Datenverarbeitungsvereinbarung

1. Definitionen und Auslegung

In dieser Vereinbarung sind die folgende Wörter und Begriffe wie folgt zu verstehen:

- **„Verarbeitung**" hat die in der Datenschutzgesetzgebung angeführte Bedeutung, und **„verarbeiten**" und **„Verarbeiter**" sind dementsprechend auszulegen.
- **„Datenverantwortlicher**" hat die in der Datenschutzgesetzgebung angegebene Bedeutung.
- **„Datenverarbeiter**" hat die in der Datenschutzgesetzgebung angegebene Bedeutung.
- Unter „**geltende Gesetzgebung**" werden Gesetze, Bestimmungen oder verbindliche Richtlinien von Behörden verstanden, die bei der Verarbeitung personenbezogener Daten gemäß dieser Vereinbarung angewendet werden.
- Unter **„Behörde**" werden alle relevanten staatlichen oder gesetzlich vorgeschriebenen Organe oder Behördeninstanzen in dem betreffenden Land oder andere relevante Behörden oder Einheiten verstanden, welche für die Regelung oder Verwaltung einer Partei oder der Leistungen zuständig sind, hierunter, aber nicht darauf begrenzt, nationale Datenschutzbehörden.
- Unter „**Verletzung des Schutzes personenbezogener Daten**" werden Sicherheitsverstöße verstanden, welche zu unbeabsichtigter oder gesetzeswidriger Vernichtung, Verlust, Änderung oder zu unzulässiger Weitergabe von oder Zugang zu personenbezogenen Daten, die übertragen, aufbewahrt oder in anderer Weise verarbeitet werden, führen können.
- Unter „**Datenschutzgesetzgebung**" wird die deutsche Verordnung über die Verarbeitung personenbezogener Daten (DSGVO), die ab dem 25. Mai 2018 gilt, zumindest als in die nationale Gesetzgebung der einzelnen Mitgliedsstaaten des Europäischen Wirtschaftsraumes aufgenommen, verstanden, sowie jedwede geltende Gesetzgebung hinsichtlich der Verarbeitung von Personendaten und des Privatlebens und der Unabhängigkeit von natürlichen Personen.
- „**Personenbezogene Daten**" haben die in der Datenschutzgesetzgebung angegebene Bedeutung.
- Der „**Registrierte**" meint die betroffene Person und hat die in der Datenschutzgesetzgebung angegebene Bedeutung.
- Unter „**Drittland**" wird ein Land verstanden, welches nicht Teil des Europäischen Wirtschaftsraumes ist.
- Unter „**Leistungen**" werden die unter Punkt 3 beschriebenen Leistungen verstanden.
- Unter „**ChurchDesk-Abonnement**" werden, neben dieser Datenverarbeitungsvereinbarung, die aufgrund der Vereinbarung geltenden Bedingungen für den Abonnementbezug und die Datenschutzerklärung, die unterzeichnete Vereinbarung über Zusammenarbeit und/oder eine gezahlte Rechnung verstanden.
- Unter „**ChurchDesk-Applikation**" werden die Dienstleistungen verstanden, welche ChurchDesk dem Datenverantwortlichen zur Verfügung stellt, die in den Bedingungen für den Abonnementbezug beschrieben wurden.

Alle Verweise auf gesetzliche Bestimmungen sind so zu verstehen, dass sie sämtliche nachfolgenden weitergeltenden Bestimmungen oder Änderungsbestimmungen umfassen.

2. Allgemeine Anforderungen

Der Datenverarbeiter darf personenbezogene Daten lediglich entsprechend den dokumentierten Anweisungen des Datenverantwortlichen, wie in dieser Vereinbarung angegeben, verarbeiten, oder wenn der Datenverantwortliche dem Datenverarbeiter auf andere Weise eine schriftliche Anweisung erteilt hat.
Der Umfang der Verarbeitung personenbezogener Daten, welche durch diese Vereinbarung geregelt ist, ist auf die in Punkt 3 beschriebene Verarbeitung, „Beschreibung der Verarbeitung personenbezogener Daten“, begrenzt.
Der Datenverarbeiter darf den Inhalt personenbezogener Daten in keiner Weise ändern oder weitergeben, oder die Weitergabe einiger der personenbezogenen Daten an Dritte erlauben, es sei denn:

- dies geht konkret aus dieser Vereinbarung hervor,
- der Datenverantwortliche hat in anderer Weise eine Ermächtigung und/oder Anweisung hierzu erteilt,

und/oder

- die Verarbeitung ist gemäß geltender Gesetzgebung, welcher der Datenverarbeiter unterliegt, erforderlich,
- die Weitergabe ist von Punkt 2.8 umfasst, dann muss der Datenverarbeiter den Datenverantwortlichen, soweit es gemäß der geltenden Gesetzgebung möglich ist, darüber in Kenntnis setzen, bevor die Verarbeitung dieser personenbezogenen Daten erfolgt.

