LANDSFORENINGEN
AF MENIGHEDSRÅD

Værd at vide om GDPR

for menighedsråd

8. udgave marts 2024

Indholdsfortegnelse

1.0 Indledning

Et menighedsråd har ansvar for at overholde reglerne om persondatabeskyttelse – det kaldes også GDPR-regler.

Denne *Værd at vide om GDPR for menighedsråd* indeholder viden og praktiske tips til, hvordan I konkret kan leve op til reglerne. Der er regler både for registrering af personlige data, følsomme data, behandling af oplysninger, oplysningspligt om indsamling, ret til indsigt og flere emner. Vejledningen bliver udbygget efterhånden som GDPR-nyhederne udgives i Landsforeningens nyhedsbrev. Tilmelding til Landsforeningens nyhedsbrev kan ske på Landsforeningens hjemmeside.

Denne vejledning kan menighedsrådene benytte som opslagsværk, finde svar på de mest stillede spørgsmål om GDPR samt finde konkret vejledning til, hvordan menighedsrådet kan gribe arbejdet med GDPR an. Det sidste afsnit i vejledningen beskriver den juridiske baggrund for de praktiske anvisninger.

De gældende regelsæt er EU's Databeskyttelsesforordning (Forordning (EU) nr. 2016/679 af 27. april 2016) samt databeskyttelsesloven (Lov nr. 502 af 23/05/2018).

I løbet af dokumentet henvises der flere gange til et grupperum. Grupperummet findes på Folkekirkens IntraNet (kræver login) og hedder *Databeskyttelse*.

Betragt persondata som noget, I låner. Dvs. pas på det (data skal beskyttes), lån det ikke ud til andre (data bør ikke deles med andre) og aflever det efter brug (data skal slettes).

1.1 Afgrænsning

Menighedsrådet er kun dataansvarlig for behandling af personoplysninger, som falder under menighedsrådets ansvarsområde.

Behandling af personoplysninger i forbindelse med opgaver, som hører under embedets (præstens) ansvarsområde, er menighedsrådet ikke dataansvarlig for. Det er fx kirkebogsføring og behandling af anmodninger om kirkelige handlinger (nadver, dåb, konfirmation, vielse, begravelse). I det omfang en kirkefunktionær bistår præsten eller løser opgaven under præstens instruktion, hører det under præstens ansvarsområde.

2.0 De grundlæggende begreber

2.1 Behandling af personoplysninger

Databeskyttelsesreglerne finder anvendelse, når menighedsrådet "behandler" personoplysninger. Det er derfor afgørende at være opmærksom på, hvornår I udfører en behandling af personoplysninger om andre, fordi I ofte vil have forpligtelser efter databeskyttelsesreglerne og være ansvarlig for beskyttelsen af oplysningerne.

Det er endvidere en betingelse, at behandlingen sker elektronisk eller i manuelle registre, før GDPR finder anvendelse.

En behandling kan efter databeskyttelsesforordningen omfatte *enhver* håndtering af personoplysninger, herunder indsamling, registrering, organisering, systematisering, opbevaring, tilpasning eller ændring, genfinding, søgning, brug, videregivelse ved transmission, formidling eller enhver anden form for overladelse, sammenstilling eller samkøring, begrænsning, sletning eller tilintetgørelse.

Finder blot en af de nævnte former for håndtering af personoplysninger sted, vil der være tale om en behandling, som er omfattet af databeskyttelsesreglerne.

Fx er det en behandling(indsamling) af personoplysning, hvis kirke-kulturmedarbejderen modtager tilmeldinger til babysalmesang på sin arbejdsmail, eller på sognets officielle mail.

2.1.1 Menighedsrådet som dataansvarlig

Menighedsrådet er en selvstændig myndighed, der som andre myndigheder har ansvaret for at passe på de personoplysninger, der indsamles og behandles.

Som dataansvarlig skal menighedsrådet sikre sig:

- at I har lov til at behandle de oplysninger, som I og jeres databehandlere er i besiddelse af (om I har en behandlingshjemmel (se punkt 2.3)
- at I er i stand til at efterleve registrerede personers rettigheder (f.eks. opfylde jeres oplysningspligt eller give den registrerede indsigt se punkt 2.4)
- at opbevaring og sletning af personoplysninger sker efter de af menighedsrådet fastsatte regler (se punkt 5.1 og punkt 5.4)
- at I får indberettet eventuelle brud på persondatasikkerheden til Datatilsynet inden for 72 timer (se punkt 5.3)
- at der er hjemmel til videregivelse og ved deling af data oprettes en aftale om deling af data – eller en databehandleraftale og gives en instruks (se punkt 6.0).

2.2 Typer af personoplysninger

En personoplysning er enhver form for information, der kan henføres til en bestemt person, også selv om personen kun kan identificeres, hvis oplysningen kombineres med andre oplysninger.

Personoplysninger kan for eksempel være navn, adresse, personnumre, registreringsnumre, et billede, et fingeraftryk, en stemme, lægejournaler eller biologisk materiale, når det i praksis er muligt at identificere en person ud fra oplysningerne eller i kombination med andre. Man siger, at oplysningen er "personhenførbar".

Databeskyttelsesforordningen opdeler personoplysninger i tre typer:

- Almindelige oplysninger
- Særlige kategorier af oplysninger (følsomme oplysninger)
- Oplysninger om straffedomme og lovovertrædelser eller tilknyttede sikkerhedsforanstaltninger.

Herudover har Danmark indført en særskilt regel for CPR-nummer.

Opdelingen findes, fordi der gælder forskellige betingelser og procedurer for behandling af personoplysninger afhængig af oplysningernes følsomhed. Du kan læse mere om disse behandlingsregler under punkt 2.3 "Hjemmelsgrundlag - Betingelser for behandling af personoplysninger".

2.2.1 Almindelige (ikke-følsomme) personoplysninger

Almindelige personoplysninger[1] omfatter alle oplysninger, der ikke er klassificeret som særlige kategorier af oplysninger (følsomme personoplysninger). Det kan for eksempel være identifikationsoplysninger som navn og adresse eller oplysninger om økonomi, skat, gæld, væsentlige sociale problemer, andre rent private forhold, sygedage, tjenstlige forhold, familieforhold, bolig, bil, eksamen, ansøgning, CV, ansættelsesdato og stilling, arbejdsområde og arbejdstelefon.

Fx behandler menighedsrådet personoplysninger, når I modtager ansøgninger til en opslået stilling. Herved registrerer og behandler I personoplysninger med formål, at besætte stillingen.

På samme måde behandler menighedsrådet personoplysninger, når I laver tilmeldingslister til fx sangaftener, hvis I modtager navn og evt. telefonnummer eller mailadresse på deltagere.

