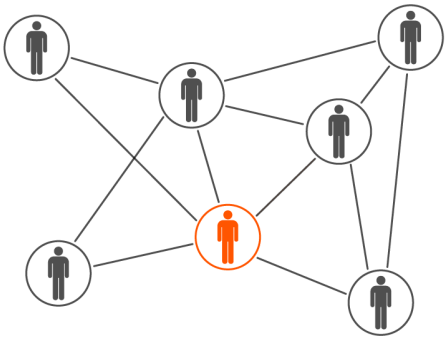
Nimmerland
Nextcloud Service Berlin
take control of all your data



Vereinbarung zur Auftragsverarbeitung

zwischen

Thomas Michalak
Nimmerland Nextcloud Service c/o
MACHWERK in der Alte Münze
Am Krögel 2
10179 Berlin

- nachfolgend Auftragnehmer -

und

- nachfolgend Auftraggeber -

1. Allgemeines

(1) Der Auftragnehmer bietet dem Auftraggeber Cloudspeicherplatz und verarbeitet damit möglicherweise personenbezogene Daten im Auftrag des Auftraggebers i.S.d. Art. 4 Nr. 8 und Art. 28 der Verordnung (EU) 2016/679 – Datenschutz-Grundverordnung (DSGVO). Dieser Vertrag regelt die Rechte und Pflichten der Parteien im Rahmen der Leistungserbringung gemäß Auftrag, Leistungsbeschreibung und AGB (nachfolgend Hauptvertrag), soweit eine Verarbeitung von personenbezogenen Daten durch den Auftragnehmer als Auftragsverarbeiter für den Auftraggeber gemäß Art. 28 DSGVO erfolgt. Dies umfasst alle Tätigkeiten, die der Auftragnehmer zur Erfüllung des Auftrags erbringt und die eine Auftragsverarbeitung darstellen. Dies gilt auch, sofern der Auftrag nicht ausdrücklich auf diese Vereinbarung zur Auftragsverarbeitung verweist.

(2) Sofern in diesem Vertrag der Begriff „Datenverarbeitung“ oder „Verarbeitung“ (von Daten) benutzt wird, wird die Definition der „Verarbeitung“ i.S.d. Art. 4 Nr. 2 DSGVO zugrunde gelegt.

(3) Die Dauer der Verarbeitung entspricht der im Hauptvertrag vereinbarten Laufzeit.

2. Gegenstand des Auftrags

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

3. Rechte und Pflichten des Auftraggebers

(1) Der Auftraggeber ist Verantwortlicher i.S.d. Art. 4 Nr. 7 DSGVO für die Verarbeitung von Daten im Auftrag durch den Auftragnehmer. Dies gilt auch im Hinblick auf die in dieser Vereinbarung geregelten Zwecke und Mittel der Verarbeitung. Dem Auftragnehmer steht nach Ziff. 4 Abs. 5 das Recht zu, den Auftraggeber darauf hinzuweisen, wenn eine seiner Meinung nach rechtlich unzulässige Datenverarbeitung Gegenstand des Auftrags und/oder einer Weisung ist.

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

(3) Der Auftraggeber hat das Recht, jederzeit ergänzende Weisungen über Art, Umfang und Verfahren der Datenverarbeitung gegenüber dem Auftragnehmer zu erteilen. Weisungen müssen in Textform (z.B. E-Mail) erfolgen. Die Weisungen werden anfänglich durch den Hauptvertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in einem elektronischen Format (Textform) durch einzelne Weisungen geändert werden (Einzelweisung). Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen. Weisungen, die im Hauptvertrag nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt. Bei Änderungsvorschlägen teilt der Auftragnehmer dem Auftraggeber mit, welche Auswirkungen sich auf die vereinbarten Leistungen, insbesondere die Möglichkeit der Leistungserbringung, Termine und Vergütung ergeben. Ist dem Auftragnehmer die Umsetzung der Weisung nicht zumutbar, so ist der Auftragnehmer berechtigt, die Verarbeitung zu beenden. Eine Unzumutbarkeit liegt insbesondere vor, wenn die Leistungen in einer Infrastruktur erbracht werden, die von mehreren Auftraggebern / Kunden des Auftragnehmers genutzt wird (Shared Services), und eine Änderung der Verarbeitung für einzelne Auftraggeber nicht möglich oder nicht zumutbar ist. Der Auftragnehmer ist berechtigt, für diese Leistungen eine angemessene Vergütung vom Auftraggeber zu verlangen.

