**Misbrug af data? Ikke hvis din kirke følger denne vejledning**

Misbrug af personoplysninger er i dag et stort problem. Hvert år udsættes flere end 40.000 danskere for eksempel for identitetstyveri.

***Hvad har det med frikirker at gøre?***

Rigtig meget.

For persondata af forskellig slags nærmest flyder rundt i nogle frikirker – fordi mange opfatter deres kirke som en udvidet familie, hvor man gerne deler den slags data på kryds og tværs. Men samtidig er frikirker juridiske enheder, der håndterer personfølsomme data – og til dette er der knyttet nogle krav.

Disse krav er blevet skærpet på EU-plan, hvilket betyder, at en ny dansk databeskyttelseslov træder i kraft den 25. maj i år. Formålet er at beskytte borgerne og deres personlige oplysninger. Det er primært rettet mod de store multinationale selskaber, men ændringen i mentalitet og kultur gælder alle – også os som kirker.

Se evt. en lille pixibog om den nye lov [her.](http://frikirkenet.dk/sites/default/files/pdf-upload/pixibog_0.pdf)
(Eller se den efter at have læst nedenstående – måske vil den så give mere mening.)

Oplysninger om religiøst tilhørsforhold (med mere) er i loven defineret som information, der skal ydes en særlig beskyttelse. Den beskyttelse er frikirker pligtig til at yde, og det er et ansvar, vi skal tage på os. Ikke fordi vi frygter de meget store bøder, som kan følge af ikke at tage dette ansvar alvorligt, men fordi vi som frikirker ikke kan være ligeglade med, hvordan vi behandler folks persondata. Vi tager vores etiske og juridiske forpligtelse alvorligt.

* De data, som folk overlader til os, er folks ejendom, som de betror os - og de skal behandles som sådan. Vi skal passe på dem – have styr på dem – og vide, hvornår vi sletter dem.
* Det kan sammenlignes med, hvis du lader en barnepige passe dine børn:
	1. Barnepigen får kun lov til at passe dem, hvis du udtrykkeligt har givet lov
	2. Du forventer, at barnepigen ved, hvor de er
	3. At barnepigen passer på dem
	4. At du kan få fat på dem
	5. At de bliver afleveret igen
* I kirkeligt regi er enhver form for persondata per definition følsom:
	1. Du må kun opbevare dem med samtykke
	2. Du skal have styr på, hvor de bliver opbevaret
	3. De skal opbevares sikkert
	4. De skal kunne berettiges
	5. Det skal være klart, hvornår data afleveres igen (slettes)
* Se en anden type illustration af det [her.](http://frikirkenet.dk/sites/default/files/pdf-upload/gdpr_-_hvis_gdpr_handlede_om_en_bil.pdf)

**Det handler om en kulturændring:**

* Alle i kirken skal tænke på samme måde om menneskers personlige oplysninger.
* Alle skal vide, hvilke procedurer og hvilke produkter der skal til for at håndtere dataene.
* Det kommer ikke til at ske af sig selv.

**Som leder er du nødt til at gå foran i at tage dette seriøst:**

* Lav en gruppe, der vil være ansvarlig for processen i at skabe de nye procedurer og produkter.
* Vær forberedt på, at det koster ekstra penge, men du behøver ikke blive flået. Der er også billige it-løsninger.
* Lave en proces for alle kirkens frivillige nøglemedarbejdere.
* Sørg for kontinuerlig opfølgning.

Det kan måske virke uoverskueligt. Derfor har repræsentanter for Apostolsk Kirke, Missionsforbundet, Vineyard, Mosaik, Baptistkirken, Isobro og FrikirkeNet sat sig sammen for at lave så enkel og overskuelig vejledning og oversigt som muligt. Den følger nedenfor:

* Der er nogle nøgleord og begreber, som er vigtige at have styr på i forbindelse med den nye lov. Kender I ikke til disse udtryk, vil I ikke forstå, hvad vi skriver i det følgende – derfor vi lavet en [miniordbog.](http://frikirkenet.dk/sites/default/files/pdf-upload/miniordbogen_0.pdf)
* Den kommende lov opererer som nævnt med begrebet **personfølsomme** data. Fordi oplysninger om folks religiøse tilhørsforhold defineres som følsomme er enhver registrering af, at man er medlem af eller har tilknytning til en frikirke, per definition personfølsom - også selv om de enkelte persondata i sig selv – fx et navn – ikke er personfølsomt.