Der Datenverarbeiter hat laufend ein Verzeichnis über die Verarbeitung personenbezogener Daten sowie ein Verzeichnis über alle Sicherheitsverstöße zu führen.

2.1. Sicherheit

Der Datenverarbeiter hat dafür Sorge zu tragen und zu gewährleisten, dass seine Mitarbeiter im Hinblick auf den Schutz personenbezogener Daten angemessene technische und organisatorische Maßnahmen gegen unzulässige oder unerlaubte Verarbeitung und gegen zufälligen Verlust, Vernichtung, Beschädigung, Änderung oder Weitergabe ergreifen. Der Datenverarbeiter hat in diesem Zusammenhang die neueste Entwicklung, die Kosten der Durchführung, Art der Verarbeitung, Umfang, Zusammenhang und Zweck sowie die Gefahr für die Rechte und Freiheitsrechte für natürliche Personen zu berücksichtigen.

Der Abschnitt über Datensicherheit, vgl. Punkt 4, enthält eine allgemeine Beschreibung der technischen und organisatorischen Sicherheitsmaßnahmen. Der Datenverarbeiter muss zudem die personenbezogenen Daten, wie in der deutschen Verordnung über die Verarbeitung personenbezogener Daten sowie in eventuellen nationalen ergänzenden Regeln beschrieben, durch technische und organisatorische Sicherheitsmaßnahmen sichern.

Der Datenverarbeiter wird angemessene Schritte unternehmen, um zu gewährleisten, dass alle Mitarbeiter, Vertreter oder Vertragsparteien, welche Zugang zu personenbezogenen Daten haben könnten, zuverlässig handeln und dass alle diese Personen einer Geheimhaltungsverpflichtung oder der beruflichen oder gesetzlichen Schweigepflicht unterliegen. Der Datenverarbeiter muss außerdem sicherstellen, dass der Zugang zu personenbezogenen Daten in jedem einzelnen Fall genau auf die Personen begrenzt wird, die Zugang zu den Daten benötigen, und dass dieses erforderlich ist, um die Leistungen im Rahmen der Aufgaben der betreffenden Person beim Datenverarbeiter liefern zu können, sowie dass alle diese Personen (i) über den vertraulichen Charakter der personenbezogenen Daten informiert sind, (ii) eine entsprechende Ausbildung bezüglich der geltenden Gesetzgebung

absolviert haben, und (iii) ihnen in Verbindung mit dem Datenschutz gemäß dieser Vereinbarung die Verpflichtungen des Datenverarbeiters bekannt sind.

Der Datenverarbeiter wird mindestens einmal jährlich seine internen Sicherheitsvorschriften und Richtlinien für die Verarbeitung personenbezogener Daten im Hinblick darauf überprüfen, dass gewährleistet ist, dass die erforderlichen Sicherheitsmaßnahmen ständig beachtet wurden, vgl. Abschnitt über „Datensicherheit" bzw. Punkt 4 in dieser Vereinbarung.

2.2. Support

Der Datenverarbeiter muss den Datenverantwortlichen dabei unterstützen sicherzustellen, dass der Datenverantwortliche dem Registrierten in Bezug auf personenbezogene Daten die Wahrnehmung seiner Rechte gemäß der Datenschutzgesetzgebung ermöglichen kann, hierbei eine Beurteilung, Anfrage, Mitteilung oder Untersuchung gemäß der Datenschutzgesetzgebung ermöglichen, oder alle Angaben liefern, um die der Datenverantwortliche innerhalb einer angemessenen Frist bittet.

Der Datenverarbeiter wird den Datenverantwortlichen soweit möglich bei der Umsetzung technischer und organisatorischer Maßnahmen in der Weise unterstützen, dass der Datenverantwortliche Anfragen des Registrierten bei beispielsweise der Ausübung seiner Rechte beantworten kann, vgl. die Datenschutzgesetzgebung.

Der Datenverarbeiter muss den Datenverantwortlichen umgehend informieren, sobald dem Datenverarbeiter eine Verletzung des Schutzes personenbezogener Daten bekannt wird, und der Datenverarbeiter muss mit dem Datenverantwortlichen zusammenarbeiten und den Datenverantwortlichen in Verbindung mit der Abhilfe einer Datenschutzverletzung unterstützen. Der Datenverarbeiter darf über eine Datenschutzverletzung weder öffentlich noch mit Dritten ohne vorhergehende schriftliche Vereinbarung mit dem Datenverantwortlichen über den Inhalt einer solchen Kommunikation kommunizieren, es sei denn es besteht eine rechtliche Verpflichtung für den Datenverarbeiter zu einer solchen Kommunikation.