(4) Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch ergänzende Weisungen des Auftraggebers beim Auftragnehmer entstehen, bleiben unberührt.

(5) Der Auftraggeber kann weisungsberechtigte Personen benennen. Sofern weisungsberechtigte Personen benannt werden sollen, werden diese in der **Anlage 1** benannt. Für den Fall, dass sich die weisungsberechtigten Personen beim Auftraggeber ändern, wird der Auftraggeber dies dem Auftragnehmer in Textform mitteilen.

(6) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch den Auftragnehmer feststellt.

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

(8) Im Falle der Beendigung des Hauptvertrages verpflichtet sich der Auftraggeber, diejenigen personenbezogenen Daten vor Vertragsbeendigung zu löschen, die er in der zur Verfügung gestellten Cloud gespeichert hat.

4. Allgemeine Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und/oder unter Einhaltung der ggf. vom Auftraggeber erteilten ergänzenden Weisungen. Ausgenommen hiervon sind gesetzliche Regelungen, die den Auftragnehmer ggf. zu einer anderweitigen Verarbeitung verpflichten. In einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Zweck, Art und Umfang der Datenverarbeitung richten sich ansonsten ausschließlich nach diesem Vertrag und/oder den Weisungen des Auftraggebers. Eine hiervon abweichende Verarbeitung von Daten ist dem Auftragnehmer untersagt, es sei denn, dass der Auftraggeber dieser schriftlich zugestimmt hat.

(2) Der Auftragnehmer verpflichtet sich, die Datenverarbeitung im Auftrag nur in Mitgliedsstaaten der Europäischen Union (EU) oder des Europäischen Wirtschaftsraums (EWR) durchzuführen.

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

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

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

(6) Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter und anderen für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass sich

die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

(7) Der Auftragnehmer wird die Daten, die er im Auftrag für den Auftraggeber verarbeitet, getrennt von anderen Daten verarbeiten. Eine physische Trennung ist nicht zwingend erforderlich.

(8) Der Auftragnehmer kann dem Auftraggeber die Person(en) benennen, die zum Empfang von Weisungen des Auftraggebers berechtigt sind. Sofern weisungsempfangsberechtigte Personen benannt werden sollen, werden diese in der **Anlage 1** benannt. Für den Fall, dass sich die weisungsempfangsberechtigten Personen beim Auftragnehmer ändern, wird der Auftragnehmer dies dem Auftraggeber in Textform mitteilen.

5. Datenschutzbeauftragter des Auftragnehmers

(1) Der Auftragnehmer ist nach Art. 37 DSGVO nicht verpflichtet, einen Datenschutzbeauftragten zu benennen.

(2) Es steht dem Auftragnehmer frei zu einem späteren Zeitpunkt einen Datenschutzbeauftragten nach Art. 37 DSGVO zu benennen. In diesem Fall wird der Auftragnehmer dem Auftraggeber den Namen und die Kontaktdaten seines Datenschutzbeauftragten gesondert in Textform mitteilen.

6. Meldepflichten des Auftragnehmers

(1) Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden. Der Auftragnehmer trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen für die betroffenen Personen.

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

7. Mitwirkungspflichten des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nach Art. 12-23 DSGVO. Es gelten die Regelungen von Ziff. 11 dieses Vertrages. Der Auftragnehmer kann hierfür eine angemessene Vergütung verlangen.

