

Databehandlersaftale

1. Definitioner og fortolkning

Den 25. maj 2018 erstattes Persondataloven af Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 (herefter Persondataforordningen), således at Aftalen træder i kraft når Persondataforordningen og eventuelle nationale udfyldningsregler i Danmark, erstatter Persondataloven, herunder Sikkerhedsbekendtgørelsen og Sikkerhedsvejledningen. Der henvises endvidere til Aftalens punkt 2.9.

I Aftalen er indarbejdet de krav, som reglerne i Persondataforordningen stiller til databehandlersaftaler. Såfremt yderligere krav fremgår af Persondataforordningen eller nationale udfyldningsregler efter tidspunktet for Aftalens indgåelse, er Parterne enige om, at de fornødne ændringer i Aftalen foretages, således at kravene overholdes. Der henvises endvidere til Aftalens punkt 2.9.

Den Dataansvarlige er forpligtet til at informere Databehandleren om den Dataansvarliges it-sikkerhedsregulativ, it-sikkerhedspolitik og følge de eventuelle, dertilhørende uddybende it-sikkerhedsregler, og Databehandleren har pligt til at gøre sig bekendt hermed.

I denne Aftale skal følgende ord og udtryk forstås, som følger:

- **"Behandling"** har den i Persondatalovgivningen anførte betydning, og **"Behandle"** og **"Behandler"** skal fortolkes i overensstemmelse hermed.
- Den **"Dataansvarlige"** har den i Persondatalovgivningen anførte betydning.
- **"Databehandleren"** har den i Persondatalovgivningen anførte betydning.
- Ved **"Gældende Lovgivning"** forstås love, regler eller bindende vejledninger fra myndigheder, der finder anvendelse på Behandlingen af Persondata i henhold til denne Aftale.
- Ved **"Myndighed"** forstås alle relevante statslige eller lovbestemte organer eller myndighedsinstanser i det pågældende land eller andre relevante myndigheder eller enheder med ansvar for reguleringen eller forvaltningen af en Part eller Ydelserne, herunder, men ikke begrænset til, nationale databeskyttelsesmyndigheder.
- Ved **"Persondatabrud"** forstås brud på sikkerheden, som kan føre til hændelig eller ulovlig tilintetgørelse, tab, ændring eller uautoriseret videregivelse af eller adgang til Personoplysninger, der er transmitteret, opbevaret eller på anden måde Behandlet.
- Ved **"Persondatalovgivningen"** forstås fra og med den 25. maj 2018 Persondataforordningen, i hvert tilfælde som indarbejdet i den nationale lovgivning i de enkelte medlemsstater i Det Europæiske Økonomiske Samarbejdsområde, samt al gældende lovgivning vedrørende Behandling af Personoplysninger og fysiske personers privatliv og uafhængighed.
- **"Personoplysninger"** har den i Persondatalovgivningen anførte betydning.
- Den **"Registrerede"** har den i Persondatalovgivningen anførte betydning.
- Ved **"Tredjeland"** forstås et land, som ikke er en del af Det Europæiske Økonomiske Samarbejdsområde.
- Ved **"Ydelser"** forstås [de i afsnittet punkt 3 beskrevne ydelser].
- Ved **"ChurchDesk Abonnement"** forstås, udover denne Databehandlersaftale, de ved aftalen gældende Abonnementsvilkår og Privatlivspolitik, den underskrevne Samarbejdsaftale og/eller en betalt faktura.
- Ved **"ChurchDesk Applikation"** forstås de serviceydelser som ChurchDesk stiller til rådighed til den Dataansvarlige, som defineret i Abonnementsvilkårene.

Alle henvisninger til lovbestemmelser skal anses for at omfatte alle efterfølgende videreførte bestemmelser eller ændringsbestemmelser

2. Generelle krav

Databehandleren må alene Behandle Personoplysningerne i overensstemmelse med den Dataansvarliges dokumenterede instrukser som anført i denne Aftale, eller såfremt den Dataansvarlige på anden måde har meddelt skriftlig instruks til Databehandleren.

Omfanget af Behandlingen af Personoplysninger, der er reguleret af denne Aftale, er begrænset til den i punkt 3. "Beskrivelse af behandling af personoplysninger" beskrevne Behandling.