Der Datenverarbeiter muss beachten und dafür Sorge tragen, dass das Personal des Datenverarbeiters (i) die firmeninternen Sicherheitsmaßnahmen und alle sonstigen Maßnahmen, die dem Datenverarbeiter mitgeteilt wurden, einhält, hierunter in dem Abschnitt über Datensicherheit, (ii) alle geltende Sicherheitsanforderungen für konkrete Standorte beim Datenverantwortlichen, die dem Datenverarbeiter jeweils schriftlich mitgeteilt wurden, und (iii) die eigenen internen Sicherheitsstandards des Datenverarbeiters.
Der Datenverarbeiter ist auf Anfrage verpflichtet, unter Angabe der präzisen Adresse mitzuteilen, wo die personenbezogenen Daten des Datenverantwortlichen aufbewahrt werden. Der Datenverarbeiter muss bei jeder Änderung die Angaben dem Datenverantwortlichen gegenüber aktualisieren.

2.3. Auftragsdatenverarbeitung

Der Datenverarbeiter hat die generelle Genehmigung des Datenverantwortlichen zur Hinzuziehung von Auftragsdatenverarbeitern. Der Datenverarbeiter hat jedoch den Datenverantwortlichen über eventuell geplante Änderungen bezüglich einer zusätzlichen Verwendung oder eines Ersatzes anderer Datenverarbeiter zu unterrichten und dem Datenverantwortlichen dadurch die Möglichkeit eines Einspruchs gegen solche Änderungen zu geben. Eine solche Mitteilung muss der Datenverantwortliche mindestens 30 Tage, bevor die Verwendung oder Änderung in Kraft treten soll, vorliegen haben. Falls der Datenverantwortliche Einwendungen gegen die Änderungen hat, muss der Datenverantwortliche den Datenverarbeiter hierüber innerhalb von 14 Tagen nach Erhalt der

Mitteilung informieren. Der Datenverantwortliche kann nur Einspruch erheben, wenn der Datenverantwortliche angemessene, konkrete Gründe hierfür hat.

Die vorausgehende Zustimmung des Datenverantwortlichen ist davon abhängig, dass der Datenverarbeiter:

- eine hinreichende Untersuchung jedes einzelnen Auftragsdatenverarbeiters im Hinblick darauf durchführt, zu gewährleisten, dass dieser in der Lage ist, in Bezug auf die Verarbeitung personenbezogener Daten einen Schutz zu bieten, so wie es in dieser Vereinbarung gefordert wird,
- in den Vertrag zwischen dem Datenverarbeiter und dem einzelnen Auftragsdatenverarbeiter Bedingungen aufnimmt, die denselben Schutz bieten wie die Bedingungen in dieser Vereinbarung,

Der Datenverantwortliche kann vom Datenverarbeiter jederzeit einen Nachweis über die Existenz und und den Inhalt von Auftragsdatenverarbeiter-Vereinbarungen für die Auftragsdatenverarbeiter verlangen, die der Datenverarbeiter in Verbindung mit der Erfüllung seiner Verpflichtungen gegenüber dem Datenverantwortlichen einsetzt.

Im Falle einer Insolvenz des Datenverarbeiters kann der Datenverantwortliche sich direkt an die in Punkt 5. „Auftragsdatenverarbeiter" angegebenen Auftragsdatenverarbeiter wenden.

2.4. Genehmigung bezüglich der Übertragung personenbezogener Daten in ein Drittland

Gemäß Kapitel 5 der Datenschutz-Grundverordnung erkennt der Datenverantwortliche die Übertragung personenbezogener Daten an Datenverarbeiter bzw. Auftragsdatenverarbeiter in Drittländern an, die von der EU-Kommission als sicher klassifiziert wurden.

Der Datenverantwortliche genehmigt dem Datenverarbeiter, die in Abschnitt 5 genannten Auftragsdatenverarbeiter für die Datenverarbeitung zu verwenden.

Es kann vorkommen, dass die in Abschnitt 5 genannten Auftragsdatenverarbeiter Daten in Drittländern verarbeiten. Die in Abschnitt 5 genannten Auftragsdatenverarbeiter werden nur von ChurchDesk verwendet, wenn es gemäß Artikel 49 der DSGVO notwendig ist, um die vertraglichen Pflichten, wie in den Allgemeinen Geschäftsbedingungen festgehalten, einzuhalten.

