Data Processor Agreement

1. Definitions and interpretation

On 25 May, 2018, the Act on Processing of Personal Data will be replaced by Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (hereinafter referred to as the General Data Protection Regulation), and the Agreement becomes effective when the General Data Protection Regulation and any national residual rules in Denmark replace the Act on Processing of Personal Data, including the directive on security and the security guide. Reference is furthermore made to clause 2.9 of the Agreement.

The Agreement incorporates the requirements put forward by the rules in the General Data Protection Regulation with regard to data processor agreements. Where additional requirements appear from the General Data Protection Regulation or national residual rules after the time where the Agreement is entered into, the parties shall agree that such necessary changes to the Agreement are made to ensure compliance with the requirements. Reference is furthermore made to section 2.9 of the Agreement.

The data controller is obligated to inform the data processor about the data controller's IT security regulations, IT security policy and to follow any associated supplemental IT security rules, and the data processor is obligated to review these.

In this Agreement, the following words and expressions will have the following meanings:

- "**Processing**" means what is set out in the Act on processing of personal data, and "**Process**" and "**Processor**" must be interpreted accordingly.
- The **"Data controller**" means what is specified in the Act on processing of personal data.
- The **"Data processor"** means what is specified in the Act on processing of personal data.
- **"Applicable law"** means acts, rules or binding guides from authorities which apply to the processing of personal data under this Agreement.
- **"Authority"** means all relevant government or statutory bodies or authorities in the country in question or other relevant authorities or units responsible for the regulation or management of a party or the services including, without limitation, national data protection authorities.
- "Personal data breach" means a breach of security which may lead to accidental or unlawful destruction, loss, alteration or unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.
- As of 25 May 2018, **"Act on processing of personal data"** means the General Data Protection Regulation, in each instance as incorporated into national legislation of the individual member states of the European Economic Area as well as all applicable legislation concerning processing of personal data and natural persons' privacy and independence.
- **"Personal Data"** has the meaning specified in the Act on processing of personal data.
- The **"Data Subject"** has the meaning specified in the Act on processing of personal data.
- **"Third Country"** means a country which is not part of the European Economic Area.
- **"Services"** means [the services described in clause 3 of the section].
- In addition to this Data processor agreement, **"ChurchDesk Subscription"** shall mean the Terms of Service and Privacy Policy as made applicable through the Agreement, the signed Service Order and/or a paid invoice.
- **"ChurchDesk Application"** means services provided by ChurchDesk to the data controller as defined in the Terms of Service.

All references to legal provisions shall be considered to include all subsequently re-enacted provisions or amendment provisions.

2. General requirements

The data processor may only process the personal data in accordance with documented instructions from the data controller as specified in this Agreement or where the data controller has provided written instructions to the data processor by other means.

The scope of the processing of personal data governed by this Agreement, is limited to the processing described in clause 3. "Description of processing of personal data".

The data processor may not alter the content of the personal data in any manner or disclose or allow disclosure of any of the personal data to a third party, unless:

- it is specifically indicated in this Agreement,
- the data controller has authorised this and/or provided instructions hereto by other means, and/or
- the processing is required in accordance with applicable legislation which the data processor is governed by.
- disclosure is covered by clause 2.9., the data processor must as far as possible according to applicable law notify the data controller before processing the personal data.

The data processor must, on an ongoing basis, keep a record of the processing of personal data as well as a record of all security breaches.

2.1. Security

The data processor must implement and ensure that the data processor's staff implement technical and organisational measures appropriate to protect personal data against unauthorised or unlawful processing and against accidental loss, destruction, damage, alteration or disclosure. For those purposes, the data processor must take into account the latest developments, the costs of implementation, the nature, scope, context and purposes of the processing and the risk to the rights and freedoms of natural persons. The section on Data security as referred to in clause 4, provides a general description of the technical and organisational security measures. The data processor must furthermore secure personal data through technical and organisational security measures as set out in the General Data Protection Regulation and any national residual rules.

