Vertrag über die Verarbeitung von Daten im Auftrag

zwischen

dem Kunden/der Gemeinde

- Auftraggeber -

und

ChurchDesk ApS
Nørrebrogade 45E
2200 Kopenhagen N
Dänemark

- Auftragnehmer -

1. Allgemeines

(1) Der Auftragnehmer verarbeitet 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 Zusammenhang mit der Verarbeitung von personenbezogenen Daten.

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

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. Dem Auftragnehmer steht nach Ziff. 4 Abs. 3 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.

(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. 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.

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 wird die Datenverarbeitung im Auftrag grundsätzlich in Mitgliedsstaaten der Europäischen Union (EU) oder des Europäischen Wirtschaftsraums (EWR) durchzuführen. Dem Auftragnehmer ist eine Datenverarbeitung auch außerhalb von EU oder EWR erlaubt, wenn entsprechende Unterauftragnehmer im Drittland unter Einhaltung der Voraussetzungen von Ziff. 9 eingesetzt werden und die Voraussetzungen der Art. 44-48 DSGVO erfüllt sind bzw. eine Ausnahme i.S.d. Art. 49 DSGVO vorliegt.

(3) 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.

(4) Der Auftragnehmer kann dem Auftraggeber die Person(en) benennen, die zum Empfang von Weisungen des Auftraggebers berechtigt sind. Für den Fall, dass sich die weisungsempfangsberechtigten Personen beim Auftragnehmer ändern, wird der Auftragnehmer dies dem Auftraggeber in Textform mitteilen.

5. Datenschutzbeauftragter des Auftragnehmers

Der Auftragnehmer ist verpflichtet, einen fachkundigen und zuverlässigen Datenschutz beauftragten zu bestellen, sofern und solange die gesetzlichen Voraussetzungen für eine Bestellpflicht gegeben sind. Der Auftragnehmer gewährleistet, dass die Anforderungen an den Datenschutzbeauftragten und seine Tätigkeit gemäß Art. 38 DSGVO erfüllt wer den.

6. Meldepflichten des Auftragnehmers

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

(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.

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

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

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. 12 dieses Vertrages.

(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.

(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 im erforderlichen Umfang zu kontrollieren.

(2) Für den Fall, dass der Auftraggeber Teil einer Gliedkirche (Landeskirche) der Evangelischen Kirche Deutschlands ist, wird die Kontrollbefugnis des Auftraggebers an die zuständige Aufsichtsbehörde und Kirchenleitung der jeweiligen Landeskirche übertragen. Unbenommen hiervon bleibt das bestehende Kontrollrecht der zuständigen staatlichen Aufsichtsbehörde.

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

(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. Die Parteien gehen davon aus, dass eine Kontrolle höchstens einmal jährlich erforderlich ist. Weitere Prüfungen sind vom Auftraggeber unter Angabe des Anlasses zu begründen. Im Falle von Vor-Ort-Kontrollen wird der Auftraggeber dem Auftragnehmer die entstehenden Aufwände inkl. der Personalkosten für die Betreuung und Begleitung der Kontrollpersonen vor Ort in angemessenen Umfang ersetzen. Die Grundlagen der Kostenberechnung werden dem Auftraggeber vom Auftragnehmer vor Durchführung der Kontrolle mitgeteilt.

(5) Nach Wahl des Auftragnehmers kann der Nachweis der Einhaltung der technischen und organisatorischen Maßnahmen anstatt einer Vor-Ort-Kontrolle auch durch die Vorlage eines geeigneten, aktuellen Testats, von Berichten oder Berichtsauszügen unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicher heitsabteilung, Datenschutzauditoren oder Qualitätsauditoren), oder einer geeigneten Zertifizierung erbracht werden, wenn der Prüfungsbericht es dem Auftraggeber in angemessener Weise ermöglicht, sich von

der Einhaltung der technischen und organisatorischen Maßnahmen gemäß Anlage 3 zu diesem Vertrag zu überzeugen. Sollte der Auftraggeber begründete Zweifel an der Eignung des Prüfdokuments i.S.d. Satzes 1 haben, kann eine Vor-Ort-Kontrolle durch den Auftraggeber erfolgen.

