: Juni 4, 2021, English)
- **Annex 2:** Purpose, type and scope of data processing, type of data and data subject categories
- **Annex 3:** Sub-processors
- **Annex 4:** Technical and organizational measures in accordance with Art. 32 GDPR
- **Annex 5:** Additions to the EU Standard Contractual Clauses

Annex 1: EU Standard Contractual Clauses (as per June 4, 2021)

Section I

Clause 1 – Purpose and scope

a) The purpose of these Standard Contractual Clauses (the Clauses) is to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
b) The controllers and processors have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 and/or Article 29(3) and (4) of Regulation (EU) 2018/1725.
c) These Clauses apply to the processing of personal data as specified in Annex 2.
d) Annexes 2 to 5 are an integral part of the Clauses.
e) These Clauses are without prejudice to obligations to which the controller is subject by virtue of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.
f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

Clause 2 – Invariability of the Clauses

a) The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.
b) This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

Clause 3 – Interpretation

a) Where these Clauses use the terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively, terms shall have the same meaning as in that Regulation.
b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively.

c) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

Clause 4 – Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties existing at the time when these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 5 – Optional Docking clause

a) Any entity that is not a Party to these Clauses may, with the agreement of all the Parties, accede to these Clauses at any time as a controller or a processor by completing the Annexes and signing Annex I.
b) Once the Annexes in (a) are completed and signed, the acceding entity shall be treated as a Party to these Clauses and have the rights and obligations of a controller or a processor, in accordance with its designation in Annex I.
c) The acceding entity shall have no rights or obligations resulting from these Clauses from the period prior to becoming a Party.

Section II

Clause 6 – Description of processing(s)

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in Annex 2.

Clause 7 – Obligations of the Parties

7.1 Instructions

a) The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.
b) The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe Regulation (EU) 2016/679 / Regulation

(EU) 2018/1725 or the applicable Union or Member State data protection provisions.

7.2 Purpose limitation

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex 2, unless it receives further instructions from the controller.

7.3 Duration of the processing of personal data

Processing by the processor shall only take place for the duration specified in the principal contract (Terms and Conditions).

7.4 Security of processing

a) The processor shall at least implement the technical and organisational measures specified in Annex III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (personal data breach). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects.
b) The processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The processor shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7.5 Sensitive data

If the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences ("sensitive data"), the processor shall apply specific restrictions and/or additional safeguards insofar as this is possible.

7.6 Documentation and compliance

a) The Parties shall be able to demonstrate compliance with these Clauses.
b) The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with these Clauses.

c) The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725. At the controller's request, the processor shall also permit and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the controller may take into account relevant certifications held by the processor.
d) The controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the processor and shall, where appropriate, be carried out with reasonable notice.
e) The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

7.7 Use of sub-processors

a) GENERAL WRITTEN AUTHORISATION: The processor has the controller's general authorisation for the engagement of sub-processors from an agreed list. The processor shall specifically inform in writing the controller of any intended changes of that list through the addition or replacement of sub-processors at least 30 days (see Annex 5, point 2) in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The processor shall provide the controller with the information necessary to enable the controller to exercise the right to object.
b) Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with these Clauses. The processor shall ensure that the sub-processor complies with the obligations to which the processor is subject pursuant to these Clauses and to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.
c) At the controller's request, the processor shall provide a copy of such a sub-processor agreement and any subsequent amendments to the controller. To the extent necessary to protect business secret or other confidential information, including personal data, the processor may redact the text of the agreement prior to sharing the copy.
d) The processor shall remain fully responsible to the controller for the performance of the sub-processor's obligations in accordance with its contract with the processor. The processor shall notify the controller of any failure by the sub-processor to fulfil its contractual obligations.
e) The processor shall agree a third party beneficiary clause with the sub-processor whereby - in the event the processor has factually disappeared, ceased to exist in law or has become insolvent - the controller shall have the right to terminate the

sub-processor contract and to instruct the sub-processor to erase or return the personal data.