Alle Auftragsdatenverarbeiter haben angemessene Informationssicherheitsmaßnahmen implementiert, um persönliche Daten gemäß geltendem Recht zu schützen. Die Datenschutzerklärungen und die Datenverarbeitungsvereinbarungen der Auftragsdatenverarbeiter sind mit dem Beschluss der EU-Kommission vom 5. Februar 2010 über Standardvertragsklauseln konform.

Alle persönliche Daten der besonderen Kategorien werden nur in der EU verarbeitet und nicht an Drittländer weitergeleitet.

Wenn der Datenverantwortliche bezüglich der Übertragung personenbezogener Daten in ein Drittland keine Anweisung oder Genehmigung in diesem Abschnitt oder mittels einer nachfolgenden schriftlichen Mitteilung erteilt hat, darf der Datenverarbeiter eine solche Übertragung im Rahmen der Datenverarbeitungsvereinbarung nicht vornehmen.

2.5. Einhaltung der Gesetzgebung u.a.m.

Der Datenverarbeiter muss personenbezogene Daten gemäß der Datenschutzgesetzgebung verarbeiten und verpflichtet sich, keine Handlungen vorzunehmen, zuzulassen und/oder zu unterlassen, die mit sich bringen könnten, dass der Datenverantwortliche gegen die Datenschutzgesetzgebung verstößt. Falls eine Anweisung nach Auffassung des Datenverarbeiters einen Verstoß gegen die Datenschutzgesetzgebung darstellt, muss der Datenverarbeiter den Datenverantwortlichen hierüber unverzüglich in Kenntnis setzen.

Der Datenverarbeiter verpflichtet sich, eine von dem Datenverantwortlichen oder einer anderen Kontrollperson mit Ermächtigung durch den Datenverantwortlichen durchgeführte Kontrolle, Inspektion und/oder Prüfung bezüglich der Verarbeitung von personenbezogenen Daten zu ermöglichen, vgl. Abschnitt 2.11. Kontrollen und Erklärungen.

2.6. Kündigung

Eine Kündigung der Datenverarbeitungsvereinbarung kann gemäß den Kündigungsbedingungen, einschl. Kündigungsfrist, erfolgen, was sich aus dem ”ChurchDesk-Abonnement”, mit Ausnahme des nachfolgenden Abschnitts, ergibt.

Bei Kündigung dieser Vereinbarung muss der Datenverarbeiter

- das Verarbeiten personenbezogener Daten beenden, und
- auf Wunsch des Datenverantwortlichen (i) alle personenbezogenen Daten, welche sich im Besitz des Datenverarbeiters befinden, oder über die er Kontrolle hat, sowie alle Kopien dessen an den Datenverantwortlichen zurückgeben. Der erste Export, den der Datenverarbeiter vornimmt, ist für den Datenverantwortlichen kostenfrei. Wünscht der Datenverantwortliche weiteren Export, kann der Datenverarbeiter von dem Datenverantwortlichen auf der Grundlage des Zeitaufwands für die Verarbeitung des weiteren Exports, außer für den ersten Export, eine Zahlung verlangen, (ii) alle Kopien hiervon vernichten und dem Datenverantwortlichen gegenüber bestätigen, dass dieses erfolgt ist, es sei denn, der Datenverarbeiter ist aufgrund der geltenden Gesetzgebung verhindert, oder durch eine Behörde daran gehindert, alle oder Teile der personenbezogenen Daten zu vernichten oder zurückzugeben; in diesem Fall muss der Datenverarbeiter diese Angaben vertraulich behandeln, sie weiterhin gemäß den Bedingungen dieser Vereinbarung verarbeiten und darf diese nicht in weiterem Umfang verarbeiten, als was verlangt wird, um die Anforderungen der betreffenden geltenden Gesetzgebung oder der betreffenden Behörde zu erfüllen.

Die Beendigung dieser Vereinbarung ungeachtet des Grundes hierfür beeinflusst nicht die Rechte oder Verpflichtungen der Parteien gemäß dieser Vereinbarung. Die Rechte und Verpflichtungen der Parteien haben somit weiterhin Gültigkeit nach Beendigung der Vereinbarung.

2.7. Übertragung

Mit Ausnahme von Punkt 2.3 darf der Datenverarbeiter seine Rechte oder Verpflichtungen gemäß dieser Vereinbarung in keiner Weise ohne die vorherige schriftliche Genehmigung seitens des Datenverantwortlichen ganz oder teilweise auf Dritte übertragen (oder versuchen zu übertragen).