2.2.2 Følsomme personoplysninger

Følsomme personoplysninger[2] er udtrykkelig afgrænset i databeskyttelsesforordningen, og adgangen til at behandle sådanne oplysninger er snævrere end ved almindelige personoplysninger.

Følsomme oplysninger er oplysninger om:

- Race og etnisk oprindelse
- Politisk overbevisning
- Religiøs eller filosofisk overbevisning
- Fagforeningsmæssige tilhørsforhold
- Genetiske data
- Biometriske data med henblik på entydig identifikation

[1] Databeskyttelsesforordningen art. 6
[2] Databeskyttelsesforordningen art. 9

- Helbredsoplysninger
- Seksuelle forhold eller seksuel orientering.

Kun de oplysninger, der er nævnt ovenfor, er følsomme personoplysninger.

Fx vil det være en følsom personoplysning, når menighedsrådet ved tilmelding til et arrangement om fællesspisning, får oplyst at en tilmeldt deltager har glutenallergi (helbredsoplysning).

Også oplysninger om en ansats sygdom, som kommer frem, eller gives af den ansatte ved behandlingen af en sygefraværssag vil være følsomme.

På samme vis er oplysning om medlemskab af folkekirken en følsom oplysning. Forudsætningen for medlemskab af folkekirken er dåben, og dåben er en følsom oplysning, da den fortæller om vedkommendes religiøse tilhørsforhold.

2.2.3 CPR-nummer

Personnummer (CPR-nummer) er en fortrolig oplysning, der er særskilt reguleret i dansk ret[3].

Personnummer kan benyttes med henblik på entydig identifikation, fx gravstedsadministration eller som journalnummer.

2.2.4 Oplysninger om strafbare forhold

Der skal anlægges en ganske vid forståelse af begrebet strafbare forhold[4]. Begrebet omfatter således ikke kun oplysninger om overtrædelse af lovgivning, men også eventuelle andre sanktioner, som fx rettighedsfrakendelse. Det kan også være en oplysning om adresse i et fængsel. Oplysninger fra en indhentet straffe-/børneattest omfattes også.

2.2.5 Fortrolige oplysninger

Fortrolige oplysninger er en særlig kategori af oplysninger, der ikke nævnes i databeskyttelsesreglerne, men hvor særlige beskyttelsesbehov kan have betydning ved anvendelsen af databeskyttelsesreglerne. Fortrolige oplysninger vil ofte være underlagt særregulering i anden lovgivning.

Det afgørende for, om en oplysning skal anses for fortrolig, vil være en vurdering af, om oplysningen efter den almindelige opfattelse i samfundet bør kunne forlanges unddraget offentlighedens kendskab, jf. straffelovens § 152 sammenholdt med forvaltningslovens § 27.

Følsomme personoplysninger vil utvivlsomt være fortrolige oplysninger. Omvendt er en fortrolig oplysning ikke altid følsom.

2.3 Hjemmelsgrundlag – Betingelser for behandling af personoplysninger

Det er nødvendigt at have en gyldig grund – kaldet hjemmel – til lovligt at indsamle og behandle personoplysninger. De betingelser, der gælder for at man lovligt kan behandle personoplysninger, fremgår af databeskyttelsesforordningen. Betingelserne kaldes også for hjemler til at behandle personoplysninger.

Inden menighedsrådet behandler personoplysninger, skal menighedsrådet sikre sig, at behandlingen har et lovligt grundlag. Menighedsrådet skal med andre ord fastlægge, hvilken behandlingshjemmel der ligger til grund for behandlingen, og eventuelt hvilken hjemmel, der er mest hensigtsmæssig at anvende.

[3] Databeskyttelsesloven § 11
[4] Databeskyttelsesforordningen art. 10 samt Databeskyttelsesloven § 8

De hjemler, menighedsrådet kan anvende, vil for det første afhænge af typen af personoplysninger (almindelige, følsomme, CPR-nummer, strafbare forhold) som behandles. Der kan læses mere om denne opdeling under punkt 2.2 "Typer af personoplysninger".

Menighedsrådet skal for det andet overveje den situation, som nødvendiggør behandlingen af personoplysninger. Er der tale om en retlig forpligtelse? Er der tale om udførelse af en offentlig myndigheds opgaver? Eller en opgave af samfundsmæssig interesse? Det er ofte den sammenhæng, som en behandling indgår i, der afgør, hvilken hjemmel der er relevant for menighedsrådet.

I alle tilfælde må menighedsrådet kun indsamle og behandle de nødvendige oplysninger. Som udgangspunkt skal kun personer med arbejdsmæssigt behov derfor have adgang til oplysningerne.

2.3.1 Kontraktlig eller retlig forpligtelse

Når der behandles almindelige personoplysninger i forbindelse med samarbejde med en leverandør eller anden samarbejdspartner, er det kontrakten, der er hjemlen for behandling af data[5]. Et eksempel på behandling af personoplysninger er fx, når der indsamles og behandles oplysninger om en leverandør. Et andet eksempel kan være, når man i forbindelse med et foredrag i sognet behandler og offentliggør oplysninger om foredragsholder. Det er en god ide, at man i den skriftlige aftale med foredragsholder supplerer med aftale/vilkår om brug af oplysninger og billeder fx til annoncering af arrangementet (dette kan være billeder, foromtale, eller foredragsholderens CV som vedkommende selv har lagt offentligt tilgængeligt[6], eller medsendt til menighedsrådet i forbindelse med aftalens indgåelse).

Menighedsrådet kan også have en retlig forpligtelse[7] til at behandle almindelige oplysninger om fx betalinger og overførsler, som det gælder i forhold til bogføringsloven. Herudover er menighedsrådet retligt forpligtet til at administrere gravsteder, og må på den baggrund behandle nødvendige oplysninger om afdøde og pårørende jf. bekendtgørelse om folkekirkens kirkebygninger og kirkegårde.

Hvis der i forbindelse med gravstedsadministration behandles følsomme oplysninger, fx om medlemskab af Folkekirken, er menighedsrådet berettiget til at behandle denne oplysning[8].

2.3.2 En opgave i samfundets interesse eller offentlig myndighedsudøvelse

En opgave i samfundets interesse[9], er en opgave, som er af betydning for en bredere kreds af personer. Menighedsrådet varetager styrelsen af lokale kirkelige og administrative anliggender efter nærmere fastsatte regler i den kirkelige lovgivning og skal virke for gode vilkår for evangeliets forkyndelse i sognet. Størstedelen af det menighedsrådet laver, er sognepleje. Det kendetegnende ved sognepleje er, at det er i samfundets interesse og på den baggrund, kan menighedsrådet behandle almindelige personoplysninger. Det kan være i forbindelse med sognets diakonale arbejde, kirkelige aktiviteter (sorggrupper, fællesspisninger), julehjælp, kirkebil mv.