(6) 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.

9. Unterauftragsverhältnisse

(1) Der Auftragnehmer ist berechtigt, die in der **Anlage 2** zu diesem Vertrag angegebenen Unterauftragnehmer für die Verarbeitung von Daten im Auftrag einzusetzen. Der Wechsel von Unterauftragnehmern oder die Beauftragung weiterer Unterauftragnehmer ist unter den in Absatz 2 genannten Voraussetzungen zulässig.

(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. Der Auftragnehmer wird den Auftraggeber im Falle eines geplanten Wechsels eines Unterauftragnehmers oder bei geplanter Beauftragung eines neuen Unterauftragnehmers rechtzeitig vor dem Wechsel bzw. der Neubeauftragung in Textform informieren („Information“). Der Auftraggeber hat das Recht, dem Wechsel oder der Neubeauftragung des Unterauftragnehmers unter Angabe einer Begründung in Textform nach Zugang der „Information“ zu widersprechen. Der Widerspruch kann vom Auftraggeber jederzeit in Textform zurückgenommen werden. Im Falle eines Widerspruchs kann der Auftragnehmer das Vertragsverhältnis mit dem Auftraggeber mit einer Frist von mindestens 14 Tagen zum Ende eines Kalendermonats kündigen. Der Auftragnehmer wird bei der Kündigungsfrist die Interessen des Auftraggebers angemessen berücksichtigen. Wenn kein Widerspruch des Auftraggebers bin nen fünf Tagen nach Zugang der „Information“ erfolgt gilt dies als Zustimmung des Auftraggebers zum Wechsel bzw. zur Neubeauftragung des betreffenden Unterauftragnehmers.

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

(4) Der Auftragnehmer hat mit dem Unterauftragnehmer einen Auftragsverarbeitungs vertrag 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.

(5) Nicht als Unterauftragsverhältnisse i.S.d. Absätze 1 bis 4 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, Transport leistungen, 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.

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.

(2) Der Auftragnehmer hat seine Beschäftigten mit den für sie maßgeblichen Bestimmungen des Datenschutzes vertraut gemacht und zur Vertraulichkeit verpflichtet.

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

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 unterstützen. 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.

(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.

(3) 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, 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. 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.

14. Dauer des Auftrags

(1) Der Vertrag beginnt mit dem Beginn des Hauptvertrages und läuft für die Dauer des zwischen den Parteien bestehenden Hauptvertrages über die Nutzung der Dienstleistungen des Auftragnehmers durch den Auftraggeber.

(2) Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen. Dies gilt insbesondere, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen die anzuwendenden Datenschutzvorschriften oder gegen wesentliche Pflichten aus diesem Vertrag vorliegt oder der Auftragnehmer eine Weisung des Auftraggebers nicht aus führen will.

15. Haftung

(1) Auftraggeber und Auftragnehmer haften für den Schaden, der durch eine nicht der DSGVO entsprechende Verarbeitung verursacht wird, gemeinsam im Außenverhältnis gegenüber der jeweiligen betroffenen Person.

(2) Der Auftragnehmer haftet ausschließlich für Schäden, die auf einer von ihm durchgeführten Verarbeitung beruhen, bei der

(a) er den aus der DSGVO resultierenden und speziell für Auftragsverarbeiter auferlegten Pflichten nicht nachgekommen ist oder

(b) er unter Nichtbeachtung der rechtmäßig erteilten Weisungen des Auftraggebers handelte oder

(c) er gegen die rechtmäßig erteilten Weisungen des Auftraggebers gehandelt hat.

(3) Soweit der Auftraggeber zum Schadensersatz gegenüber dem Betroffenen verpflichtet ist, bleibt ihm der Rückgriff auf den Auftragnehmer vorbehalten.

(4) Im Innenverhältnis zwischen Auftraggeber und Auftragnehmer haftet der Auftragnehmer für den durch eine Verarbeitung verursachten Schaden jedoch nur, wenn er (a) seinen ihm speziell durch die DSGVO auferlegten Pflichten nicht nachgekommen ist oder (b) unter Nichtbeachtung der rechtmäßig erteilten Weisungen des Auftraggebers oder gegen diese Weisungen gehandelt hat.