Databehandleren må ikke på nogen måde ændre Personoplysningernes indhold eller videregive eller tillade videregivelse af nogen af Personoplysningerne til tredjemand, medmindre:

- det konkret fremgår af denne Aftale,
- den Dataansvarlige på anden måde har givet bemyndigelse og/eller instruks hertil,

og/eller

- behandlingen er påkrævet i henhold til Gældende Lovgivning, som Databehandleren er underlagt.
- videregivelsen er omfattet af punkt 2.9., skal Databehandleren, i det omfang det i henhold til Gældende Lovgivning er muligt, give den Dataansvarlige meddelelse herom, inden Behandling af disse Personoplysninger sker.

Databehandleren skal løbende føre en fortegnelse over behandlingen af Personoplysninger samt en fortegnelse over alle sikkerhedsbrud.

2.1. Sikkerhed

Databehandleren skal gennemføre og sikre, at dennes medarbejdere gennemfører passende tekniske og organisatoriske foranstaltninger med henblik på at beskytte Personoplysningerne mod uautoriseret eller ulovlig Behandling og mod hændeligt tab, tilintetgørelse, beskadigelse, ændring eller videregivelse. Databehandleren skal i denne forbindelse tage højde for den nyeste udvikling, omkostningerne ved gennemførelsen, Behandlingens karakter, omfang, sammenhæng og formål samt risikoen for fysiske personers rettigheder og frihedsrettigheder. I afsnittet om Datasikkerhed, jf. punkt 4 findes der en generel beskrivelse af de tekniske og organisatoriske sikkerhedsforanstaltninger. Databehandleren skal desuden sikre Personoplysningerne via tekniske og organisatoriske sikkerhedsforanstaltninger, som beskrevet i Persondataforordningen samt eventuelle nationale udfyldningsregler.

Databehandleren skal tage rimelige skridt til at sikre, at alle medarbejdere, repræsentanter eller kontraktparter, der måtte have adgang til Personoplysningerne, er pålidelige, og at alle disse personer er underlagt fortrolighedsforpligtelser eller erhvervsmæssig eller lovbestemt tavshedspligt. Databehandleren skal tillige sikre, at adgangen til Personoplysningerne i hvert enkelt tilfælde nøje begrænses til de personer, der har behov for adgang til oplysningerne, og at dette er nødvendigt for at kunne levere Ydelserne som led i den pågældende persons opgaver hos Databehandleren, samt at alle disse personer (i) er oplyst om Personoplysningernes fortrolige karakter, (ii) har gennemført passende uddannelse vedrørende Gældende Lovgivning, og (iii) er bekendt med Databehandlerens forpligtelser i forbindelse med databeskyttelse i henhold til denne Aftale.

Databehandleren skal mindst en gang årligt gennemgå sine interne sikkerhedsforskrifter og retningslinjer for behandlingen af Personoplysninger med henblik på at sikre, at de fornødne sikkerhedsforanstaltninger til stadighed er iagttaget, jf. afsnit om "Datasikkerhed" hhv. Punkt 4 i denne aftale.

2.2. Bistand

Databehandleren skal bistå den Dataansvarlige med at sikre, at den Dataansvarlige kan imødekomme den Registreredes udøvelse af dennes rettigheder i henhold til Persondatalovgivningen vedrørende Personoplysninger, herunder imødekomme en vurdering, forespørgsel, meddelelse eller undersøgelse i henhold til Persondatalovgivningen, eller levere alle de oplysninger, som den Dataansvarlige anmoder om indenfor en rimelig tidsfrist.

Databehandleren skal bistå den Dataansvarlige med så vidt muligt at gennemføre tekniske og organisatoriske foranstaltninger, således at den Dataansvarlige kan besvare anmodninger ved eksempelvis udøvelsen af den Registreredes rettigheder, jf. Persondatalovgivningen.

Databehandleren skal uden ugrundet ophold give meddelelse til den Dataansvarlige, så snart Databehandleren bliver bekendt med Persondatabrud, og Databehandleren skal samarbejde og yde bistand til den Dataansvarlige i forbindelse med afhjælpningen af Persondatabrud. Databehandleren må ikke hverken offentligt eller til tredjeparter kommunikere om Persondatabrud uden forudgående skriftlig aftale med den Dataansvarlige om indholdet af en sådan kommunikation, medmindre Databehandleren har en retlig forpligtelse til sådan kommunikation.