2.8. Änderungen

Es kann lediglich rechtskräftig auf Anforderungen, Bestimmungen, Verpflichtungen oder Bedingungen in dieser Vereinbarung verzichtet werden oder es können diesbezüglich nur Änderungen erfolgen, soweit dieses schriftlich erfolgt und von einer zeichnungsberechtigten Person derjenigen Partei unterzeichnet wird, die verzichtet oder Änderungen vorzunehmen wünscht. Der Datenverarbeiter muss bei derartigen Änderungen umgehend gewährleisten, dass Auftragsdatenverarbeiter zugleich zu den Änderungen verpflichtet werden.

Falls eine Voraussetzung, eine Bedingung oder eine Bestimmung dieser Vereinbarung von einer zuständigen Behörde in dem einen oder anderen Umfang für ungültig, gesetzeswidrig oder rechtsunwirksam erklärt wird, wird diejenige Voraussetzung, Bedingung oder Bestimmung in dem betreffenden Umfang von den übrigen Voraussetzungen, Bedingungen und Bestimmungen abgetrennt, die ihrem Inhalt nach im weitest möglichen Umfang gesetzlich weiterhin zulässig ist.

Soweit Änderungen in der Gesetzgebung, vgl. Punkt 1 der Vereinbarung, oder dazugehörende Praxis, einen Anlass dazu geben, sind die Parteien mit einer Frist von 30 Tagen, und ohne dass sich hierdurch ein Zahlungsanspruch seitens der anderen Partei ergibt] berechtigt, Änderungen in der Vereinbarung vorzunehmen.

2.9. Mitteilungen

Alle Mitteilungen, die gemäß dieser Vereinbarung übermittelt werden müssen, müssen schriftlich erfolgen.

2.10. Schweigepflicht und Vertraulichkeit

Der Datenverarbeiter unterliegt – während und nach Beendigung der Vereinbarung mit ChurchDesk – der vollständigen Schweigepflicht bezüglich aller Angaben, die ihm durch die Zusammenarbeit zur Kenntnis gelangen.

Der Datenverarbeiter muss ab dem 25. Mai 2018 gewährleisten, dass alle, hierunter Angestellte, Dritte (z.B. ein Reparaturbetrieb) und Auftragsdatenverarbeiter, die Angaben verarbeiten, die unter diese Vereinbarung fallen, sich zur Vertraulichkeit verpflichten oder einer entsprechenden gesetzlichen Schweigepflicht unterliegen.

2.11. Kontrollen und Erklärungen

Der Datenverarbeiter ist verpflichtet, dem Datenverantwortlichen umgehend die erforderlichen Angaben zu übermitteln, damit der Datenverantwortliche sich jederzeit rückversichern kann, dass der Datenverarbeiter die Bedingungen, die sich aus dieser Vereinbarung ergeben, einhalten kann.

Der Datenverantwortliche, ein Vertreter des Datenverantwortlichen oder dessen Prüfer (sowohl intern als auch extern) haben Zugang, um beim Datenverarbeiter Inspektionen und eine Prüfung vorzunehmen, sich Dokumentationen, hierunter Protokolle, aushändigen zu lassen, können Fragen stellen u.a.m., um feststellen zu können, ob der Datenverarbeiter die Anforderungen, die sich aus dieser Vereinbarung ergeben, einhält. Die Kosten in Verbindung mit der Überprüfung des Datenverarbeiters durch den Datenverantwortlichen werden vom Datenverantwortlichen übernommen.

Es wird vereinbart, dass der Datenverarbeiter jährlich eine eigene Aufsicht darüber führt, dass die Auftragsdatenverarbeiter eine Prüfung ihrer Datensicherheit ermöglichen.

Dem Datenverantwortlichen obliegt – falls es als erforderlich erachtet wird – die Entscheidung darüber, ob eine Überprüfung des Auftragsdatenverarbeiters durchgeführt wird. Dies kann aktuell werden, falls der Datenverantwortliche vermutet, dass die Beaufsichtigung des Auftragsdatenverarbeiters durch den Datenverarbeiter dem Datenverantwortlichen keine hinreichende Sicherheit gegeben hat, dass die Verarbeitung beim Auftragsdatenverarbeiter gemäß dieser Datenverarbeitungsvereinbarung erfolgt.

Im Falle dessen, dass der Datenverantwortliche beabsichtigt, eine Inspektion der oben genannten Maßnahmen gemäß dieser Vereinbarung vorzunehmen, kann der Datenverantwortliche eine Inspektion vornehmen, indem er Zeit und Ressourcen hierfür zur Verfügung stellt.