7.8 International transfers

a) Any transfer of data to a third country or an international organisation by the processor shall be done only on the basis of documented instructions from the controller or in order to fulfil a specific requirement under Union or Member State law to which the processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.
b) The controller agrees that where the processor engages a sub-processor in accordance with Clause 7.7. for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub-processor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

Clause 8 – Assistance to the controller

a) The processor shall promptly notify the controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorised to do so by the controller.
b) The processor shall assist the controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), the processor shall comply with the controller's instructions
c) In addition to the processor's obligation to assist the controller pursuant to Clause 8(b), the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:
    1) the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;
    2) the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk;
    3) the obligation to ensure that personal data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;
    4) the obligations in Article 32 of Regulation (EU) 2016/679.

d) The Parties shall set out in Annex III the appropriate technical and organisational measures by which the processor is required to assist the controller in the application of this Clause as well as the scope and the extent of the assistance required.

Clause 9 – Notification of personal data breach

In the event of a personal data breach, the processor shall cooperate with and assist the controller for the controller to comply with its obligations under Articles 33 and 34 of Regulation (EU) 2016/679 or under Articles 34 and 35 of Regulation (EU) 2018/1725, where applicable, taking into account the nature of processing and the information available to the processor.

9.1 Data breach concerning data processed by the controller

In the event of a personal data breach concerning data processed by the controller, the processor shall assist the controller:

a) in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the controller has become aware of it, where relevant/(unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);
b) in obtaining the following information which, pursuant to Article 33(3) of Regulation (EU) 2016/679 shall be stated in the controller's notification, and must at least include:
    1) the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
    2) the likely consequences of the personal data breach;
    3) the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

c) in complying, pursuant to Article 34 of Regulation (EU) 2016/679, with the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

9.2 Data breach concerning data processed by the processor

In the event of a personal data breach concerning data processed by the processor, the processor shall notify the controller
without undue delay after the processor having become aware of the breach. Such notification shall contain, at least:

a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);
b) the details of a contact point where more information concerning the personal data breach can be obtained;
c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

The Parties shall set out in Annex 4 all other elements to be provided by the processor when assisting the controller in the compliance with the controller's obligations under Articles 33 and 34 of Regulation (EU) 2016/679.

Section III

Clause 10 – Non-compliance with the Clauses and termination

a) Without prejudice to any provisions of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725, in the event that the processor is in breach of its obligations under these Clauses, the controller may instruct the processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The processor shall promptly inform the controller in case it is unable to comply with these Clauses, for whatever reason.
b) The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if
    1) the processing of personal data by the processor has been suspended by the controller pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;
    2) the processor is in substantial or persistent breach of these Clauses or its obligations under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725;
    3) the processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.
c) The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1 (b), the controller insists on compliance with the instructions.
d) Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or, return all the personal data to the controller and delete existing copies unless Union or Member State law requires storage of

the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with these Clauses.

Annex 2: Purpose, type and scope of data processing, type of data and data subject categories

1. Purpose of the processing

Lime Connect offers a messenger function for web and mobile support. The software-based chat communication solution offers customer support in real time and asynchronous communication and helps to develop the customer service.

2. Categories of data

The categories of data affected by the processing depend on the use of Lime Connect services by the Controller. The possible categories of data that fall within the subject matter of the processing are:

End user

- Chat transcript
- E-mail address
- Browser
- Operating system
- Device
- Number of page requests
- Number of page visits
- Referrer
- URL (where the chat originated)
- Questionnaire before and after the chat (optional)
- Chat topic
- Chat status (new, pending, closed)
- Chat evaluation after the chat
- Duration of the chat
- Date of the chat
- Geo location (voluntary, optional)
- Media files shared by the contact with the operator during the chat
- Optional data fields that the Controller passes on to Lime Connect
- IP addresses

Operator's profile settings

- Username
- First name
- Surname
- Alias name
- E-mail address
- Language
- Time zone
- Operator group
- Profile photo
- Chat transcripts
- Analytics figures on chat performance
- IP addresses

3. Retention Period and Deletion Schedule

Deletion of personal data takes place either automatically or at the initiative of the Controller. It is triggered by:

- fulfilment of the processing purpose (e.g., deletion of the customer account by the Controller),
- expiry of the retention periods set out below,
- receipt of a valid erasure request from a data subject, or
- withdrawal of consent or an objection to the processing.