(5) Weitergehende Haftungsansprüche nach den allgemeinen Gesetzen bleiben unberührt.

16. Beendigung

(1) Nach Beendigung des Vertrages hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, Daten und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, nach Wahl des Auftraggebers an diesen zurückzugeben oder zu löschen. Die Löschung ist in geeigneter Weise zu doku
mentieren.

(2) Der Auftragnehmer darf personenbezogene Daten, die im Zusammenhang mit dem Auftrag verarbeitet worden sind, über die Beendigung des Vertrages hinaus speichern, wenn und soweit den Auftragnehmer eine gesetzliche Pflicht zur Aufbewahrung trifft. In diesen Fällen dürfen die Daten nur für Zwecke der Umsetzung der jeweiligen gesetzlichen Aufbewahrungspflichten verarbeitet werden. Nach Ablauf der Aufbewahrungspflicht sind die Daten unverzüglich zu löschen.

17. Zurückbehaltungsrecht

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

18. Schlussbestimmungen

(1) 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.

(2) Änderungen, Ergänzungen und die Aufhebung dieser Vereinbarung und aller seiner Bestandteile bedürfen der Schriftform. Gleiches gilt für eine Änderung oder Aufhebung des Schriftformerfordernisses.

(3) Sollten sich einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise als unwirksam oder undurchführbar erweisen oder infolge Änderungen der Gesetzgebung nach Vertragsabschluss unwirksam oder undurchführbar werden, bleiben die übrigen

Vertragsbestimmungen und die Wirksamkeit des Vertrages im Ganzen hiervon unberührt. An die Stelle der unwirksamen oder undurchführbaren Bestimmung soll die wirksame und durchführbare Bestimmung treten, die dem Sinn und Zweck der nichtigen Bestimmung möglichst nahekommt. Erweist sich der Vertrag als lückenhaft, gelten die Bestimmungen als vereinbart, die dem Sinn und Zweck des Vertrages entsprechen und im Falle des Bedachtwerdens vereinbart worden wären.

(4) Im Fall von Widersprüchen zwischen diesem Vertrag und sonstigen Vereinbarungen zwischen den Parteien, insbesondere dem Hauptvertrag, gehen die Regelungen dieses Vertrags vor.

Anlage 1 - Gegenstand des Auftrags

1. Gegenstand und Zweck der Verarbeitung

Der Auftrag des Auftraggebers an den Auftragnehmer umfasst folgende Arbeiten und/oder Leistungen:

Angesichts der gegenwärtigen COVID19-Pandemie sind Kirchen und Gemeinden aufgefordert, Gottesdienste und (Gemeinde-) Veranstaltungen anders als bislang durchzuführen. Dazu werden Schutzkonzepte aufgelegt und verabschiedet müssen, die dann nur eine individuelle Maximalanzahl Teilnehmer je Veranstaltung zulassen.

Um diese Maximalanzahl zu gewährleisten sollten sich Teilnehmer vorher für einen Gottesdienst oder eine Veranstaltung registrieren können. Dadurch erhält der Teilnehmer einen Überblick, ob es für die gewünschte Veranstaltung noch verfügbare Plätze gibt, kann seinen Platz reservieren und muss nicht am Veranstaltungstag wegen Überfüllung »nach Hause« geschickt werden. Genau hierfür bietet das Buchungsportal church-events eine maßgeschneiderte organisatorische Unterstützung.

Gemeinden und christliche Werke können sich auf diesem Portal grundsätzlich kostenfrei registrieren und ihre Veranstaltungen ihren Teilnehmern einfach und eigenverantwortlich bekannt machen sowie die Teilnehmer verwalten.

