Vertrag über die Auftragsverarbeitung personenbezogener Daten i.S.d. Art. 28 DSGVO

1 Einleitung, Geltungsbereich, Definitionen

Dieser Vertrag regelt die Rechte und Pflichten von nooa und dem Kunden (im Folgenden „Parteien“ genannt) im Rahmen einer Verarbeitung von personenbezogenen Daten im Auftrag.
Dieser Vertrag findet auf alle Tätigkeiten Anwendung, bei denen Mitarbeiter von nooa oder durch ihn beauftragte Unterauftragnehmer (Subunternehmer) personenbezogene Daten des Kunden in dessen Auftrag verarbeiten.
In diesem Vertrag verwendete Begriffe sind entsprechend ihrer Definition in der EU Datenschutz-Grundverordnung zu verstehen. In diesem Sinne ist der Kunde als Auftraggeber der „Verantwortliche“, nooa als Auftragnehmer der „Auftragsverarbeiter“. Soweit Erklärungen im Folgenden „schriftlich“ zu erfolgen haben, ist die Schriftform nach § 126 BGB gemeint. Im Übrigen können Erklärungen auch in anderer Form erfolgen, soweit eine angemessene Nachweisbarkeit gewährleistet ist.

Die Verarbeitung beruht auf dem zwischen den Parteien bestehenden Vertrag „**Abonnementvertrag**“ (im Folgenden „Hauptvertrag“).

2 Gegenstand und Dauer der Verarbeitung

Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte des Verantwortlichen ergeben sich aus Anlage 1 dieses Vertrages und der Leistungsbeschreibung des Hauptvertrages.

3 Pflichten von nooa

(1) nooa verarbeitet personenbezogene Daten ausschließlich wie vertraglich vereinbart oder wie vom Kunden angewiesen, es sei denn, nooa ist gesetzlich zu einer bestimmten Verarbeitung verpflichtet. Sofern solche Verpflichtungen bestehen, teilt nooa diese dem Kunden vor der Verarbeitung mit, es sei denn, die Mitteilung ist ihm gesetzlich verboten. nooa verwendet darüber hinaus die zur Verarbeitung überlassenen Daten für keine anderen, insbesondere nicht für eigene Zwecke.
(2) nooa bestätigt, dass ihm die einschlägigen, allgemeinen datenschutzrechtlichen Vorschriften bekannt sind und beachtet die Grundsätze ordnungsgemäßer Datenverarbeitung.
(3) nooa verpflichtet sich, bei der Verarbeitung die Vertraulichkeit streng zu wahren.
(4) Personen, die Kenntnis von den im Auftrag verarbeiteten Daten erhalten können, haben sich schriftlich zur Vertraulichkeit zu verpflichten, soweit sie nicht bereits gesetzlich einer einschlägigen Geheimhaltungspflicht unterliegen.
(5) nooa sichert zu, dass die bei ihm zur Verarbeitung eingesetzten Personen vor Beginn der Verarbeitung mit den relevanten Bestimmungen des Datenschutzes und dieses Vertrags vertraut gemacht wurden. Entsprechende Schulungs- und Sensibilisierungsmaßnahmen sind angemessen regelmäßig zu wiederholen. nooa trägt dafür Sorge, dass zur Auftragsverarbeitung eingesetzte Personen hinsichtlich der Erfüllung der Datenschutzanforderungen laufend angemessen angeleitet und überwacht werden.
(6) Im Zusammenhang mit der beauftragten Verarbeitung unterstützt nooa den Kunden soweit erforderlich bei der Erfüllung seiner datenschutzrechtlichen Pflichten, insbesondere bei Erstellung und Fortschreibung des Verzeichnisses der Verarbeitungstätigkeiten, bei Durchführung der Datenschutzfolgeabschätzung und einer notwendigen Konsultation der Aufsichtsbehörde. Die erforderlichen Angaben und Dokumentationen sind vorzuhalten und dem Kunden auf Anforderung unverzüglich zuzuleiten.
(7) Wird der Kunde durch Aufsichtsbehörden oder andere Stellen einer Kontrolle unterzogen oder machen betroffene Personen ihm gegenüber Rechte geltend, verpflichtet sich nooa den Kunden im erforderlichen Umfang zu unterstützen, soweit die Verarbeitung im Auftrag betroffen ist.
(8) Auskünfte an Dritte oder den Betroffenen darf nooa nur nach vorheriger Zustimmung durch den Kunden erteilen. Direkt an ihn gerichtete Anfragen wird er unverzüglich an den Kunden weiterleiten.
(9) Soweit gesetzlich verpflichtet, bestellt nooa eine fachkundige und zuverlässige Person als Beauftragten für den Datenschutz. Es ist sicherzustellen, dass für den Beauftragten keine Interessenskonflikte bestehen. In Zweifelsfällen kann sich der Kunde direkt an den Datenschutzbeauftragten wenden. nooa teilt dem Kunden unverzüglich die Kontaktdaten des Datenschutzbeauftragten mit oder

begründet, weshalb kein Beauftragter bestellt wurde. Änderungen in der Person oder den innerbetrieblichen Aufgaben des Beauftragten teilt nooa dem Kunden unverzüglich mit.

(10) Die Auftragsverarbeitung erfolgt ausschließlich innerhalb der EU oder des EWR.

4 Sicherheit der Verarbeitung

(1) Die in Anlage 2 beschriebenen Datensicherheitsmaßnahmen werden als verbindlich festgelegt. Sie definieren das seitens nooa geschuldete Minimum. Die Beschreibung der Maßnahmen muss so detailliert erfolgen, dass für einen sachkundigen Dritten allein aufgrund der Beschreibung jederzeit zweifelsfrei erkennbar ist, was das geschuldete Minimum sein soll. Ein Verweis auf Informationen, die dieser Vereinbarung oder ihren Anlagen nicht unmittelbar entnommen werden können, ist nicht zulässig.