The following retention periods and deletion methods apply to the data categories listed below:

Data Category	Storage Location	Deletion Trigger	Method	Deletion Performed By	Logging
Chat Transcript	Database	Immediately (customer-initiated)	Deletion from database	Customer action	Log file
Chat Transcript	Backup (on-site and off-site)	After 90 days	Removal of backup snapshots	Cronjob	Log file
Chat Transcript	Database	Configurable (1–36 months)	Deletion from database	Cronjob (customer-configurable)	Log file
Customer Account Data	Database	Immediately (customer-initiated)	Deletion from database	Customer action	Log file + audit log
Customer Account Data	Backup (on-site and off-site)	After 90 days	Removal of backup snapshots	Cronjob	Log file
Operator Data	Database	Immediately (customer-initiated)	Deletion from database	Customer action	Log file + audit log
Operator Data	Backup (on-site and off-site)	After 90 days	Removal of backup snapshots	Cronjob	Log file
Application Log Files	File system + database	After 90 days	Retention policy applied	System retention mechanisms	–

System Log Files	File system + database	After 90 days	Retention policy applied	System retention mechanisms	–
LLM Inputs/Outputs (Anthropic models)	AWS Bedrock (EU geography	Not stored (zero data retention, zero operator access)	No storage	–	–
LLM Inputs/Outputs flagged as potentially abusive (OpenAI models)	MS Azure OpenAI (EU geography)	Zero data retention (after max. 30 days for content flagged for abuse)	Flagged content: Automatic deletion at end of Microsoft's retention period	Microsoft abuse monitoring	–

Backups are subject to a separate 90-day retention period irrespective of any prior deletion from the production database; restoration from backups is no longer possible after this period has expired. All deletion actions are logged and reviewed regularly by the responsible Compliance/Security function.

4. Categories of data subjects

The categories of data subjects affected by the processing depend on the individual use of Lime Connect services by the Controller. Possible categories of data subjects are:

- Customers
- Website visitors
- Interested parties
- Controller's operators

Annex 3: Sub-processors

Lime Connect engages the following sub-processors for the processing:

Service provider	Explanation and purpose	Function within the scope of which the subcontract or is being engaged	Server location	Legal basis for possible third country transfer
Hetzner Online GmbH Industriestr. 25 91710 Gunzenhausen Germany	*Hosting of the servers* *Data storage* Data processing: See Annex 2, Section 2	Inherent in the system	Germany	–
Myra Security GmbH Landsberger Str. 187 80687 München Germany	*Expanded DDoS protection* Data processing: See Annex 2, Section 2	Inherent in the system	Germany	–
Scaleway SAS 8 rue de la Ville l'Evêque, 75008 Paris, France	*Storage of encrypted data backups* Data processing: See Annex 2, Section 2	Inherent in the system	EU – France, the Netherlands, Poland, Italy	–
	Connect AI. *Hosting AI Model.* Data categories: • Conversations • Contact info	Optional (immanent when using Connect AI)	EU – France, the Netherlands, Poland, Italy	
BunnyWay, informacijske storitve d.o.o. Škofjeloška Cesta 13 1215 Medvode, Slovenia	Displaying of the technical components (DNS, website images, JavaScript code, stylesheet files) • IP address • Browser • Operating system • Operator profile images	Inherent in the system	region-dependent	–
Lime technologies Sweden AB	*Access to services for internal administrative and operational purposes that require access to the*	Inherent in the system	Sweden	-