Ein Auszug aus den Funktionen und Möglichkeiten von church-events:

- Deine Gemeinde bekommt ihr eigenes »Portal« und damit auch eine eigene Sub domain für Veranstaltungen. Sie könnte beispielsweise meinegemeinde.church events.de lauten und wird bei der Anmeldung festgelegt.
- Jeder, der die Webadresse Deiner Gemeinde kennt, kann sich die Veranstaltungen ansehen und dazu anmelden (unter Angabe von Namen und E-Mail). ▪ Ein Administrator (z.B. der Pastor oder Gemeindeleiter) kann Veranstaltungen anlegen, löschen und bearbeiten.
- Für jede Veranstaltung kann eine maximale Teilnehmerzahl festgelegt werden und auch definiert werden, wie viele Teilnehmer »auf einmal« angemeldet werden können.
- Es gibt eine optional nutzbare Funktion, um bestimmte »Sitzplatzanordnungen« im Raum abdecken zu können.
- Bei erfolgter Anmeldung wird man entweder in die bevorstehende Veranstaltung »eingebucht« oder gelangt auf eine Warteliste (sofern die Anzahl verfügbarer freier Plätze überschritten wurde).
- Wird ein Platz frei, so rücken Personen von der Warteliste für die Veranstaltung automatisch nach.
- Es wird eine Bestätigung über die Anmeldung versendet. In dieser E-Mail gibt es ferner einen Link, um sich wieder von einer Veranstaltung abzumelden und den Platz freizugeben.
- Der Administrator kann die Teilnehmer einsehen und auch Teilnehmer löschen (bei Abmeldungen).

Alle Daten von angemeldeten Personen werden nach einer voreingestellten Aufbewahrungszeit automatisch gelöscht.

2. Art(en) der personenbezogenen Daten

Folgende Datenarten sind regelmäßig Gegenstand der Verarbeitung:

- Vorname
- Nachname
- Wohnort / Adresse (Straße, PLZ, Ort)
- Telefonnummer
- E-Mail-Adresse
- Gemeinde
- Veranstaltungsbezogene Daten (z.B. Notfallkontakte)
- Teilnahme an Veranstaltungen (Ort / Inhalt)
- Begleiter
- Geburtstag

Abhängig von der konkreten Nutzung der Software im Einzelfall können auch besondere Kategorien der personenbezogenen Daten, vgl. Datenschutz-Grundverordnung, Artikel 9, verarbeitet werden.

3. Kategorien betroffener Person

Kreis der von der Datenverarbeitung betroffenen Personen:

- Pastoren
- Gemeindeleiter
- Mitglieder von Gemeinden
- Besucher von Veranstaltungen
- Kirchenmitglieder
- Spender/Sponsoren
- Mitarbeiter

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:

Navn	Webseite	Beschreibung der Verarbeitung
Hetzner Online	www.hetzner.de	Stellt Server in einer sicherheitszertifizierten Umgebung zur Verfügung, wo die Daten der ChurchDesk-Applikation gespeichert sind. Hetzner hat keinen Zugang zu Kundendaten.
Mailjet	www.mailjet.de	Wird für den Versand von E-Mails genutzt, welche von der ChurchDesk-Applikation versendet werden.
Stripe	www.stripe.com	Wird vom Datenverantwortlichen für die Zahlung seines ChurchDesk-Abonnements und für die Verarbeitung von Spenden in ChurchDesk genutzt.
Compaya	www.compaya.dk	Nutzung zum Versand von SMS, welche von ChurchDesk versendet werden.
Amazon Web Service	www.aws.amazon.com	Wird für den Versand von E-Mails genutzt, welche von ChurchDesk Applikation versendet werden. Kein anderen Services werden von AWS in der ChurchDesk Applikation verwendet.
Sentry	www.sentry.io	Fehlererkennung, die dafür sorgt, dass die Entwickler von ChurchDesk Fehler überwachen und in Echtzeit berichtigen können.
Google Cloud	www.cloud.google.com	Verarbeitet Adresssuchen über Google Maps und Verwahren von Metadaten über BigQuery. Keine anderen Services werden von Google in der ChurchDesk Applikation verwendet.
Upscope	www.upscope.io	Ermöglicht das Teilen des Bildschirms bei Kundenanfragen. Kunden erhalten eine Benachrichtigung wenn der Bildschirm geteilt wird.
Borgbase	www.borgbase.com	Zusätzliches sicheres Backup. Daten werden vor der Übertragung verschlüsselt. Der Standort des Datenspeichers ist in der Europäischen Union, Deutschland.