Dette stiller nogle **særlige krav** til, hvordan vi håndterer persondata som folks navn, adresse, e-mailadresse, telefonnummer, fødselsdato, cpr-nummer med videre. Det gælder både data om medlemmer, frivillige, gæster, deltagere i arrangementer, modtagere af julehjælp og så videre – alle persondata, som vi på en eller anden måde håndterer. Se evt. mere om, hvad persondata er, [her.](https://startvaekst.virk.dk/Privacykompasset/viden-og-regler/hvad-er-personoplysninger)

**Forslag til proces**

Nedenfor følger en liste over produkter/processer, som alle frikirker SKAL lave eller SKAL igennem. Vi har taget det udgangspunkt, at I er dataansvarlige, da det gør sig gældende for langt de fleste frikirker.
Det vigtigste i alt dette er at forstå, at det handler om en **kulturændring** i forhold til, hvordan vi håndterer persondata. Den kulturændring skal ud i alle kroge og hjørner af organisationen, og det kræver naturligvis infomøder for nøglemedarbejdere i de enkelte kirker samt udarbejdelser af diverse procedurer. Det kræver lidt arbejde til at begynde med, men når de nye rutiner først er indarbejdet, er det ikke så voldsom en arbejdsbyrde.

Vi foreslår, at I begynder med en af disse to ting:

**Følgende *skal* gøres:**

1. Foretag en **analyse** af, hvilke data I har/får ind – og hvordan I håndterer dem – opbevarer dem – sletter dem.
	1. Formålet er at få et overblik over/fornemmelse af, hvilket arbejde, der ligger foran jer.
	2. Vi har lavet [13 spørgsmål](http://frikirkenet.dk/sites/default/files/pdf-upload/13_spoergsmaal_til_proces.pdf) samt en [oversigt](http://frikirkenet.dk/sites/default/files/pdf-upload/liste_over_typiske_omraader_med_persondata_i_frikirker.pdf) som I kan bruge som en hjælp til dette første skridt.
2. Lav en oversigt over de data, som I behandler (bruger) hos jer – en såkaldt d**atabehandlingsfortegnelse.** Denne fortegnelse skal I have liggende i organisationen fysisk eller digitalt – det er et lovkrav, når man behandler følsomme persondata:
	1. Hvem er **dataansvarlig** hos jer?
	2. Hvilket formål har databehandlingen?
	3. Hvad er lovhjemlen?
	4. Hvilke oplysninger gemmes?
	5. Hvilke oplysninger gives videre til tredje part?
	6. Hvor opbevares dataene?
	7. Hvornår slettes de?

I kan nøjes med at lave **databehandlingsfortegnelser** for følgende fem hovedområder:

1. Personaleforhold (HR),
2. Medlemmer (og bidragsydere)
3. Frivillige
4. Deltagere i arrangementer/modtagere af julehjælp
5. Samarbejdspartnere (som fx B&U-forening med selvstændig cvr-nummer)

Med tanke på at skabe en kulturændring i hele organisation kunne en idé være at sammenkalde lederne for frivillige arbejdsområder som lovsang, børnekirke, café, økonomi etc. og give dem en kort introduktion til den nye lovgivning og dens konsekvenser for jer - hvorefter I beder dem udfylde en såkaldt databehandlingsfortegnelse for deres område. I behøver dog kun at opbevare én fortegnelse for hele området ”frivillige medarbejdere”.
Se eksempel [her](http://frikirkenet.dk/sites/default/files/pdf-upload/databehandlingsfortegnelse-medlem.pdf) og [her](http://frikirkenet.dk/sites/default/files/pdf-upload/databehandlingsfortegnelsehr.pdf).

Grunden til, at I må opbevare dataene**,** kaldet **Lovhjemmel,** vil for HR og medlemsregistrering være som i eksemplerne i ovenanførte links; for frivillige og for samarbejdspartnere vil det være i langt de fleste tilfælde være retsligt – EU’s persondataforordning Art 9 stk. 2, litra d for at være helt præcis.
Kirken har som nævnt pligt til at opbevare disse fortegnelser i et aflåst skab i et aflåst rum – eller digitalt bag tofaktorlogin (se mere nedenfor).

