Software-as-a-Service-Rahmenvertrag

zwischen der

omneva Group GmbH,
Fuhlsbüttler Straße 387, 22309 Hamburg

- im Folgenden: **„Provider“** -

und dem

in den Kundenangaben genannten Vertragspartner

- im Folgenden: **„Kunde“** -

- Der Provider und der Kunde gemeinsam im Folgenden: **„Parteien“** -

Inhaltsverzeichnis:

1. Vertragsgegenstand

1.1 Der Provider vertreibt den Messenger „myneva safechat“. Dieser Messenger besteht aus einem WEB-Portal (www.mysafechat.de/admin), einem WEB-Portal zur Administration (www.mysafechat.de) (im Folgenden gemeinsam: **„safechat“**) sowie aus einer Android App, beziehbar über den Google Play Store, und einer iOS App, beziehbar mit Codes aus den Apple Business Stores in den Ländern DE, AT, NL (im Folgenden: **„App“**).

1.2 Gegenstand dieses Software-as-a-Service-Rahmenvertrags (im Folgenden: **„SaaS-Vertrag“**) ist (i) die auf die Vertragslaufzeit befristete Nutzungsmöglichkeit von safechat in der zum Vertragszeitpunkt aktuellen Version, (ii) die Einräumung von Speicherplatz für die durch die Nutzung von safechat erzeugten und/oder die zur Nutzung von safechat erforderlichen Daten des Kunden und (iii) die Einräumung der in Ziff. 6 beschriebenen Nutzungsrechte.

1.3 Auf Basis dieses SaaS-Vertrags kann der Kunde Berechtigungsfreigaben für Nutzer erteilen. Entsprechend der erteilten Berechtigungen können die Nutzer sodann die von ihnen selbst bezogene App (vgl. Ziff. 1.1) verwenden. Die Berechtigungsfreigabe erfolgt, gemäß der internen Rollenvorgaben beim Kunden, z.B. durch den IT-Administrator des Kunden, der in diesem Zusammenhang über das WEB-Portal in seinem Dashboard ein Profil mit den Kontaktdaten des Nutzers anlegen muss.

1.4 Die Software safechat sowie der notwendige Speicherplatz für Daten werden über ein vom Provider beauftragtes Rechenzentrum bereitgestellt.

1.5 Die Beschaffenheit und Funktionalität von safechat ergibt sich abschließend aus der Produktbeschreibung. Der Kunde konnte die Produktbeschreibung im Rahmen des Abschlusses dieses SaaS-Vertrags unter https://www.myneva.eu/solidaritaet einsehen und sich über die Beschaffenheit und Funktionalität von safechat informieren. Die darin enthaltenen Angaben sind als Beschaffenheitsbeschreibungen zu verstehen.

1.6 Der Zugang des Kunden zum Internet ist nicht Gegenstand dieses SaaS-Vertrags. Der Kunde trägt die alleinige Verantwortung für die Funktionsfähigkeit seines Internetzugangs einschließlich der Übertragungswege seines Rechners.

1.7 Die Rechte und Pflichten der Parteien ergeben sich allein aus den Bestimmungen dieses SaaS-Vertrags und dessen **Anlagen.** Allgemeine Geschäftsbedingungen des Kunden werden nicht Vertragsinhalt, selbst wenn der Provider diesen nicht ausdrücklich widerspricht. Im Fall von Widersprüchen zwischen den Bestimmungen des SaaS-Vertrags und den **Anlagen** gehen die Bestimmungen der **Anlagen** vor.

2. Vertragsschluss/ergänzende Einzelaufträge/Musterdokumente

2.1 Die Leistungen des Providers richten sich ausschließlich an Unternehmer.

2.2 Auf der Webseite des Providers erhält der Kunde Zugang zu sämtlichen Vertragsdokumenten im Zusammenhang mit safechat und kann diese ausdrucken und/oder gesondert auf seinem Endgerät speichern.

2.3 Für ein Angebot muss der Kunde auf der vorgenannten Webseite (i) die Bedingungen dieses SaaS-Vertrags durch Anklicken des entsprechenden Buttons akzeptieren (ii) das Formular mit den Angaben zu dem Kunden-Unternehmen, dem Administrator und den benötigten Accounts online vollständig ausfüllen und schließlich (iii) den Button „Absenden“ anklicken. Das ausgefüllte Formular wird mit der Versendung als **Anlage 1** Teil dieses SaaS-Vertrags.

2.4 Unmittelbar nach dem Absenden des Angebots erhält der Kunde eine automatische Eingangsbestätigung mit seinen Angaben zur **Anlage 1** an seine E-Mail-Adresse. Diese Bestätigung stellt jedoch noch keine Vertragsannahme dar. Eine Vertragsannahme und damit der Vertragsschluss kommen erst durch eine separate Auftragsbestätigung an die E-Mail-Adresse des Kunden zustande. Nimmt der Provider das Angebot an, erhält der Kunde innerhalb von sieben (7) Tagen eine E-Mail an die in den Kundenangaben (**Anlage 1**) angegebenen E-Mail-Adresse des Administrators. Diese E-Mail enthält sodann einen Link zum Web-Portal, über welches sich der Administrator des Kunden anmelden und die erforderlichen Berechtigungsfreigaben für safechat erteilen kann.

2.5 Den Parteien steht es während der Laufzeit des SaaS-Vertrags frei, ergänzende Einzelaufträge zur Nutzung von safechat zu vereinbaren. Auf diese Einzelaufträge finden die Bestimmungen dieses SaaS-Vertrags, insbesondere gemäß Ziff. 7, entsprechend Anwendung.

2.6 Die App (vgl. Ziff. 1.1) enthält eigene Nutzungsbedingungen und eine Datenschutzerklärung. Diese finden lediglich im Verhältnis zwischen dem Provider und dem Nutzer der App Anwendung und sind nicht Bestandteil des SaaS-Vertrags. Darüber hinaus findet sich auf der Webseite mysafechat.de, auf die der Nutzer der App im Rahmen der Erstregistrierung gelangt, eine Datenschutzerklärung, die sich an diesen richtet. Auch diese Datenschutzerklärung ist nicht Bestandteil des SaaS-Vertrags. Aus informatorischen Gründen werden dem Kunden allerdings die Nutzungsbedingungen und die Datenschutzerklärung für die App sowie die Datenschutzerklärung für die Webseite, als Muster auf der Webseite des Providers zur Verfügung gestellt.

3. Bereitstellung von safechat

Mit der Annahme des Angebots (vgl. Ziff. 2) übermittelt der Provider dem Kunden die für die Nutzung von safechat erforderlichen Zugangsdaten zur Identifikation und Authentifikation (im Folgenden: **„Zugangsdaten“**). Mit diesen Zugangsdaten hat der Kunde die Möglichkeit, safechat über seinen Internetzugang zu nutzen.

4. Einräumung von Speicherplatz/Verfügbarkeit

4.1 Der Kunde hat die Möglichkeit, auf dem für ihn vom Provider eingerichteten virtuellen Datenserver die durch die Nutzung von safechat erzeugten und/oder die zur Nutzung von safechat erforderlichen Daten zu speichern und auf diese im Rahmen der Nutzung von safechat zuzugreifen. Der Provider stellt dem Kunden hierfür den erforderlichen Speicherplatz zur Verfügung.

4.2 Der Provider wird sich bemühen, safechat unterbrechungsfrei verfügbar zu halten. Ein Anspruch darauf besteht jedoch nicht.

5. Pflichten des Kunden

5.1 Der Kunde hat den Provider bei der Bereitstellung von safechat zu unterstützen und hierfür insbesondere alle Informationen, Unterlagen etc. bereitzustellen.

5.2 Der Kunde verpflichtet sich, auf dem zur Verfügung gestellten Speicherplatz keine rechtswidrigen, die Gesetze, behördlichen Auflagen oder Rechte Dritter verletzenden Inhalte zu speichern.

5.3 Der Kunde wird die Zugangsdaten durch geeignete Maßnahmen vor dem Zugriff durch unbefugte Dritte sichern.

5.4 Der Kunde wird ein dem Stand der Technik entsprechendes Virenschutzprogramm einsetzen und insbesondere vor dem Versenden von Daten an den Provider diese auf Viren prüfen.

5.5 Mängel an safechat sind stets detailliert, insbesondere unter Angabe der Symptome und Auswirkungen, zu beschreiben. Die Mängelrüge soll die Reproduzierbarkeit des Mangels ermöglichen. Soweit erforderlich, unterstützt der Kunde den Provider unentgeltlich bei der Diagnose und Behebung von Mängeln an safechat im Rahmen des Zumutbaren.

5.6 Sofern der Kunde die App selbst verwendet, wird er insbesondere die nachfolgenden Systemvoraussetzungen zur Nutzung der App beachten. Der Kunde wird die von ihm berechtigten Nutzer zudem gesondert auf diese Voraussetzungen hinweisen.