Expo	www.expo.io	Wird für die Versendung von Push-Nachrichten mit Hilfe der ChurchDesk App auf iOS oder Android Geräten verwendet.
Pushpad	www.pushpad.xyz	Pushpad erlaubt es Benutzern im Web-Browser auf Notifikationen der ChurchDesk Applikation zu abonnieren.
Stonly	www.stonly.com	Mit Stonly kann ChurchDesk digitale Leitfäden erstellen, die die optimale Nutzung von ChurchDesk ermöglicht.
Rademacher consulting	www.radermacher-consulting.de/	Rademacher Consulting betreibt für ChurchDesk die Anwendung church-events.de.

Anlage 3 - Technische und organisatorische Maßnahmen des Auftragnehmers

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

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

Informationen zum Standort von Datenverarbeitungsanlagen und Rechenzentren

Der Standort des Rechenzentrums (hauptsächlich Hosting/Housing und E-Mail-Server) liegt grundsätzlich bei der Hetzner GmbH. Die Serverstandorte befinden sich in Deutschland. Weitere Datenverarbeitungen finden Inhouse statt, ein eigenes Rechenzentrum wird allerdings nicht betrieben. Mit den Rechenzentrumsbetreibern wurden AV-Verträge abgeschlossen, die vorgelegt werden können.

Zutrittskontrolle

Maßnahmen, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen die personenbezogenen Daten verarbeitet und genutzt werden, zu verwehren:

- Zugänge zu den Büroräumen grundsätzlich verschlossen
- Zentrales Schließsystem mit Sicherheitsschlössern
- Öffnen der Zugangstüren nur mit Schlüssel und Chipschlüssel
- Besucherregelung: Abholung von Besuchern (nach Klingeln) am Eingang zum Bürotrakt
- Dokumentierte Verfahrensweise für Ausgabe und Rückgabe der Zugangsmittel
- Dokumentierte Verfahrensweise für die Meldung des Verlusts eines Zugangsmittels
- Alarmanlage und Videoüberwachung der Büroräume
- Videoüberwachung der angemieteten Bereiche in den Rechenzentren
- Spezielle Räume abschließbar. Regelung über Arbeitsanweisung.

Zugangskontolle

Maßnahmen, um zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können:

- Nur benutzte Netzwerkdosen gepatched
- WLAN nur im Büro-Bereich
- Firewall, Intrusion Detection System
- Zugang zu DV-Geräten mit persönlicher Benutzer-ID und Kennwort
- Dokumentierte Vergabe-Richtlinie für Benutzer-IDs und Kennwörter
- Zusätzliche Share-Berechtigungen
- Zusätzliches Login für spezielle Applikationen
- Zwei-Faktor-Authentifizierung
- Spezifische Kennwortverfahren: mindestens 8 Zeichen, bestehend aus Sonderzeichen, Groß- und Kleinbuchstaben sowie Zahlen (3 aus 4)

- Protokollierung der Logins und Kennwortfehleingaben
- Home Partition der Arbeitsplatzrechner verschlüsselt und allgemeine Datenträger werden nach Möglichkeit verschlüsselt
- Verbindung zur Applikation im Rechenzentrum nur über VPN
- Whitelisting / Blacklisting
- Pausenschaltung: automatische Sperrung nach angemessener Zeit
- Mobile Device Management System: Möglichkeit zur Fernlöschung und -sperrung von mobilen wie auch anderen IT Systemen
- Hardware wird regelmäßig an den Stand der Technik angepasst.

