Opdateret 8. februar 2023

Politik for hvordan personoplysninger opbevares

Luthersk Mission Bornholm

Denne politik har til hensigt at beskrive Luthersk Mission Bornholms (LM-Bornholm) retningslinjer for sikker opbevaring af persondata, herunder vurdering af foreningens risikoprofil ift. behandlingen af persondata.

Dokumentet er grundlag for "Politik for opbevaring og sletning af personoplysninger".

Dokumentet omhandler fysiske og elektroniske dokumenter med personoplysninger med særlig fokus på de personfølsomme data. Vi definerer personfølsomme data som oplysninger om konkret person, der samfundsmæssigt har høj følsomhed (f.eks. religiøs orientering), og som direkte kan sammenkobles med den pågældende.

Da LM-Bornholm er en kirkelig organisation, falder alle personer i og omkring inden for denne kategori, og al persondata om dem skal behandles som værende personfølsomt. For at kunne håndtere dette, skelner vi mellem to kategorier:

Den første kategori er personer, som figurerer på en hjemmeside (ansatte og frivillige med særligt hverv). Deres religiøse tilhørsforhold er dermed offentliggjort og skal ikke længere behandles som personfølsomt.

Den anden kategori er alle andre personer. Så længe deres personoplysninger befinder sig inden for LM-organisationen (sekretariatet, afdelinger, kredse og lign.), kan deres oplysninger behandles som almindelige personoplysninger.

Alle personoplysninger, som kommer ud af LM-organisationen, skal betragtes som personfølsomt, og den person, der behandles oplysninger om, skal give et konkret samtykke til, at dette må forekomme.

Risikoprofil

Forhold, der taler for høj følsomhed ift. persondata:

- LM er en kirkelig organisation og betegnes dermed ift. Persondataforordningen (GDPR) som en religiøs organisation. Dermed er alle oplysninger, der kan identificere en person til LM, af personfølsom karakter.
- Tro og værdier, som de praktiseres i LM, kan fremkalde stærke modreaktioner hos modstandere. Vi oplever det yderst sjældent i Danmark. I Danmark vurderes den største risiko til at være negativ omtale på diverse medieplatforme.

Forhold, der taler for lav følsomhed ift. persondata:

- Mennesker med tilknytning til LM har selv valgt det. Desuden er det karakteristisk for kristendommen, at man er åben omkring sin tro. Det gælder både ansatte og frivillige medarbejdere.
- Kulturen i LM – ikke mindst i den lokale foreningsdel – er meget åben og tillidsbaseret.

Samlet vurdering; Vi er klar over, at tilknytning til LM-Bornholm kan være meget følsomt og personligt. Samtidig vurderer og erfarer vi, at dna'et i den kristne tro er baseret på offentlighed og gensidig tillid. Vi har årelang tradition for åben demokratisk struktur, som vi ønsker at bevare. Samtidig ønsker vi at opbevare de nødvendige persondata sikkert i respekt for de implicerede personer.

Retningslinjer for, hvem der har adgang til persondata

En lang række nødvendige persondata er af en sådan karakter, at det kun er udvalgte nøglepersoner, som må have kendskab til dem. Det kan f.eks. være materiale i forbindelse med gaver, rekrutteringsforløb, sjælesørgeriske samtaler o. lign. Her benytter vi kun udvalgte folk som har underskrevet en frivillighedskontrakt, hvor de tilkendegiver, at de er bevidste om deres tavshedspligt og ansvar.

Retningslinjer for fysiske arkiver og dokumenter

Man skal efterleve følgende i forhold til persondata:

- Der opbevares kun materiale, som har relevans, og kun så længe det er nødvendigt at opbevare det.
- Det sikres, at LM-Bornholms "Politik for opbevaring og sletning af personoplysninger" overholdes.
- Personfølsomme data skal opbevares aflåst.

Retningslinjer for brug af elektroniske programmer

Der skal være en kode på computere som indeholder personoplysninger, således at en uvedkommende ikke kan komme til at se personoplysningerne, herunder ægtefælle, børn etc. – Dette medfører personligt login.

Deling af dokumenter

Man skal indgå databehandleraftaler med de virksomheder der udbyder fildelingsprogrammer. Luthersk Mission Bornholm benytter NextCloud hostet hos One.com til fildeling. Adgang til data tildeles på mappeniveau til hver enkelt person.