S:t Lars väg 46 SE-222 70 Lund Sweden	*product/service, i.e. for development, security work, and IT functions* Data processing: See Annex 2, Section 2			
Amazon Web Services EMEA SARL 38 Avenue John F. Kennedy L-1855 Luxembourg	Displaying of the technical components (JavaScript code, pictures). • IP address • Browser • Operating system • Operator profile images	Inherent in the system	Germany	EU Standard contractual clauses (Art. 46 (2) lit. c) GDPR) EU-US Data Privacy Framework
	File upload offer. Expansion and improvement of core services. • User file uploads • Operator file uploads • IP address • Browser • Operating system	Optional	Germany	EU Standard contractual clauses (Art. 46 (2) lit. c) GDPR) EU-US Data Privacy Framework
	Offer of a notification email regarding the operator's response that is sent to the end user whilst the latter is offline and sending the operator notifications and chat transcripts. Expansion and improvement of core services. • E-mail address • User-generated content • IP address • Browser • Operating system	Optional	Ireland	EU Standard contractual clauses (Art. 46 (2) lit. c) GDPR) EU-US Data Privacy Framework
DeepL GmbH Im Mediapark 8a 50670 Cologne Germany	*Offer of machine translation of notification content* (encrypted, for the duration of the translation). Expansion and improvement of core services. • User-generated content	Optional	Germany	–
Mailgun Technologies, Inc. 112 E Pecan St #1135 San Antonio, Texas 78205 USA	*Optional end user email notifications* Serves as backup for AWS SES. Notification email (outbound) about the operator's response that is sent to the end user whilst the latter is offline as well as operator	Optional	EU	EU Standard contractual clauses (Art. 46 (2) lit. c) GDPR))

	emails, chat transcripts and operator notifications. • E-mail address • Contact name • User-generated content *Offer of an option for the end user to respond to email notifications*. Expansion and improvement of core services. • E-mail address • User-generated content • IP addresses • Browser • Operating system			
Twilio Inc. 375 Beale Street, Suite 300, San Francisco, California 94105 USA	*Audio and video chat.* Expansion and improvement of core services. • User-generated content • IP address • Browser • Operating system	Optional	USA	EU Standard contractual clauses (Art. 46 (2) lit. c) GDPR) EU-US Data Privacy Framework
OMQ GmbH Chausseestraße 22 10115 Berlin Germany	*Optional AI software offer.* Only offered when access to Chatbot API is available in the package. Option to create an AI-based knowledge base to automate customer service (e.g. via chatbots, or smart FAQ etc.) from the Lime Connect dashboard: • Operator IP address • Operator name • Operator email address	Optional	Germany	EU Standard contractual clauses (Art. 46 (2) lit. c) GDPR) EU-US Data Privacy Framework
	Optional AI software hosting offer: *Standard AI:* The algorithm removes personal data before it is stored by the AI • User-generated content (AI messages and contact responses) is anonymized	Optional (immanent when using the AI software offer)	Germany	EU Standard contractual clauses (Art. 46 (2) lit. c) GDPR) EU-US Data Privacy Framework
	Optional AI software hosting offer: *GPT AI model:* Hosted by Microsoft Azure OpenAI services	Optional (immanent when using the AI software offer)	Belgium, the Netherlands, Great Britain	EU Standard contractual clauses (Art. 46 (2) lit. c) GDPR)