(2) Der Auftragnehmer wirkt an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten durch den Auftraggeber mit. Er hat dem Auftraggeber die insoweit jeweils erforderlichen Angaben in geeigneter Weise mitzuteilen. Der Auftragnehmer kann hierfür eine angemessene Vergütung verlangen.

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

8. Kontrollbefugnisse

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

(2) Der Auftragnehmer ist dem Auftraggeber gegenüber zur Auskunftserteilung verpflichtet, soweit dies zur Durchführung der Kontrolle i.S.d. Absatzes 1 erforderlich ist.

(3) Der Auftraggeber kann eine Einsichtnahme in die vom Auftragnehmer für den Auftraggeber verarbeiteten Daten sowie in die verwendeten Datenverarbeitungssysteme und -programme verlangen.

(4) Der Auftraggeber kann nach vorheriger Anmeldung mit angemessener Frist die Kontrolle im Sinne des Absatzes 1 in der Betriebsstätte des Auftragnehmers zu den jeweils üblichen Geschäftszeiten vornehmen. Der Auftraggeber wird dabei Sorge dafür tragen, dass die Kontrollen nur im erforderlichen Umfang durchgeführt werden, um die Betriebsabläufe des Auftragnehmers durch die Kontrollen nicht unverhältnismäßig zu stören. Der Auftragnehmer ist berechtigt, eine Verschwiegenheitserklärung vom Auftraggeber und von dessen beauftragten Prüfer zu verlangen. Der Auftragnehmer stimmt der Benennung eines unabhängigen externen Prüfers durch den Auftraggeber zu, sofern der Auftraggeber dem Auftragnehmer eine Kopie des Auditberichts zur Verfügung stellt. Wettbewerber des Auftraggebers oder Personen, die für Wettbewerber des Auftraggebers tätig sind, kann der Auftragnehmer als Prüfer ablehnen.

(5) Der Auftragnehmer ist verpflichtet, im Falle von Maßnahmen der Aufsichtsbehörde gegenüber dem Auftraggeber i.S.d. Art. 58 DSGVO, insbesondere im Hinblick auf Auskunfts- und Kontrollpflichten die erforderlichen Auskünfte an den Auftraggeber zu erteilen und der jeweils zuständigen Aufsichtsbehörde eine Vor-Ort-Kontrolle zu ermöglichen. Der Auftraggeber ist über entsprechende geplante Maßnahmen vom Auftragnehmer zu informieren.

(6) Für Informationen und Unterstützungshandlungen kann der Auftragnehmer eine angemessene Vergütung verlangen. Der Aufwand für den Auftragnehmer durch eine Inspektion ist grundsätzlich auf einen Tag pro Kalenderjahr begrenzt.

9. Unterauftragsverhältnisse

(1) Der Auftraggeber erteilt dem Auftragnehmer die allgemeine Genehmigung, weitere Auftragsverarbeiter im Sinne des Art. 28 DSGVO zur Vertragserfüllung einzusetzen. Der Auftragnehmer wird alle bereits zum Vertragsschluss bestehenden Unterauftragsverhältnisse in der **Anlage 2** zu diesem Vertrag angeben. Der Auftraggeber erklärt sich mit deren Einsatz einverstanden.

(2) Der Auftragnehmer hat den Unterauftragnehmer sorgfältig auszuwählen und vor der Beauftragung zu prüfen, dass dieser die zwischen Auftraggeber und Auftragnehmer getroffenen Vereinbarungen einhalten kann. Der Auftragnehmer hat insbesondere vorab und regelmäßig während der Vertragsdauer zu kontrollieren, dass der Unterauftragnehmer die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten getroffen hat.

(3) Der Auftragnehmer informiert den Auftraggeber, wenn er eine Änderung in Bezug auf die Hinzuziehung oder die Ersetzung weiterer Auftragsverarbeiter beabsichtigt. Der Auftraggeber kann gegen derartige Änderungen Einspruch erheben.