Databehandleren skal overholde og sørge for, at Databehandlerens personale overholder (i) sikkerhedspolitikken og alle øvrige politikker, som er meddelt Databehandleren, herunder i afsnittet om Datasikkerhed, (ii) alle gældende sikkerhedskrav for konkrete lokationer hos den Dataansvarlige, som til enhver tid er meddelt Databehandleren skriftligt, og (iii) Databehandlerens egne interne sikkerhedsstandarder.

Databehandleren er ved forespørgsel forpligtet til at oplyse med præcise adresseangivelser, hvor den Dataansvarliges Personoplysninger opbevares. Databehandleren skal ajourføre oplysningerne over for den Dataansvarlige ved enhver ændring.

2.3. Underdatabehandling

Databehandleren har den dataansvarliges generelle godkendelse til at gøre brug af underdatabehandlere. Databehandleren skal dog underrette den dataansvarlige om eventuelle planlagte ændringer vedrørende tilføjelse eller erstatning af andre databehandlere og derved give den dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer. En sådan underretning skal være den dataansvarlige i hænde minimum 30 dage før anvendelsen eller ændringen skal træde i kraft. Såfremt den dataansvarlige har indsigelser mod ændringerne, skal den dataansvarlige give meddelelse herom til databehandleren inden 7 dage efter modtagelsen af underretningen. Den dataansvarlige kan alene gøre indsigelse, såfremt den dataansvarlige har rimelige, konkrete årsager hertil.

Den Dataansvarliges forudgående samtykke er betinget af, at Databehandleren:

- gennemfører tilstrækkelig due diligence-undersøgelse af den enkelte Underdatabehandler med henblik på at sikre, at denne er i stand til at yde det beskyttelsesniveau i forhold til Behandling af Personoplysninger, som kræves i denne Aftale,

- i kontrakten mellem Databehandleren og den enkelte Underdatabehandler medtager vilkår, som giver samme beskyttelse som vilkårene i denne Aftale

Den Dataansvarlige kan til enhver tid forlange dokumentation fra Databehandleren for eksistensen og indholdet af underdatabehandleraftaler for de Underdatabehandlere, som Databehandleren anvender i forbindelse med opfyldelsen af sine forpligtelser over for den Dataansvarlige.

I tilfælde af Databehandlerens konkurs kan den Dataansvarlige rette direkte henvendelse til de i punkt "5. Underdatabehandler" angivne underdatabehandlere

2.4. Godkendelse vedrørende overførsel af personoplysninger til tredjeland

I henhold til databeskyttelsesforordningens kapitel 5 så godkender den Dataansvarlige overførslen af personoplysninger til databehandlere/underdatabehandlere i tredjelande, der af EU Kommissionen er klassificeret som sikre.

Den dataansvarlige godkender databehandlere/underdatabehandlere i United States of America der er godkendt igennem aftalen "Privacy Shield" mellem EU Kommissionen og United States of America.

Hvis den dataansvarlige ikke i dette afsnit eller ved en efterfølgende skriftlig meddelelse har angivet en instruks eller godkendelse vedrørende overførsel af personoplysninger til et tredjeland, må databehandleren ikke indenfor rammerne af databehandleraftalen foretage en sådan overførsel.

2.5. Overholdelse af lovgivning mv.

Databehandleren skal Behandle Personoplysningerne i overensstemmelse med Persondatalovgivningen og forpligter sig til ikke at foretage, tillade og/eller undlade handlinger, som vil kunne medføre, at den Dataansvarlige overtræder Persondatalovgivningen. Hvis en instruks efter Databehandlerens opfattelse er en overtrædelse af Persondatalovgivningen, skal Databehandleren straks give den Dataansvarlige meddelelse herom.

Databehandleren forpligter sig til at muliggøre kontrol, inspektion og/eller revision udført af den Dataansvarlige eller en anden kontrolperson med bemyndigelse fra den Dataansvarlige vedrørende Behandlingen af Personoplysninger, jf. afsnit 2.12. Kontroller og Erklæringer.