2.12. Anzuwendendes Recht

Diese Vereinbarung unterliegt dem deutschem Recht und ist gemäß dem deutschen Recht auszulegen, und alle Parteien erkennen das Stadtgericht Berlin als ausschließlichen Gerichtsstand an.

3. Beschreibung der Verarbeitung personenbezogener Daten

Dieser Abschnitt enthält Angaben über die Verarbeitung personenbezogener Daten durch den Datenverarbeiter zur Verwendung für die Lieferung von Leistungen.

3.1. Zweck der Verarbeitung

Die Verarbeitung der Daten des Datenverantwortlichen erfolgt gemäß dem Zweck und den Leistungen, so wie es in dem „ChurchDesk-Abonnement" beschrieben ist.
Der Datenverarbeiter darf die Daten nicht zu anderen Zwecken verwenden.
Die Daten dürfen nicht auf Anweisung anderer als dem Datenverantwortlichen verarbeitet werden.

3.2. Allgemeine Beschreibung der Verarbeitung

Die übertragenen personenbezogenen Daten werden folgenden Verarbeitungen unterzogen:

- Sammeln, Registrieren, Organisieren, Systematisieren, Speichern, Anpassen oder Ändern, Datenrettung, Suche, Verwendung, Weitergabe durch Übertragung, Vermittlung oder jedwede andere Form von Überlassung, Zusammenstellen oder Koordinieren, Beschränken, Löschen oder Vernichten.

3.3. Arten personenbezogener Daten

Die Verarbeitungen enthalten personenbezogene Daten in den unten angegebenen Kategorien. Das Sicherheitsniveau für die Verarbeitung durch den Datenverarbeiter und eventuelle Auftragsdatenverarbeiter muss die Sensibilität der Daten widerspiegeln, vgl. Abschnitt über Datensicherheit.

Art und Umfang der verarbeiteten personenbezogenen Daten richten sich nach dem “ChurchDesk-Abonnement”. Die konkreten Datenarten sind dabei abhängig vom Umfang der Nutzung im Einzelfall durch den Datenverantwortlichen. Zu den verarbeiteten personenbezogenen Daten gehören jedenfalls insbesondere:

- Name
- Kontaktdaten (E-mail-Adresse, Anschrift, Telefonnummer)
- Geburtstag
- Veranstaltungsbezogene Daten (z.B. Notfallkontakte).

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

- religiöse Anschauung
- Gesundheitsdaten
- Rasse oder ethnische Herkunft
- politische Meinung
- weltanschauliche Überzeugung
- Gewerkschaftszugehörigkeit
- sexuelle Orientierung

3.4. Kategorien registrierter Personen

Es werden Daten der folgenden Kategorien registrierter Personen verarbeitet:

- Kirchenmitglieder
- Potenzielle Mitglieder
- Spender/Sponsoren
- Mitarbeiter

4. Datensicherheit

4.1. Zweck der Sicherheitsmaßnahmen

Dieser Abschnitt verweist auf eine Beschreibung der technischen und organisatorischen Sicherheitsmaßnahmen, wofür der Datenverarbeiter gemäß der Datenverarbeitungsvereinbarung die Verantwortlichkeit für die Umsetzung hat.

Die Sicherheitsmaßnahmen werden dokumentiert und aktualisiert, wenn sich Änderungen ergeben.

Die technischen und organisatorischen Maßnahmen unterliegen künftigen technischen Fortschritten und Entwicklungen. In dieser Hinsicht hat der Datenverantwortliche die Genehmigung, alternative, geeignete Maßnahmen durchzuführen, die nicht unter das Sicherheitsniveau früher festgelegter Maßnahmen fallen dürfen. Wesentliche Änderungen sind zu dokumentieren.
Der Datenverarbeiter führt folgende technische und organisatorische Sicherheitsmaßnahmen durch, um ein Sicherheitsniveau zu gewährleisten, welches der vereinbarten Verarbeitung entspricht und welches damit Artikel 32 der Datenschutz-Grundverordnung erfüllt.

Die Maßnahmen werden aufgrund folgender Überlegungen festgelegt:

- Was lässt sich aus technischer Sicht realisieren?
- Kosten der Implementierung
- Charakter, Umfang, Zusammenhang und Zweck der betreffenden Verarbeitung, vgl. Punkt 3 „Beschreibung der Verarbeitung personenbezogener Daten”
- Die Konsequenzen für die Bürger bei einem Sicherheitsverstoß
- Das Risiko, das mit den Verarbeitungen verbunden ist, hierunter das Risiko
    - einer Vernichtung der Daten
    - eines Verlustes der Daten
    - einer Änderung der Daten
    - einer unbefugten Weitergabe der Daten
    - eines unbefugten Zugriffs auf die Daten

Die Maßnahmen sind durchzuführen um zu vermeiden, dass personenbezogene Daten:

- vernichtet werden, verloren gehen, geändert oder beeinträchtigt werden,
- zur Kenntnis von Unbefugten kommen oder missbraucht werden, oder
- im Übrigen gesetzeswidrig verarbeitet werden, vgl. Punkt 1 der Vereinbarung.