1. Sørg for **sikker opbevaring** af data med tofaktorbeskyttelse – både digitalt og fysisk. Det vil for fysiske ting som fx mapper og papir sige i aflåste skab i aflåst rum. Og for digitale ting tofaktorlogin på telefoner og computere – også på frivillige medarbejderes private enheder!
	1. I forhold til computere, så skal der altid være kode på computer plus kode på personfølsomme dokumenter – eller kode på mappe med sådanne dokumenter.
	2. Samme med mobil: Kode på mobilen samt kode til personfølsomme dokumenter og oversigter.
	3. Hvis du har lavet grupper i din adresseliste, så giv grupperne anonyme navne som fx ”Glade sanglærker” fremfor ”kirkens lovsangsgruppe”. Du skal sikre, at hvis din mobil bliver stjålet, så kan andre ikke læse, hvem der er med i kirken.
	4. Når det gælder lagring i skyen, skal det være hos firmaer, som lever op til den nye databeskyttelseslov eller tilsvarende - fx USA’s privacy shield. Google og Dropbox (gratis version) lever pt. ikke op til nogen af disse – det gør derimod eksempelvis Microsoft Office 365, Jottacloud og MailChimp (som jo lagrer navne og mailadresser).
2. Udarbejd **databehandleraftaler** med leverandører, der arbejder efter instruks fra jer (som I **overlader** data til).
3. Det kunne fx være det firma, som hoster jeres hjemmeside, et bogføringsfirma, cloudtjenester eller et online regnskabsprogram. Det er dog sandsynligt, at de selv kontakter jer for at få godkendt opdaterede forretningsbetingelser for samarbejdet.
4. Hvis jeres leverandør opbevarer data i USA, skal I sikre, de er privacy shield-certificerede (som ovenfor nævt). Det er overførselsgrundlaget for data, der skal til USA.
5. Ved **videregivelse** af data til en samarbejdspartner (dvs., som ikke arbejder på instruks fra jer men ud fra andet grundlag) skal I ikke have databehandleraftaler, da de, som data **videregives** til, bliver selvstændigt dataansvarlige (fx Skat, Nets, Kirkeministeriet, bank og revisor). I skal dog stadig have en kontrakt/betingelse samt en hjemmel til at overføre persondata til dem (igen, de kontakter formentlig jer).
6. Hvis I **overlader** data til en anden aktør (gælder også ved B&U-forening som samarbejdspartner, hvis denne har et særskilt cvr-nummer), så skal der foreligge samtykke fra personen, der ejer sine oplysninger.

Skabelon til databehandleraftale findes på Isobros hjemmeside. Link hertil (samt til en række andre skabeloner) kan findes under punkt 10.

1. Skab **procedurer** for fremtidig indhentning af data, hvor I sikrer, at I får personens samtykke samt oplyser personen om dennes rettigheder (kaldet registreredes rettigheder). Det er et krav ved personfølsomme data.

Det er her, at alle frivillige skal være opmærksomme, og hvor vores store forarbejde skal give bonus i form af tryghed hos de mennesker, der betror os deres personlige data.

* 1. Vi skal have styr på samtykke, opbevaring med videre på tilsagnssedler, forbønsønsker, kontaktlister, tilmelding til arrangementer, optræden på hjemmeside etcetera etcetera.
	Se eksempel fra Bykirken [her.](http://frikirkenet.dk/sites/default/files/pdf-upload/procedurer_omkring_haandtering_af_persondata_i_bykirken.pdf)
	2. Det kan måske opleves som at skyde gråspurve med kanoner at skulle have samtykke og informere om registreredes rettigheder, hvis fx en mor, som er i kirke for første gang, overlader sit barns navn og oplysning om allergi samt sit eget telefonnummer til børnekirkens medarbejdere, og der vil vi anbefale en tolkning, som hedder pragmatisme frem for rigiditet. I det konkrete eksempel kunne en forkromet udgave være:
	*Vi vil gerne bede om barnets navn og dit telefonnummer, så vi kan ringe til dig, hvis dit barn bliver ked af det, mens det er her. Hvis dit barn lider af nogen form for allergi, vil vi også gerne vide det, så vi ikke giver dit barn noget, det ikke kan tåle. Vi destruerer denne liste, når børnekirken er slut. Regner du med, at dit barn skal kommer her jævnligt fremover, vil vi gerne have lov til at opbevare oplysningerne, indtil barnet ikke længere er at regne som en fast bruger af børnekirken. Se i øvrigt vores privatlivspolitik på xxxx.dk/privatlivspolitik, hvor du blandt andet kan læse om dine rettigheder, når du overlader data til os.*
	3. Sådan en besked kan evt. stå med lille skrift øverst eller nederst på den liste, hvor forældre kan angive oplysningerne.
	En lidt mere smidig (pragmatisk) udgave kunne være at skrive:

*XXkirke tager beskyttelse af dine data alvorligt. Derfor har vi en privatlivspolitik, som du kan se på xxkirke.dk/privatlivspolitik*

1. Hav en skriftlig politik for, hvornår I **sletter data** om folk – og hvad begrundelsen for længden på opbevaringen er (kaldet slettepolitik). Når det fx gælder givere kan bogføringsloven finde anvendelse (fem år + indeværende). I andre tilfælde slettes oplysninger, når de ikke længere er relevante.
	1. **Specifikt omkring e-mails:** Mails skal slettes fra indbakken. Vores anbefalinger er, at mailsystemet *ikke* bruges som journaliseringssystem. Mails bør som udgangspunkt ikke opbevares længere end seks måneder i mailsystemet. Vær opmærksom på også at slette mails i sendt- og slettet-mapperne. Hvis der er behov for at gemme dem længere, skal de opbevares på kirkens drev i skyen.
	2. Husk, at mails fra medlemmer/støtter/frivillige som udgangspunkt er en personfølsom oplysning uanset indholdet i mailen, da tilhørsforholdet til kirken i sig selv er en personfølsom oplysning.
	3. Men hvis et medlem afgiver særlige personfølsomme oplysninger fx oplysninger om seksualitet, er det vigtigt, at den mail ikke besvares med indholdet af mailen i. Mailen skal slettes fra kirkens mail efter **senest 24 timer**, og mailen må ikke besvares med disse informationer i.
	4. Send i øvrigt **aldrig persondata via mail,** fx deltagerliste ved lejr - med mindre mails kan afsendes og modtages krypteret. Del i stedet data via kirkens cloudtjeneste. Mail er ikke en sikker måde at dele personfølsom info på.
	5. **Om referater fra ledelsesmøder:** Vi går ud fra, I gemmer referater, årsrapporter, regnskaber og medlemsblade for evigt. Det er vores opfattelse pt., at **hjemlen** til det er en legitim interesse.
	Men det betyder også, at I så skal sørge for at overholde god dataskik i referaterne. Referater skal indeholde kirkens anliggende, men eventuelle personalesager skal behandles i lukkede punkter.
2. Lav en **privatlivspolitik**
Privatslivspolitikken er vores beskrivelse til ”brugerne” om, hvordan vi håndterer deres personlige data. Der skal bruges god tid på at lave den rigtige privatlivspolitik for jer. For her bliver I synlige med, hvordan I håndterer data, og det er ofte disse formuleringer, som folk giver samtykke til, og dermed giver jer deres samtykke til at håndtere, som I gør.
Se evt. [denne](http://frikirkenet.dk/sites/default/files/pdf-upload/privatlivspolitik_bykirken.pdf) privatlivspolitik for at få inspiration.
3. Lav en **intern privatlivspolitik** til jeres HR-afdeling.
I håndterer også personfølsomme data i forbindelse med jeres ansatte – hvilket I også skal have en politik omkring.

Se [her](http://frikirkenet.dk/sites/default/files/pdf-upload/privalivspolitik-hr-bykirken.pdf) for et eksempel på dette.

1. Sørg for at have **samtykke** fra alle personer, der ligger på **hjemmesiden** med angivelse af foto, privat mail og privat telefonnummer. Personer, der er ansatte i kirken og udelukkende fremgår af hjemmesiden med navn og kirkens kontaktdata, kræver ikke samtykke.
2. Isobro har i øvrigt lavet en række skabeloner (kaldet paradigmer), som I kan få adgang til [her](https://www.isobro.dk/medlemszonen/) (bruger: medlem, kode: isobro150).