(2) Die Datensicherheitsmaßnahmen können der technischen und organisatorischen Weiterentwicklung entsprechend angepasst werden, solange das hier vereinbarte Niveau nicht unterschritten wird. Zur Aufrechterhaltung der Informationssicherheit erforderliche Änderungen hat nooa unverzüglich umzusetzen. Änderungen sind dem Kunden unverzüglich mitzuteilen. Wesentliche Änderungen sind zwischen den Parteien zu vereinbaren.

(3) Soweit die getroffenen Sicherheitsmaßnahmen den Anforderungen des Kunden nicht oder nicht mehr genügen, benachrichtigt nooa den Kunden unverzüglich.

(4) nooa sichert zu, dass die im Auftrag verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.

(5) Kopien oder Duplikate werden ohne Wissen des Kunden nicht erstellt. Ausgenommen sind technisch notwendige, temporäre Vervielfältigungen, soweit eine Beeinträchtigung des hier vereinbarten Datenschutzniveaus ausgeschlossen ist.

(6) nooa führt den regelmäßigen Nachweis der Erfüllung seiner Pflichten, insbesondere der vollständigen Umsetzung der vereinbarten technischen und organisatorischen Maßnahmen sowie ihrer Wirksamkeit. Der Nachweis ist dem Kunden spätestens alle 12 Monate unaufgefordert und sonst jederzeit auf Anforderung zu überlassen. Der Nachweis kann durch genehmigte Verhaltensregeln oder ein genehmigtes Zertifizierungsverfahren erbracht werden. Nachweise sind mindestens bis zum Ablauf drei Kalenderjahren nach Beendigung der Auftragsverarbeitung aufzubewahren und dem Kunden jederzeit auf Verlangen vorzulegen.

5 Regelungen zur Berichtigung, Löschung und Sperrung von Daten

(1) Im Rahmen des Auftrags verarbeitete Daten wird nooa nur entsprechend der getroffenen vertraglichen Vereinbarung oder nach Weisung des Kunden berichtigen, löschen oder sperren.

(2) Den entsprechenden Weisungen des Kunden wird nooa jederzeit und auch über die Beendigung dieses Vertrages hinaus Folge leisten.

6 Unterauftragsverhältnisse

(1) Die vertraglich vereinbarten Leistungen bzw. die nachfolgend beschriebenen Teilleistungen werden unter Einschaltung der in Anlage 3 genannten Subunternehmer durchgeführt. nooa ist im Rahmen ihrer vertraglichen Verpflichtungen zur Begründung von weiteren Unterauftragsverhältnissen mit Subunternehmern („Subunternehmerverhältnis“) befugt. nooa setzt den Auftraggeber hiervon unverzüglich in Kenntnis. nooa ist verpflichtet, Subunternehmer sorgfältig nach deren Eignung und Zuverlässigkeit auszuwählen. nooa hat bei der Einschaltung von Subunternehmern diese entsprechend den Regelungen dieser Vereinbarung zu verpflichten und dabei sicherzustellen, dass der Kunde seine Rechte aus dieser Vereinbarung (insbesondere seine Prüf- und Kontrollrechte) auch direkt gegenüber den Subunternehmern wahrnehmen kann. Sofern eine Einbeziehung von Subunternehmern in einem Drittland erfolgen soll, hat nooa sicherzustellen, dass beim jeweiligen Subunternehmer ein angemessenes Datenschutzniveau gewährleistet ist (z. B. durch Abschluss einer Vereinbarung auf Basis der EU-Standarddatenschutzklauseln). nooa wird dem Auftraggeber auf Verlangen den Abschluss der vorgenannten Vereinbarungen mit seinen Subunternehmern nachweisen.

(2) Ein Subunternehmerverhältnis im Sinne dieser Bestimmungen liegt nicht vor, wenn nooa Dritte mit Dienstleistungen beauftragt, die als reine Nebenleistungen anzusehen sind. Dazu gehören z. B. Post-, Transport- und Versandleistungen, Reinigungsleistungen, Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die nooa für den Auftraggeber erbringt und

Bewachungsdienste. Wartungs- und Prüfleistungen stellen zustimmungspflichtige Subunternehmerverhältnisse dar, soweit diese für IT-Systeme erbracht werden, die auch im Zusammenhang mit der Erbringung von Leistungen für den Auftraggeber genutzt werden.