5.6.1 Voraussetzung zur Nutzung der App ist die Verwendung eines aktuellen Betriebssystems von iOS oder Android.

5.6.2 Vor der Nutzung der App ist sicherzustellen, dass das Endgerät über die neueste Version von iOS (mind. iOS 13) oder Android (mind. Android 10 – API Level 29) verfügt. Der aktuelle Versionsstand kann über die Einstellung in dem jeweiligen Endgerät überprüft werden.

5.6.3 In diesem Zusammenhang ist von dem Nutzer der App ein aktives Updatemanagement zu betreiben, um die Software auf den Geräten stets auf dem aktuellsten Stand zu halten. Sofern z.B. veraltete Versionen von iOS oder Android genutzt werden, können einige Sicherheitsmaßnahmen im Zusammenhang mit der App ggf. nicht gewährleistet werden.

6. Rechteeinräumung

6.1 Der Kunde erhält ein nichtausschließliches (einfaches), zeitlich auf die Laufzeit des SaaS-Vertrags beschränktes, nicht übertragbares und nicht unterlizenzierbares Recht zur Nutzung von safechat nach Maßgabe des im Angebot eingeräumten Umfangs (im Folgenden: **„Lizenzübersicht“**).

6.2 Der Kunde ist, mit Ausnahme eines etwaig in der Lizenzübersicht eingeräumten Umfangs, nicht berechtigt, safechat zu vermieten oder in sonstiger Weise unterzulizenzieren, safechat drahtgebunden oder drahtlos öffentlich wiederzugeben oder zugänglich zu machen oder Dritten entgeltlich oder unentgeltlich zur Verfügung zu stellen.

6.3 Der Kunde ist ausschließlich dann berechtigt, safechat zu dekompilieren und zu vervielfältigen, soweit dies gesetzlich vorgesehen ist. Dies gilt jedoch nur unter der Voraussetzung, dass der Provider dem Kunden die hierzu notwendigen Informationen auf Anforderung nicht innerhalb einer angemessenen Frist zur Verfügung gestellt hat.

6.4 Sofern nicht abweichend vereinbart, erwirbt der Kunde während der Laufzeit des SaaS-Vertrags an vom Provider explizit gegenüber dem Kunden bereitgestellten Aktualisierungen, d.h. an geänderter oder erweiterter Software von safechat, dieselben Rechte wie an der bisherigen Standardsoftware safechat.

6.5 Urhebervermerke, Seriennummern sowie sonstige der Programmidentifikation dienende Merkmale dürfen nicht von safechat entfernt oder verändert werden.

7. Unentgeltliche Gebrauchsgewährung im Zusammenhang mit COVID-19

7.1 Aus Gründen der aktuellen Situation zum Coronavirus (COVID-19) stellt der Provider dem Kunden die Gebrauchsgewährung für safechat unentgeltlich für eine Übergangsphase bis zum 31.12.2020 zur Verfügung. Sofern nach dem Vertragsschluss ergänzende Einzelaufträge (vgl. Ziff. 2.5) vereinbart werden, gilt für diese einheitlich die vorgenannte Übergangsphase. Eine individuelle Verlängerung der Übergangsphase findet nicht statt.

7.2 Spätestens zwei (2) Wochen vor Ablauf der vorgenannten Übergangsphase wird der Provider, unter Berücksichtigung der dann aktuellen Situation in Deutschland, die Frage einer entgeltlichen oder unentgeltlichen Nutzung von safechat neu bewerten und dies dem Kunden schriftlich oder via E-Mail mitteilen. Sofern keine Mitteilung erfolgt, endet der SaaS-Vertrag automatisch (vgl. Ziff. 13).

7.2.1 Für den Fall der Fortführung einer unentgeltlichen Nutzung, gelten für diese dann neue Übergangsphase die Bestimmungen in Ziff. 7.1 Satz 2 und Satz 3 sowie Ziff. 7.2 entsprechend.

7.2.2 Für den Fall einer entgeltlichen Nutzung, wird der Provider dem Kunden ein gesondertes Angebot mit den Konditionen zukommen lassen. Nimmt der Kunde das Angebot nicht vor dem Ende der Übergangsphase an, endet der Saas-Vertrag zum Ablauf der Übergangsphase automatisch (vgl. Ziff. 13).

8. Sach- und Rechtsmängel

8.1 Der Provider haftet für die vereinbarte Beschaffenheit (siehe Ziff. 1.5.) sowie dafür, dass der Kunde safechat ohne Verstoß gegen Rechte Dritter nutzen kann.

8.2 Die Haftung des Providers gilt nicht für Mängel, die darauf beruhen, dass der Kunde oder Dritte Veränderungen an safechat vorgenommen haben, ohne hierzu (a) kraft Gesetztes, (b) aufgrund dieses SaaS-Vertrages oder (c) aufgrund einer vorherigen schriftlichen Zustimmung des Providers berechtigt zu sein.

8.3 Der Provider ist im Falle eines Sachmangels berechtigt, dem Kunden ggf. einen neuen Stand der Software von safechat bereitzustellen, es sei denn, dies führt zu unzumutbaren Beeinträchtigungen. Bei Rechtsmängeln wird der Provider im Rahmen der Nacherfüllung dem Kunden nach eigener Wahl eine rechtlich einwandfreie Nutzungsmöglichkeit an safechat verschaffen oder safechat so abändern, dass keine Rechte Dritter mehr verletzt werden.

9. Supportleistungen des Providers

9.1 Während der Laufzeit des SaaS-Vertrags wird der Provider dem Kunden Supportleistungen für safechat in Form eines E-Mail-Supports (support@mysafechat.de) nach folgender Maßgabe anbieten:

(i) Vollständiger Support für die Behebung und Umgehung von Fehlern, insbesondere Annahme und Dokumentation von E-Mails, Priorisierung nach Dringlichkeit, Analyse und Eingrenzung des Fehlers.

(ii) Der Provider wird die Supportleistungen in der Zeit von Montag bis Freitag zwischen 08.00 Uhr und 17.00 Uhr erbringen. Es gilt die Zeitzone des Providers. Die Servicezeiten gelten nicht an den gesetzlichen Feiertagen in Deutschland.

(iii) Stellt sich heraus, dass ein vom Kunden gemeldeter Fehler tatsächlich nicht besteht oder z.B. auf einen Umstand gemäß Ziff. 8.2 zurückzuführen ist (im Folgenden: **„Scheinfehler“**), trägt der Kunde die im Zuge der Fehleranalyse beim Provider entstandenen Kosten gemäß der jeweils zum Zeitpunkt der Fehlermeldung geltenden aktuellen Preisliste des Providers, es sei denn, der Kunde konnte das Vorliegen des Scheinfehlers auch bei Anstrengung der erforderlichen Sorgfalt nicht erkennen.

9.2 In Bezug auf die Nutzungsrechte an den Supportleistungen gelten die Bestimmungen gemäß Ziff. 6.

9.3 Sonstige Beratungs- und Unterstützungsleistungen, insbesondere im Zusammenhang mit den Funktionen von safechat, sowie Konfigurations- und Schulungsleistungen sind nicht Bestandteil der Supportleistungen. Auf Anfrage des Kunden kann der Provider hierzu eine gesonderte Vereinbarung anbieten.

10. Haftung

10.1 Die Haftung des Providers für Schäden gleich welcher Art ist ausgeschlossen. Dieser Ausschluss gilt nicht

- für Schäden, die der Provider vorsätzlich oder grobfahrlässig herbeigeführt hat;

- in Fällen leichter Fahrlässigkeit für Schäden, die auf einer Verletzung von Leben, Körper oder Gesundheit beruhen;

- vorbehaltlich der Regelung in Ziff. 10.2 für Schäden, die auf einer Verletzung wesentlicher Vertragspflichten durch den Provider beruhen. Wesentliche Vertragspflichten sind alle Pflichten, deren Erfüllung die ordnungsgemäße Durchführung des SaaS-Vertrags erst ermöglichen und auf deren Einhaltung der Kunde regelmäßig vertraut und vertrauen darf.

10.2 In den Fällen fahrlässiger Verletzung (einfache Fahrlässigkeit) wesentlicher Vertragspflichten ist die Haftung des Providers auf den vertragstypischen, für den Provider bei Abschluss des SaaS-Vertrags oder Beginn der Pflichtwidrigkeit vorhersehbaren Schaden begrenzt. Der Haftungsausschluss in dieser Ziff. 10.2 gilt nicht für die Haftung des Providers bei der Verletzung von Leben, Körper oder Gesundheit sowie bei einer Haftung nach dem Produkthaftungsgesetz.