2.6. Opsigelse

Opsigelse af databehandleraftalen kan ske i henhold til de opsigelsesvilkår, inkl. opsigelsesvarsel, som fremgår af "ChurchDesk Abonnement", med undtagelse af følgende afsnit:

Ved opsigelsen af denne Aftale skal Databehandleren

- ophøre med at Behandle Personoplysningerne, og
- efter den Dataansvarliges ønske (i) tilbagelevere alle Personoplysninger, som Databehandleren er i besiddelse af eller har kontrol over, samt alle kopier der af, til den Dataansvarlige. Den første eksport Databehandleren foretager er uden omkostninger for den Dataansvarlige. Ønsker den dataansvarlige yderligere eksport kan Databehandleren kræve betaling fra den Dataansvarlige baseret på afholdt timeforbrug til behandling af yderligere eksport, udover den første eksport, (ii) destruere alle kopier heraf og over for den Dataansvarlige bekræfte, at dette er sket, medmindre Databehandleren i medfør af Gældende Lovgivning er afskåret fra, eller af en Myndighed forhindres i, at destruere eller tilbagelevere alle eller dele af Personoplysningerne; i så fald skal Databehandleren behandle

disse oplysninger fortroligt, fortsat Behandle dem i overensstemmelse med vilkårene i denne Aftale og må ikke Behandle dem i videre omfang, end hvad der kræves for at opfylde kravene i den pågældende Gældende Lovgivning eller fra den pågældende Myndighed.

Denne Aftales ophør uanset årsagen hertil påvirker ikke Parternes rettigheder eller forpligtelser i henhold til denne Aftale. Parternes rettigheder og forpligtelser skal således fortsat gælde efter Aftalens ophør.

2.7. Overdragelse

Med undtagelse af punkt 2.3. må Databehandleren ikke på nogen måde helt eller delvist overdrage (eller søge at overdrage) sine rettigheder eller forpligtelser i henhold til denne Aftale til tredjemand uden den Dataansvarliges forudgående skriftlige samtykke.

2.8. Aftalens fuldstændighed

Parterne er enige om, at denne Aftale er den fulde aftale mellem Parterne vedrørende de her i omhandlede forhold. Aftalen erstatter således alle tidligere aftaler mellem Parterne om de i Aftalen omhandlede forhold.

2.9. Ændringer

Der kan alene gyldigt gives afkald på eller ske ændringer i vilkår, bestemmelser, forpligtelser eller betingelser i denne Aftale, i det omfang dette sker skriftligt og underskrives af en tegningsberettiget fra den Part, der giver afkald eller ønsker at foretage ændringer. Databehandleren skal ved sådanne ændringer uden ugrundet ophold sikre, at Underdatabehandlere tillige forpligtes af ændringerne.

Såfremt et vilkår, en betingelse eller bestemmelse i denne Aftale af en kompetent myndighed i en eller anden grad erklæres ugyldig, ulovlig eller uden retskraft, udskilles vilkåret, betingelsen eller bestemmelsen i det pågældende omfang fra de øvrige vilkår, betingelser og bestemmelser, som fortsat opretholdes efter deres indhold i det efter loven videst mulige omfang.

I det omfang ændringer i lovgivningen, jf. Aftalens punkt 1. eller tilhørende praksis, giver anledning til dette, er Parterne med et varsel på [30 dage, og uden at dette medfører krav om betaling fra den anden Part], berettiget til at foretage ændringer i Aftalen.

2.10. Meddelelser

Alle meddelelser, der skal gives i henhold til denne Aftale, skal være skriftlige.

2.11. Tavshedspligt og fortrolighed

Databehandleren er - under og efter ChurchDesk aftalens ophør - pålagt fuld tavshedspligt omkring alle oplysninger, denne bliver bekendt med gennem samarbejdet.

Databehandleren skal fra den 25. maj 2018 sikre, at alle, der behandler oplysninger omfattet af Aftalen, herunder ansatte, tredjeparter (f.eks. en reparatør) og Underdatabehandlere, forpligter sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt.

2.12. Kontroller og erklæringer

Databehandleren er forpligtet til uden ugrundet ophold at give den Dataansvarlige de nødvendige oplysninger til, at den Dataansvarlige til enhver tid kan sikre sig, at Databehandleren kan overholde de krav, der følger af denne Aftale.

Den Dataansvarlige, en repræsentant for den Dataansvarlige eller dennes revision (såvel intern som ekstern) har adgang til at foretage inspektioner og revision hos Databehandleren, få udleveret dokumentation, herunder logs, kan stille spørgsmål m.v., med henblik på at konstatere, at Databehandleren overholder de krav, der følger af denne Aftale. Omkostningerne i forbindelse med den dataansvarliges inspektion af databehandleren overtages af den dataansvarlige.