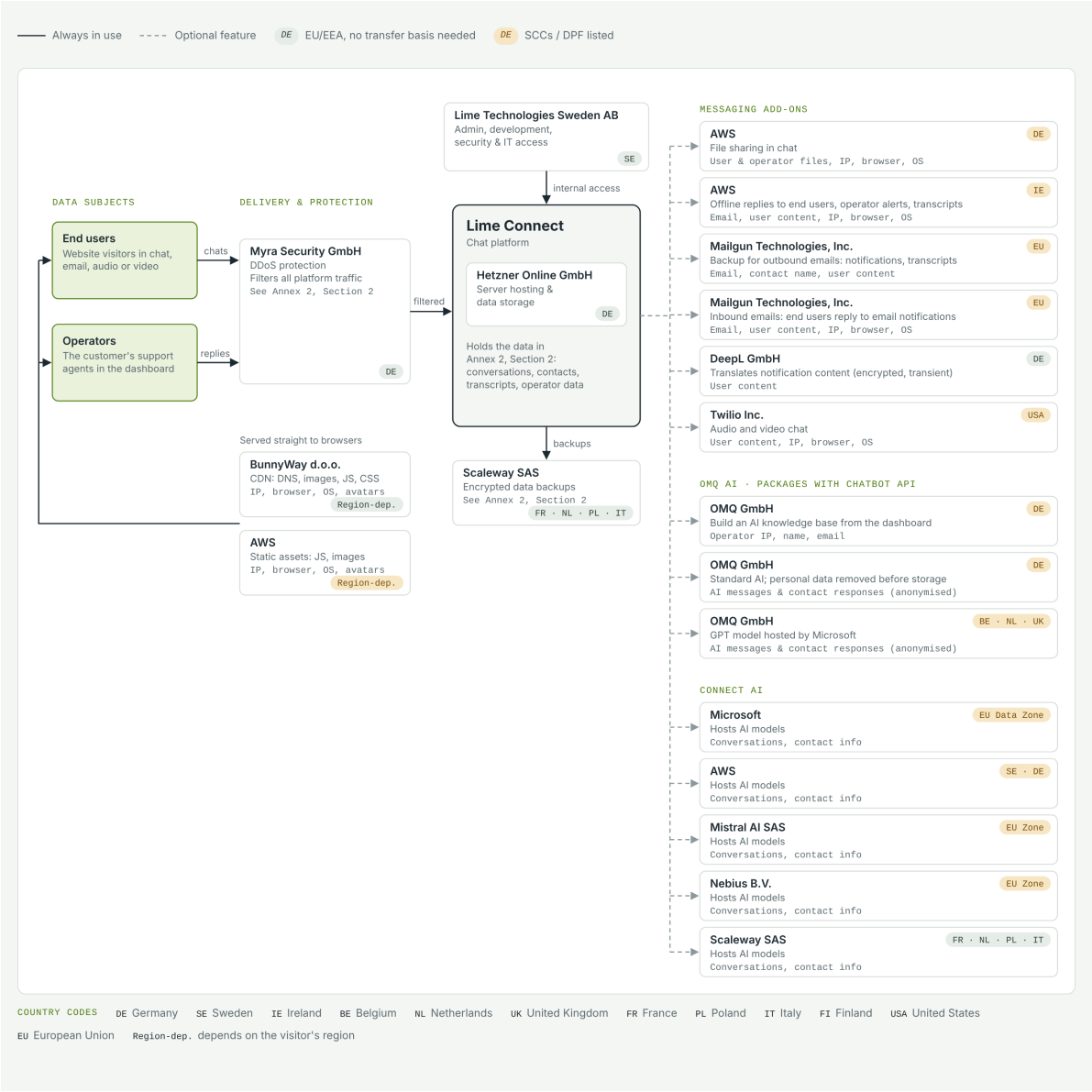
	● User-generated content (AI messages and contact responses) is anonymized			EU-US Data Privacy Framework
Amazon Web Services EMEA SARL 38 Avenue John F. Kennedy L-1855 Luxembourg	***Connect AI.*** *Hosting of knowledge base.* Service: S3 Data categories: ● Knowledge base	Optional (immanent when using Connect AI)	Germany	EU Standard contractual clauses (Art. 46 (2) lit. c) GDPR) EU-US Data Privacy Framework
Microsoft Ireland Operations, Ltd. One Microsoft Place South County Business Park Leopardstown Dublin 18, D18 P521 Ireland	***Connect AI.*** *Hosting AI model.* Service: Microsoft Azure OpenAI Services Data categories: ● Conversations ● Contact info	Optional (immanent when using Connect AI)	EU Data Zone	EU Standard contractual clauses (Art. 46 (2) lit. c) GDPR) EU-US Data Privacy Framework
Amazon Web Services EMEA SARL 38 Avenue John F. Kennedy L-1855 Luxembourg	***Connect AI.*** *Hosting AI model.* Service: Bedrock Data categories: ● Conversations ● Contact info	Optional (immanent when using Connect AI)	EU (Sweden and Germany)	EU Standard contractual clauses (Art. 46 (2) lit. c) GDPR) EU-US Data Privacy Framework
Mistral AI SAS 15 rue des Halles, 75001 Paris, France	***Connect AI.*** *Hosting AI model.* Data categories: ● Conversations ● Contact info	Optional (immanent when using Connect AI)	EU (EU Zone)	EU Standard contractual clauses (Art. 46 (2) lit. c) GDPR) EU-US Data Privacy Framework
Nebius B.V. Burgerweeshuispad 101, 1076 ER Amsterdam, Netherlands	***Connect AI.*** *Hosting AI model.* Data categories: ● Conversations ● Contact info	Optional (immanent when using Connect AI)	EU (EU Zone)	EU Standard contractual clauses (Art. 46 (2) lit. c) GDPR) EU-US Data Privacy Framework