7 Rechte und Pflichten des Kunden

(1) Für die Beurteilung der Zulässigkeit der beauftragten Verarbeitung sowie für die Wahrung der Rechte von Betroffenen ist allein der Kunde verantwortlich.
(2) nooa darf Daten nur im Rahmen des Hauptvertrags und gemäß den Weisungen des Auftraggebers erheben, verarbeiten oder nutzen; dies gilt insbesondere in Bezug auf die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation.
(3) Wird nooa durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem er unterliegt, zu weiteren Verarbeitungen verpflichtet, teilt er dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit.
(4) Der Kunde erteilt alle Aufträge, Teilaufträge oder Weisungen dokumentiert. In Eilfällen können Weisungen mündlich erteilt werden. Solche Weisungen wird der Kunde unverzüglich dokumentiert bestätigen.
(5) Der Kunde informiert nooa unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.
(6) Der Kunde ist berechtigt, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen bei nooa in angemessenem Umfang selbst oder durch Dritte, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie sonstige Kontrollen vor Ort zu kontrollieren. Den mit der Kontrolle betrauten Personen ist seitens nooa soweit erforderlich Zutritt und Einblick zu ermöglichen. nooa ist verpflichtet, erforderliche Auskünfte zu erteilen, Abläufe zu demonstrieren und Nachweise zu führen, die zur Durchführung einer Kontrolle erforderlich sind. nooa ist berechtigt, Kontrollen durch Dritte zu verweigern, soweit diese mit ihm in einem Wettbewerbsverhältnis stehen oder ähnlich gewichtige Gründe vorliegen.
(7) Kontrollen bei nooa haben ohne vermeidbare Störungen seines Geschäftsbetriebs zu erfolgen. Soweit nicht aus vom Kunden zu dokumentierenden, dringlichen Gründen anders angezeigt, finden Kontrollen nach angemessener Vorankündigung und zu Geschäftszeiten von nooa, sowie nicht häufiger als alle 12 Monate statt. Soweit nooa den Nachweis der korrekten Umsetzung der vereinbarten Datenschutzpflichten wie unter Kapitel 5 (8) dieses Vertrages vorgesehen erbringt, soll sich eine Kontrolle auf Stichproben beschränken.

8 Mitteilungspflichten

(1) nooa teilt dem Kunden Verletzungen des Schutzes im Auftrag verarbeiteter personenbezogener Daten unverzüglich mit. Auch begründete Verdachtsfälle hierauf sind mitzuteilen. Die Mitteilung hat spätestens innerhalb von 24 Stunden ab Kenntnis von nooa vom relevanten Ereignis an eine vom Kunden benannte Adresse zu erfolgen. Sie muss mindestens folgende Angaben enthalten:
    a. eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
    b. den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;
    c. eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
    d. eine Beschreibung der seitens nooa ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen
(2) Ebenfalls unverzüglich mitzuteilen sind erhebliche Störungen bei der Auftragserledigung sowie Verstöße von nooa oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die in diesem Vertrag getroffenen Festlegungen.
(3) nooa informiert den Kunden unverzüglich von Kontrollen oder Maßnahmen von Aufsichtsbehörden oder anderen Dritten, soweit diese Bezüge zur Auftragsverarbeitung aufweisen.
(4) nooa sichert zu, den Kunden bei dessen Pflichten nach Art. 33 und 34 Datenschutz-Grundverordnung im erforderlichen Umfang zu unterstützen.

9 Weisungen

(1) Der Kunde behält sich hinsichtlich der Verarbeitung im Auftrag ein umfassendes Weisungsrecht vor. Der Kunde kann weisungsberechtigte Personen benennen. Sofern weisungsberechtigte Personen benannt werden sollen, werden diese in der Anlage benannt. Für den Fall, dass sich die weisungsberechtigten Personen beim Auftraggeber ändern, wird der Kunde dies nooa in Textform mitteilen.
(2) nooa kann dem Kunden die Person(en) benennen, die zum Empfang von Weisungen des Kunden berechtigt sind. Sofern weisungsempfangsberechtigte Personen benannt werden sollen, werden diese in der Anlage benannt. Für den Fall, dass sich die weisungsempfangsberechtigten Personen beim Auftragnehmer ändern, wird nooa dies dem Auftraggeber in Textform mitteilen.
(3) Bei einem Wechsel oder einer längerfristigen Verhinderung der benannten Personen sind der anderen Partei Nachfolger bzw. Vertreter unverzüglich mitzuteilen.
(4) nooa wird den Kunden unverzüglich darauf aufmerksam machen, wenn eine vom Kunden erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt. nooa ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Kunden bestätigt oder geändert wird.
(5) nooa hat ihm erteilte Weisungen und deren Umsetzung zu dokumentieren.

10 Beendigung des Auftrags

(1) Befinden sich bei Beendigung des Auftragsverhältnisses im Auftrag verarbeitete Daten oder Kopien derselben noch in der Verfügungsgewalt von nooa, hat dieser des nach Wahl des Kunden die Daten entweder zu vernichten oder an den Kunden zu übergeben. Die Wahl hat der Kunde innerhalb von 2 Wochen nach entsprechender Aufforderung durch nooa zu treffen. Die Vernichtung hat so zu erfolgen, dass eine Wiederherstellung auch von Restinformationen mit vertretbarem Aufwand nicht mehr möglich ist. Eine physische Vernichtung erfolgt gemäß DIN 66399. Hierbei gilt mindestens Schutzklasse 3.
(2) nooa ist verpflichtet, die unverzügliche Vernichtung bzw. Rückgabe auch bei Subunternehmern herbeizuführen.
(3) nooa hat den Nachweis der ordnungsgemäßen Vernichtung zu führen und dem Kunden unverzüglich vorzulegen.
(4) Dokumentationen, die dem Nachweis der ordnungsgemäßen Datenverarbeitung dienen, sind durch nooa mindestens bis zum Ablauf des dritten Kalenderjahres nach Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung dem Kunden übergeben.

11 Vergütung

Die Vergütung von nooa ist abschließend im Hauptvertrag geregelt. Eine gesonderte Vergütung oder Kostenerstattung im Rahmen dieses Vertrages erfolgt nicht.

12 Haftung

(1) Für den Ersatz von Schäden, die ein Betroffener wegen einer nach den Datenschutzgesetzen unzulässigen oder unrichtigen Datenverarbeitung oder Nutzung im Rahmen der Auftragsverarbeitung erleidet, ist im Innenverhältnis zu nooa alleine der Kunde gegenüber dem Betroffenen verantwortlich.
(2) Die Parteien stellen sich jeweils von der Haftung frei, wenn eine Partei nachweist, dass sie in keinerlei Hinsicht für den Umstand, durch den der Schaden bei einem Betroffenen eingetreten ist, verantwortlich ist.