4.2. Allgemeine Sicherheitsmaßnahmen

Datenzentrum

- Unsere Datenzentren handhaben die physische Sicherheit 24/7 mit Videoüberwachung mit hohen Sicherheitsschwellen rund um das ganze Datenzentrum. Zutritt über elektronische Zugangskontrollterminals mit einem Transponderschlüssel oder einer Zugangskarte. Ultramoderne Überwachungskameras für die Rund-um-die-Uhr-Überwachung der Zugangswege, Eingänge, Verriegelungssysteme der Sicherheitstür und des Serverraums und der gewöhnlichen hochtechnologischen Gegenstände, die sich gewöhnlich in Datenzentren befinden, die Datenzentren immer ausschießen.
- Wir haben in allen unseren Datenzentren einen DDOS-Schutz vor Ort installiert.

Schutz gegen Datenverlust

- Kontendaten werden auf verschlüsselte Festplatten aufbewahrt.
- Firewalls von Hetzner schützen, zusammen mit unseren eigenen network access control lists (ACL’s), vor unbefugtem Zugang zu unseren Servern.
- Täglich werden eine Spiegelung und eine Sicherung der Kontendaten vorgenommen. Backups werden auf logisch und physisch separaten Servern an unserem Hauptdatencenter (Hetzner Falkenstein, Deutschland) aufbewahrt. Darüber hinaus werden Kopien der Backups an einer unterschiedlichen geographischen Lage gespeichert (Hetzner Nürnberg, Deutschland und Hetzner Tuusula/Helsinki, Finland).
- Backups werden verschlüsselt aufbewahrt.
- Backups werden 60 Tage lang aufbewahrt.

Sicherheit auf Programmebene

- Zugangscodes für Benutzerkonten werden durch Nutzung einer kryptografischen Hash-Funktion aufbewahrt.
- Ihr Passwort kann nicht abgerufen werden. Es ist zurückzusetzen.
- Alle Login-Seiten (von unserer Webseite und mobilen Webseite) übertragen Daten über SSL.

- Die ganze Applikation ist mit SSL verschlüsselt.
- Ein Login wird nach wiederholten fehlgeschlagenen Versuchen blockiert.

Interne IT-Sicherheit

- Alle Mitarbeiter werden vom Datenverarbeiter in Schutz von Kundendaten geschult. Der Datenverarbeiter hat interne Richtlinien zum Schutz von Kundendaten implementiert, welche in Übereinstimmung mit der Datenschutz-Grundverordnung sind.

4.3. Autorisierung und Zugangskontrolle

Alle Mitarbeiter beim Datenverarbeiter, welche Zugang zu persönlichen Daten haben, wurden vom Datenverarbeiter autorisiert. Die Autorisierungen beschreiben den Zweck des Zugangs des Mitarbeiters. Mitarbeiter haben nur Zugang zu persönlichen Daten für betriebliche oder technische Zwecke.

Mitarbeiter beim Datenverarbeiter haben keinen Zugang zu persönlichen Daten, die in ihrer Autorisierung nicht enthalten sind. Der Datenverarbeiter hält die Anzahl der Autorisierungen auf einem Minimum.

Der Datenverarbeiter verifiziert und aktualisiert die Autorisierungen laufend. Autorisierungen werden geändert oder annulliert, wenn ein Mitarbeiter seine Stelle, Verantwortlichkeit oder sein Anstellungsverhältnis wechselt.

Alle Änderungen der Autorisierungen werden vom Datenverarbeiter protokolliert.

4.4. Verarbeitung von Datenmaterial, welches personenbezogene Daten enthält

Die übertragenen personenbezogenen Daten werden folgenden grundlegenden Verarbeitungen unterzogen:

- Aufbewahrung
- Zugang für den Kundenservice
- Bei Anfragen an den und von dem Kundenservice
- Entsprechend ihrer Nutzung von Funktionen bei ChurchDesk
- Missbrauchsnachweis, Vorbeugung und Beseitigung
- Erhaltung, Verbesserung und Lieferung unserer Dienste.