Annex 4: Technical and organizational measures in accordance with Art. 32 GDPR

Lime Connect has implemented the following technical and organizational measures at the time of the conclusion of Agreement:

1. Data flow diagram

The general flow of data is shown on the following chart:



2. Organisational control

Objective: The processor's staff must be obligated to maintain data secrecy and to comply with confidentiality provisions. Commitment to this obligation must be documented in personnel files so that it can be produced as evidence at any time.

Corresponding documents are stored in personnel files.

- There is a text module set out in the standard contract for all employees.
- Employees are informed of their duties again in internal training sessions.

3. Physical access control

Objective: Unauthorized persons must be prevented from gaining (physical) access to data processing systems on which personal data is processed or used. The processor shall install an entry control system for this purpose.

Description of entry control systems in the office (including physical precautions):

- Mechanical locking system on main entrance and office entrances
- Electronic alarm system and unlocking with 24/7 site security
- Cameras

Description of surveillance systems:

- Alarm system with link to site security
- 3 cameras

4. System access control

Objective: Use of data processing systems by unauthorized persons must be prevented. To this end, access to DP systems must be monitored and logged (e.g. prevention of system login, unauthorized upload to and intrusion into DP system).
Intrusion of unauthorized persons into the DP systems must be prevented.

Description of the authentication mechanisms implemented (e.g. password complexity, change cycles, SSH keys):

- SSH: personalized public private keys
- S2S communication: Mesh VPN
- C2S (Client to Server) communication: TLS 1.3 and TLS 1.2

Description of measures upon temporary inactivity of users (e.g. when an employee leaves their desk):

- Hot Corners are configured in the MacOS X system; this allows users to quickly swipe the cursor to a corner to bring up the lock-out screensaver. Otherwise, the monitor locks out after 5 minutes.
- All employees are encouraged to always lock their screens.
- Microsoft Defender
- Centralized management with MDM

Description of technical safeguards for your network environment:

- iptables rules on external interfaces
- Services only listen in on internal networks
- VPN communication for servers
- Weekly nmpa scans
- Weekly OpenVAS scans
- Daily monitoring
- Daily audit of new critical errors
- Anti-DDoS in the data centre with Hetzner online GmbH
- Additional anti-DDoS service with Myra Security GmbH
- Zero trust solution to internal services (username + password + 2FA)
- Centralized logging of systems

5. Data access control

Objective: It must be ensured that persons authorized to use a data processing system are only able to access the data for which they have access authorization, and that personal data cannot be read, copied, modified or erased without authorization during processing or use or after storage.

Personal data must be encrypted in the case of persistent storage.