(4) Der Einspruch gegen die beabsichtigte Änderung kann nur aus einem wichtigen datenschutzrechtlichen Grund innerhalb einer angemessenen Frist nach Zugang der Information über die Änderung gegenüber dem Auftragnehmer erhoben werden. Im Fall des Einspruchs kann der Auftragnehmer nach eigener Wahl die Leistung ohne die beabsichtigte Änderung erbringen oder - sofern die Erbringung der Leistung ohne die beabsichtigte Änderung für den Auftragnehmer nicht zumutbar ist - die von der Änderung betroffene Leistung gegenüber dem Auftraggeber innerhalb einer angemessenen Frist nach Zugang des Einspruchs einstellen.

(5) Der Auftragnehmer hat sicherzustellen, dass die in diesem Vertrag vereinbarten Regelungen und ggf. ergänzende Weisungen des Auftraggebers auch gegenüber dem Unterauftragnehmer gelten.

(6) Der Auftragnehmer hat mit dem Unterauftragnehmer einen Auftragsverarbeitungsvertrag zu schließen, der den Voraussetzungen des Art. 28 DSGVO entspricht. Darüber hinaus hat der Auftragnehmer dem Unterauftragnehmer dieselben Pflichten zum Schutz personenbezogener Daten aufzuerlegen, die zwischen Auftraggeber und Auftragnehmer festgelegt sind. Dem Auftraggeber ist der Auftragsdatenverarbeitungsvertrag auf Anfrage in Kopie zu übermitteln.

(6) Erteilt der Auftragnehmer Aufträge an weitere Auftragsverarbeiter, so obliegt es dem Auftragnehmer, seine datenschutzrechtlichen Pflichten aus diesem Vertrag auf den weiteren Auftragsverarbeiter zu übertragen.

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

10. Vertraulichkeitsverpflichtung

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

(2) Der Auftragnehmer sichert zu, dass ihm die jeweils geltenden datenschutzrechtlichen Vorschriften bekannt sind und er mit der Anwendung dieser vertraut ist. Der Auftragnehmer sichert ferner zu, dass er seine Beschäftigten mit den für sie maßgeblichen Bestimmungen des Datenschutzes vertraut macht und zur Vertraulichkeit verpflichtet hat. Der Auftragnehmer sichert ferner zu, dass er insbesondere die bei der Durchführung der Arbeiten tätigen Beschäftigten zur Vertraulichkeit verpflichtet hat und diese über die Weisungen des Auftraggebers informiert hat.

11. Wahrung von Betroffenenrechten

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

(2) Soweit eine Mitwirkung des Auftragnehmers für die Wahrung von Betroffenenrechten - insbesondere auf Auskunft, Berichtigung, Sperrung oder Löschung - durch den Auftraggeber erforderlich ist, wird der Auftragnehmer die jeweils erforderlichen Maßnahmen nach Weisung des Auftraggebers treffen. Der Auftragnehmer wird den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nachzukommen. Für diese Leistung kann der Auftragnehmer eine angemessene Vergütung verlangen.

(3) Weitere Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch Mitwirkungsleistungen im Zusammenhang mit Geltendmachung von Betroffenenrechten gegenüber dem Auftraggeber beim Auftragnehmer entstehen, bleiben unberührt.

12. Geheimhaltungspflichten

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

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

13. Haftung

Die zwischen den Parteien im Hauptvertrag zur Leistungserbringung vereinbarte Haftungsregelung gilt auch für Ansprüche aus dieser Vereinbarung zur Auftragsverarbeitung und im Innenverhältnis zwischen den Parteien für Ansprüche Dritter nach Art 82 DSGVO, außer soweit ausdrücklich etwas anderes vereinbart ist.

14. Technische und organisatorische Maßnahmen zur Datensicherheit

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

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

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

15. Dauer des Auftrags, Änderung

(1) Die Vereinbarung beginnt nach Unterzeichnung durch Auftraggeber und Auftragnehmer. Sie endet mit dem Ende des Hauptvertrages. Insofern nach Beendigung des Hauptvertrages noch eine Auftragsverarbeitung stattfindet, gelten die Regelungen dieser Vereinbarung bis zum tatsächlichen Ende der Verarbeitung.