13 Verpflichtung zur Geheimhaltung von Berufsgeheimnissen (§ 203 StGB)

(1) Im Rahmen dieses Auftrages werden auch Daten verarbeitet, die unter ein Berufsgeheimnis (im Sinne von 203 StGB) fallen. nooa verpflichtet sich, über Berufsgeheimnisse Stillschweigen zu bewahren und sich nur insoweit Kenntnis von diesen Daten zu verschaffen, wie dies zur Erfüllung der ihm zugewiesenen Aufgaben erforderlich ist.
(2) Der Kunde weist nooa darauf hin, dass sich Personen, die an der beruflichen Tätigkeit eines Berufsgeheimnisträgers mitwirken und unbefugt ein fremdes Geheimnis offenbaren, das ihnen bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt geworden ist, strafbar machen nach § 203 Abs. 4 S. 1 StGB. Zudem macht sich eine mitwirkende Person nach § 203 Abs. 4 S. 2 StGB strafbar, sollte sie sich einer weiteren mitwirkenden Person bedienen, die ihrerseits

unbefugt ein fremdes, ihr bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenes Geheimnis offenbart, und nicht dafür Sorge getragen hat, dass diese zur Geheimhaltung verpflichtet wurde.

(3) nooa stellt sicher, dass alle mit der Verarbeitung von dem Berufsgeheimnis unterliegenden Daten des Auftraggebers befassten Beschäftigten und andere für nooa tätigen Personen (z.B. Subunternehmer), die damit befasst sind, sich in Textform dazu verpflichtet haben, die ihnen bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenen Berufsgeheimnisse nicht unbefugt zu offenbaren und sie über die mögliche Strafbarkeit nach § 203 Abs. 4 StGB belehrt wurden. Der Kunde weist nooa darauf hin, dass sich eine mitwirkende Person nach § 203 Abs. 4 S. 2 StGB strafbar macht, sollte sie sich einer weiteren mitwirkenden Person bedienen, die ihrerseits unbefugt ein fremdes, ihr bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenes Geheimnis offenbart, und die mitwirkende Person nicht dafür Sorge getragen hat, dass die weitere, mitwirkende Person zur Geheimhaltung verpflichtet wurde. nooa wird etwaige Unterauftragnehmer sorgfältig auswählen und diese, soweit sie im Rahmen ihrer Tätigkeit Kenntnis von fremden Geheimnissen im Sinne dieser Vereinbarung erlangen könnten, zum Stillschweigen verpflichten. nooa wird ferner etwaige Unterauftragnehmer dazu verpflichten, sämtliche von diesen eingesetzten Personen und etwaige weitere Unterauftragnehmer, die bestimmungsgemäß mit Geheimnisschutzdaten in Berührung kommen oder bei denen dies nicht auszuschließen ist, nach den zuvor genannten Grundsätzen zur Verschwiegenheit zu verpflichten und über die Folgen einer Pflichtverletzung zu belehren.

(4) Des Weiteren werden Subunternehmer über das bestehende Schweigerecht gemäß § 53a StPO sowie den Beschlagnahmeschutz gemäß §97 StPO informiert; dies beinhaltet auch den Hinweis auf das Recht des Berufsgeheimnisträgers über dieses Recht zu entscheiden und die damit verbundene Pflicht, unverzüglich den Auftraggeber bzgl. der Wahrnehmung dieser Rechte zu kontaktieren. Diese Verpflichtung gilt für sämtliche weitere Unterbeauftragungen.

(5) nooa wird darauf hingewiesen, dass Daten, die er im Auftrag eines Berufsgeheimnisträgers verarbeitet u.U. dem Zeugnisverweigerungsrecht von sogenannten mitwirkenden Personen unterliegt (§ 53a Strafprozessordnung (StPO)). Entsprechend § 53a StPO entscheidet jedoch der Berufsgeheimnisträger über die Ausübung des Schweigerechts. Im Falle einer Befragung wird nooa unter Hinweis auf § 53a StPO dieser widersprechen und unverzüglich den Auftraggeber informieren, der daraufhin bzgl. der Wahrnehmung des Schweigerechts entscheidet.

(6) nooa wird darauf hingewiesen, dass die sich in seinem Gewahrsam befindenden Geheimnisschutzdaten dem Beschlagnahmeverbot gemäß § 97 Abs. 2 StPO unterliegen. Die Daten dürfen nicht ohne das Einverständnis des Auftraggebers (Berufsgeheimnisträger) herausgegeben werden. Im Falle einer Beschlagnahme wird nooa dieser widersprechen und unverzüglich den Auftraggeber informieren.

14 Sonderkündigungsrecht

(3) Der Kunde kann den Hauptvertrag und diese Vereinbarung jederzeit ohne Einhaltung einer Frist kündigen („außerordentliche Kündigung“), wenn ein schwerwiegender Verstoß von nooa gegen Datenschutzvorschriften oder die Bestimmungen dieser Vereinbarung vorliegt, nooa eine rechtmäßige Weisung des Kunden nicht ausführen kann oder will oder nooa Kontrollrechte des Kunden vertragswidrig verweigert.

(4) Ein schwerwiegender Verstoß liegt insbesondere vor, wenn nooa die in dieser Vereinbarung bestimmten Pflichten, insbesondere die vereinbarten technischen und organisatorischen Maßnahmen in erheblichem Maße nicht erfüllt oder nicht erfüllt hat.