Needs-oriented design of the authorization concept and access rights, as well as monitoring and logging thereof:

Description of the prevention of unauthorized activity in DP systems outside of granted authorizations (roles and authorizations according to the need-to-know principle):

- Rights and role management
- Technical onboarding and offboarding of employees

- Access rights only as required
- Access rights are checked at least once per month

Description of measures to prevent unauthorized access (e.g. brute force, SQL injection, login validation):

- SSH: CrowdSec
- SQL injections are systematically excluded by using query parameterization for database queries.
- All critical endpoints are protected against brute force attacks with rate limits.
- The usual Django Framework security features (CSRF tokens etc.) are used.
- Access for Lime Connect employees is protected by a 2-factor authentication.
- Customers can activate further security features such as login validation by email.

Description of mechanisms to ensure that only personalized user accounts are used to access the systems (one account per user):

- 1 account per user
- 1 account set up with Zero trust solution per user with F2A
- 1 account on a computer

Description of encryption measures implemented for personal data:

- Hard drive encryption with LUKS2 (cipher: aes-xts-plain64, keysize: 512 bits)
- Transport encryption with TLS 1.3 and TLS 1.2
- VPN
- SSH safeguards: GPG

5.1. Transfer control

Objective: It must be ensured that personal data cannot be read, copied, modified or erased without authorization during electronic transfer or during transport or storage on data carriers, and that it is possible to check and identify where transfer of personal data by data transfer systems is expected to take place.

Personal data must be encrypted for transfer (transport encryption).

Description of transport encryption:

- Transport encryption with TLS 1.3 and TLS 1.2
- VPN

- SSH

Description of the logging of personal data transfer:

- Not applicable. Personal data is not downloaded or transferred from servers. Back-ups are the exception. Back-ups are logged and encrypted. Manually checked on a daily basis.
- Hard drives are always encrypted and overwritten before being returned.

Description of transport protection for physical transport:

- Not applicable. Personal data is not physically transported from servers.

5.2. Input control

Objective: It must be ensured that it is possible to check and establish later whether personal data was entered, modified in, or erased from data processing systems, and by whom.

A detailed logging system for the input, modification, and erasure of personal data (e.g. log files) must be implemented and assessed on a regular basis.

Description of the logging/monitoring system for monitoring access:

- The customer has an audit log available to them. The audit log is a log listing all changes to the customer's account.
- Various logs are kept on server level; these are compiled upon login of employees during maintenance work. These logs are checked on a random basis and stored centrally.
- In addition, various logs showing the technical status of the system are generated.

5.3. Availability control

Objective: It must be ensured that personal data is protected against accidental loss or destruction.

Description of the data security concept (e.g. back-up procedure, redundancies, UPS, emergency plans):

- 3 data centres (system available in triplicate)

- 2 different sites/data centres
- UPSs and diesel generators
- Mirrored hard drives
- Enterprise hard drives
- Automated monitoring
- Daily back-ups of all data
- Back-ups in 2 different locations
- Several employees managing the process

5.4. Separation rule

Objectives: It must be ensured that personal data collected for different purposes can be processed separately. The processor shall ensure demonstrable logical separation of the client's data, i.e. data from different controllers must be processed separately. Mutual access must be excluded. In addition, data must only be processed for a specific purpose.

Description of implementation for multi-client capability:

- Data is processed for a specific purpose and is separated logically by client on database level (multi-client capability).

Description of mechanisms to ensure the separation of development, testing and productive systems:

Physical separation (different servers) in 3 environments:

- Development
- Staging
- Production

5.5. Information security

Description of the information security management system (ISMS):

- Lime Connect is ISO 27001 certified
- Trust Center resources: https://trust.lime-technologies.com/
- Responsibility:
    - IT Security: security@lime-connect.com
    - Data Privacy: privacy@lime-connect.com
- Regular training

- IT security
- Data protection
- Fixed processes
- Onboarding
- Offboarding

5.6. Miscellaneous

Description of mechanisms to ensure confidential storage and erasure or destruction of test and scrap materials containing personal data (e.g. paper):

- Not applicable. No paper used. Excluding bookkeeping and contracts. Documents are shredded.
- Hard disks are always encrypted and overwritten several times before delivery.