(2) Der Auftragnehmer kann die Vereinbarung nach billigem Ermessen mit angemessener Ankündigungsfrist ändern. Änderungen dienen in der Regel Anpassungen an neue technische Möglichkeiten oder gesetzliche Regelungen.

16. Beendigung

Nach Abschluss der Erbringung der Verarbeitungsleistungen löscht der Auftragnehmer nach Wahl des Auftraggebers entweder alle personenbezogenen Daten oder gibt sie dem Kunden zurück, sofern nicht nach dem Unionsrecht oder nach dem anwendbaren Recht eines Mitgliedstaates eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht oder sich aus jeweiligen vertraglichen Vereinbarungen etwas anderes ergibt. Macht der Auftraggeber von diesem Wahlrecht keinen Gebrauch gilt die Löschung als vereinbart. Wählt der Auftraggeber die Rückgabe, kann der Auftragnehmer eine angemessene Vergütung verlangen.

17. Schlussbestimmungen

(1) Ergänzend gelten die AGB des Auftragnehmers, abrufbar unter https://nimmerland.de/agb.html. Bei etwaigen Widersprüchen gehen Regelungen dieser Vereinbarung zur Auftragsverarbeitung den Regelungen des Hauptvertrages vor. Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarungen im Übrigen nicht.

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

(3) Für Nebenabreden ist die Schriftform erforderlich.

(4) Sollte das Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu informieren. Der Auftragnehmer wird die Gläubiger über die Tatsache, dass es sich um Daten handelt, die im Auftrag verarbeitet werden, unverzüglich informieren.

(5) Ausschließlicher Gerichtsstand für alle Streitigkeiten aus und im Zusammenhang mit diesem Vertrag ist Berlin. Dieser gilt vorbehaltlich eines etwaigen ausschließlich gesetzlichen Gerichtsstandes. Dieser Vertrag unterliegt den gesetzlichen Bestimmungen der Bundesrepublik Deutschland.

Ort, Datum	Ort, Datum
Unterschrift	Unterschrift
- für den Auftragnehmer -	- für den Auftraggeber -

Anlage 1 - Gegenstand des Auftrags

1. Gegenstand und Zweck der Verarbeitung

Der Auftragnehmer stellt dem Auftraggeber eine individuelle Nextcloud-Installation zur Verfügung. Nextcloud ist eine Open-Source Software zur Datenspeicherung und zum Teilen von Dateien in der Cloud. Die Software wird „as is“ zur Verfügung gestellt. Es werden keine Garantien für die Funktion der Software übernommen. Näheres ergibt sich aus Leistungsbeschreibung und der AGB (Hauptvertrag). Der Upload, Download, die Veränderung und das Teilen von Dateien geschieht ausschließlicher durch und in Verantwortung des Auftraggebers.

Je nach Auftrag übernimmt der Auftragnehmer neben dem Betrieb, die Einrichtung, Anpassung, Administration, das Backup und die Pflege der Nextcloud-Installation.

Die Art der Verarbeitung umfasst alle Arten von Verarbeitungen im Sinne der DSGVO zur Erfüllung des Auftrags (Hauptvertrag).

Zwecke der Verarbeitung sind alle zur Erbringung der vertraglich vereinbarten Leistung im Bereich Cloud-Dienstleistungen, Hosting, Software as a Service (SaaS) und IT-Support erforderlichen Zwecke.

2. Art(en) der personenbezogenen Daten

Folgende Datenarten sind regelmäßig Gegenstand der Verarbeitung:

Die vom Auftraggeber gespeicherten (personenbezogenen) Daten werden vom Auftragnehmer nicht reglementiert. Es kann sich - in Verantwortung des Auftraggebers - um jede Form personenbezogener Daten handeln.