The data controller should take reasonable steps to ensure that all staff, representatives or contractual parties who may have access to the personal data are reliable and that all these persons are subject to confidentiality obligations or business or legal obligations of professional secrecy. Furthermore, the data processor must ensure that access to the personal data is in all cases carefully limited to persons who require access to the data and that this access is necessary in order to provide the services within the context of such persons' tasks for the data processor and that such persons (i) have been informed about the confidential nature of the personal data, (ii) have completed the relevant training with regard to applicable law, and (iii) are aware of the obligations of the data processor with regard to data protection under this Agreement.

At least once a year, the data processor must review his or her internal security instructions and guidelines for processing of personal data for the purposes of ensuring that the necessary security

measures are observed at all times in accordance with the section on "Data security" clause 4 of this agreement.

2.2. Assistance

The data processor will assist the data controller in ensuring that the data controller can comply with the data subject's exercise of his or her rights under the Act on processing of personal data with regard to personal data, including compliance with an assessment, inquiry, communication or investigation under the Act on processing of personal data or provide all the information requested by the data controller within a reasonable time limit.

The data processor will assist the data controller in completing technical and organisational measures where possible in order to allow the data controller to respond to requests for example for the exercise of the rights of the data subject in accordance with the Act on processing of personal data.

As soon as the data processor becomes aware of a personal data breach, the data processor must, without undue delay, notify the data controller, and the data processor will cooperate with and assist the data controller with regard to addressing such personal data breach. The data processor should not make any communication about the personal data breach, neither publicly nor to third parties, without prior written agreement with the data controller regarding the content of this communication, unless the data processor has a legal obligation to provide such communication.

The data processor must comply with and ensure that the data processor's staff comply with (i) the security policy and all other policies which have been provided to the data processor, including in the section on Data security, (ii) all applicable security requirements for the data controller's concrete locations which have been communicated to the data processor in writing at all times, and (iii) the data processor's own internal security standards.

The data processor is obligated to respond to inquiries with precise address information as to where the data controller's personal data are stored. The data processor will keep the data up to date vis-à-vis the data controller following any alteration.

2.3. Processing of sub data

The data processor has obtained a general authorisation from the data controller to use sub-processors. The data processor will, however, notify the data controller of any intended changes concerning the addition or replacement of other data processors, thereby giving the data controller the opportunity to object to such changes. Such communication must be received by the data controller no later than 30 days before application or before the change becomes effective. Where the data controller has objections to the changes, the data controller must notify the data processor within 7 days of receipt of the information. The data controller may only object where the data controller has fair and concrete reasons for doing so.

The prior consent of the data controller is conditional upon the data processor:

- carrying out adequate due diligence investigation of the individual sub-processor for the purposes of ensuring that said sub-processor is able to provide the level of protection with regard to processing of personal data which is required under this Agreement,
- ensuring that the agreement between the data processor and the individual sub-processor includes terms which provide the same protection as the terms of this Agreement.

The data controller will at any time be entitled to request documentation from the data processor of the existence and content of sub-processor agreements for the sub-processors used by the data processor for the purpose of fulfilling the data processor's obligations toward the data controller.

In the event of the data processor going into winding-up proceedings, the data controller may make direct contact with the sub-processors specified in clause "5. Sub-processor".

2.4. Authorisation relating to the transfer of personal data to third countries

Pursuant to chapter 5 of the data protection regulation, the data controller authorises the transfer of personal data to data processors/sub-processors in third countries which have been classified as safe by the European Commission.

The data controller authorises the data processor/sub-processors in the United States which have been authorised through the "Privacy Shield" agreement between the European Commission and the United States.

Where the data controller has not provided instructions either in this section or by means of a subsequent written communication relating to the transfer of personal data to a third country, the data processor will not carry out such a transfer within the framework of the Data processor agreement.

2.5. Compliance with legislation, etc.

The data processor will process personal data in accordance with the Act on processing of personal data and is under an obligation to not carry out, allow and/or omit actions which may result in the data controller's violation of the Act on processing of personal data. Where the data processor is of the opinion that an instruction constitutes a violation of the act on processing of personal data, the data processor must promptly notify the data controller.

The data processor is obligated to enable control, inspection and/or review by the data controller or by any other person who has been authorised to do so by the data controller with regard to processing of personal data as referred to in section 2.12. Controls and declarations.