Zugriffskontrolle

Maßnahmen, 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:

- Benutzerrollen-/Gruppenkonzept
- Erteilung und Verwaltung von Benutzerrechten voneinander getrennt
- Überprüfung/Aktualisierung der Berechtigungen
- Zentrales Virenschutzprogramm mit automatischer Aktualisierung
- Zeitgesteuerte Bildschirmsperre mit Wiederanmeldung
- Bildschirme so aufgestellt, dass ein unbefugtes Lesen verhindert wird
- Papier-Shredder für Dokumentenvernichtung

Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können:

- in Datenbanken »interne Mandantenfähigkeit«
- Kontrolle der Zweckbindung erfasster Daten
- Datenbanken werden separiert
- Separierung von Tabellen und Inhalten
- Funktionstrennung nach Produktion, Test & Sandboxing
- Sofern technisch/inhaltlich möglich: Identifizierung von Datensätzen mit IDs an stelle von Klarnamen
- möglichst keine „Echtdaten“ von Kunden zur Entwicklung und Test von Programmen

2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

Weitergabekontrolle

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

- Zugang über VPN
- Verschlüsselte Übertragung soweit möglich
- Prüfung der Rechtmäßigkeit der Weitergabe von Daten
- Identifizierung / Authentifizierung
- Regelungen für Datenträgervernichtung
- wenn technisch möglich und inhaltlich nicht anders erforderlich: Weitergabe von Daten an Dritte ausschließlich in anonymisierter oder pseudonymisierter Form

Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich geprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind:

- sofern technisch möglich: Protokollierung bei Eingabe, Änderung und Löschung von Daten
- Regelungen zum Zugriff und zur Löschung der Protokolle

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. bn DSGVO)

Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, gegen zufällige Zerstörung oder Verlust geschützt sind:

- Alle Server stehen in Rechenzentren in Deutschland
- Rechenzentren sind DIN ISO 27001-zertifiziert
- Schutzmaßnahmen:
    - Geeignete Zutrittskontrollsysteme
    - Videoüberwachung
    - Redundante unterbrechungsfreie Stromversorgung
    - Überspannungsschutz
    - Schutz gegen Feuer und Wassereintritt
    - Monitoring der Leitungskapazitäten
    - Intrusion Detection System (DoS/DDoS-Angriffe)
- Redundante IT-Infrastruktur (z.B. durch Virtualisierung)
- RAID-Festplattenspeicher
- Ersatz- und Austauschkomponenten vor Ort vorhanden
- Datensicherungskonzept vorhanden
- Prüfung der Rücksicherung/Wiederherstellung
- Einheitliche Beschaffungsstrategie für Soft- und Hardware
- Virenscanner und Firewalls im Einsatz (zentrale Aktualisierung)
- Rauchverbot in Server- und PC-Arbeitsräumen
- Sichere Hinterlegung von Notfallpasswörtern

4. Technische und organisatorische Umsetzung des Rechts auf Löschung, "Recht auf Vergessenwerden" (Art. 17 DS-GVO)

Maßnahmen, die eine technische und organisatorische Umsetzung des Rechs auf Lösung bzw. das Recht auf Vergessenwerden gewährleisten:

- Möglichst randomisiertes Überschreiben
- Fernlöschung auf mobilen Endgeräten
- Zerstörung von Datenträgern vor einer Entsorgung (geschreddert oder ausreichend mechanisch deformiert)
- Sofern technisch möglich: grundsätzlich automatische Löschung von Datensätzen nach einem festgelegten Ablaufdatum

5. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden kön nen:

- Bestimmung von Ansprechpartnern und verantwortlichen Projektmanagern für den konkreten Auftrag
- Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis
- Sorgfältige Auswahl der Auftragnehmer
- Zwischen Auftragnehmer und evtl. Unterauftragnehmer werden AVV-Verträge geschlossen.

Datenschutz-Management

- Schriftliche Verpflichtung der Mitarbeiter auf Datenschutz und Geheimhaltun
- Durchführung von Datenschutz-Folgenabschätzungen bei Anforderung

Incident-Response-Management

- Einbindung Datenschutzbeauftragten in Sicherheitsvorfälle und Datenpannen
- Dokumentation von Sicherheitsvorfällen und Datenpannen
- Formaler Prozess und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen
- Belehrung der Mitarbeiter zu Datensicherheit und Verhalten bei Sicherheitsvorfällen und Datenpannen

Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 EU-DSGVO)

- Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind
- Einfache Ausübung des Widerspruchsrechts des Betroffenen durch technische Maßnahmen (Löschung, Sperren)