Die Art der verarbeiteten Daten bestimmt der Auftraggeber durch die Produktwahl, die Konfiguration, die Nutzung der Dienste und die Übermittlung von Daten.

3. Kategorien betroffener Person

Die Kategorien von Betroffenen bestimmt der Auftraggeber durch die Produktwahl, die Konfiguration, die Nutzung der Dienste und die Übermittlung von Daten.

Die von der Datenverarbeitung betroffenen Personen können zum Beispiel Kunden, Mitarbeiter, Vertragspartner oder andere Personen sein, die in einem Verhältnis zum Auftraggeber stehen.

4. Weisungsberechtigte Personen des Auftraggebers

Falls keine weisungsberechtigten Personen benannt werden sollen, streichen.

Name	Funktion	E-Mail	Telefon

5. Weisungsempfangsberechtigte Personen des Auftragnehmers

Falls keine weisungsberechtigten Personen benannt werden sollen, streichen.

Name	Funktion	E-Mail	Telefon

Anlage 2 - Unterauftragnehmer

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

Dabei handelt es sich um nachfolgende Unternehmen:

STRATO AG

Pascalstraße 10
10587 Berlin

Die Strato AG betreibt die Rechenzentren, in denen die von uns angemieteten Server stehen, auf welchen die Datenverarbeitung im Auftrag stattfindet. Die Rechenzentren der STRATO AG sind nach ISO 27001 zertifiziert.

MailerLite Limited
Ground Floor, 71 Lower Baggot Street
Dublin 2, D02 P593
Ireland

MailerLite Limited ist unser Dienstleister für Newsletter und Support-E-Mails. Der Dienstleister arbeitet DSGVO-konform. Die AGBs und Datenschutzerklärungen finden Sie hier: https://www.mailerlite.com/legal

Anlage 3
Technische und organisatorische Maßnahmen des Auftragnehmers

Der Auftragsverarbeiter setzt folgende technische und organisatorische Maßnahmen zum Schutz der vertragsgegenständlichen personenbezogenen Daten um. Die Maßnahmen wurden im Einklang mit Art. 32 DSGVO festgelegt und mit dem Auftraggeber abgestimmt.

1. Vertraulichkeit

Zutrittskontrolle

Die Datenverarbeitung findet ausschließlich im Rechenzentrum und auf Servern der Strato AG (s. Unterauftragnehmer) statt. Dort haben wir im Auftrag zur Datenverarbeitung vereinbart:

Unbefugten ist der Zutritt zu Räumen zu verwehren, in denen Datenverarbeitungsanlagen untergebracht sind.
Festlegung von Sicherheitsbereichen

- Realisierung eines wirksamen Zutrittsschutzes
- Protokollierung des Zutritts
- Festlegung zutrittsberechtigter Personen
- Verwaltung von personengebundenen Zutrittsberechtigungen
- Begleitung von Fremdpersonal
- Überwachung der Räume

In den Räumen des Auftragnehmers befinden sich dauerhaft keine Daten der Auftraggeber. Ein Zugriff (s.u.) wäre prinzipiell möglich. Es wurden daher folgende Maßnahmen getroffen, um Unbefugte am Zutritt zu den Räumen des Auftragnehmers zu hindern (Zutrittskontrolle):

- Manuelles Schließsystem
- Sicherheitsschlösser
- Schlüsselregelung

Zugangskontrolle

Die Datenverarbeitung findet ausschließlich im Rechenzentrum und auf Servern der Strato AG statt. Dort haben wir im Auftrag zur Datenverarbeitung vereinbart:

Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden.