Det aftales at databehandleren fører et årligt eget tilsyn med at underdatabehandlerne muliggør en revision af deres datasikkerhed.

Den dataansvarlige kan – hvis det findes nødvendigt – vælge at initiere en revision af underdatabehandleren. Dette kan blive aktuelt, såfremt den dataansvarlige vurderer, at databehandlerens tilsyn med underdatabehandleren ikke har givet den dataansvarlige tilstrækkelig sikkerhed for, at behandlingen hos underdatabehandleren sker i overensstemmelse med denne databehandleraftale.

I tilfælde af, at den Dataansvarlige ønsker at foretage en inspektion af de ovennævnte foranstaltninger i henhold til denne aftale, kan den Dataansvarlige foretage en inspektion ved at stille tid og ressourcer til rådighed herfor.

2.13. Lovvalg

Denne Aftale er underlagt og skal fortolkes i overensstemmelse med dansk ret, og alle Parter anerkender Københavns Byret som eksklusivt værning.

3. Beskrivelse af behandling af personoplysninger

Dette afsnit indeholder oplysninger om Databehandlerens Behandling af Personoplysninger til brug for leveringen af Ydelserne.

3.1. Behandlingens formål

Behandling af den Dataansvarliges oplysninger sker i henhold til formålet og ydelserne beskrevet i "ChurchDesk Abonnementet".

Databehandleren må ikke anvende oplysningerne til andre formål.

Oplysningerne må ikke behandles efter instruks fra andre end den Dataansvarlige.

3.2. Generel beskrivelse af behandlingen

De overførte personoplysninger vil blive underlagt følgende behandlinger:

- Indsamling, registrering, organisering, systematisering, opbevaring, tilpasning eller ændring, genfindning, søgning, brug, videregivelse ved transmission, formidling eller enhver anden form for overladelse, sammenstilling eller samkøring, begrænsning, sletning eller tilintetgørelse.

3.3. Typen af Personoplysninger

Behandlingerne indeholder Personoplysninger i de nedenfor angivne kategorier. Databehandlerens og eventuelle Underdatabehandleres niveau for behandlingssikkerhed bør afspejle oplysningernes følsomhed, jf. afsnit om Datasikkerhed.

Almindelige Personoplysninger, jf. Persondataforordningens artikel 6:

- Almindelige Personoplysninger

Oplysninger om CPR-nummer

- CPR-numre

Særlige kategorier af personoplysninger, jf. Persondataforordningens artikel 9:

- Religiøs overbevisning
- Helbredsforhold
- Racemæssig eller etnisk baggrund
- Politisk overbevisning
- Filosofisk overbevisning
- Fagforeningsmæssige tilhørsforhold
- Seksuelle forhold

3.4. Kategorier af registrerede

Der behandles oplysninger om følgende kategorier af registrerede:

- Medlemmer
- Potentielle medlemmer
- Donorer/Sponsorer
- Medarbejdere

4. Datasikkerhed

4.1. Sikkerhedsforanstaltningernes formål

Dette afsnit henviser til en beskrivelse af de tekniske og organisatoriske sikkerhedsforanstaltninger, som Databehandleren i medfør af Databehandleraftalen har ansvar for at gennemføre.

Sikkerhedsforanstaltningerne dokumenteres og vil blive opdateret, hvis der er ændringer.

De tekniske og organisatoriske foranstaltninger er underlagt fremtidige tekniske fremskridt og udviklinger. I denne henseende har Dataansvarlige tilladelse til at gennemføre alternative, egnede foranstaltninger, som ikke må falde under sikkerhedsniveauet for de tidligere fastsatte foranstaltninger. Væsentlige ændringer skal dokumenteres.

Databehandleren gennemfører følgende tekniske og organisatoriske sikkerhedsforanstaltninger for at sikre et sikkerhedsniveau, der passer til de aftalte Behandlinger, og som dermed opfylder Persondataforordningens artikel 32.

Foranstaltningerne fastlægges ud fra overvejelser om:

- Hvad der kan lade sig gøre rent teknisk
- Implementeringsomkostningerne
- Den pågældende behandlings karakter, omfang, sammenhæng og formål, jf. Pkt. "3. Beskrivelse af behandling af personoplysninger"
- Konsekvenserne for borgerne ved et sikkerhedsbrud
- Den risiko, der er forbundet med behandlingerne, herunder risikoen for
 - tilintetgørelse af oplysningerne
 - tab af oplysningerne
 - ændring af oplysningerne
 - uautoriseret videregivelse af oplysningerne
 - uautoriseret adgang til oplysningerne

Foranstaltningerne gennemføres for at undgå at Personoplysninger:

- tilintetgøres, mistes, ændres eller forringes,
- kommer til uvedkommendes kendskab eller misbruges, eller
- i øvrigt behandles i strid med lovgivningen, jf. Aftalens punkt 1.