6. Use of sub-contractors

The technical and organizational measures implemented by the other processors that we use at the point at which this agreement is concluded are available on request. We regularly verify the appropriateness and effectiveness of the measures implemented by our subcontractors.

7. Processor's assurance

The processor guarantees that all information provided in this document is truthful.

Annex 5: Additions to the EU Standard Contractual Clauses

The Parties agree on the following additions and updates to the EU Standard Contractual Clauses (Annex 1):

1. Documentation and compliance (Clause 7.6)

Clause 7.6 of the EU Standard Contractual Clauses is supplemented by the following provisions:

> In order to perform audits in accordance with clause 7.6 c) ff., the Controller may enter Lime Connect's business premises where the Controller data is being processed during ordinary working hours (Monday to Friday from 10.00 am to 6.00 pm), after giving adequate notice in accordance at its own costs, without disrupting daily operations, and under strictest non-disclosure of Lime Connect's operating and business secrets.

2. Use of sub-processors (Clause 7.7)

Clause 7.7. a) of the EU Standard Contractual Clauses is supplemented by the following provisions:

> Lime Connect shall inform the Controller in electronic format about planned changes regarding the engagement or replacement of additional processors 30 days in advance. In exceptional circumstances, Lime Connect may give 5 days' notice to the Controller about planned changes, for example, if the involvement or replacement of additional processors appears necessary for acute IT security reasons. In individual cases, the Controller may object to the potential engagement of an additional processor. The Controller may only raise an objection for good cause that shall be proven to Lime Connect. Failure of the Controller to raise an objection within 14 working days from receipt of the notification shall result in its right to object against the corresponding engagement expiring. If the Controller raises an objection, Lime Connect may terminate the principal contract and this Agreement at the next possible date after the principal contract (Terms and Conditions).

3. International transfers (Clause 7.8)

Clause 7.8 of the EU Standard Contractual Clauses is supplemented by the following provisions:

> Lime Connect may also process Controller data in compliance with the provisions of this Agreement outside the EEA if Lime Connect informs the Controller in advance about the place where the data is to be processed and the conditions of Art. 44 to 48 GDPR have been met or there is an exception in accordance with Art. 49 GDPR.

4. Scope of the contract

The EU Standard Contractual Clauses are supplemented by the following provisions:

> Lime Connect reserves the right to anonymize Controller Data. Anonymization is carried out by way of aggregation, provided that the identification of individual data subjects is no longer possible. Lime Connect is permitted to use such anonymized data for the purpose of demand-based optimization and further development, as well as for the provision of the service agreed under the Main Agreement (Terms and Conditions). The parties agree that Controller Data anonymized in accordance with the foregoing no longer constitutes Controller Data within the meaning of this Agreement.

5. Security of processing (Clause 7.4)

Clause 7.4 of the EU Standard Contractual Clauses is supplemented by the following provisions:

> Lime Connect shall implement appropriate technical and organizational measures in accordance with Article 32 of the GDPR to ensure a level of security appropriate to the risk involved in the processing of personal data.
> Lime Connect is entitled to further develop or adapt these technical and organizational measures, taking into account the state of the art as well as the nature, scope, context, and purposes of the processing, provided that this does not result in a level of protection lower than that agreed upon.
> Lime Connect shall inform the Controller in an appropriate manner of any significant changes to the technical and organizational measures that may affect the security of the processing.

6. Duration of Processing (Clause 7.3)

Clause 7.3 of the EU Standard Contractual Clauses is supplemented by the following provisions:

> The specific retention and deletion periods applicable to the individual categories of personal data, as well as the respective deletion triggers and procedures, are set out in Annex 2.