Der Datenverantwortliche erlaubt dem Datenverarbeiter ausdrücklich, auf die folgenden Anfragen zu reagieren, welche er direkt vom Datenverantwortlichen erhält: Abmeldungen, Updates der Daten, Entfernung von Daten oder Blockieren von Daten der registrierten Personen, welche im System des Datenverarbeiters gespeichert sind.

Der Datenverantwortliche erlaubt dem Datenverarbeiter ausdrücklich Daten zu senden, und zur Förderung der Nutzung von ChurchDesk die Kommunikation des Datenverantwortlichen mit den Nutzern der ChurchDesk-Applikation. Die Kommunikation seitens ChurchDesk kann vom Verhalten des Nutzers bei der Nutzung der ChurchDesk Applikation anhängig sein.

Der Datenverantwortliche kann die eingegebenen Daten der ChurchDesk Applikation jederzeit löschen, wonach der Datenverantwortliche nicht länger auf die Daten zugreifen kann. Die Daten

können nach Kontakt mit dem Support innerhalb eines Zeitraumes von 60 Tagen wiederhergestellt werden. Der Datenverarbeiter kann für die Wiederbeschaffung der durch den Datenverantwortlichen gelöschten Daten eine Zahlung verlangen. Nach 60 Tagen sind die Daten vernichtet und können nicht mehr wiederhergestellt werden.

Bei Kündigung des Vertrages werden alle eingegebenen Daten in der Datenbank 60 Tage nach der Kündigung automatisch gelöscht.

Nach der Löschung sind Daten im Backup vorzufinden, siehe Abschnitt „Schutz gegen Datenverlust".

Externe Kommunikationsverbindungen

Die Kommunikation zwischen dem Nutzer bei dem Datenverantwortlichen und der ChurchDesk-Applikation ist sowohl über die Webapplikation als auch über mobile Apps verschlüsselt. Die Kommunikation zwischen anonymen Nutzern und Zahlungen oder Formularen ist ebenfalls verschlüsselt. Die Server sind so aufgestellt, dass eine Kommunikation nur über verschlüsselte Verbindungen möglich ist und leiten den Nutzer sofort zu einer verschlüsselten Verbindung weiter, falls der Nutzer versucht, eine unsichere Verbindung aufzubauen.

Gewöhnliche E-Mail- und SMS-Kommunikation mit den registrierten Personen kann nicht verschlüsselt werden. Daher bestätigt der Datenverantwortliche durch seine Unterschrift, dass keine personenbezogenen Informationen in E-Mails und SMS, die über ChurchDesk versendet werden, enthalten sind.

Protokollierung

Alle Zugänge und Zugangsversuche in die ChurchDesk Applikation werden automatisch für 31 Tage protokolliert. Dieses schließt IP-Adresse, Zeitpunkt und Nutzeridentifikation ein.

Die Registrierung enthält Informationen über Zeitpunkt, Nutzer und den Art der Anwendung. Das Protokoll wird für 31 Tage Aufbewahrt, wonach es gelöscht wird.

Heimarbeitsplätze

Die Verarbeitung personenbezogener Daten durch den Datenverarbeiter erfolgt teilweise durch Nutzung von Heimarbeitsplätzen.

Mitarbeiter beim Datenverarbeiter können mit denselben Sicherheitsmaßnahmen wie in „Externe Kommunikationsverbindungen" beschrieben von externen Standorten in die Applikation. Alle Mitarbeiter sind angewiesen, nur Arbeitscomputer zu nutzen, welche eine vollständige Verschlüsselung der Festplatte haben.

Ein Zugang zu Servern für betriebliche oder technische Zwecke kann lediglich durch die Nutzung eines verschlüsselten Fernzugangs erfolgen, SSH.

5. Auftragsdatenverarbeiter

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.com	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 die Verarbeitung von Spenden an den Datenverantwortlichen 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.

6. Unterschriften: Datenverarbeitungsvereinbarung*

Zwischen

Organisationsnamen einsetzen:
Adresse:
Ort:
(der „Datenverantwortliche")

und

Churchdesk GmbH
Friedrichstraße 123
10117 Berlin
(„der Datenverarbeiter ")

jeder für sich genannt „Partei" und zusammen genannt „die Parteien"

wurde die Datenverarbeitungsvereinbarung („Datenverarbeitungsvereinbarung" oder „Vereinbarung") geschlossen.

_____, _____ 20_____

Für:

_____

Kopenhagen, _____

Für Churchdesk GmbH:

_____
Christian Steffensen
Geschäftsführer

*Für ChurchDesk ist die elektronische Bestätigung der Datenverarbeitungsvereinbarung rechtlich verbindlich. Diese Unterschriftsseite ist der Datenverarbeitungsvereinbarung beigefügt, für die interne Verwendung in der Kirche.