10.3 Schadensersatzansprüche des Kunden wegen einfacher Fahrlässigkeit des Providers sind in jedem Fall ausgeschlossen, wenn sie nicht binnen einer Frist von drei Monaten nach Ablehnung der Ansprüche mit einem entsprechenden Hinweis durch den Kunden oder dessen Versicherer gerichtlich geltend gemacht werden. Alle etwaigen, auf einfacher Fahrlässigkeit des Providers beruhende Schadensersatzansprüche verjähren, unter Berücksichtigung von § 199 BGB und der Ausnahmen in Ziff. 10.2 Satz 2, in einem (1) Jahr.

10.4 Die verschuldensunabhängige Haftung des Providers gemäß § 536a Abs. 1, 1. Alternative BGB wegen Mängeln, die bereits zum Zeitpunkt des Vertragsschlusses vorhanden sind, ist ausgeschlossen.

10.5 Eine über die vorgenannten Bestimmungen hinausgehende Haftung des Providers besteht nicht.

10.6 Die vorstehende Haftungsbeschränkung gilt auch für die persönliche Haftung der Mitarbeiter, Vertreter und Organe des Providers.

11. Vertraulichkeit

11.1 Die Parteien vereinbaren, über vertrauliche Informationen Stillschweigen zu wahren. „Vertrauliche Informationen“ sind alle Informationen i.S.v. § 2 Nr. 1 GeschGehG sowie alle sonstigen Informationen und Unterlagen der jeweils anderen Partei, die als vertraulich gekennzeichnet oder aus den Umständen heraus als vertraulich anzusehen sind, insbesondere Informationen über safechat, betriebliche Abläufe und sonstiges Know-how.

11.2 Die Verpflichtung auf die Vertraulichkeit gilt unbefristet und unabhängig von der Beendigung des Vertragsverhältnisses fort.

11.3 Von dieser Verpflichtung ausgenommen sind solche vertraulichen Informationen, die

(a) dem Empfänger bei Abschluss des SaaS-Vertrags nachweislich bekannt waren oder danach von dritter Seite bekannt werden, ohne dass dadurch eine Vertraulichkeitsvereinbarung, gesetzliche Vorschriften oder behördliche Anordnungen verletzt werden;

(b) bei Abschluss des SaaS-Vertrags öffentlich bekannt sind oder danach öffentlich bekannt gemacht werden, soweit dies nicht auf einer Verletzung dieses SaaS-Vertrags beruht, oder

(c) die aufgrund gesetzlicher Verpflichtungen oder auf Anordnung eines Gerichts oder einer Behörde offen gelegt werden müssen. Soweit zulässig oder möglich, wird der zur Offenlegung Verpflichtete die andere Partei vorab unterrichten und ihr Gelegenheit geben, gegen die Offenlegung vorzugehen.

11.4 Die Parteien werden nur solchen Beschäftigten und/oder sonstigen Personen Zugang zu vertraulichen Informationen gewähren, die dem Berufsgeheimnis unterliegen oder denen zuvor den Geheimhaltungsverpflichtungen dieses SaaS-Vertrags entsprechende Verpflichtungen auferlegt worden sind. Diese Verpflichtung auf die Geheimhaltung muss, soweit hinsichtlich der Beschäftigten arbeitsrechtlich zulässig, auch nach Beendigung der Tätigkeit fortgelten. Ungeachtet dessen sind sämtlichen verpflichteten Beschäftigten und sonstigen Personen nur diejenigen vertraulichen Informationen offenzulegen, die diese für die Leistungserbringung kennen müssen.

12. Datenschutz

12.1 Die Parteien verpflichten sich, die jeweils einschlägigen gesetzlichen Bestimmungen zum Umgang mit personenbezogenen Daten, insbesondere der EU-Datenschutzgrundverordnung (DSGVO) und des Bundesdatenschutzgesetzes (BDSG) einzuhalten.

12.2 Die Parteien vereinbaren im Zusammenhang mit den Leistungen gemäß Ziff. 1.2 einen Vertrag zur Auftragsverarbeitung (**Anlage 2**)**.**

13. Laufzeit/Kündigung

13.1 Dieser SaaS-Vertrag endet automatisch, d.h. ohne eine ausdrückliche Kündigung oder eine sonstige Erklärung einer Partei, am 31.12.2020.

13.2 Vereinbaren die Parteien gemäß Ziff. 7.2.2 die Fortführung einer entgeltlichen Nutzung, wird der Vertrag auf unbestimmte Zeit geschlossen. Er kann von jeder Partei mit einer Frist von drei (3) Monaten zum Ende des Jahres gekündigt werden, frühestens jedoch zum Ende des Jahres, in dem sich das Abschlussdatum dieses entgeltlichen SaaS-Vertrags erstmals jährt.

13.3 Der SaaS-Vertrag kann darüber hinaus von jeder Partei ohne Einhaltung einer Frist aus wichtigem Grund schriftlich gekündigt werden. Ein wichtiger Grund liegt insbesondere vor, wenn der Kunde Nutzungsrechte des Providers dadurch verletzt, dass er safechat

über das nach diesem SaaS-Vertrag gestattete Maß hinaus nutzt und die Verletzung auf eine Abmahnung des Providers hin nicht innerhalb angemessener Frist abstellt.

13.4 Eine Kündigung des Kunden gemäß § 543 Abs. 2 S. 1 Nr. 1 BGB wegen Nichtgewährung des vertragsgemäßen Gebrauchs ist erst zulässig, wenn dem Provider ausreichende Gelegenheit zur Mängelbeseitigung gegeben wurde und diese fehlgeschlagen ist. Von einem Fehlschlagen der Mängelbeseitigung ist erst auszugehen, (a) wenn diese unmöglich ist, (b) wenn sie vom Provider verweigert oder in unzumutbarer Weise verzögert wird, (c) wenn begründete Zweifel bzgl. der Erfolgsaussichten der Mängelbeseitigung bestehen oder (d) wenn aus anderen Gründen eine Unzumutbarkeit für den Kunden gegeben ist.

13.5 Sofern der SaaS-Vertrag nicht automatisch endet und somit eine Kündigung erforderlich ist, bedarf diese Kündigung zu ihrer Wirksamkeit der Schriftform.

14. Vertragsbeendigung/Ende des Nutzungsrechts

14.1 Im Falle der Vertragsbeendigung oder bei einer sonstigen Beendigung der Nutzungsberechtigung gibt der Kunde alle etwaig von dem Provider erhaltenen Daten, insbesondere die Zugangsdaten, unverzüglich an den Provider heraus bzw. löscht diese sowie sämtliche Kopien hiervon, soweit er nicht gesetzlich zu einer längeren Aufbewahrung verpflichtet ist.

14.2 Die ordnungsgemäße Löschung sämtlicher erhaltener Daten hat der Kunde gegenüber dem Provider unverzüglich nach Vertragsbeendigung oder bei einer sonstigen Beendigung der Nutzungsberechtigung schriftlich zu versichern. Eine gesetzlich notwendige längere Aufbewahrung hat der Kunde dem Provider ebenfalls mitzuteilen.

14.3 Sofern der Kunde auch nach Beendigung der Nutzungsberechtigung Zugriff auf seine Daten benötigt, hat der Kunde dies dem Provider vorab rechtzeitig schriftlich mitzuteilen. Auf Nachfrage des Kunden, können die Parteien eine gesonderte Vereinbarung zur Aufbewahrung, Überführung und/oder Retransition von Daten durch den Provider schließen. Für sämtliche Unterstützungsleistungen, wie z.B. die Bereitstellung der Daten auf einem separaten Datenträger, erhält der Provider eine gesonderte Vergütung nach Maßgabe der jeweils aktuell gültigen Preisliste des Providers.

15. Abtretung/Aufrechnung/Zurückbehaltungsrechte

15.1 Der Kunde darf Ansprüche gegen den Provider nur nach schriftlicher Zustimmung des Providers auf Dritte übertragen. Die Regelung in § 354 a HGB bleibt unberührt.

15.2 Der Kunde darf nur mit unbestrittenen oder rechtskräftig festgestellten Forderungen aufrechnen. Entsprechendes gilt für die Ausübung von Zurückbehaltungsrechten.

16. Anwendbares Recht/Gerichtsstand

16.1 Auf diesen SaaS-Vertrag findet das deutsche Recht Anwendung.

16.2 Erfüllungsort ist der Sitz des Providers. Ausschließlicher Gerichtsstand für alle Streitigkeiten aus oder im Zusammenhang mit diesem SaaS-Vertrag ist der Sitz des Providers. Der Provider ist allerdings berechtigt, den Kunden auch an dessen Sitz zu verklagen.

17. Schriftform/salvatorische Klausel

17.1 Änderungen und Ergänzungen dieses SaaS-Vertrags bedürfen der Schriftform. Dies gilt auch für die Änderung und Aufhebung dieser Klausel.