Er der behov for at menighedsrådet i forbindelse med administration af sognepleje behandler følsomme oplysninger, kan opgaven anses som værende af væsentlig samfundsmæssig interesse[10]. Derfor kan

[5] Databeskyttelsesforordningen art. 6, stk. 1, litra b
[6] Hvis foredragsholder har offentliggjort følsomme oplysninger om sig selv, er menighedsrådets hjemmel til behandling af dette Databeskyttelsesforordningens art. 9, stk. 2, litra e.
[7] Databeskyttelsesforordningen art. 6, stk. 1, litra c
[8] Databeskyttelsesforordningen art. 9, stk. 2, litra b
[9] Databeskyttelsesforordningen art. 6, stk. 1, litra e
[10] Databeskyttelseslovens § 7, stk. 4 jf. Databeskyttelsesforordningen art. 9, stk. 2, litra g

menighedsrådet også behandle følsomme personoplysninger fx om oplysning om allergener ifm. fællesspisning.

Offentlig myndighedsudøvelse er en anden betegnelse for udøvelse af embedsmyndighed. Kerneopgaven for offentlig myndighedsudøvelse er udstedelse af forvaltningsakter, samt udførelse af opgaver der traditionelt betegnes som faktisk forvaltningsvirksomhed.

Menighedsrådet er pålagt opgaver som en del af offentlig myndighedsudøvelse, når der fx behandles anmodninger om flytning af urner, eller der skal nedlægges gravsteder, hvis der ikke er betalt for vedligehold, eller gravsten lægges ned, hvis der ikke betales for sikring af dem.

Kirkebogsføring, som er et eksempel på offentlig myndighedsudøvelse, hører ikke under menighedsrådet, men hører under præstens embede. Derfor er menighedsrådet ikke ansvarlig for behandlingen af personoplysninger i forbindelse med kirkebogsføringen, heller ikke selvom det er kordegnen, der varetager opgaven, idet præsten har instruktionspligten.

2.3.3 Samtykke

Behandling af personoplysninger kan som udgangspunkt altid ske, hvis den registrerede har givet sit samtykke til dette[11].
Hvis ikke hjemlen til behandling kan findes i kontrakt, retlig forpligtelse, myndighedsudøvelse eller ansættelsesretlig forpligtelse, så kan behandling af personoplysninger som udgangspunkt altid ske, hvis den registrerede har givet sit samtykke til dette.

Et samtykke inden for databeskyttelsesretten skal opfylde en række særlige betingelser. Det er derfor vigtigt at være opmærksom på, at et samtykke inden for databeskyttelsesretten *skal* opfylde følgende betingelser. Samtykket skal være frivilligt, specifikt, informeret og utvetydigt. Det betyder blandt andet, at et samtykke ikke kan afgives stiltiende, og at der ikke må være tilknyttet (unødvendige) negative konsekvenser ved ikke at afgive et samtykke[12].

Hvis behandlingen indeholder følsomme oplysninger, fx billeder af nadver eller dåb, skal samtykket være udtrykkeligt[13]. Det betyder, at I skal være helt sikre på, at I har et samtykke.

Det er også vigtigt at være opmærksom på, at et samtykke altid kan trækkes tilbage. **Samtykke er derfor ikke altid den mest hensigtsmæssige hjemmel**. Hvis I har indledt en behandling på baggrund af et samtykke, er I desuden som regel bundet af det formål, som den registrerede er blevet oplyst om, da samtykket blev indhentet.

2.3.4 CPR-nummer og strafbare forhold

Hjemlen til at behandle CPR-nummer findes i Databeskyttelsesloven § 11.

Hjemlen til at behandle oplysninger om strafbare forhold findes i Databeskyttelsesforordningen art. 10 samt Databeskyttelsesloven § 8.

2.3.5 Personale

Ansættelsesforhold har en særlig hjemmel i databeskyttelsesloven § 12, der giver en arbejdsgiver mulighed for at behandle oplysninger om medarbejdere for at opfylde forpligtelser i henhold til lovgivning eller

[11] Databeskyttelsesforordningen art. 6, stk. 1, litra a
[12] Se mere i https://www.datatilsynet.dk/Media/0/C/Samtykke%20(3).pdf
[13] Databeskyttelsesforordningen art 9, stk. 2, litra a

kollektive overenskomster. Det betyder, at oplysninger om medarbejdere, som er nødvendige at behandle som led i ansættelsen, ikke kræver medarbejderens samtykke.

Arbejdsgiver kan behandle:

- Identitets- og kontaktoplysninger, herunder privatadresse, telefonnummer og e-mailadresse
- uddannelse, tidligere ansættelser og andre oplysninger indeholdt i et CV
- alder, køn, ansættelsessted, afdeling, funktion, lønramme, løn
- oplysninger indhentet fra referencer
- oplysninger i forbindelse med person- og logiktest
- oplysninger, der indgår i korrespondance med medarbejderen
- børne- og straffeattest, hvis det er nødvendigt for stillingen
- løn, bankkonto og skatteoplysninger og pensionsforhold
- oplysninger om MUS-materiale, herunder kompetenceudvikling med mere
- oplysninger om ferie, sygdom, barsel, orlov og andet fravær
- oplysninger om it-udstyr, telefon og eventuelt firmakort, som stilles til medarbejderens disposition til brug for vedkommendes arbejde
- oplysninger om antal børn, herunder alder på børn, til administration af omsorgsdage
- oplysninger om brug af e-mail og internet
- oplysninger om ophør af ansættelse, herunder evt. afskedigelse eller bortvisning.
- oplysninger om CPR-nummer for at sikre en entydig identifikation, når der skal indberettes oplysninger om løn mv. efter reglerne i skattelovgivningen om indberetningspligt (følger af databeskyttelseslovens § 11)
- strafbare forhold (følger af databeskyttelsesloven § 8)
- medlemskab af fagforening i forbindelse med eventuelle tvister og hverv som tillidsrepræsentant
- religiøst tilhørsforhold, hvis medarbejderen fx skal varetage forkyndelse
- helbredsmæssige forhold (arbejdsskader, sygefravær, herunder mulighedserklæringer og lægeattester, oplysninger om barsel i forbindelse med dagpengerefusion, fleksjob eller ansættelse på særlige vilkår, fx ved handicap).