(5) Bei unerheblichen Verstößen setzt der Kunde nooa eine angemessene Frist zur Abhilfe. Erfolgt die Abhilfe nicht rechtzeitig, so ist der Kunde zur außerordentlichen Kündigung wie in diesem Abschnitt beschrieben berechtigt.

(6) nooa hat dem Kunden alle Kosten zu erstatten, die diesem durch die verfrühte Beendigung des Hauptvertrages oder dieses Vertrages in Folge einer außerordentlichen Kündigung durch den Aufraggeber entstehen.

15 Sonstiges

(1) Sollte Eigentum des Kunden bei nooa durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat nooa den Kunden unverzüglich zu verständigen.

(2) Für Nebenabreden ist die Schriftform und die ausdrückliche Bezugnahme auf diese Vereinbarung erforderlich.

(3) Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der im Auftrag verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.
(4) Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.
(5) nooa kann diesen Vertrag von Zeit zu Zeit durch Veröffentlichung der geänderten Version auf seiner Website ändern. Sind die vorgeschlagenen Änderungen nach nooas alleinigem Ermessen wesentlich, lässt nooa dem Kunden eine Mitteilung mindestens zwanzig (20) Tage vor dem Datum des Inkrafttretens der vorgenommenen Änderungen zukommen. Durch den weiteren Zugriff auf den Dienst oder seine weitere Nutzung nach dem veröffentlichten Datum des Inkrafttretens der Änderungen dieses Vertrages stimmt der Kunde der geänderten Version des Vertrages zu.

Anlage 1: Beschreibung der Auftragsverarbeitung

1. Kundendaten

1.1. Art und Umfang der erhobenen Daten

(A) Bestandsdaten
- Kontoinformationen: Name, Art und Adresse der Organisation; Erstellungsdatum und Status des Kontos; Name und E-Mail-Adresse des Kontoinhabers; Verband (optional)
- Rechnungsinformationen: Name und E-Mail-Adresse des Rechnungskontakts; Abonnements; Zahlweise; Rechnungsadresse; USt-IdNr. (optional)

(B) Nutzungsdaten
- Anzahl, Art, Status von Nutzern und Zugriffscodes; Anzahl, Art von verknüpften Organisationen und Nutzern; Anzahl, Art, Status von Pinnwänden; Anzahl von Beiträgen, Kommentaren und “Gefällt-mir”-Angaben; Anzahl, Art, Status von Aufgaben; Anzahl, Art von Nachrichten und Unterhaltungen; Anzahl, Art, Status von Einladungen; Zeitstempel von Nutzeraktivitäten

1.2. Zweck und Rechtsgrundlage

nooa verarbeitet personenbezogene Daten, um Kunden einen Zugang zur Administrationsschnittstelle der Dienste sowie die Abwicklung von Bestellungen zu ermöglichen. Die Verarbeitung dieser Daten ist zur Erfüllung des Kaufvertrags gem. Art. 6 Abs.1 lit.b DSGVO erforderlich. Personenbezogene Daten werden, gestützt auf Art. 5 Abs. 1 DSGVO, ausschließlich aufgrund ihrer Selbstdeklaration und in dem Umfang verarbeitet, wie es für die Nutzung der Dienstleistung erforderlich ist.

1.3. Löschfrist

Die Daten werden nach Aufhebung des Kundenkontos nach der gesetzlich vorgeschriebenen Datenspeicherung zur Geschäftsabwicklung archiviert:
- Vertragsdaten 6 Jahre nach Vertragsende
- Rechnungen 10 Jahre

2. Nutzerdaten

2.1. Art und Umfang der erhobenen Daten

(A) Bestandsdaten
- Automatisch generierte, nicht personenbezogene Daten: nooa ID; Erstellungsdatum des Nutzerkontos
- Persönliche Daten, eingegeben von der Organisation oder dem Nutzer: Name; Nutzername; Funktion; Organisation; Rolle; Passwort; Status; E-Mail-Adresse (optional, verpflichtend bei Administratoren); Profilbild (optional); Geburtsdatum (optional); Kurzbiographie (optional); Name und Datum der Verknüpfung mit externen Kontakten; Persönliche Einstellungen (z.B. Sprache, Töne)

(B) Nutzungsdaten
- Automatisch generierte, nicht personenbezogene Daten: Zugriffscode (falls zutreffend); Verfallsdatum des Zugriffscodes; “Asset hash” – ein einzigartiger, zufälliger String um cloud-URLS für Medien zu erstellen
- Geräte und Protokolldaten: Eingehende Netzwerkparameter; Version der App; Gerät und Betriebssystem; Art und Version des Browsers; Log-Informationen

(C) Inhaltsdaten
- Pinnwände: Name; geteilt/intern; Mitglieder; Titelbild (optional); Beschreibung (optional)
- Direktnachrichten, Posts, Kommentare, Likes, Aufgaben, falls zutreffend: Art; Sender ID; Empfänger ID; Erstelldatum; Bearbeitungsdatum; Titel; Inhalt inkl. Text oder Medien; Status flags

Sämtliche Inhaltsdaten können nur von eingeloggten und autorisierten Nutzern eingesehen werden.

2.2. Zweck und Rechtsgrundlage

nooa verarbeitet personenbezogene Daten, um die Dienste gemäß Weisungen des Hauptvertrags bereitzustellen.

2.3. Löschfrist

Alle Daten von Nutzern werden nach Aufhebung des Kunden- oder Nutzerkontos archiviert und nach 3 Monaten gelöscht.