17.2 Sollten Bestimmungen dieses SaaS-Vertrags unwirksam sein, berührt dies die Gültigkeit der übrigen Bestimmungen nicht. Die Parteien werden sich bemühen, anstelle der unwirksamen Bestimmungen eine wirksame zu finden, die den wirtschaftlichen Bedeutungsgehalt der unwirksamen Bestimmungen am ehesten nahekommt. Entsprechendes gilt bei einer Lücke in diesem SaaS-Vertrag

Anlagen

Anlage 1: Kundenangaben zum SaaS-Vertrag

Anlage 2: Vertrag zur Auftragsverarbeitung

Anlage 2: Vertrag zur Auftragsverarbeitung

Vertrag zur Auftragsverarbeitung gemäß Art. 28 Datenschutzgrundverordnung (DSGVO)

zwischen
dem Kunden
nachfolgend: „Verantwortlicher"-
und
omneva Group GmbH
Fuhlsbüttler Straße 387
22309 Hamburg
nachfolgend: „Auftragsverarbeiter"
der Verantwortliche und der Auftragsverarbeiter nachfolgend gemeinsam: „Parteien"

Präambel
Die Parteien haben einen Vertrag über die Erbringung von Leistungen im Zusammenhang mit personenbezogenen Daten geschlossen (nachfolgend: **„Hauptvertrag"**). Dieser Vertrag über die Auftragsverarbeitung (nachfolgend: **„Vertrag"**) konkretisiert die Verpflichtungen der Parteien zum Datenschutz, die sich aus dem Hauptvertrag ergeben. Er findet Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei denen der Auftragsverarbeiter, Beschäftigte des Auftragsverarbeiters oder durch den Auftragsverarbeiter Beauftragte mit personenbezogenen Daten des Verantwortlichen in Berührung kommen können.

1. Ansprechpartner für Datenschutzfragen

1.1. Die Parteien vereinbaren Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen. Auf Seiten des Auftragsverarbeiters ist dies Herr Roland Schroeder (E-Mail: datenschutz@myneva.eu). Der Verantwortliche wird seinen Ansprechpartner dem Auftragsverarbeiter unverzüglich nach Abschluss dieses Vertrages mitteilen.

1.2. In dringenden Fällen darf der Verantwortliche aber auch jedem anderen Beschäftigten des Auftragsverarbeiters z.B. Weisungen erteilen, sofern weder der Ansprechpartner noch sein Stellvertreter für den Verantwortlichen erreichbar waren.

1.3. Ein Wechsel in der Person der Ansprechpartner bzw. deren dauerhafte Verhinderung ist von den Parteien möglichst frühzeitig schriftlich, unter Benennung der Kontaktdaten der neuen Ansprechpartner, mitzuteilen. Bis zum Zugang einer solchen Mitteilung gelten die benannten Ansprechpartner weiter als weisungs- bzw. empfangsberechtigt für alle Datenschutzfragen.

2. Gegenstand der Verarbeitung (Art. 28 Abs. 3 S. 1 DSGVO)

Der Auftragsverarbeiter verarbeitet personenbezogene Daten im Auftrag des Verantwortlichen zur Erfüllung seiner vertraglichen Pflichten gegenüber dem Verantwortlichen.

☒ Der Gegenstand der Verarbeitung ergibt sich aus dem Hauptvertrag.

☐ Der Gegenstand der Verarbeitung ergibt sich aus **Annex 1**.

☐ Gegenstand der Verarbeitung ist:

3. Dauer der Verarbeitung (Art. 28 Abs. 3 S. 1 DSGVO)

Die Dauer des Vertrags ergibt sich aus dem Hauptvertrag. Eine Beendigung des Hauptvertrags bewirkt automatisch eine Beendigung des Vertrags. Der Verantwortliche kann den Hauptvertrag jederzeit außerordentlich kündigen, wenn der Auftragsverarbeiter gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrags verstößt, insbesondere wenn der Auftragsverarbeiter eine Weisung des Verantwortlichen nicht ausführt.

4. Art und Umfang der Verarbeitung (Art. 28 Abs. 3 S. 1 DSGVO)

☒ Art und Umfang der Verarbeitung ergibt sich aus dem Hauptvertrag.

☐ Art und Umfang der Verarbeitung ergeben sich aus **Annex 1**.

☐ Art und Umfang der Verarbeitung ist:

5. Zweck der Verarbeitung (Art. 28 Abs. 3 S. 1 DSGVO)

☒ Der Zweck der Verarbeitung ergibt sich aus dem Hauptvertrag.

☐ Der Zweck der Verarbeitung ergibt sich aus **Annex 1**.

☐ Zweck der Verarbeitung ist:

6. Art der personenbezogenen Daten (Art. 28 Abs. 3 S. 1 DSGVO)

☒ Die Arten der personenbezogenen Daten ergeben sich aus dem Hauptvertrag.

☐ Die Arten der personenbezogenen Daten ergeben sich aus **Annex 1**.

☐ Die Verarbeitung betrifft folgende Arten personenbezogener Daten:

7. Kategorien betroffener Personen (Art. 28 Abs. 3 S. 1 DSGVO)

☒ Die Kategorien betroffener Personen ergeben sich aus dem Hauptvertrag.

☐ Die Kategorien betroffener Personen ergeben sich aus **Annex 1**.

☐ Die Verarbeitung betrifft folgende Kategorien von Personen:

8. Rechte und Pflichten des Verantwortlichen (Art. 28 Abs. 3 S. 1 DSGVO)

Die Rechte und Pflichten des Verantwortlichen ergeben sich aus dem Hauptvertrag und diesem Vertrag. Im Falle einer Inanspruchnahme des Auftragsverarbeiters durch eine betroffene Person nach Art. 82 DSGVO unterstützt der Verantwortliche den Auftragsverarbeiter in einem angemessenen Umfang.

9. Verarbeitung personenbezogener Daten nur auf dokumentierte Weisung (Art. 28 Abs. 3 S. 2 lit. a DSGVO)

9.1. Der Auftragsverarbeiter verarbeitet personenbezogene Daten des Verantwortlichen nur nach Maßgabe des Hauptvertrages sowie nach den in diesem Vertrag enthaltenen Bestimmungen und auf dokumentierte Weisung des Verantwortlichen. Das gilt insbesondere für die Übermittlung personenbezogener Daten des Verantwortlichen an einen Empfänger in einem Drittland oder an eine internationale Organisation. Zur Dokumentation der Weisungen führt der Auftragsverarbeiter ein Verzeichnis, welches dem Verantwortlichen auf Aufforderung vorzulegen ist.

9.2. Weisungen des Verantwortlichen, die über die bisherigen (Haupt-)Vertragsbestimmungen hinausgehen oder diese modifizieren, sollen grundsätzlich in Schrift- oder Textform erfolgen. Soweit erforderlich, kann der Verantwortliche Weisungen auch mündlich oder telefonisch erteilen. Mündlich und telefonisch erteilte Weisungen bedürften jedoch einer unverzüglichen Bestätigung durch den in Ziff. 1 dieses Vertrags genannten Weisungsberechtigten des Verantwortlichen in Schrift- oder Textform.

9.3. Soweit Weisungen aus Sicht des Auftragsverarbeiters unklar oder missverständlich sein sollten, hat er den Verantwortlichen unverzüglich schriftlich darüber zu informieren und eine Klarstellung einzuholen. Der Auftragsverarbeiter ist nach rechtzeitiger vorheriger Ankündigung gegenüber dem Verantwortlichen berechtigt, die Ausführung der Weisung bis zu einer Bestätigung oder Änderung der Weisung durch den Verantwortlichen auszusetzen.

9.4. Der Auftragsverarbeiter darf personenbezogene Daten des Verantwortlichen auch verarbeiten, wenn er hierzu durch das Recht der Europäischen Union oder eines Mitgliedstaats verpflichtet ist (Art. 28 Abs. 3 S. 2 lit. a DSGVO). In diesem Fall teilt er dem Verantwortlichen diese rechtlichen Anforderungen mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

10. Verpflichtung eingeschalteter Personen (Art. 28 Abs. 3 S. 2 lit. b DSGVO)

Der Auftragsverarbeiter verpflichtet zur Verarbeitung der personenbezogenen Daten eingesetzte oder befugte Personen vorab zur Vertraulichkeit und Wahrung des Datengeheimnisses oder stellt sicher, dass sie einer angemessenen gesetzlichen Verschwiegenheitspflicht in Bezug auf die personenbezogenen Daten unterliegen. Der Auftragsverarbeiter stellt zudem sicher, dass die vorgenannten Verpflichtungen auch nach Beendigung dieses Vertrags fortbestehen.

11. Technische und organisatorische Maßnahmen (Art. 28 Abs. 3 S. 2 lit. c DSGVO)

11.1. Der Auftragsverarbeiter gestaltet seine innerbetriebliche Organisation so, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er trifft technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Verantwortlichen, die den datenschutzrechtlichen Anforderungen genügen. Diese ergeben sich aus Art. 32 DSGVO. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen

Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DSGVO zu berücksichtigen. Die konkret getroffenen Maßnahmen sind in **Annex 2** dokumentiert.