- Festlegung des Schutzbedarfs
- Zugangsschutz
- Umsetzung sicherer Zugangsverfahren, starke Authentisierung
- Umsetzung einfacher Authentisierung per Username Passwort
- Protokollierung des Zugangs
- Monitoring bei kritischen IT-Systemen
- Gesicherte (verschlüsselte) Übertragung von Authentisierungsgeheimnissen
- Sperrung bei Fehlversuchen/Inaktivität und Prozess zur Rücksetzung gesperrter Zugangskennungen
- Verbot Speicherfunktion für Passwörter und/oder Formulareingaben (Server/Clients)
- Festlegung befugter Personen
- Verwaltung und Dokumentation von personengebundenen Authentifizierungsmedien und
- Zugangsberechtigungen
- Automatische Zugangssperre und Manuelle Zugangssperre

Zugang ist prinzipiell auch allen Administratoren des Auftragnehmers von ihren jeweiligen Arbeitsplätzen möglich. Es wurden daher folgende Maßnahmen getroffen, die die Nutzung der Datensysteme durch unbefugte Dritte verhindern (Zugangskontrolle):

- Festlegung befugter Personen
- Zuordnung von Benutzerrechten
- Erstellen von Benutzerprofilen
- Passwortvergabe
- Passwortrichtlinie (Mindestlänge, Komplexität)
- Authentifikation mit Benutzername und Passwort
- Zuordnung von Benutzerprofilen zu IT-Systemen
- Einsatz stark verschlüsselter Verbindungen (SSH, HTTPS, VPN) bei der Übertragung von Daten
- Verschlüsselung mobiler Datenträger
- Verschlüsselung mobiler IT-Systeme
- Manuelle Zugangssperre

- Einsatz von Anti-Viren-Software
- Einsatz einer Software Firewall

Zugriffskontrolle

Die Datenverarbeitung findet ausschließlich im Rechenzentrum und auf Servern der Strato AG statt. Dort haben wir im Auftrag zur Datenverarbeitung vereinbart:

Es kann nur auf die Daten zugegriffen, für die eine Zugriffsberechtigung besteht. Daten können bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden.

- Erstellen eines Berechtigungskonzepts
- Umsetzung von Zugriffsbeschränkungen
- Vergabe minimaler Berechtigungen
- Verwaltung und Dokumentation von personengebundenen Zugriffsberechtigungen
- Vermeidung der Konzentration von Funktionen

Zugriff ist prinzipiell auch allen Administratoren des Auftragnehmers möglich. Es wurden folgende Maßnahmen getroffen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle):

- Berechtigungskonzept
- Verwaltung der Rechte durch Systemadministrator
- Regelmäßige Überprüfung und Aktualisierung der Zugriffsrechte (insb. bei
- Ausscheiden von Mitarbeitern o.Ä.)
- Anzahl der Administratoren auf das „Notwendigste“ reduziert.
- Passwortrichtlinie inkl. Passwortlänge, Passwortkomplexität
- Sichere Aufbewahrung von Datenträgern
- Physische Löschung von Datenträgern vor Wiederverwendung
- Einsatz von Aktenvernichtern (Sicherheitsstufe P4 nach DIN 66399)
- Verschlüsselung mobiler Datenträger un mobiler IT-Systeme

Trennung

- Der Auftraggeber speichert seine Daten auf einer je eigenen Nextcloud Instanz. Der Zugang zu Daten anderer Kunden ist nicht möglich.
- Logische Mandantentrennung (softwareseitig)
- Berechtigungskonzept
- Produktiv- und Testsysteme sind getrennt.

Pseudonymisierung & Verschlüsselung

- Bei der Datenspeicherung in einer Cloud ist der Auftraggeber typischerweise selbst für Art und Inhalt der gespeicherten Daten und damit für Pseudonymisierung und Verschlüsselung seiner Daten verantwortlich.
- Nextcloud bietet eine serverseitige Verschlüsselung der Dateien (nicht der in der Datenbank abgelegten Daten), die - prinzipbedingt - nur einen eingeschränkten Schutz ermöglicht.
- Der Auftraggeber ist darüber informiert, dass einzig eine Ende-zu-Ende Verschlüsselung starken Schutz der Dateien bietet. Eine Ende-zu-Ende Verschlüsselung der in der Cloud abgelegten Dateien bieten externe Anbieter wie zum Beispiel Boxcryptor, Cryptomator oder AXCrypt.