En medarbejder skal samtykke til, at menighedsrådet må opbevare kontaktoplysninger på pårørende, hvis menighedsrådet fx opbevarer en liste med oplysninger på pårørende i tilfælde af at medarbejderen er udsat for en ulykke, og der er behov for at kunne komme i kontakt med en pårørende.

Vedrørende helbredsmæssige forhold må menighedsrådet kun behandle oplysninger om en diagnose, hvis medarbejderen giver samtykke hertil. Det kan fx være hvis medarbejderen oplyser diagnosen til en sygefraværssamtale eller det direkte fremgår af en mulighedserklæring.

2.4 Den registreredes rettigheder

Den registrerede har nogle rettigheder – ret til indsigt, berigtigelse, sletning, begrænsning af behandling, indsigelse og til at trække samtykke tilbage[14].

De fleste af den registreredes rettigheder forudsætter, at den registrerede retter henvendelse til menighedsrådet og gør sin ret gældende. Der er dog nogle forpligtelser, menighedsrådet skal opfylde over for den registrerede, uanset om vedkommende henvender sig eller ej, og det er oplysningspligten.

[14] Se mere i Datatilsynets vejledning om de registreredes rettigheder

2.4.1 Processuelle krav ved iagttagelse af den registreredes rettigheder

Som udgangspunkt er det menighedsrådet som dataansvarlig, der skal sørge for at iagttage de registreredes rettigheder, hvorfor jeres eventuelle databehandlere ikke kan pålægges et selvstændigt ansvar for at iagttage rettighederne. Der er dog ikke noget til hinder for, at jeres databehandler – efter aftale med og instruks fra menighedsrådet som dataansvarlig – iagttager de registreredes rettigheder på jeres vegne og under jeres ansvar.

I øvrigt kan det være en forudsætning for, at menighedsrådet kan iagttage de registreredes rettigheder, at jeres eventuelle databehandlere medvirker i et eller andet omfang. I kan f.eks. have brug for jeres databehandlers medvirken, når der skal slettes eller berigtiges oplysninger, der fysisk befinder sig hos databehandleren, herunder på dennes servere eller lignende.

2.4.1.1 Tidsfrister og klagevejledning

Menighedsrådet skal svare på en anmodning fra en registreret om indsigt, berigtigelse, sletning osv. *uden unødig forsinkelse* og *senest en måned* efter, at have modtaget anmodningen.

Hvis anmodningen er kompliceret, kan svarfristen forlænges med yderligere to måneder. I disse tilfælde skal menighedsrådet dog senest en måned efter at have modtaget anmodningen, gøre den registrerede opmærksom på den forlængede sagsbehandlingstid og begrundelsen herfor. Der er således en absolut frist for besvarelse af anmodninger fra en registreret på tre måneder, men det må antages, at langt de fleste anmodninger ikke vil være komplicerede, hvorfor de skal besvares senest en måned efter modtagelsen.

En afvisning af en anmodning kan bl.a. være begrundet i, at menighedsrådet ikke behandler oplysninger om den registrerede, eller at menighedsrådet ikke er enig i, at der skal ske sletning mv. Se også afsnit 2.4.5.1 om undtagelse til retten til sletning som følge af journaliserings- og notatpligten.

Afviser menighedsrådet en anmodning fra den registrerede, skal I underrette denne om dette straks og senest en måned efter, I har modtaget anmodningen. I de tilfælde, hvor menighedsrådet afviser en anmodning fra en registreret, skal I begrunde afslaget og vejlede om, at den pågældende kan klage til en Datatilsynet eller indbringe sagen for domstolene.

2.4.2 Oplysningspligt

Menighedsrådet skal på eget initiativ give den registrerede en række oplysninger, når I indsamler eller modtager personoplysninger om vedkommende – se punkt 4.1 om privatlivspolitik og punkt 4.3. om standardmeddelelser ved mails.

For at menighedsrådet kan iagttage sin oplysningspligt, er det vigtigt, at menighedsrådet *giver* oplysningerne til den registrerede. Det betyder, at menighedsrådet som dataansvarlig skal tage aktive skridt til at give oplysningerne, og det vil derfor ikke være tilstrækkeligt kun at have oplysningerne liggende på en hjemmeside eller lignende, som den registrerede selv skal finde.

2.4.3 Ret til indsigt

Den registrerede har ret til at få indsigt i de oplysninger, menighedsrådet behandler[15], samt hvordan menighedsrådet behandler oplysningerne. På denne måde vil den registrerede nemlig bedst kunne forvisse sig om, hvorvidt de konkrete oplysninger, der behandles om den pågældende, er korrekte og lovlige. Det betyder også, at det ikke er tilstrækkeligt blot at oplyse til at der behandles *"navn, adresse, mailadresse og*

[15] Databeskyttelsesforordningen art. 15

telefonnummer". Det skal oplyses hvilket navn, hvilken adresse og mailadresse og hvilket telefonnummer der er registreret på den pågældende.

Sammen med oplysninger om selve indholdet som behandles, skal menighedsrådet også oplyse hvilken type oplysning der er tale om (se punkt 2.2 Typer af personoplysninger), hvad formålet er med behandlingen, om oplysningen evt. videregives til andre og til hvem, i hvilket tidsrum oplysningen behandles, og hvorfra oplysningerne stammer.
Herudover skal menighedsrådet oplyse den registrerede om, at vedkommende har ret til at anmode om berigtigelse, sletning eller begrænsning af behandlingen, at den registrerede har ret til at gøre indsigelse mod behandlingen i særlige situationer, og at den registrerede har ret til at indgive klage over behandlingen til Datatilsynet (se punkterne 2.4.4-2.4.9 nedenfor).

Udlevering af materiale kan ske ved kopi af de originale dokumenter eller ved at samle oplysningerne i et nyt dokument. Materialet kan sendes via Digital Post, via en elektronisk adgang fra den registreredes egen pc eller udleveres fysisk. Udlevering af en kopi skal ske gratis. Kun hvis der anmodes om yderligere kopier, kan menighedsrådet opkræve et rimeligt gebyr fastsat ud fra de administrative omkostninger.

Det er kun oplysninger om den registrerede, der må fremgå af materialet. Hvis der indgår oplysninger om andre personer, skal de sløres eller på anden vis fjernes.

Menighedsrådet kan helt eller delvist undlade at imødekomme en anmodning om indsigt, hvis oplysningerne kan undtages efter reglerne i offentlighedsloven § 19-29 og § 35[16], fx foreløbige interne dokumenter eller hvis dokumenterne er underlagt tavshedspligt.