Anlage 2: Technische und organisatorische Maßnahmen

Im Folgenden werden die auftragsbezogenen technischen und organisatorischen Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit festgelegt, die nooa mindestens einzurichten und laufend aufrecht zu erhalten hat.

Ziel ist die Gewährleistung insbesondere der Vertraulichkeit, Integrität und Verfügbarkeit der im Auftrag verarbeiteten Informationen.

Maßnahmenübersicht und gesetzliche Grundlage	**Maßnahmen**
Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)	Maßnahmen zur Pseudonymisierung haben den Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren: 1. Die Ablage und Zusammenführung personenbezogener Kunden- und Nutzerdaten erfolgt so, dass ein unbefugter Dritter nicht auf diese Daten zugreifen kann.
Verschlüsselung (Art. 32 Abs. 1 lit. a DSGVO)	Maßnahmen zur Verschlüsselung haben den Zweck, die Nutzung und den Missbrauch der Daten durch unberechtigte Dritte zu verhindern: 1. Die Kommunikation zwischen Servern und verbundenen Clients wird mithilfe der branchenüblichen Verschlüsselung auf Transportebene verschlüsselt: HTTPS, SSL, TLS. 2. Nutzer-Passwörter werden nicht gespeichert. Stattdessen wird ein sicheres Verfahren verwendet, das auf kryptografischen Hash-Funktionen basiert („Salted Cryptographic Hash“). 3. Der Zugriff auf die nooa Web App erfolgt über einen sicheren Transportweg: HTTPS, SSL, TLS. 4. Die mobilen Endgeräte kommunizieren verschlüsselt mit dem Endpunkt.
Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)	Zutrittskontrolle: 1. Die verwendete IT-Infrastruktur wird durch Amazon Web Services (AWS) am Standort Frankfurt zur Verfügung gestellt. 2. Die Zutrittskontrolle zu den hochsicheren AWS-Rechenzentren erfolgt durch Verwendung von elektronischen Überwachungsmaßnahmen, mehrstufigen Zugangskontrollsystemen, Besetzung der Rechenzentren rund um die Uhr mit ausgebildetem Sicherheitspersonal sowie Gewährung des Zugriffs streng nach dem Prinzip der geringsten Rechte und ausschließlich zum Zweck der Systemadministration.
	Zugangskontrolle: 3. Die Zugangsberechtigungen für IT-Systeme werden nach einem definierten und dokumentierten Prozess nach dem Vier-Augen-Prinzip und dem Prinzip der geringsten Rechtevergabe (“Need-to-Know-Prinzip”) vergeben, nachdem Mitarbeiter nur diejenigen Zugänge erhalten, die für die Erfüllung ihrer Aufgaben nötig sind, und regelmäßig überprüft. 4. Für den Zugang zu IT-Systemen mit wird ein Passwort-Manager mit einem Sicherheitsmodell nach dem Zero-Knowledge-Prinzip und einer SSL/TSL-Verschlüsselung in Kombination einem integrierten Dark-Web-Monitoring eingesetzt. 5. Arbeitsgeräte sind mit Sicherheitssoftware wie bspw. Firewalls, Antivirus-Software und Malware-Erkennung ausgestattet. Schriftliche Regelungen zum Umgang mit mobilen Geräten und Datenträgern, zur Anwendung einer Bildschirmsperre und Ausrichtung der Bildschirme, zur sicheren Datenlöschung, zur Vernichtung von Datenträgern, sowie zur Remote-Arbeit (Home-Office) bestehen. Unbeaufsichtigte Geräte werden automatisch gesperrt.

	6. In der Applikation werden Kunden- und Nutzerkontos bei Erstellung durch angemessene Authentifizierungs- und Autorisierungsmechanismen wie zufällig generierten Aktivierungs- und Zugriffscodes gegen unbefugten Zugang gesichert. 7. Die Anmeldeinformationen für Kunden- und Nutzerkontos sind durch Verwendung der nooa ID pseudonymisiert und durch die Implementierung von sicheren, dem Stand der Technik entsprechenden Passwortvorgaben (Passwortlänge, -komplexität, etc.) geschützt. 8. Die Zugangsberechtigungen für die Applikation können von Administratoren des Kunden nach dem Prinzip der geringsten Rechtevergabe ("Need-to-Know-Prinzip") vergeben werden, nachdem Nutzer nur diejenigen Zugänge erhalten, die für die Erfüllung ihrer Aufgaben nötig sind. 9. Alle erfolgten Zugänge und Zugangsversuche zu IT-Systemen und zur Applikation werden protokolliert und dokumentiert.
	Zugriffskontrolle: 1. Die Zugriffsrechte für IT-Systeme werden im Rahmen eines Rollen-/Berechtigungskonzeptes definiert und dokumentiert, sind entsprechend der aufgabenbedingten Erfordernisse den jeweiligen Rollen zugeordnet und werden regelmäßig überprüft und entzogen, sobald die geschäftliche Notwendigkeit für den Zugriff nicht mehr besteht. Kritische administrative Rechtekombinationen werden überwacht ("Separation-of-Duty-Prinzip"). 2. Die Zugriffsrechte für die Applikation können von Administratoren des Kunden im Rahmen eines Rollen-/Berechtigungskonzeptes definiert und dokumentiert und entsprechend der aufgabenbedingten Erfordernisse den jeweiligen Rollen zugeordnet werden. 3. Zugriffe zur Applikation werden zeitlich beschränkt. 4. Alle Zugriffe zu IT-Systemen und zur Applikation werden protokolliert und dokumentiert.
	Trennungskontrolle: 1. Sowohl die IT-Systeme als auch die Applikation sind mandantenfähig. 2. Kunden- und Nutzerdaten werden auf der Basis jeweils eigener Kunden- und Nutzerkontos logisch und technisch voneinander getrennt sowie verschlüsselt. 3. Daten, die zu unterschiedlichen Zwecken erhoben werden, werden getrennt verarbeitet. 4. Produktiv-, Demo- und Testsysteme sind als solche gekennzeichnet und strikt voneinander getrennt.
Integrität (Art. 32 Abs. 1 lit. b DSGVO)	Weitergabekontrolle: 1. Daten zwischen nooas Servern und dem Internet werden immer verschlüsselt übertragen.
	Eingabekontrolle: 1. Die Erstellung, Änderung und Löschung von Daten sowie Änderungen an den Einstellungen der IT-Systeme und der Applikation wird, soweit möglich, protokolliert. 2. Durch das Rollen-/Berechtigungskonzept innerhalb der Applikation können Berechtige zur Eingabe, Änderung und Löschung personenbezogener Daten vom Kunden definiert werden.
Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)	Verfügbarkeitskontrolle: 1. Die Rechneranlagen befinden sich in klimatisierten Räumlichkeiten und sind mit einem Überspannungsschutz gegen Überspannungsspitzen sowie vor Überschwemmungen und gegen elektromagnetische Felder geschützt. Es werden Brandschutzmaßnahmen, Maßnahmen zur Sicherstellung einer störungsarmen und kontinuierlichen Stromversorgung sowie gegen