11.2. Der Auftragsverarbeiter gewährleistet, seinen Pflichten nach Art. 32 Abs. 1 lit. d) DSGVO nachzukommen und ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen.

11.3. Technische und organisatorische Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Während der Dauer dieser Verarbeitung sind die technischen und organisatorischen Maßnahmen durch den Auftragsverarbeiter fortlaufend an die Anforderungen dieses Vertrags anzupassen und weiterzuentwickeln. Das hier und in **Annex 2** vereinbarte Schutzniveau darf dabei nicht unterschritten werden.

12. Einschaltung von Unterauftragsverarbeitern (Art. 28 Abs. 3 S. 2 lit. d DSGVO)

12.1. Der Verantwortliche ist damit einverstanden, dass der Auftragsverarbeiter für die Verarbeitung personenbezogener Daten des Verantwortlichen die in **Annex 3** aufgezählten Unterauftragsverarbeiter einsetzt.

12.2. Der Verantwortliche gestattet die Beauftragung weiterer Unterauftragsverarbeiter ohne vorherige gesonderte Genehmigung. Der Auftragsverarbeiter informiert den Verantwortlichen vorab über jede beabsichtigte Beauftragung weiterer Unterauftragsverarbeiter oder die Änderung bestehender Beauftragungen. Der Verantwortliche hat gegen die Beauftragung neuer Unterauftragsverarbeiter oder die Änderung bestehender Beauftragungen ein Recht zum Einspruch, welches er innerhalb von zwei (2) Wochen nach Erhalt der Information wahrnehmen kann. Legt der Verantwortliche innerhalb der vorgenannten Frist keinen Einspruch ein oder ist der Einspruch nicht datenschutzrechtlich begründet, gilt die Genehmigung zur Einschaltung des Unterauftragsverarbeiters als erteilt. Im Falle eines Einspruchs, stimmen sich der Verantwortliche und der Auftragsverarbeiter unverzüglich über das weitere Vorgehen ab.

12.3. Nimmt der Auftragsverarbeiter die Dienste eines in **Annex 3** genannten oder eines weiteren Unterauftragsverarbeiters für die Verarbeitung personenbezogener Daten des Verantwortlichen in Anspruch, so erlegt er dem Unterauftragsverarbeiter vorab vertraglich oder durch ein anderes anwendbares Rechtsinstrument nach dem Recht der Europäischen Union oder des betreffenden Mitgliedstaats dieselben Datenschutzpflichten auf, die zwischen ihm und dem Verantwortlichen in diesem Vertrag oder durch ein anderes anwendbares Rechtsinstrument des Rechts der Europäischen Union festgelegt sind. Er stellt dabei insbesondere sicher, dass dem Verantwortlichen eigene Kontrollrechte eingeräumt werden und der Unterauftragsverarbeiter hinreichende Garantien bietet, dass geeignete technische und organisatorische Maßnahmen getroffen sind und so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen des Datenschutzrechts und dieses Vertrags erfolgt.

13. Ort der Verarbeitung

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen schriftlichen Zustimmung des Verantwortlichen und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

14. Unterstützung des Verantwortlichen bei der Erfüllung datenschutzrechtlicher Pflichten (Art. 28 Abs. 3 S. 2 lit. e und f DSGVO)

14.1. Der Auftragsverarbeiter unterstützt den Verantwortlichen nach seinen Möglichkeiten bei der Beantwortung von Anfragen und Ansprüchen betroffener Personen gemäß Kapitel III der DSGVO. Der Auftragsverarbeiter beantwortet Auskunftsanfragen und andere Begehren von betroffenen Personen nicht selbst, sondern verweist die betroffenen Personen insoweit an den Verantwortlichen.

14.2. Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Einhaltung der in Art. 32 bis 36 DSGVO genannten Pflichten, z.B. bei der Sicherheit der Verarbeitung, bei der Meldung von Datenschutzverletzungen an die Aufsichtsbehörden, bei der Benachrichtigung von betroffenen Personen über Datenschutzverletzungen, bei den Pflichten zur Datenschutz-Folgenabschätzung und bei den Abstimmungen mit der Datenschutzaufsichtsbehörde.

15. Löschung und Rückgabe von Daten nach Abschluss der Verarbeitung (Art. 28 Abs. 3 S. 2 lit. g DSGVO)

15.1. Nach Wahl des Verantwortlichen hat der Auftragsverarbeiter sämtliche Daten des Verantwortlichen nach Beendigung der vertragsgegenständlichen Leistungserbringung (insbesondere bei Kündigung oder sonstiger Beendigung des Hauptvertrages) - oder früher nach Aufforderung durch den Verantwortlichen - zu löschen und von dem Verantwortlichen ggf. erhaltene Datenträger und Unterlagen an diesen zurückzugeben.

15.2. Über eine Löschung bzw. Vernichtung von Daten hat der Auftragsverarbeiter ein Protokoll zu erstellen, das dem Verantwortlichen auf Verlangen vorzulegen ist.

15.3. Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung oder gesetzlichen Aufbewahrungsfristen dienen, sind durch den Auftragsverarbeiter entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren.

16. Datenschutzrechtliche Pflichten des Auftragsverarbeiters, Nachweis und Kontrollrechte (Art. 28 Abs. 3 S. 2 lit. h DSGVO)

16.1. Der Verantwortliche kann sich vor der Aufnahme der Datenverarbeitung und sodann regelmäßig von den getroffenen technischen und organisatorischen Maßnahmen des Auftragsverarbeiters überzeugen. Hierfür kann er insbesondere Auskünfte des Auftragsverarbeiters einholen, sich vorhandene Testate eines Sachverständigen vorlegen lassen und zur Verarbeitung seiner Daten eingesetzte Datenverarbeitungsanlagen prüfen oder durch beauftragte Dritte prüfen lassen.

16.2. Der Auftragsverarbeiter kontrolliert regelmäßig die getroffenen technischen und organisatorischen Maßnahmen und bestellt einen Datenschutzbeauftragten, soweit er gesetzlich dazu verpflichtet ist. Die Kontaktdaten des Datenschutzbeauftragten sind dem Verantwortlichen bei Vertragsschluss (siehe Ziff. 1.1) und sodann unverzüglich bei jeder Änderung mitzuteilen.

16.3. Der Auftragsverarbeiter führt das Verzeichnis von Verarbeitungstätigkeiten gemäß Art. 30 DSGVO und stellt dies dem Verantwortlichen auf Anforderung zur Verfügung.

16.4. Der Auftragsverarbeiter stellt dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung seiner vertraglichen und gesetzlichen Pflichten als

Auftragsverarbeiter zur Verfügung. Er gestattet und ermöglicht dem Verantwortlichen und von ihm beauftragten Prüfern entsprechende Überprüfungen – einschließlich Inspektionen – im Rahmen der üblichen Geschäftszeiten des Auftragsverarbeiters (mit Ausnahme der gesetzlichen Feiertage in Deutschland: montags bis freitags zwischen 08:00 und 17:00 Uhr) und trägt in zweckmäßigem Maß dazu bei. Sollte der von dem Verantwortlichen beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Auftragsverarbeiter stehen, hat der Auftragsverarbeiter ein Einspruchsrecht.

16.5. Beauftragt der Verantwortliche einen Dritten mit der Durchführung der Inspektion, hat der Verantwortliche den Dritten auf Verschwiegenheit und Geheimhaltung zu verpflichten, es sei denn, dass der Dritte einer beruflichen Verschwiegenheitsverpflichtung unterliegt. Auf Verlangen des Auftragsverarbeiters hat der Verantwortliche diesem die Verpflichtungsvereinbarung mit dem Dritten unverzüglich vorzulegen.

16.6. Sofern eine Inspektion erforderlich sein sollte, hat der Verantwortliche den Auftragsverarbeiter rechtzeitig (in der Regel mindestens zwei (2) Wochen vorher) über alle mit der Durchführung der Inspektion zusammenhängenden Umstände zu informieren.

16.7. Der Auftragsverarbeiter erhält von dem Verantwortlichen für eigene Mitwirkungsleistungen im Rahmen einer Prüfung eine Aufwandsentschädigung nach Maßgabe der jeweils gültigen Preisliste des Auftragsverarbeiters. Zeigt sich durch die Kontrolle nachweislich ein Verstoß des Auftragsverarbeiters gegen Bestimmungen dieses Vertrags, entfällt der Anspruch auf die Aufwandsentschädigung.

17. Information über datenschutzwidrige Weisungen (Art. 28 Abs. 3 S. 3 DSGVO)

Ist der Auftragsverarbeiter der Auffassung, dass eine Weisung des Verantwortlichen gegen den Hauptvertrag und/oder diesen Vertrag und/oder geltendes Datenschutzrecht verstößt, hat er den Verantwortlichen unverzüglich darauf hinzuweisen.