4.2. Generelle sikkerhedsforanstaltninger

Datacenter

- Vores datacentre håndterer fysisk sikkerhed 24/7 med videoovervågning med høj sikkerhedsgrænser rundt om hele datacentret. Indgang via elektroniske adgangskontrolterminaler med en transpondernøgle eller adgangskort. Ultramoderne overvågningskameraer til døgnet rundt overvågning af adgangsruiter, indgange, sikkerhedsdørens låsesystemer og serverrum og det sædvanlige højteknologiske ting, datacentre altid skyder af.
- Vi har DDOS-beskyttelse på plads i alle vores datacentre.

Beskyttelse mod tab af data

- Kontodata er opbevaret på krypterede harddiske.
- Hetznerns firewalls sikrer, sammen med vores egen network access control lists (ACL's), imod uautoriseret adgang til vores servere.
- Kontodata afspejles og sikkerhedskopieres dagligt. Backups er opbevaret på logisk og fysisk separate servere.
- Backups opbevares krypteret.
- Backup opbevares i 60 dage.

Sikkerhed på programniveau

- Brugerkonto adgangskoder opbevares ved brug af en kryptografisk hash-funktion.
- Dit kodeord kan ikke hentes. Det skal nulstilles.
- Alle login-sider (fra vores hjemmeside og mobilwebsted) overfører data via SSL.
- Hele applikationen er krypteret med SSL.
- Login blokeres efter gentagne fejlslåede forsøg.

Intern it-sikkerhed

- Alle medarbejderne instrueres af databehandleren i beskyttelse af kundedata. Databehandleren har implementeret interne retningslinjer til beskyttelse af kundedata, der er i overensstemmelse med databeskyttelsesforordningen.

4.3. Autorisation og adgangskontrol

Alle medarbejder hos Databehandleren, som har adgang til personlige oplysninger er autoriseret af Databehandleren. Autorisationer beskriver formålet med medarbejderens adgang. Medarbejdere har kun adgang til personlige oplysninger for driftsrelaterede eller tekniske formål.

Medarbejdere hos Databehandleren har ikke adgang til personlige oplysninger, som ikke er indeholdt i deres autorisation. Databehandleren holder antallet af autorisationer til et minimum.

Databehandleren verificerer og opdaterer autorisationer løbende. Autorisationer vil blive ændret eller annulleret når en medarbejder skifter stilling, ansvar eller ansættelsesforhold.

Alle ændringer i autorisationer bliver logget af Databehandleren.

4.4. Behandling af datamateriale som indeholder personoplysninger

De overførte personoplysninger vil blive underlagt følgende grundlæggende behandlinger:

- opbevaring
- adgang for kundeservice
- ved henvendelser til og fra kundeservice
- i overensstemmelse med din brug af funktioner i ChurchDesk
- misbrugsdetektion, forebyggelse og afhjælpning
- opretholdelse, forbedring og levering af vores tjenester.

Den dataansvarlige tillader udtrykkeligt databehandleren til at reagere på følgende anmodninger, der modtages direkte fra de registrerede: afmeldinger, opdateringer af oplysninger, fjernelse af oplysninger eller blokering af den registreres oplysninger, der lagres i databehandlerens system.

Den dataansvarlige tillader udtrykkeligt databehandleren til at sende oplysninger, og kommunikation til at fremme brugen af ChurchDesk, til den dataansvarliges brugere af ChurchDesk Applikationen. Kommunikation fra ChurchDesk kan være afhængig af brugerens adfærd i ChurchDesk Applikationen.

Den Dataansvarlige kan på hvilket som helst tidspunkt slette indtastede data i ChurchDesk Applikationen, hvorefter dataen ikke kan tilgås længere af den Dataansvarlige. Dataen kan genskabes efter kontakt med support inden for en periode på 60 dage. Databehandleren kan opkræve betaling for at genskabe data slettet af den Dataansvarlige. Efter 60 dage er dataen destrueret og kan ikke længere genskabes.