2.4.3.1 Ret til dataportabilitet

En registreret har ret til at modtage egne personoplysninger i et struktureret, almindeligt anvendt og maskinlæsbart format. Menighedsrådet bør altid vælge et format, som gør oplysningerne så forståelige som muligt, og som giver den registrerede de bedste muligheder for at administrere og videreanvende oplysningerne. Et format, der eksempelvis er underlagt dyre licensbegrænsninger, bør derfor ikke anvendes.

Oplysningerne skal gives uden hindring. Det betyder, at menighedsrådet ikke må iværksætte tiltag eller udvise adfærd, der har til formål eller følge at undgå eller begrænse den registreredes ret til dataportabilitet. Eksempler på sådanne tiltag kan være at opkræve gebyr, anvende et kompliceret dataformat eller udvise adfærd, der på lignende måde besværliggør eller forhaler adgangen til oplysningerne.

2.4.4 Ret til berigtigelse

Den registrerede har ret til at få urigtige oplysninger om sig selv rettet[17]. Det indebærer for det første, at en registreret har ret til at få urigtige (forkerte) personoplysninger om sig selv rettet og for det andet har ret til at få fuldstændiggjort ufuldstændige personoplysninger.

Hvis menighedsrådet modtager en anmodning fra en registreret, der ønsker urigtige personoplysninger berigtiget, skal menighedsrådet berigtige oplysningerne uden unødig forsinkelse. Idet menighedsrådet er

[16] Bekendtgørelse af lov om offentlighed i forvaltningen LBK nr 145 af 24/02/2020
[17] Databeskyttelsesforordningen art. 16

en offentlig myndighed, må de forkerte oplysninger ikke slettes, men den efterfølgende korrekte oplysning skal tilføjes sagen, og det skal fremgå at den korrekte oplysning er gældende.

Hvis menighedsrådet ikke er enig med den registrerede i, at oplysningerne er urigtige, så er menighedsrådet ikke forpligtet til at berigtige oplysningerne. Det kan fx være et notat fra et møde, hvor der efterfølgende er uenighed om, hvad der er sagt. Her kan menighedsrådet beholde sin version og så tilføje, at den registrerede er uenig i oplysningerne, herunder hvad den registrerede mener er korrekt.

Hvis oplysningerne er videregivet til tredjemand, er menighedsrådet forpligtet til *på eget initiativ* at oplyse tredjemand om, at oplysningerne er forkerte eller ufuldstændige.

2.4.5 Ret til sletning ("retten til at blive glemt")

I særlige tilfælde har den registrerede ret til at få slettet oplysninger om sig, inden tidspunktet for menighedsrådets almindelige generelle sletning indtræffer[18]. Se punkt 5.0 om sikkerheds- og slettepolitik samt punkt 5.4 hvad "sletning" indebærer.

Den registrerede har ret til at få sine personoplysninger slettet *uden unødig forsinkelse*, hvis:

1. Det ikke længere er nødvendigt for menighedsrådet at have oplysningerne af hensyn til de formål, som oplysningerne blev indsamlet på baggrund af,
2. at behandlingen er baseret på samtykke, og samtykket trækkes tilbage,
3. at oplysningerne behandles ulovligt, altså uden hjemmel (se punkt 2.3 om hjemmelsgrundlag),
4. at menighedsrådet er forpligtet til at slette oplysningerne som følge af EU-lovgivning eller anden dansk lovgivning *eller*
5. at menighedsrådet er forpligtet til at slette oplysningerne som konsekvens af, at den registrerede udøver sin ret til indsigelse (se punkt 2.4.7 om Ret til indsigelse)

Den registreredes ret til sletning får som udgangspunkt kun praktisk betydning, hvis en registreret anmoder om sletning før det tidspunkt, hvor oplysningerne ville være blevet slettet som følge af de af menighedsrådet fastsatte slettefrister.

Menighedsrådet er ikke forpligtet til at slette, hvis den fortsatte behandling er *nødvendig for at overholde en retlig forpligtelse* fx jf. bogføringsloven eller er *nødvendig for at udføre en opgave i samfundets interesse eller en opgave, som henhører under offentlig myndighedsudøvelse* jf. fx journaliserings- og notatpligt – se eller er *nødvendig for, at et retskrav kan fastlægges, gøres gældende eller forsvares*.

2.4.5.1 Undtagelse som følge af journaliserings- og notatpligt

Menighedsrådet er som offentlig myndighed underlagt en journaliseringspligt som gør, at dokumenter, der sendes eller modtages som led i sagsbehandling, skal journaliseres og gemmes.

Det betyder også, at en registreret ikke kan få journaliseret materiale slettet på trods af opfordring hertil, idet menighedsrådet som offentlig myndighed har en pligt til journalisering ifølge offentlighedsloven.

2.4.6 Ret til begrænsning af behandling

Den registrerede har i visse tilfælde ret til at få behandlingen af sine personoplysninger begrænset[19], så menighedsrådet kun må opbevare oplysningerne.

[18] Databeskyttelsesforordningen art. 17
[19] Databeskyttelsesforordningen art. 18

Det kan ske i tilfælde, hvor den registrerede bestrider rigtigheden af oplysningerne. Så længe menighedsrådet undersøger, om personoplysningerne er korrekte, skal behandlingen af oplysningerne begrænses. Det kan også være, at den registrerede har gjort indsigelse mod behandlingen. Også i dette tilfælde, skal menighedsrådet begrænse behandlingen så længe det undersøges, om menighedsrådet legitime interesser går forud for den registreredes legitime interesser. Det kan også være at menighedsrådet ikke længere har brug for oplysningerne til en behandling, men de er nødvendige for at et retskrav kan fastlægges, gøres gældende eller forsvares.

Hvis behandling af personoplysninger er begrænset, så må menighedsrådet *kun* opbevare oplysningerne, men må som udgangspunkt ikke på anden måde behandle, herunder bruge eller videregive, oplysningerne. Hvis der søges om aktindsigt i oplysninger, som er underlagt begrænset behandling, skal tredjemand informeres om, at oplysningerne er underlagt begrænset behandling og hvad begrundelsen er herfor.

2.4.7 Ret til indsigelse

Den registrerede har i visse tilfælde ret til at gøre indsigelse mod menighedsrådets ellers lovlige behandling af sine personoplysninger[20].

Rettigheden gælder kun i tilfælde, hvor menighedsrådet behandler personoplysninger af hensyn til udførelse af en opgave i samfundets interesse (fx sognepleje) eller som henhører under offentlig myndighedsudøvelse (fx gravstedsadministration), som menighedsrådet som dataansvarlig har fået pålagt.

Det kan også være hvis menighedsrådet som dataansvarlig eller en tredjemand kan forfølge en legitim interesse, medmindre den registreredes interesser eller grundlæggende rettigheder og frihedsrettigheder, der kræver beskyttelse af personoplysninger, går forud herfor, navnlig hvis den registrerede er et barn.

