Datasikkerhed

Politik for Datasikkerhed af Persondata i Baptistkirken Bornholm

Baptistkirken Bornholms Privatlivspolitik skitserer kirkens værdier vedrørende behandling af persondata.
Kirkens Forretningsorden er retningsgivende for hvem gør hvad i kirken og hvordan det gøres.
Den interne persondatapolitik for ansatte og frivillige sætter rammerne for pligter og rettigheder for de ansatte og frivillige.
Dokumentet - Procedurer omkring håndtering af persondata i Baptistkirken Bornholm, sætter rammerne for indsamlingen og håndteringen af persondata i kirken.
Politikken for håndtering af Persondata skal sikre kirken og dens brugere, frivillige og ansatte imod sikkerhedsbrud.

Medlemsoplysninger

1. Opbevares på platformene Access og Microsoft Office med back-up i Skyen og på USB-pen. Fysisk materiale er i aflåst.
2. Det er kun menighedens ledelse, kirkens præster og de valgte ansvarlige der har direkte adgang til databaserne.
3. Medlemsoplysninger slettes ved udmeldelse (endt kalender år).

Gave-, bidrags-, og donationsgiveroplysninger

1. Opbevares i Winfinans, Microsoft Office og Googleplatformen med back-up på eksternt drive, USB-pen og fysisk.
2. Adgang kun tilgængelig for kasserer, bidragssekretær og revisor.
3. Gavegiveroplysninger i 5 år + indeværende år efter senest modtagne gave.
4. Tilsagnsoplysninger opbevares ligeledes i på Googleplatformen og i Microsoft Office.
5. Adgang er kun tilgængelig for kasserer, bidragssekretær og revisor.
6. Tilsagnsoplysninger slettes senest 1 måned efter de er registreret i database.
7. Forpligtigelseserklæringer opbevares i 5 år + indeværende år efter senest modtagne gave.
8. Fysisk materiale opbevares aflåst.

Personaleoplysninger

1. Personaleoplysninger opbevares i Microsoft Office, Googleplatformen og Dropbox.
2. Ansættelseskontrakter der er på papir opbevares aflåst i skab.
3. Adgang til platformene er kun tilgængelig for personaleudvalg og kasserer der udbetaler løn.
4. Personaleoplysninger gemmes i 5 år + indeværende år efter afsluttet ansættelse.

5. Jobansøgninger slettes efter 6 måneder.

Tilmelding til aktiviteter og arrangement oplysninger

1. Tilmeldingslister laves og gemmes i Microsoft Office.
2. Adgang er kun tilgængeligt for aktivitets- og arrangements ansvarlige.
3. Tilmeldingslister slettes umiddelbart efter afholdelse af arrangement.

Oplysninger om frivillige

1. Oplysninger om frivillige opbevares i Microsoft Office, E-boks og Dropbox.
2. Adgang er kun tilgængelig for kirkens ledelse og aktivitetsleder.
3. Oplysninger om frivillige slettes når opgaven som frivillig er afsluttet.

Menighedsrådet

1. Referater gemmes i Microsoft Office.
2. Fysiske referater opbevares aflåst.
3. Adgang er kun tilgængelig for Menighedsrådet.

Bornholm Matu Christian Fellowship

1. Medlemsoplysninger opbevares i Microsoft Office og Viber.
2. Adgang til oplysninger administreres af foreningens formand og næstformand og tildeles kun til de aktiviteter medlemmet er en del af.
3. Fysisk materiale opbevares aflåst.
4. Back-up findes på USB pen som opbevares hos Formand og næstformand.

Børne- og Ungdomsarbejde

1. Medlemsoplysninger opbevares i forhold til Minimax I Baptistkirkens Børne og Ungdomsforenings (BBU) centrale medlemsregistrering.
2. I forhold til Danske Baptisters Spejderkorps - Rønne Kreds (DBS) opbevares data i DBS centrale medlemsregistrering (Spejdernes Medlemsservice) og i Microsoft Office.
3. Adgang til databaserne er forbeholdt landskontorets personale og lokalafdelingens kasserer og aktivitetsledere.
4. I forhold til Børnekirken opbevares oplysninger i Microsoft Office og på Googleplatformen.
5. Fysisk materiale opbevares aflåst.

Data beskyttelse

1. Data beskyttes af firewalls og antivirus.
2. Alle computere er beskyttede af kodeord.
3. Der bruges login på centrale systemer.
4. Fysisk materiale opbevares aflåst.

5. Fysisk materiale der ikke skal opbevares til fysisk dokumentation, destrueres når det fysiske materiale ikke længere skal bruges.

Brud på Datasikkerhed

1. Dataansvarlige for Persondata kontakter Datatilsynet ved brud på datasikkerheden i kirken.
2. Den dataansvarlige informerer kirkens ledelse om sikkerhedsbruddet.
3. Den dataansvarlige igangsætter en undersøgelse for at udrede sikkerhedsbruddets omfang.
4. Den dataansvarlige informerer de personer som har været udsat for sikkerhedsbrud.
5. Kirkens underafdelinger og ansatte informerer kontaktpersonen indenfor 24 timer ved mistanke om brud på datasikkerheden.
6. Den dataansvarlige informerer Datatilsynet inden for 72 timer.

Denne politik er senest opdateret den 22. september 2021