Retningslinjer for brug af USB-nøgle og andre bærbare medier

Man bør ikke have persondata på USB-nøgler og andre bærbare medier. Hvis man af en eller anden årsag er nødt til at have persondata på et bærbart medie, skal de beskyttes med adgangskode eller krypteres. Efter brug skal persondata slettes fra det bærbare medie.

Retningslinjer for frivillige der arbejder med persondata

Udgangspunktet er, at al persondata opbevares på en sådan måde, at det ikke er tilgængeligt for uvedkommende. Det betyder, at noget skal opbevares aflåst.

Al persondata, som kun er tilgængeligt for en autoriseret person, må ikke efterlades frit på f.eks. skrivebord, når man ikke arbejder med det. Og det skal opbevares i aflåst skuffe eller skab, når man ikke er til stede. Man skal sikre sig at de persondata, man har ansvar for, ikke bliver tilgængeligt for uvedkommende, herunder ægtefælle, børn etc.

Al persondata, der ikke har været offentliggjort, skal enten bortskaffes på betryggende vis eller arkiveres, når sagen er afsluttet, som angivet i "Politik for opbevaring og sletning af personoplysninger".

De beskrevne retningslinjer (f.eks. adgangskoder, aflåst skab etc.) forventes implementeret i hjemmet. Såfremt man bruger IT-udstyr, skal man sikre sig, at persondata ikke er tilgængelige for andre end de tilsigtede.

Retningslinjer for ansatte der arbejder med persondata

Udgangspunktet er, at al persondata opbevares på en sådan måde, at det ikke er tilgængeligt for uvedkommende. Det betyder, at noget skal opbevares aflåst.

Al persondata, må ikke efterlades frit på f.eks. skrivebord, når man ikke arbejder med det. Og det skal opbevares i aflåst skuffe eller skab, når man ikke er til stede. Man skal sikre sig at de persondata, man har ansvar for, ikke bliver tilgængeligt for uvedkommende, herunder kollegaer etc. Kontor skal være aflåst når man ikke er til stede.

Al persondata, der ikke har været offentliggjort, skal enten bortskaffes på betryggende vis eller arkiveres, når sagen er afsluttet, som angivet i "Politik for opbevaring og sletning af personoplysninger".

Såfremt man udlåner sin pc eller bruger IT-udstyr hvor andre er til stede, skal man sikre sig, at persondata ikke er tilgængelige for andre end de tilsigtede.

De beskrevne retningslinjer forventes implementeret på alle ens faste arbejdssteder.

Tavshedspligt

Man må ikke videregive fortrolige oplysninger, som man har fået kendskab til under sin tjeneste. Tavshedspligten gælder også efter fratrædelse af tjenesten.

Retningslinjer for opbevaring af referater.

I en foreningskultur som LM's er referater vigtige arbejds- og styringsredskaber.

Referater skal opbevares sikkert. Det anbefales ikke, at de rundsendes på e-mail. I stedet bør de gemmes på en serverløsning, og der sendes et link til referatet. Hvis referatet downloades eller printes, skal det slettes, når det ikke bruges længere. Indehaveren af referatet er ansvarlig for, at det enten slettes eller gemmes i henhold til "Politik for opbevaring og sletning af personoplysninger", når det ikke længere er relevant.

Hvis man ønsker at gemme et referat for eftertiden, bør man holde personfølsomme oplysninger ude af referatet. Lav evt. et sideløbende referat med det personfølsomme indhold, som slettes når det er færdigbehandlet.

Retningslinjer i forbindelse med databrud

Databrud skal hurtigst muligt meldes til LM's sekretariat (resurseteamet), der vil sørge for at databruddet bliver anmeldt til Datatilsynet. Databrud skal anmeldes til Datatilsynet inden der er gået 72 timer.

Et databrud kan f.eks. være hvis man har mistet en computer som indeholder persondata, eller hvis man er kommet til at give nogle fortrolige oplysninger videre til en forkert person. Databrud skal dog ikke meldes, hvis det er usandsynligt, at bruddet vil indebære en risiko for fysiske personers rettigheder.