2.6. Termination

Termination of the Data processor agreement may be made in accordance with the conditions of termination, including termination notice as specified in the "ChurchDesk Subscription" with the exception of the following section:

In connection with termination of this Agreement, the data processor will

- discontinue processing of the personal data, and
- following request from the data controller, (i) return all personal data which are in the data processor's possession or which he or she has control over as well as all copies thereof to the data controller. The first export made by the data processor is provided without costs for the data controller. Where the data controller requires additional export, the data processor may demand payment from the data controller based on time incurred for processing of further export in addition to the first export, (ii) destroy all copies thereof and confirm with the data controller that it has taken place, unless the data processor, by virtue of applicable law, is restricted, or prevented by an authority, from destroying or returning all or part of the personal

data, and in such a case the data processor must process those data confidentially, continue to process them in accordance with the terms of this Agreement, and may not process them on a more considerable scale than what is required in order to comply with the requirements found in the applicable law or from the authority in question.

Whatever the reason, the termination of this Agreement does not affect the rights or obligations of the parties under this Agreement. Consequently, the rights and obligations of the parties remain in force after termination of the Agreement.

2.7. Assignment

With the exception of clause 2.3., the data processor will not in any way, in whole or in part, assign (or attempt to assign) his or her rights or obligations under this Agreement to a third party without the prior written consent of the data controller.

2.8. Completeness of agreement

The parties agree that this Agreement is the complete agreement between the parties concerning the subject matter hereof. To this extent, this Agreement supersedes any and all prior agreements between the parties about the subject matter of the Agreement.

2.9. Changes

No waiver or changes of the terms, conditions or obligations in this Agreement will be valid unless this is done in writing and signed by a person authorised to sign for and on behalf of the party providing the waiver or requiring the changes. In the event of such changes, the data processor will, without undue delay, ensure that sub-processors are also bound by the changes.

If any term or condition of this Agreement is found to be invalid, unlawful or unenforceable to a certain extent by a competent authority, the term or condition shall, in the scope required, be severed from the remaining terms and conditions which will remain in effect according to their content to the maximum extent possible by law.

To the extent changes in legislation, as referred to in clause 1. of the Agreement or associated practices, give rise hereto, the parties are entitled to carry out changes of the Agreement with a notice of [30 days and without resulting requirements of payment from the other party].

2.10. Communication

All communication to be provided in accordance with this Agreement must be in writing.

2.11. Secrecy and confidentiality

During the term of the ChurchDesk Agreement and after it's termination, the data processor is subject to an obligation of secrecy with regard to all data which said data processor obtains knowledge of through the cooperation.

As of 25 May 2018, the data processor must ensure that everyone processing data covered by the Agreement, including staff, third parties (for example repairers) and sub-processors, are subject to an obligation of confidentiality or covered by relevant statutory obligation of secrecy.

2.12. Controls and declarations

The data processor will, without undue delay, provide the data controller with requested information so that the data controller may at all times ensure that the data processor is capable of complying with the requirements arising from this Agreement.

The data controller, a representative of the data controller or data controller's audit (both internal and external) has access to carry out inspections and audits at the data processor's, to receive documentation, including logs, ask questions, etc. for the purpose of determining that the data processor comply with the requirements arising from this Agreement. Costs in connection with the data controller's inspection of the data processor are taken over by the data controller.

It is agreed that the data processor will conduct yearly supervision to ensure that the sub-processors enable audit of their data security.

Where it is deemed necessary, the data controller may choose to initiate audit of the sub-processor. This may happen if, according to the data controller's assessment, the data processor's supervision of the sub-processor has not provided the data controller with adequate security that the processing at the sub-processor's location is carried out in accordance with this Data processor agreement.

In the event that the data controller wants to carry out inspection of the above mentioned measures pursuant to this Agreement, the data controller may carry out an inspection by allocating the necessary time and resources.

2.13. Choice of applicable law

This Agreement will be governed by and construed in accordance with Danish legislation, and all parties acknowledge Københavns Byret (Copenhagen District Court) as exclusive jurisdiction.

3. Description of processing of personal data

This section provides information about the data processor's processing of personal data for provision of the Services.

3.1. Purposes of the processing

Processing of the data controller's data is carried out in accordance with the purposes and services described in "ChurchDesk Subscription".