18. Berichtigung, Löschung und Sperrung von Daten

18.1. Der Auftragsverarbeiter berichtigt, löscht oder sperrt personenbezogene Daten des Verantwortlichen, wenn der Verantwortliche dies anweist. Die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien übernimmt der Auftragsverarbeiter auf Grund einer Einzelbeauftragung durch den Verantwortlichen, sofern dies nicht im Vertrag oder Hauptvertrag bereits vereinbart ist. In besonderen, vom Verantwortlichen zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe.

18.2. Für die vorgenannten Leistungen erhält der Auftragsverarbeiter eine gesonderte Vergütung nach Maßgabe der jeweils aktuell gültigen Preisliste des Auftragsverarbeiters.

19. Mitteilung von Verstößen (Art. 33 Abs. 2 DSGVO)

Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich bei der Möglichkeit einer unrechtmäßigen Kenntniserlangung der personenbezogenen Daten durch Dritte oder bei sonstigen schwerwiegenden Verstößen des Auftragsverarbeiters oder der bei ihm im Rahmen des Auftrags beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten des Verantwortlichen oder in diesem Vertrag getroffene Festlegungen. Er trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der Betroffenen und spricht sich hierzu unverzüglich mit dem Verantwortlichen ab. Die vorstehende Mitteilungspflicht greift stets dann, wenn die Möglichkeit nicht ausgeschlossen werden kann, dass der Verstoß zu einer Meldepflicht des Verantwortlichen nach Art. 33 Abs. 2 DSGVO oder einer entsprechenden Regelung führt. Der Auftragsverarbeiter meldet insbesondere jegliche Verletzung des Schutzes personenbezogener Daten im Sinne von Art. 4 Nr. 12 DSGVO unverzüglich dem Verantwortlichen gemäß Art. 33 Abs. 2 DSGVO.

20. Haftung

20.1. Sofern in diesem Vertrag nicht abweichend geregelt, gelten die gesetzlichen Bestimmungen zur Haftung.

20.2. Sofern Dritte Ansprüche gegen den Auftragsverarbeiter wegen der Verletzung datenschutzrechtlicher Bestimmungen geltend machen, die auf einen Verstoß des Verantwortlichen gegen datenschutzrechtliche Bestimmungen oder gegen die Bestimmungen des Vertrags basieren, übernimmt der Verantwortliche auf eigene Kosten die Verteidigung des Rechtsstreits und stellt den Auftragsverarbeiter von sämtlichen Ansprüchen sowie den angemessenen Kosten der Rechtsverfolgung auf erstes Anfordern frei. Der Auftragsverarbeiter wird den Verantwortlichen unverzüglich über die entsprechenden Anspruchsschreiben Dritter informieren und – soweit möglich – dem Verantwortlichen die Befugnisse einräumen, sich selbstständig gegen die Ansprüche zu verteidigen.

21. Kosten

21.1. Sofern nicht anderweitig in diesem Vertrag geregelt, sind alle Leistungen des Auftragsverarbeiters nach diesem Vertrag mit der Vergütung nach Maßgabe des Hauptvertrags abgegolten.

21.2. Sofern Einzelweisungen über die bisherigen Vertragsbestimmungen hinausgehen und einen zusätzlichen Aufwand für den Auftragsverarbeiter erfordern, bedürfen diese einer vorherigen Zustimmung des Auftragsverarbeiters und sind gesondert nach Maßgabe der jeweils aktuell gültigen Preisliste des Auftragsverarbeiters zu vergüten.

22. Standardvertragsklauseln für Verträge zur Auftragsverarbeitung

Sollte die EU-Kommission oder die zuständige Aufsichtsbehörde gemäß Art. 28 Abs. 7 und 8 DSGVO Standardvertragsklauseln für Verträge zur Auftragsverarbeitung entwickeln, werden sich die Parteien auf eine mögliche Anpassung oder Ersetzung des Vertrags verständigen.

23. Weitere Unterstützungs- und Informationspflichten des Auftragsverarbeiters

23.1. Im Falle einer Inanspruchnahme des Verantwortlichen durch eine betroffene Person nach Art. 82 DSGVO unterstützt der Auftragsverarbeiter den Verantwortlichen in einem angemessenen Umfang.

23.2. Sollten die Daten des Verantwortlichen beim Auftragsverarbeiter durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren, durch Verlangen nach Offenlegung im Zusammenhang mit gerichtlichen Verfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragsverarbeiter den Verantwortlichen unverzüglich darüber zu informieren. Der Auftragsverarbeiter wird alle in diesem Zusammenhang verantwortlichen Stellen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Verantwortlichen liegen.

23.3. Für die vorgenannten Informations- und Unterstützungsleistungen erhält der Auftragsverarbeiter eine gesonderte Vergütung nach Maßgabe der jeweils aktuell gültigen Preisliste des Auftragsverarbeiters.

24. Anwendbares Recht / Gerichtsstand

24.1. Auf diesen Vertrag findet das deutsche Recht Anwendung.

24.2. Ausschließlicher Gerichtsstand für alle Streitigkeiten aus oder im Zusammenhang mit diesem Vertrag ist der Sitz des Auftragsverarbeiters. Der Auftragsverarbeiter ist berechtigt, den Verantwortlichen auch an dessen Sitz zu verklagen.

25. Schlussbestimmungen

25.1. Änderungen oder Ergänzungen dieses Vertrags bedürfen der Schriftform. Dies gilt auch für die Änderung und Aufhebung dieser Klausel.

25.2. Soweit in diesem Vertrag keine Sonderregelungen enthalten sind, gelten die Bestimmungen des Hauptvertrags. Im Falle von Widersprüchen zwischen diesem Vertrag und Regelungen aus dem Hauptvertrag gehen die Regelungen aus diesem Vertrag vor.

25.3. Sollten Bestimmungen dieses Vertrags unwirksam sein, berührt dies die Gültigkeit der übrigen Bestimmungen nicht. Die Parteien werden sich bemühen, anstelle der unwirksamen Bestimmungen eine wirksame zu finden, die den wirtschaftlichen Bedeutungsgehalt der unwirksamen Bestimmungen am ehesten nahekommt. Entsprechendes gilt bei einer Lücke in diesem Vertrag.

Annexe:

1. Angaben zur Verarbeitung

2. Technische und Organisatorische Maßnahmen des Auftragsverarbeiters

3. Unterauftragnehmer

Annex 1

Angaben zur Verarbeitung

Gegenstand Art und Umfang der Verarbeitung
Zwecke der Verarbeitung
☐ Durchführung von Beschäftigungsverhältnissen ☐ Erfüllung von vertraglichen Pflichten gegenüber den Betroffenen ☐ Erfüllung rechtlicher Pflichten ☐ Verfolgung berechtigter Interessen ☐ andere:
Art der personenbezogenen Daten
☐ Persönliche Angaben, nämlich insbesondere ☐ Name ☐ Anschrift ☐ Telefonnummer ☐ E-Mail ☐ Alter ☐ Familienstand ☐ Geburtsdatum ☐ Anzahl der Kinder ☐ andere: ☐ Vertragsdaten, nämlich insbesondere Angaben über ☐ Bestellungen ☐ Umsätze ☐ Vertragshistorie ☐ Bewertungen ☐ Abrechnungen ☐ Produktpräferenzen ☐ Vertragslaufzeit ☐ Kosten ☐ Belegnummern ☐ andere: ☐ Beschäftigtendaten, nämlich insbesondere Angaben über ☐ Arbeitszeiten ☐ Qualifikationen ☐ Bewertungen ☐ Personalnummern ☐ Eintrittsdatum ☐ Freistellungen ☐ Abrechnungskreis ☐ Kostenstelle ☐ Abteilung ☐ Zulagen ☐ Pfändungen ☐ Freistellungen ☐ Lohnsteuerklasse ☐ (Kinder)freibeträge ☐ Krankenkasse ☐ Renten- und Sozialversicherung ☐ andere: ☐ Telekommunikations-, Telemediendaten und ähnliche Daten ☐ Verbindungsdaten ☐ Inhaltsdaten ☐ IP-Adressen ☐ Cookie IDs ☐ Standortdaten ☐ andere: ☐ besondere Kategorien personenbezogener Daten, nämlich Angaben über: ☐ Rasse oder ethnische Herkunft ☐ politische Meinung ☐ religiöse oder philosophische Überzeugung ☐ Gewerkschaftszugehörigkeit

☐ Gesundheit ☐ Sexualleben ☐ biometrische Informationen zur eindeutigen Identifikation ☐ Zahlungsdaten, nämlich insbesondere ☐ Bankverbindung ☐ Kreditkartennummer ☐ andere: ☐ Aufnahmen, nämlich insbesondere ☐ Videoaufzeichnungen ☐ Fotos ☐ Tonaufnahmen ☐ andere: ☐ andere:
Kategorien betroffener Personen
☐ Beschäftigte ☐ Mandanten ☐ Dienstleister ☐ andere:

Annex 2

Technische und organisatorische Maßnahmen des Auftragsverarbeiters

Übersicht der zur Datenverarbeitung eingesetzten IT-Systeme	
1.	Eingesetzte Hardware
	☐ folgende selbst betriebene Rechenzentren: ☐ folgende externen Rechenzentren: ☒ folgende externe IT-Infrastruktur (z.B. Cloud-Dienste): AWS Services (siehe Ziff. 15 und Annex 3) ☐ folgende internen Serverräume: ☐ folgende Netzwerkinfrastruktur: ☐ folgende Desktop Clients: ☐ folgende mobilen Clients: ☐ folgende anderen Hardwarekomponenten:
2.	Eingesetzte Software
	safechat

Technische und organisatorische Sicherheitsmaßnahmen

3.	Zutrittskontrolle (Maßnahmen, die verhindern, dass Unbefugte Zutritt zu Gebäuden und Räumen bekommen in denen sich Datenverarbeitungsanlagen befinden)
	Technische Maßnahmen ☐ Perimetersicherung ☐ Zaun ☐ Flutlicht ☐ Bewegungsmelder ☐ Vereinzelungsanlagen ☐ Glasbruchsensoren ☐ biometrische Identifikation ☐ andere: ☐ Schutzgraben ☐ Videoüberwachung ☒ Zutrittskontrollsystem ☐ Alarmanlage ☐ Lichtschranken ☐ Gebäudesicherung ☐ Videoüberwachung ☐ Bewegungsmelder ☒ Sicherheitstüren / -fenster ☒ Zutrittskontrollsystem ☐ Alarmanlage ☐ Glasbruchsensoren ☒ elektronisches Schließsystem ☐ Smartcams ☐ Tür- / Fenstersicherungen (z.B. Gitter) ☐ Vereinzelungsanlagen ☐ manuelles Schließsystem ☐ Lichtschranken ☐ biometrische Identifikation

	☐ RDIF/Bluetooth/NFC-Transponder ☐ andere: ☐ Innenraumsicherung ☐ Videoüberwachung ☐ Bewegungsmelder ☐ Zutrittskontrollsystem ☐ Vereinzelungsanlagen ☐ Alarmanlage ☐ Glasbruchsensoren ☐ Lichtschranken ☐ manuelles Schließsystem ☐ elektronisches Schließsystem ☐ fensterlose Räume ☐ biometrische Identifikation ☐ Absicherung von Gebäudeschächten ☐ Einteilung in Sicherheitszonen/Sperrbereiche ☐ andere: Organisatorische Maßnahmen ☐ Zutrittskonzept ☒ Schlüsselregelung ☒ dokumentierte Schlüsselausgabe ☐ Besucherprozess ☐ Personenkontrollen ☐ Berechtigungsausweise ☐ Sperrbereiche und Sicherheitszonen ☐ Mitarbeiterschulung ☐ Werkschutz / Sicherheitsdienst ☐ offen getragene ID-Karten ☐ Verpflichtung und Kontrolle von Dienstleistern ☐ andere:
4.	Zugangskontrolle (Maßnahmen, die sicherstellen, dass Unbefugten kein Zugang zu Datenverarbeitungssystemen haben)
	Technische Maßnahmen ☒ zentrale Steuerung von Berechtigung (z.B. per Verzeichnisdienst und Identitätsmanagement) ☐ Schnittstellen-Sperren (USB, Firewire etc.) ☒ Benutzeranmeldung mit Kennung und Passwort ☒ Benutzeranmeldung mit biometrischer Authentifizierung ☐ Benutzeranmeldung mit Hardware Kennung (z.B. RFID Token) ☐ passwortgeschützter Bildschirmschoner ☐ Hardwaresicherung (Gehäuseverriegelungen, Kensington-Locks) ☐ Host-basierte Intrusion-Detection-Systeme ☐ Netzwerkbasierte Intrusion-Detection-Systeme ☐ Zugangsprotokollierung ☐ Pseudonymisierung von Daten ☐ mobile-Device-Management mit Remote-Wipe-Funktion ☐ Softwarefirewall ☒ Hardwarefirewall ☐ Firewall mit Deep Packet Inspection ☐ Reverse Proxy ☐ Application Layer Gateway ☒ Verschlüsselung von (mobilen) Endgeräten ☒ Verschlüsselung von Massenspeichern (in mobilen Endgeräten, Desktops und

	Servern) ☐ Entfernen nicht genutzter Applikationen und Services ☐ Deaktivieren des Bootens von externen Medien ☐ keine Administrator-Konten für normale Nutzer ☐ Einrichten einer DMZ ☒ regelmäßiges Einspielen sicherheitsrelevanter Patches, Updates und Service Packs ☐ VPN-Tunnel für Remote-Zugriffe ☐ Segmentierung z.B. mittels VLANs oder Layer-3-Switche ☐ Port-Sperren ☐ Sperrung von Clients bei Inaktivität ☐ andere: Organisatorische Maßnahmen ☐ Berechtigungskonzept ☐ Passwortregelung ☐ Routine zur Passworterneuerung ☐ Passwortrichtlinie (zu Komplexität, Änderung und Geheimhaltung) ☐ restriktive Vergabe von Admin-Rechten auf Clients ☐ Routine zur Kontrolle der Rechtevergabe ☐ Routine zur Warnung bei akuten Bedrohungen ☐ Mitarbeiterschulung ☐ Zentrale Auswahl und Beschaffung von Hard- und Software (Zwecks Kompatibilität, Gewährleistung von Mindeststandards) ☐ IT-Richtlinie (z.B. zur Installation von Fremdsoftware, zum Umgang mit Mails mit unbekanntem Absender) ☐ Richtlinie zum Umgang mit mobilen Endgeräten (zentrale Einrichtung, Ausgabe und Kontrolle; verschlossene Aufbewahrung bei Nichtbenutzung; keine Weitergabe an Dritte/Angehörige etc.) ☐ Patch-und Änderungsmanagement für Software; Sicherstellung der Patchverträglichkeit auf Testsystemen vor dem Produktivbetrieb ☐ Penetrationstests ☐ andere:
5.	Zugriffskontrolle (Maßnahmen, die sicherstellen, dass Unbefugte keinen Zugriff auf personenbezogene Daten haben)
	Technische Maßnahmen ☒ zentrale Steuerung von Berechtigung, z.B. durch Verzeichnisdienst ☒ Zugriffsprotokollierung ☒ Verschlüsselung von Massenspeichern ☐ Verschlüsselung von Datenträgern ☐ Pseudonymisierung von Daten und getrennte Aufbewahrung des Zuordnungsschlüssels ☐ sichere Aufbewahrung von Datenträgern ☐ sichere Löschung von Datenträgern vor Wiederverwendung ☐ ordnungsgemäße Vernichtung von Datenträgern

	☐ Protokollierung der Vernichtung Datenträgern ☒ Vernichtung von Papierdokumenten und -akten (Aktenvernichter, Dienstleister) ☐ andere: Organisatorische Maßnahmen ☒ Passwortregelung ☒ Berechtigungskonzept ☐ Rechteverwaltung durch eine minimale Gruppe von Administratoren ☐ Vier-Augen-Prinzip für kritische Administrationstätigkeiten ☒ Mitarbeiterschulung ☐ restriktive Vergabe von Admin-Rechten auf Clients ☐ Routine zur Warnung bei akuten Bedrohungen ☐ Routine zur Kontrolle der Rechtevergabe ☐ andere:
6.	Weitergabekontrolle (Maßnahmen, die sicherstellen, dass personenbezogene Daten bei der Übertragung oder Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft werden kann, welche Personen oder Stellen personenbezogene Daten erhalten haben)
	Technische Maßnahmen ☒ zentrale Steuerung von Berechtigung ☐ getunnelte Datenfernverbindungen (VPN) ☐ dedizierte Verbindungen zwischen Standorten (z.B. MPLS mit Layer-2-VPN) ☒ E-Mail-Verschlüsselung ☐ Verschlüsselung von E-Mail-Anlagen ☒ Verschlüsselung von VoIP-Telefonie ☐ Verschlüsselung von mobilen Datenträgern ☒ SSL-Verschlüsselung bei Web-Access ☐ Passwortschutz für E-Mail-Anlagen ☐ Pseudonymisierung von Daten ☐ Protokollierung von Datenübermittlungen ☐ Transportsicherung von Datenträgern und Transportbehältern ☐ Sicherung gegen Verkehrsflussanalyse (Traffic Flow Confidentiality) bei Übermittlung von Daten mit hohem Schutzbedarf über öffentliche Netze ☐ Weitergabe von Daten in anonymisierter oder pseudonymisierter Form ☐ sichere Löschung von Datenträgern vor Wiederverwendung ☐ andere: Organisatorische Maßnahmen ☐ Berechtigungskonzept ☐ Dokumentation der Empfänger von Daten und der Zeitspanne der geplanten Überlassung bzw. vereinbarte Löschfristen ☐ Mitarbeiterschulung ☐ sorgfältige Auswahl von Transportpersonal und -fahrzeugen