Hvis menighedsrådet modtager en anmodning om indsigelse, skal menighedsrådet på ny foretage en vurdering om behandling fortsat er nødvendigt. Hvis det vurderes, at fortsat behandling er nødvendigt, skal dette forklares for den registrerede og begrundes hvorfor indsigelsen ikke kan imødekommes.

2.4.8 Ret til at trække samtykke tilbage

Hvis menighedsrådets behandling af en registrerets personoplysninger er baseret på den registreredes samtykke, har denne til enhver tid ret til at trække sit samtykke tilbage. Dette kan gøres ved at kontakte menighedsrådet.

Hvis den registrerede vælger at trække sit samtykke tilbage, påvirker det ikke lovligheden af menighedsrådets behandling af personoplysninger på baggrund af et tidligere meddelte samtykke og op til tidspunktet for tilbagetrækningen. Hvis den registrerede trækker sit samtykke tilbage, har det derfor først virkning fra dette tidspunkt.

2.4.9 Mulighed for at klage til Datatilsynet

Den registrerede har ret til at indgive en klage til Datatilsynet, hvis vedkommende er utilfreds med den måde, som menighedsrådet behandler vedkommendes personoplysninger på.

3.0 Medarbejdere

Læs også Datatilsynets vejledning om databeskyttelse i forbindelse med ansættelsesforhold.

[20] Databeskyttelsesforordningen art. 21

Privatlivspolitik for ansøgere, medarbejdere og fratrådte medarbejdere findes i punkt 4.1.1.

3.1 Ansættelse af medarbejdere

3.1.1 Jobansøgninger på mail

Datatilsynet oplyser, på deres hjemmeside, at der er ikke problemer i at modtage ansøgninger på mail, men man skal selvfølgelig håndtere ansøgningerne forsvarligt, når først man har modtaget dem.

Vi anbefaler, at I i forbindelse med stillingsopslag oplyser sognets officielle mailadresse. Når I har modtaget ansøgningerne, anbefaler vi, at I lægger dem i arkivet på FIN, så de medlemmer af rådet, der skal deltage i ansættelsesudvalg, kan hente dem der.

Send kvittering for modtagne oplysninger til ansøgerne og vedlæg jeres privatlivspolitik jf. punkt 4.1.1.

3.1.2 Samtykke til indhentelse af referencer

En ansøger skal give samtykke til, at menighedsrådet indhenter referencer fra nuværende eller tidligere arbejdsgivere. Ansøger skal vide, hvilke oplysninger der indhentes; om det er almindelige oplysninger om fx ansættelsestidspunkt, arbejdsopgaver og lignende "neutrale" oplysninger, eller om der også indhentes oplysninger om fx ansøgerens faglige eller sociale kompetencer samt følsomme oplysninger.

3.1.3 Indhentelse af børne- og straffeattester

Menighedsrådet må kun indhente nødvendige oplysninger. Dvs. der må kun indhentes børneattester på de medarbejdere (og frivillige), som har direkte kontakt eller fast færdes blandt børn under 15 år og dermed har mulighed for direkte kontakt med børn under 15 år som led i deres arbejde.

På samme vis må der kun indhentes straffeattester på medarbejdere og frivillige, der har en betroet stilling.

Indhentelse af attester kan ske ved ansættelsen eller undervejs i ansættelsen, hvis opgaverne ændrer sig så medarbejderen får en betroet stilling eller får mulighed for at opnå kontakt til børn og unge under 15 år.

Medarbejderen skal give samtykke til indhentelse af attester.

3.1.4 Sletning af ansøgninger fra ansøgere, der har fået afslag

Under et rekrutteringsforløb vil menighedsrådet ofte modtage en række oplysninger, som ikke vil være nødvendige for at træffe beslutning om mulig ansættelse. I har ikke pligt til under processen at tage stilling til spørgsmålet om oplysningernes relevans med henblik på eventuel sletning af oplysninger.

Når ansættelsesprocessen er færdig, er udgangspunktet, at ansøgninger slettes. Menighedsrådet kan komme i en situation, hvor det kan være nødvendigt at skulle kunne dokumentere et konkret rekrutteringsforløb, fx ved indsigelse om forskelsbehandling. Menighedsrådet skal dog konkret vurdere, om der er behov for at opbevare oplysninger om ansøgere.

Udbetales der rejsegodtgørelse til en ansøger, skal dokumentation herfor gemmes i fem år i henhold til bogføringslovens bestemmelser.

3.1.5 Opbevaring af ansøgninger til senere brug

Menighedsrådet kan gemme ansøgninger for kandidater, der har fået afslag, hvis menighedsrådet vurderer, at det er aktuelt til en eventuel senere ansættelse. Det kræver ansøgerens samtykke at gemme ansøgningen.

Menighedsrådet kan ligeledes gemme uopfordrede ansøgninger. Ansøgninger må gemmes, hvis menighedsrådet vurderer, at de i løbet af den kommende periode vil have brug for en medarbejder til den type stilling som er søgt. Menighedsrådet fastsætter, hvor længe uopfordrede ansøgninger gemmes.

3.2 Medarbejdere i ansættelse

3.2.1 Periode for opbevaring

Generelt må personoplysninger opbevares i det tidsrum, oplysningerne er nødvendige til at opfylde de formål, som de oprindelig blev indsamlet til.

Det betyder, at man skal vurdere konkret, hvor længe en oplysning opbevares. Desuden stiller lovgivningen i visse tilfælde krav om, hvor længe personoplysninger skal opbevares.

Se om opbevaring af fratrådte medarbejderes personalemappe under punkt 3.3.3.

3.2.2 Samtykke til behandling

Der kræves som udgangspunkt ikke samtykke til at behandle personoplysninger om jeres medarbejdere i forbindelse med ansættelsesforholdet.

I behøver derfor ikke samtykke til behandling af identifikationsoplysninger såsom medarbejderens navn, adresse og telefonnummer, fødselsdato, nær familie, oplysninger om uddannelse, udtalelser, tidligere beskæftigelse, nuværende stilling, arbejdsopgaver, arbejdstider og andre tjenstlige forhold, oplysninger om løn, skat, sygefravær og sygdomsperioder, oplysninger om andet fravær fra arbejdet, oplysninger om pensionsforhold, skatteoplysninger og oplysninger om kontonummer, hvortil løn skal anvises.

Oftest kan I kun registrere følsomme oplysninger, fx helbredsoplysninger, hvis medarbejderen har givet udtrykkeligt samtykke til dette. Dog kan det fremgå af lovgivning eller bestemmelser ifølge overenskomster, at I er forpligtet til at registrere følsomme oplysninger, fx helbredsoplysninger i en § 56-aftale eller hvis I gennemfører en afskedigelsessag, hvor årsagen skal fremgå.