The data processor is not allowed to use the data for other purposes.

The data may only be processed on instructions received from the data controller.

3.2. General description of the processing

The transferred personal data will be subjected to the following processing:

- Collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, search, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

3.3. Type of personal data

The processing operations contain personal data in the categories specified below. The level of security of processing provided by the data processor and any sub-processors should reflect the sensitivity of the data, in accordance with the section on Data security.

Ordinary personal data as per Article 6 of the General Data Protection Regulation:

- Ordinary personal data

Information about social security number

- Social security numbers

Special categories of personal data in accordance with Article 9 of the General Data Protection Regulation:

- Religious beliefs
- Health
- Racial or ethnic background
- Political opinions
- Philosophical beliefs
- Trade union membership
- Sexual orientation

3.4. Categories of data subjects

Data about the following categories of data subjects will be processed:

- Members
- Potential members
- Donors/sponsors
- Staff

4. Data security

4.1. Purpose of the security measures

This section refers to a description of the technical and organisational security measures which the data processor is responsible for implementing under the Data processor agreement.

The security measures are documented and will be updated if there are changes.

The technical and organisational measures are subject to future technical advancements and developments. For this purpose, data controllers are permitted to implement alternative, suitable measures which may not fall below the security level for the measures previously set out. Important changes must be documented.

The data processor will implement the following technical and organisational security measures to ensure a level of security appropriate to the processing operations agreed upon and which thus fulfil Article 32 of the General Data Protection Regulation.

The measures are determined according to the following considerations:

- What is technically possible
- Costs of implementation
- The nature, scope, context and purpose of the processing in question in accordance with clause "3. Description of processing of personal data"
- The consequences of a security breach for the citizens
- The risk associated with the processing operations, including the risk of
    - destruction of the data
    - loss of the data
    - change of the data
    - unauthorised disclosure of the data
    - unauthorised access to the data

The measures are implemented to avoid that the personal data should be:

- destroyed, lost, altered or adversely affected,
- are made available to unauthorised persons or misused, or
- otherwise processed in infringement of the law, as referred to in clause 1 of the Agreement.

4.2. General security measures

Data centre

- Our data centres handle physical security 24/7 with video monitoring with high security boundaries around the entire data centre. Entrance via electronic access control terminals using a transponder key or access card. Ultra-modern surveillance cameras for 24-hour monitoring of access ways, entrances, locking systems for security doors and server rooms and the usual high technology appliances which are always found in data centres.
- We have established DDOS protection in all our data centres.

Protection against loss of data

- Account data are stored on encrypted hard disks.
- Together with our own network access control lists (ACLs), Hetzner's firewalls safeguard against unauthorised access to our servers.
- Account data are mirrored and backed up on a daily basis. Backups are stored on logical and physically separate servers at our main datacenter (Hetzner Falkenstein, Germany). Furthermore backups are copied and stored at a different geographical location (Hetzner Nuremberg, Germany).
- Backups are stored in encrypted state.
- Backups are kept for 60 days.

Security at application level

- Access codes for user accounts are stored using a cryptographic hash function.
- You cannot fetch your password. It must be reset.
- All login pages (from our home page and mobile site) transfer data via SSL.
- The entire application is SSL encrypted.
- Login is blocked after recurring failed attempts.

Internal IT security

- All members of staff receive instructions from the data processor with regard to protection of client data. The data processor has implemented internal guidelines for protection of client data which are in compliance with the data protection regulation.

4.3. Authorisation and access control

All the data processor's members of staff who have access to personal data have been authorised by the data processor. Authorisations describe the purpose of staff members' access. Staff only have access to personal data for operational or technical purposes.

The data processor's staff do not have access to personal data which are not covered by their authorisation. The data processor will keep the number of authorisations at a minimum.

The data processor verifies and updates authorisations on an ongoing basis. Authorisations are changed or cancelled when a member of staff changes job title, area of responsibility or conditions of employment.

All changes of authorisations are logged by the data processor.

4.4. Processing of data material which contains personal data

The transferred personal data will be subjected to the following basic processing:

- storage
- access for customer service
- contact to and from customer service
- in compliance with your use of ChurchDesk functions
- detection of misuse, prevention and remediation
- maintaining, improving and providing our services.