	Erschütterung und Vandalismus und Diebstahl durchgeführt. 2. AWS überwacht und wartet die elektrischen und mechanischen Geräte präventiv, um den unterbrechungsfreien Betrieb der Systeme in den AWS-Rechenzentren zu gewährleisten. Die Gerätewartung wird von qualifiziertem Personal entsprechend einem dokumentierten Wartungszeitplan durchgeführt. 3. AWS überprüft die Infrastrukturnutzung und -anforderungen mindestens einmal im Monat anhand eines Kapazitätsplanungsmodell. Mit diesem Modell lässt sich auch der künftige Bedarf prognostizieren. Es umfasst auch Überlegungen zu Informationsverarbeitung, Telekommunikation und der Speicherung von Audit-Protokollen. 4. Kritische Systemkomponenten werden an mehreren, voneinander isolierten Standorten (Availability Zones genannt) gesichert. Jede Availability Zone ist auf einen unabhängigen Betrieb mit hoher Zuverlässigkeit ausgelegt. Die Availability Zones sind vernetzt. Dies ermöglicht die Nutzung von Anwendungen, für die ein automatischer, unterbrechungsfreier Failover zwischen den Availability Zones eingerichtet ist. 5. Die Inbetriebnahme der bereitgestellten Produktiv-Systeme, deren Konfiguration und das Einspielen von Änderungen erfolgen nachvollziehbar und transparent
	Belastbarkeitskontrolle (Fähigkeit der Systeme, mit risikobedingten Veränderungen umzugehen und Aufweisen einer Toleranz und Ausgleichsfähigkeit gegenüber Störungen): 1. AWS überwacht elektrische und mechanische Systeme und Anlagen, sodass Probleme sofort erkannt werden. Hierfür werden fortlaufend Audit-Tools und Informationen der Gebäudemanagement- und elektrischen Überwachungssysteme ausgewertet. Es werden vorbeugende Wartungen vorgenommen, um

	eine kontinuierliche Funktionsfähigkeit der Anlagen sicherzustellen. Das Betriebspersonal bietet eine kontinuierliche Besetzung rund um die Uhr, sieben Tage die Woche und an 365 Tagen im Jahr, um Störfälle zu erkennen und deren Auswirkungen und Behebung zu verwalten. 2. Die Rechenzentren sind darauf ausgelegt, Funktionsausfälle zu antizipieren und zu tolerieren und dabei Servicelevel aufrecht zu erhalten. Für das Eintreten eines Funktionsausfalls wird der Datenverkehr von dem vom Ausfall betroffenen Bereich auf einen anderen umgeleitet. Für wichtige Anwendungen gilt ein N+1-Standard. Kommt es in einem Rechenzentrum zu einem Funktionsausfall, stehen genügend Kapazitäten zur Verfügung, damit der Datenverkehr auf die verbleibenden Standorte aufgeteilt werden kann. 3. Der AWS-Betriebskontinuitätsplan umfasst Maßnahmen zur Vermeidung und Verringerung von Störungen durch Umwelteinflüsse. Er enthält betriebliche Details zu den Maßnahmen, die vor, während und nach einem entsprechenden Ereignis ergriffen werden. Der Betriebskontinuitätsplan wird durch Tests gestützt, die auch Simulationen verschiedener Szenarios umfassen. Während und nach diesen Tests dokumentiert AWS die Leistung seiner Mitarbeiter und Prozesse, Korrekturmaßnahmen und die abgeleiteten Erfahrungen zur kontinuierlichen Verbesserung. 4. AWS berücksichtigt bei seiner Notfallwiederherstellungsplanung auch Reaktionsrichtlinien und -verfahren für Pandemien, um im Fall des Ausbruchs einer Infektionskrankheit schnell reagieren zu können. Die Abhilfemaßnahmen umfassen alternative Personalmodelle, bei denen kritische Prozesse an Ressourcen in anderen Regionen ausgelagert werden, sowie die Aktivierung eines