Menighedsrådet skal kun registrere fagforeningsforhold, hvis det er nødvendigt, fx fordi medarbejderen er tillidsrepræsentant.

3.2.3 Indsigt i opbevarede personoplysninger

Hvis en medarbejder beder om indsigt i de personoplysninger menighedsrådet har, da skal menighedsrådet oplyse de konkrete oplysninger, så medarbejderen har mulighed for at vurdere, om oplysningerne er korrekte.

3.2.4 Videregivelse af personoplysninger

Menighedsrådet må give personaleoplysninger videre, hvis der er hjemmel hertil.

Der er lovhjemmel til, at menighedsrådet må give personoplysninger til SKAT eller til kommunen i forbindelse med en refusionssag. Oplysninger må også videregives til virk.dk i forbindelse med anmeldelse af en arbejdsskadesag.

I kan også give personoplysninger til de forhandlingsberettigede organisationer (i forbindelse med lønforhandlinger eller personalesager) og til pensionsselskaberne.

Menighedsrådene må orientere en medarbejders kolleger om, at en medarbejder har ferie, fri, orlov eller sygdom. Menighedsrådet må dog ikke oplyse, hvorhen medarbejderen skal på ferie, hvilken type orlov eller sygdom medarbejderen har. Menighedsrådet må ikke orientere menigheden eller samarbejdspartnere om årsagen til fravær.

3.2.4.1 Aktindsigt i medarbejderens personoplysninger

Hvis menighedsrådet modtager en anmodning om aktindsigt i en sag, som en medarbejders personoplysninger indgår i, skal I normalt videregive oplysningerne, medmindre oplysningerne er fortrolige.

Hvis menighedsrådet modtager en anmodning om aktindsigt i en medarbejders personalesag, skal I give indsigt i oplysninger om medarbejderens navn, stilling, uddannelse, arbejdsopgaver, lønmæssige forhold og tjenesterejser. For så vidt angår ansatte i chefstillinger, gives endvidere indsigt i oplysninger om disciplinære reaktioner i form af advarsel eller derover. Det gælder dog kun for et tidsrum af 2 år efter, at den endelige afgørelse er truffet.

Hvis der meddeles aktindsigt, så skal medarbejderen orienteres om, hvilke oplysninger, der gives indsigt i. Orienteringen skal ske inden oplysningerne udleveres.

Reglerne omkring aktindsigt er ikke en følge af GDPR-reglerne men følger af offentlighedsloven.

3.2.5 MUS-samtaler

Menighedsrådet skal opbevare udviklingsplanen, udarbejdet i forbindelse med den årlige MUS, i medarbejderens personalemappe. Oplysningerne må kun deles med personer, der har en ledelsesopgave overfor medarbejderen. Dog må oplysninger vedrørende finansiering af kurser/uddannelse deles med hele menighedsrådet, for at menighedsrådet kan træffe beslutning om kompetenceudvikling.

3.2.6 Offentliggørelse af medarbejders navn, kontaktoplysninger og billede

Menighedsrådet må gerne oplyse medarbejderes navn, arbejdsområde og arbejdsmæssige kontaktoplysninger på sogn.dk, egen hjemmeside og kirkebladet uden samtykke.

En medarbejder skal ikke anvende privattelefonnummer og privat mail- og postadresse som led i sit arbejde. Hvis det alligevel sker, så skal medarbejder give samtykke til offentliggørelse heraf. Intern deling af en medarbejders private kontaktoplysninger kan kun ske med samtykke.

Det kræver samtykke fra medarbejderen at offentliggøre billeder (både portræt- og situationsbilleder) af denne på sognets informationssider fx kirkebladet, hjemmeside, sogn.dk, facebook, instagram og andre elektroniske platforme. I skal også have samtykke, hvis I bruger deres billede på opslagstavler, dørskilte og andet. Hvis den ansatte vælger at trække sit samtykke tilbage, påvirker det ikke lovligheden af den behandling, der er baseret på samtykke, inden tilbagekaldelsen. Tilbagekaldelse af samtykke vedrører kun den fremtidige brug af billeder.

Et samtykke kan være skriftligt, og skal opbevares i medarbejderens personalemappe. På samtykkeerklæringen skal det angives, at samtykket kan tilbagekaldes – og at det medfører, at der efter tilbagekaldelsen ikke mere må benyttes billeder af medarbejderen.

Vi har udarbejdet en skabelon til en samtykkeerklæring til foto og videooptagelse af medarbejdere, som menighedsrådene kan benytte.

3.2.7 Pårørendeliste

En pårørendeliste er en notits på den ansattes personalesag eller lignende, f.eks. en liste, hvor den ansatte kan indføre – eller få indført – en pårørendes telefonnummer med henblik på, at den pårørende kan kontaktes, hvis der skulle ske et uheld involverende den ansatte.

Hvis menighedsrådet vælger at oprette en pårørendeliste, med angivelse af en pårørendes navn, relation og telefonnummer, skal menighedsrådet overholde oplysningspligten overfor den registrerede. Det vil sige,

at menighedsrådet skal oplyse den pårørende om, hvilke oplysninger der behandles, hvor længe oplysningerne behandles, hvorfor I behandler oplysningen og hvor oplysningen kommer fra, samt hvilken hjemmel der anvendes[21]. Herudover skal informationerne fra privatlivspolitikken oplyses. Oplysningerne skal gives indenfor en måned.

Den pårørende har mulighed for at bede menighedsrådet om at slette oplysningerne.

Hvis medarbejderne selv vælger at lave en pårørendeliste, så er menighedsrådet ikke dataansvarlig for listen, og ovenstående gælder ikke.

3.3 Fratrådte medarbejdere

3.3.1 Orientering til øvrige medarbejdere

Menighedsrådet må gerne orientere øvrige medarbejdere om, at en medarbejder er fratrådt eller er blevet opsagt. Menighedsrådet må ikke oplyse baggrunden for afskedigelsen.

3.3.2 Lukning af en fratrådt medarbejders mail

Når en medarbejder er fratrådt og ikke længere kan få adgang til sin personlige mailkonto på arbejdspladsen, må mailkontoen kun holdes aktiv i en periode, der er så kort som muligt. Periodens længde fastsættes under hensyntagen til den fratrådte medarbejders stilling og funktion og kan maksimalt være på 12 måneder.

Den aktive mailkonto må kun benyttes til modtagelse af mails. Hvis der modtages private mails, kan mailkontoen dog benyttes til at videresende disse til den fratrådte medarbejders private mailkonto. Kun en enkelt eller ganske få betroede medarbejdere bør have adgang til den fratrådte medarbejders mailkonto.