Ved opsigelse af kontrakten slettes alt indtastet data i databasen automatisk 60 dage efter opsigelse.

Efter sletning forefindes data i backup, se afsnit "Beskyttelse mod tab af data".

Eksterne kommunikationsforbindelser

Kommunikationen mellem brugeren hos den Dataansvarlige og ChurchDesk Applikationen er krypteret både via webapplikationen og mobile apps. Kommunikation mellem anonyme brugere og betalinger eller formularer er ligeledes krypteret. Serverne er opsat til kun at tillade kommunikation via krypterede forbindelser og videresender straks brugeren til en krypteret forbindelse såfremt brugeren forsøger at etablere en usikker forbindelse.

Almindelig email og sms kommunikation til den registrerede kan ikke krypteres. Derfor bekræfter den dataansvarlige med sin underskrift, at der ikke vil blive inkluderet personfølsom information i E-mails og SMS'er udsendt via ChurchDesk

Logning

Alle adgange og adgangsforsøg i ChurchDesk Applikationen bliver automatisk logget i seks måneder. Dette inkluderer IP-adresse, tidspunkt og brugeridentifikation.

Registreringen indeholder oplysning om tidspunkt, bruger og type af anvendelse. Loggen opbevares i 6 måneder hvorefter den slettes.

Hjemmearbejdspladser

Databehandlerens behandling af Personoplysninger sker delvist ved anvendelse af hjemmearbejdspladser.

Medarbejdere hos Databehandleren kan tilgå applikationen fra eksterne lokationer med samme sikkerhedsforanstaltninger som beskrevet i "Eksterne kommunikationsforbindelser". Alle medarbejdere er blevet instrueret i kun at bruge arbejdscomputere, som har fuld kryptering af harddisken.

Adgang til servere for driftsrelaterede eller tekniske formål kan kun udføres ved brug af krypteret fjernadgang, SSH.

5. Underdatabehandlere

Navn	Hjemmeside	Beskrivelse af behandling
Hetzner Online	www.hetzner.de	Stiller servere til rådighed i et sikkerhedscertificeret miljø, som oplysningerne fra ChurchDesk Applikationen er gemt på. Hetzner har ikke adgang til kundedata.
Mailjet	www.mailjet.com	Benyttes til forsendelse af e-mails der sendes fra ChurchDesk Applikationen.
Stripe	www.stripe.com	Benyttes til den Dataansvarliges betaling af ChurchDesk Abonnement og behandling af donationer til den Dataansvarlige.
Compaya	www.compaya.dk	Benyttelse til forsendelse af SMS'er fra ChurchDesk.
Amazon Web Service	aws.amazon.com	Benyttes til forsendelse af e-mails der sendes fra ChurchDesk.
Sentry	www.sentry.io	Fejldetektion som sørger for at ChurchDesks udviklere kan overvåge og rette fejl i realtid.
Intercom	www.intercom.com	Muliggør en sikker behandling af henvendelser fra chatten i ChurchDesk. Benyttes af ChurchDesk til henvendelser til brugerne i ChurchDesk.
Segment	www.segment.com	Bruges til at videresende informationer til Intercom, Google Analytics samt BigQuery.

Google Cloud	cloud.google.com	Behandler addressesøgninger via Google Maps og opbevaring af metadata via BigQuery.
Hubspot	www.hubspot.com	Behandler oplysninger af besøgende på hjemmesiden, bruges til at sende nyhedsbreve ud til ChurchDesk brugere, og til at håndtere skriftlige og telefoniske henvendelser fra og til kundeservice.

Underskrifter: Databehandlersaftale*

Mellem

Indsæt organisationens navn:
Adresse:
By:
(herefter den "Dataansvarlige")

og

Churchdesk ApS
Njalsgade 21G, 3.
2300 København S
CVR-nr. 32150489
(herefter "Databehandleren")

hver for sig benævnt "Part" og samlet benævnt "Parterne"

er der indgået følgende databehandlersaftale ("Databehandlersaftalen" eller "Aftalen").

_____, den _____ 20____

For:

København, den _____

For Churchdesk ApS:

Christian Steffensen
Adm. Direktør

*ChurchDesk anser den elektroniske godkendelse af Databehandlersaftalen for juridisk bindende. Til kirkens interne brug har vi her tilføjet en underskriftsside til Databehandlersaftale, underskrevet af ChurchDesk ApS.