	☐ Richtlinie zur Aufbewahrung, Löschung und Sperrung personenbezogener Daten ☐ andere:

7.	Eingabekontrolle (Maßnahmen, die sicherstellen, dass geprüft werden kann, wer personenbezogene Daten zu welcher Zeit in Datenverarbeitungsanlagen verarbeitet hat)
	Technische Maßnahmen ☒ zentrale Steuerung von Berechtigung, z.B. durch Verzeichnisdienst ☒ personenscharfe Nutzerkonten ☐ Eingabeprotokollierung ☐ andere: Organisatorische Maßnahmen ☒ Passwortregelung ☒ Berechtigungskonzept ☒ personenscharfe Nutzerprofile ☐ Mitarbeiterschulung ☐ Dokumentation der Verarbeitungsprozesse einschließlich der eingesetzten Software und der damit jeweils verarbeiteten Daten (Verarbeitungsübersicht) ☐ andere:
8.	Auftragskontrolle (Maßnahmen, die sicherstellen, dass personenbezogene Daten nur entsprechend den Weisungen des Verantwortlichen verarbeitet werden)
	Technische Maßnahmen ☒ zentrale Steuerung von Berechtigung, z.B. durch Verzeichnisdienst ☒ Protokollierung von Systemzugriffen ☐ automatisierte Meldungen zum Status der Verarbeitung ☐ andere: Organisatorische Maßnahmen ☒ Auswahl von Auftragnehmern nach definierten Sorgfaltsgesichtspunkten ☒ Kontrolle von Auftragnehmern getroffener Datensicherheitsmaßnahmen ☐ Mitarbeiterschulung ☐ Live-Monitoring von Systemzugriffen ☒ schriftliche Weisungen für Auftragnehmer (ADV-Vertrag) ☐ Dokumentation von Weisungen ☐ Vereinbarung von Vertragsstrafen bei Verstößen ☐ Auftragnehmer-Auditierung ☐ andere:
9.	Verfügbarkeitskontrolle (Maßnahmen, die sicherstellen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt und für den Verantwortlichen stets verfügbar sind)
	Technische Maßnahmen ☐ Unterbrechungsfreie Stromversorgung (USV) ☐ Überspannungsschutz ☐ Notstromversorgung ☐ Brandmeldeanlage mit direkter Aufschaltung zur Feuerwehr

	☐ Spiegelung von Systemen ☐ Mitarbeiterschulung ☐ Klimatisierte Serverräume ☐ Überwachung von Temperatur und Feuchtigkeit in Serverräumen ☐ Datensicherung in unterschiedlichen Brandabschnitten ☐ Dateisysteme mit Integritätsprüfung und Fehlerkorrektur (z.B. ZFS, Btrfs, ReFS) ☐ externe Datensicherung ☐ Monitoring relevanter Datenquellen (Systemstatus, fehlgeschlagene Authentisierungsversuche) ☐ Klimaanlage mit redundanten Komponenten (Pumpen, Kühlkreislauf, Wärmetauscher) ☐ Überwachung der Klimaanlage (z.B. Fühler im Kühlmittelstrom) ☐ bauliche Abschirmung gegen Wassereinbruch ☐ baulicher Brandschutz ☐ Brandfrüherkennung ☐ Brandvermeidung durch Sauerstoffreduzierung ☐ Löschtechnik (z.B. Handlöscher, Löschsysteme mit Wasser, Löschgas oder Inertgas; Stufenkonzept von Rack-, Mehrbereichs- bis zur Rumlöschung) ☐ redundante Systemkomponenten (z.B. RAID, Hot Spare, doppelte Netzteile, Verkabelung) ☐ redundante Systeme in unterschiedlichen Brandabschnitten ☐ redundante Netzanbindung ☐ andere: Organisatorische Maßnahmen ☒ Backup-Konzept ☒ Recovery-Konzept ☐ Notfallhandbuch ☒ Recovery-Tests ☐ Auswahl von Dienstleistern mit zertifiziertem Notfallmanagement (z.B. BS 25999, BSI-Standard 100-4) ☐ Routine zur Warnung bei akuten Bedrohungen ☐ Mitarbeiterschulung ☐ andere:
10.	Trennungskontrolle (Maßnahmen, die sicherstellen, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden)
	Technische Maßnahmen ☒ physikalisch getrennte Speicherung ☒ logisch getrennte Speicherung ☒ Trennung von Produktiv- und Testsystem ☐ Trennung von Netzwerksegmenten ☒ Einsatz zertifizierter Hypervisoren bei virtualisierter Umgebung ☐ Versehen der Datensätze mit Zweckattributen ☒ einheitliche Verschlüsselung von Daten, die zu einem Zweck verarbeitet werden ☐ andere:

	Organisatorische Maßnahmen ☐ Mitarbeiterschulung ☐ Kennzeichnen von Datensätzen mit Zweckattributen (Tagging) ☒ Rechtevergabe nach Need-To-Know-Prinzip (Least Privilege Model) ☐ Richtlinien für Softwaretests ☐ andere:
11.	Pseudonymisierung und Verschlüsselung (bitte angeben soweit genutzt)
	☐ Pseudonymisierung, nämlich: …….. ☐ Verschlüsselung von ruhenden Daten, nämlich: …….. ☒ Verschlüsselung von Daten beim Transport über interne Netze, nämlich: SSL …… ☒ Verschlüsselung von Daten beim Transport über öffentliche Netze, nämlich: SSL ……
12.	Belastbarkeit der Systeme und Dienste (Maßnahmen, die sicherstellen, dass die eingesetzten Systeme und Dienste fehlertolerant sind und bei Störungen und Teilausfällen die wesentlichen Funktionen aufrechterhalten)
	Technische Maßnahmen ☐ Server-Cluster für Datenbanken, Webservices und sonstige Dienste ☒ Load-Balancing ☐ Redundanz von Systemen und Komponenten ☐ Vorbereitung auf netzbasierte Angriffe (DDoS-Mitigation) ☐ andere: Organisatorische Maßnahmen ☒ Monitoring der Systemverfügbarkeit ☐ Vereinbarung angemessener Service-Level, Reaktions- und Wiederherstellungszeiten mit Dienstleistern ☒ Überwachung von Service-Leveln ☐ andere:
13.	Wiederherstellung der Verfügbarkeit von Daten nach Störfällen in angemessener Zeit
	Technische Maßnahmen ☒ Backup-Verfahren ☐ Spiegelung produktiver Systeme (mit Hot Standby) ☐ andere: Organisatorische Maßnahmen ☐ Festlegung angemessener Recovery Point Objektives

	☐ Festlegung angemessener Recovery Time Objektives ☐ 24/7 -erreichbares, handlungsfähiges Team für Sicherheitsvorfälle ☐ Verpflichtung von Dienstleistern auf sofortige Benachrichtigung bei Vorfällen ☐ Planung für Exit / Remigration / Second Level Outsourcing (z.B. Einsatz portabler virtueller Maschinen und standardisierter / dokumentierter APIs) ☐ andere:
14.	Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit technisch-organisatorischer Maßnahmen
	Technische Maßnahmen ☐ Protokollierung von sicherheitsrelevanten Vorgängen ☐ Einsatz von Vulnerability-Scannern ☐ Penetrationstests ☐ Simulation von Angriffen, Störereignissen und Datenverlust ☐ andere: Organisatorische Maßnahmen ☒ Routine zur Überprüfung implementierter Sicherheitsmaßnahmen ☐ Auswertung von Sicherheitsvorfällen ☐ Auswertung von Protokollen sicherheitsrelevanter Vorgänge ☐ Sicherheitsanalysen (Penetrationstests) ☐ regelmäßige interne Audits ☐ regelmäßige externe Audits ☐ regelmäßige Brandschutz- und Notfallübungen ☐ andere:
15.	Informationen zu den technischen und organisatorischen Maßnahmen von AWS
	https://d1.awsstatic.com/legal/aws-gdpr/AWS_GDPR_DPA.pdf https://aws.amazon.com/de/about-aws/global-infrastructure/ https://d1.awsstatic.com/whitepapers/compliance/GDPR_Compliance_on_AWS.pdf

Annex 3

Unterauftragsverarbeiter

Unterauftragsverarbeiter	Kontaktdaten	Gegenstand der Verarbeitung
Amazon Web Services Inc.	Amazon Web Services, EMEA SARL 38 avenue John F. Kennedy, L-1855, Luxembourg Fax: +352 27890057	Rechenzentrum in Frankfurt am Main