	Krisenmanagementplans, der kritische betriebliche Operationen unterstützen soll. Die Pandemiepläne enthalten Informationen zu internationalen Gesundheitsbehörden und -bestimmungen einschließlich Kontaktdaten für internationale Behörden.
Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO)	1. Die Architektur ist durch interne Replizierungsmechanismen innerhalb der AWS Plattform per se gegen Datenverlust gesichert. 2. Der Einsatz von Availability Zones und Datenreplikation erlaubt extrem kurze Wiederherstellungszeiträumen und Wiederherstellungspunktziele. 3. Die Datenbestände werden regelmäßig in Form von Backup-Kopien innerhalb der AWS Plattform gesichert. Das Backup-Konzept ist dokumentiert und wird regelmäßig überprüft und aktualisiert. Backup-Medien sind vor unbefugtem Zugriff geschützt.
Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)	Datenschutz-Management: 1. Es gilt der Grundsatz, dass Datenschutz und -sicherheit Aufgabe des gesamten Unternehmens ist. 2. Alle Mitarbeiter sind im Umgang mit vertraulichen Daten unterrichtet und schriftlich auf die Wahrung der Vertraulichkeit verpflichtet. Schriftliche Regeln für die Einsichtnahme in und die Offenlegung von sensiblen Daten, für die Übertragung und Weitergabe von Daten sowie für Regelungen zu Datenschutz und -sicherheit nach dem aktuellen Stand der Technik bestehen. Disziplinarmaßnahmen bei Zuwiderhandlung gegen Geheimhaltungsverpflichtungen bestehen. 3. Alle Mitarbeiter werden regelmäßig bzgl. der Gefahren und Risiken sensibilisiert sowie geschult, um die Einhaltung der Vorschriften der DSGVO und die Einhaltung von Weisungen sicherzustellen. Es erfolgen regelmäßig Nachschulungen.

	4. Ein Datenschutzbeauftragter und Datenschutzkoordinator sind definiert und beauftragt Änderungen in den internen Arbeitsprozessen aus Datenschutzsicht zu begleiten, auf Datenschutzaspekte hinzuweisen, und mit dem Datenschutzbeauftragten abzustimmen. Mitarbeiter sind angewiesen erkannte Verletzungen der Datenschutzbestimmungen, Verdacht auf mögliche Verletzungen, sowie sonstige Vorfälle mit Bezug zur Informationssicherheit umgehend zu melden. 5. Die Produktentwicklung und -gestaltung erfolgt nach den Prinzipien und Grundsätzen von “Data Privacy by Design”, “Data Privacy by Default”, “Zero Knowledge”, Datensparsamkeit und der “OWASP”. 6. Die eingesetzten Verfahren werden regelmäßig einer dokumentierten Datenschutz-Folgeabschätzung unterzogen, bestehend aus Schutzbedarfsfeststellung, Risikoanalyse und Sicherheitskonzept. 7. Es erfolgen regelmäßige Datenschutzaudit durch interne und externe Datenschutzbeauftragte. 8. Sicherheitsprüfungen (bspw. Penetrationstests) durch externe Parteien werden aktiv unterstützt.
	Incident-Response-Management: 1. Verfahren zum Umgang und der Meldung von Störungen inklusive der Erkennung und Reaktion auf mögliche Sicherheitsvorfälle sind definiert.
	Datenschutzfreundliche Voreinstellungen: 1. Die Grundeinstellung der Applikation ist so gestaltet, dass die Daten des Kunden und der Nutzer bestmöglich geschützt sind. 2. Kunden und Nutzer können Einstellungen an der Applikation vornehmen, die von dieser empfohlenen Grundeinstellung abweichen. Dies wird immer als eine Abweichung gekennzeichnet sowie mit Warnhinweisen versehen.
	Auftragskontrolle:

	1. Die Verarbeitung personenbezogener Daten erfolgt ausschließlich entsprechend den Weisungen des Auftraggebers. 2. Weisungen von Kunden sowie ausgeführte Tätigkeiten im Rahmen der Auftragsverarbeitung werden kundenbezogen dokumentiert.

Anlage 3: Zugelassene Subdienstleister

Nr.	Subdienstleister	Verarbeitete Datenkategorien	Zweck der Unterauftragsverarbeitung
1	**Amazon Web Services EMEA SARL (AWS Europe)** 38 avenue John F. Kennedy, L-1855 Luxembourg	Kunden- und Nutzerdaten	Speicherung und Verarbeitung der Auftragsdaten
2	**HubSpot Inc.** 2nd Floor, 25 First Street, Cambridge MA 02141, USA	Kundendaten	Speicherung und Verarbeitung der Vertragsdaten
3	**Stripe Payments Europe, Ltd.** C/O A&L Goodbody, 25-28 North Wall Quay, Dublin 1, Ireland	Kundendaten	Abrechnung und Rechnungsstellung
4	**Twilio Ireland Limited** 25-28 North Wall Quay Dublin 1, Ireland	Kunden- und Nutzerdaten	Bereitstellung von Infrastruktur für Telefonie, Videotelefonie und Nachrichten

5	**OpenAI, L.L.C.** 1st Floor, The Liffey Trust Centre, 117-126 Sheriff Street Upper, Dublin 1, D01 YC43, Irland	Nutzerdaten	Speicherung und Verarbeitung von Inhaltsdaten
6	**Google Cloud EMEA Limited** 70 Sir John Rogerson's Quay, Dublin 2, Ireland	Kunden- und Nutzerdaten	Speicherung und Verarbeitung von Adressdaten

Anlage 4: Datenschutzbeauftragter, Adresse zur Meldung von Datenschutzverletzungen

Die Kontaktdaten des internen Datenschutzbeauftragten sowie zur Meldung über die Verletzung personenbezogener Daten:

Datenschutzbeauftragter
nooa GmbH
Rheinkaistraße 1
68159 Mannheim
privacy@nooa.app