2. Integrität

Eingabekontrolle

- Die Eingabe personenbezogener Daten erfolgt ausschließlich durch den Auftraggeber und die von ihm berechtigten Personen.
- Der Auftraggeber erarbeitet dafür ein Berechtigungskonzept. Der Auftragnehmer kann den Auftraggeber bei der Erarbeitung eines passenden Berechtigungskonzeptes beraten und es im Auftrag umsetzen. Der Auftragnehmer ist berechtigt, eine für diese Leistung angemessene Vergütung zu verlangen.
- Der Auftraggeber ist darüber informiert, dass sämtliche Aktivitäten, insbesondere das Eingeben, Löschen und Verändern von Dateien, durch eine Nextcloud-App (Activity) protokolliert und aufgezeichnet werden können. Die Nextcloud-App (Activity) wird auf Weisung des Auftraggebers (z.B. durch den Hauptvertrag) ein- oder ausgeschaltet. Falls eingeschaltet, wird das Protokoll für 90 Tage gespeichert.
- Diese Protokollierung erfolgt dateibezogen. Der Auftraggeber und von ihm beauftrage Personen (z.B. Mitarbeiter) haben insofern Zugriff auf diese Protokolle, als sie auch Zugriff auf die entsprechenden Dateien haben.
- Übernimmt der Auftragnehmer im Rahmen des Hauptvertrages die Benutzer- und Rechteverwaltung der Nextcloud im Auftrag des Kunden, so haben dessen Administratoren ebenfalls Zugriff auf die Protokolle.

- Mitarbeiter des Auftragnehmers sind nicht zum Eingeben, Verändern oder Löschen von Dateien berechtigt, es sei denn, es liegt eine Weisung des Auftraggebers vor.

Weitergabekontrolle

Folgende Maßnahmen gewährleisten, dass personenbezogene Daten bei der Weitergabe (physisch und / oder digital) nicht von Unbefugten erlangt oder zur Kenntnis genommen werden können (Transport- bzw. Weitergabekontrolle):

- Einsatz von VPN-Tunneln
- Fernzugriff ausschließlich über verschlüsselte Verbindungen
- Transportverschlüsselung (SSH, HTTPS, SFTP, etc.)
- Regelmäßige Überprüfung der Sicherheit und Zulässigkeit der eingesetzten Verschlüsselungstechniken
- Verschlüsselung physikalischer Datenträger beim Transport.

3. Verfügbarkeit und Belastbarkeit

Die Datenverarbeitung findet ausschließlich im Rechenzentrum und auf Servern der Strato AG statt. Dort haben wir im Auftrag zur Datenverarbeitung vereinbart:

- Brandschutz
- Redundanz der Primärtechnik
- Redundanz der Stromversorgung
- Redundanz der Kommunikationsverbindungen
- Monitoring
- Resourcenplanung und Bereitstellung
- Abwehr von systembelastendem Missbrauch
- Datensicherungskonzepte und Umsetzung
- Regelmäßige Prüfung der Notfalleinrichtungen

Zusätzlich hat der Auftragnehmer ein eigenes System für das Desaster Recovery

- Nächtliche Spiegelung der Nextcloud Instanz inklusive aller Daten des Auftraggebers auf einem Backup-Server.
- In einigen Verträgen (siehe Hauptvertrag) ist darüber hinaus eine 21-tägige Versionierung der vom Auftraggeber gespeicherten Dateien und der Datenbanken vorgesehen. Für die Wiederherstellung von Dateien/Informationen aus diesem Backup kann der Auftragnehmer eine angemessene Vergütung verlangen.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Der Auftragnehmer wird die in dieser Anlage niedergelegten technischen und organisatorischen Maßnahmen jährlich und anlassbezogen, prüfen, evaluieren und bei Bedarf anpassen.