The data controller explicitly allows the data processor to respond to the following requests received directly from the data subjects: unsubscriptions, data updates, removal of data or blocking of data subject's data which are stored in the data processor's system.

The data controller explicitly allows the data processor to send information and communication to enhance the use of ChurchDesk to the data controller's users of the ChurchDesk Application. The communication from ChurchDesk may depend on the behaviour of the users of the ChurchDesk Application.

The data controller may at any time delete data entered into the ChurchDesk Application, after which the data can no longer be accessed by the data controller. The data may be restored following communication with support within a period of 60 days. The data processor may demand payment for restoring data deleted by the data controller. After 60 days the data are destroyed and can no longer be restored.

In connection with termination of the Agreement, all data entered into the database are automatically deleted 60 days after termination.

Following deletion, the data can be found in backup; please refer to the section "Protection against loss of data".

External communications links

Communication between the user at the data controller and the ChurchDesk Application is encrypted both for web application and mobile apps. Communication between anonymous users and payments or forms is also encrypted. The servers are configured to allow communication only via encrypted connections and promptly redirects the user to an encrypted connection in case the user attempts to create an insecure connection.

Ordinary mail and text communications to the data subject cannot be encrypted. With his or her signature, the data controller therefore verifies that no personal data will be included in mails and texts sent via ChurchDesk

Logging

All access and attempted access to the ChurchDesk Application are automatically logged for six months. This includes IP address, time and user identification.

This recording comprises information about time, user and type of use. The log is retained for six months and subsequently deleted.

Work places at home

The data processor's processing of personal data is partly carried out via the use of work places at home.

The data processor's staff can access the application from external locations featuring the same security measures as described in "External communications links". All members of staff have been instructed in using only work computers with full encryption of the hard disk.

Access to servers for operational or technical purposes is only possible when using encrypted remote access, SSH.

5. Sub-processors

Name	Home page	Description of processing
Hetzner Online	www.hetzner.de	Provides servers in a security certified environment where the data from the ChurchDesk Application are stored. Hetzner do not have access to client data.
Mailjet	www.mailjet.com	Used for forwarding mails sent from the ChurchDesk Application.
Stripe	www.stripe.com	Used for the data controller's payment of ChurchDesk Subscription and for handling donations to the data controller.
Compaya	www.compaya.dk	Used for forwarding texts from ChurchDesk.
Amazon Web Service	aws.amazon.com	Used for forwarding mails sent from ChurchDesk.
Sentry	www.sentry.io	Error detection which ensures that ChurchDesk's developers are able to monitor and correct errors in real time.

Intercom	www.intercom.com	Enable secure processing of inquiries from the ChurchDesk chat. Used by ChurchDesk for communication with the users of ChurchDesk.
Google Cloud	www.cloud.google.com	Handles address searches via Google Maps.
Hubspot	www.hubspot.com	Processes data from visitors to the home page, used to send newsletters to users of ChurchDesk and for handling written communication and communication by telephone to and from customer service.
Upscope	www.upscope.io	Used for screen sharing with customers, if necessary to resolve a support request. Users will be notified before screen sharing is started.
Borgbase	www.borgbase.com	Additional secure back-up. Data is encrypted before being transferred. Location of encrypted data storage is in the European Union, Germany.
Helpscout	www.helpscout.com	Enable secure processing of inquiries from the ChurchDesk chat. Used by ChurchDesk for communication with the users of ChurchDesk.
Aircall	www.aircall.io	IP-Phone used to handle communication via mobile and telephone to and from customer service.

Signatures: Data Processor Agreement*

Between

Insert organisation name:
Address:
City:
(the "Data controller")

and

Churchdesk ApS
Njalsgade 21G, 3.
2300 København S
CVR-nr. 32150489
(the "Data processor")

Separately called a "Party" and collectively called the "Parties"

the Data Processing Agreement is hereby entered into (the "Data Processor Agreement" or the "Agreement").

_____, _____ 20_____

For:

_____

Copenhagen, _____

For Churchdesk ApS:

_____
Christian Steffensen
CEO

*ChurchDesk considers your electronic approval of the Data Processing Agreement to be legally binding. We've added this singaturepage for the Church's internal use.