Eventuelle oplysninger om en direkte mailadresse til den pågældende bør hurtigst muligt fjernes fra arbejdspladsens hjemmeside og fra andre offentligt tilgængelige informationssteder. I forbindelse med fratrædelsen bør der indsættes et autosvar med besked om medarbejderens fratræden og eventuel anden relevant information.

3.3.3 Opbevaring af oplysninger

For personalemapper på fratrådte medarbejdere er udgangspunktet, at de må opbevares i 5 år efter ansættelsesforholdets ophør. Bogføringsmateriale – herunder lønsedler, pension, kørselsgodtgørelse, dokumentation for udlæg, mv. skal gemmes i 5 år fra udløbet af det pågældende regnskabsår.

Vær opmærksom på forældelsesloven, da der gælder en absolut forældelsesfrist på 10 år i personalesager og 30 år i arbejdsskadesager. Dvs. hvis I har haft en personalesag eller en arbejdsskadesag, så kan det være nødvendigt at opbevare oplysningerne i længere tid.

4.0 Menighedsrådets oplysningspligt

4.1 Privatlivspolitik

Alle menighedsråd skal udarbejde en privatlivspolitik, der informerer om hvordan I indhenter, opbevarer og sletter oplysninger om personer, der har kontakt til kirken eller menighedsrådet. Det kan fx være oplysninger om medlemmer af menigheden, medarbejdere, samarbejdsparter og øvrige personer, som menighedsrådet er i kontakt med.

[21] Databeskyttelsesforordningen art. 6, stk. 1, litra f

Hvis I ikke selv har udarbejdet en privatlivspolitik, kan I se en tekstskabelon til privatlivspolitik, som blot skal udfyldes med menighedsrådets navn og kontaktoplysninger. Klik her for tekstskabelon til privatlivspolitik. Skabelon kan også findes i grupperummet på FIN under "Registreredes rettigheder".

Når I har lavet en privatlivspolitik, skal I informere om jeres privatlivspolitik overfor personer, der henvender sig til sognet og som I behandler oplysninger om.

Når I modtager en mail på en af de officielle mailadresser, skal I sende et (auto)svar. Svaret skal enten indeholde jeres privatlivspolitik - eller indeholde et link til sognets hjemmeside, der viser privatlivspolitikken (man skal lande direkte på privatlivspolitikken ved at klikke på linket).

En officiel mailadresse er de mailadresser, der fremgår af jeres hjemmeside og www.sogn.dk. Det kan fx være 1234@sogn.dk, 1234fortrolig@sogn.dk, kirke.sogn@km.dk.

Ved behov for hjælp til opsætning af autosvar, kontakt Folkekirkens IT. Se mere om autosvar på mails indeholdende privatlivspolitikken under punkt 4.3.

Privatlivspolitikken skal derudover placeres på egen hjemmeside og i nyhedsbreve samt på opslagstavler, hvis der fx laves tilmeldingslister til arrangementer.

Gennemgå og opdater privatlivspolitikken en gang om året.

Tjekliste

- Har I udarbejdet en privatlivspolitik?
  - Hvis nej, se vejledning til hvordan privatlivspolitik udarbejdes
  - Hvis ja, gør den tilgængelig på egen hjemmeside
  - Hvis ja, henvis til den i autosvar ved henvendelser til jeres hovedpostkasse(r).

4.1.1 Privatlivspolitik for ansøgere, nuværende og fratrådte medarbejdere

Ansøgere og medarbejdere skal oplyses om, hvordan I behandler deres personoplysninger. Menighedsrådet skal derfor udarbejde en privatlivspolitik for ansøgere, nuværende og tidligere medarbejdere.

Hvis I ikke selv har udarbejdet en privatlivspolitik for ansøgere, nuværende og fratrådte medarbejdere, kan I se en tekstskabelon til privatlivspolitik her, som blot skal udfyldes med menighedsrådets navn og kontaktoplysninger.

I skal linke til privatlivspolitikken i stillingsopslag eller alternativt sende den med kvitteringen for modtagelse af ansøgningen. I skal også udlevere privatlivspolitikken til nuværende medarbejdere.

Tjekliste

- Har I udarbejdet en privatlivspolitik for ansøgere, nuværende og fratrådte medarbejdere?
  - Hvis nej, se vejledning til hvordan privatlivspolitik udarbejdes
  - Hvis ja, udlever den til jeres medarbejdere
  - Hvis ja, henvis til den i stillingsopslag alternativt send til ansøgerne med kvitteringsmail.

4.2 Cookies på hjemmeside

I har informationspligt overfor personer, der bruger jeres hjemmeside, hvis I har en hjemmeside der anvender cookies[22].

Hvad er en cookie?
En cookie er en tekstfil, der sættes på besøgerens computer, når vedkommende besøger en hjemmeside. I denne tekstfil gemmer hjemmesiden informationer, som den gerne vil kunne læse, næste gang vedkommende besøger siden. Det er ofte informationer, der bruges til statistik og analyse, og er helt ufarlige.

En cookie er en tekstfil, ikke en programfil. Det betyder, at cookien ikke selv kan gøre noget på besøgerens computer. Den kan ikke indsamle oplysninger, sprede virus eller på anden måde gøre skade. Indholdet af cookies læses og skrives af de hjemmesider, vedkommende som bruger besøger.

Menighedsrådet er ikke forpligtet til at indhente cookies. Hvis der ikke anvendes cookies på egen hjemmeside, så skal menighedsrådet ikke gøre mere.

Hvis menighedsrådet anvender cookies på egen hjemmeside (ikke sogn.dk, da siden hører under Kirkeministeriet), skal der oplyses herom, når man benytter hjemmesiden. Bemærk, at informationen skal beskrive alle de cookies, som anvendes.

Når sognets hjemmeside besøges, skal der straks komme en "pop-up" med cookiepolitikken og et "Accept"-felt til accept af indhentelse af nødvendige/andre cookies.

Spørg evt. jeres hjemmesideudbyder, hvilke cookie-løsninger der tilbydes.

Se cookiepolitik her. Den findes også på FIN i grupperummet under "Registreredes rettigheder".

Tjekliste

- Bruger I cookies?
  - Hvis ja, har I en cookiepolitik?
  - Hvis ja, så skal I have en pop-up "accept"-knap på hjemmeside
  - Hvis nej, så skal I ikke gøre mere

4.3 Standardmeddelelser ved mails

Når der indsamles personoplysninger, skal de registrerede modtage en række informationer, blandt andet om den påtænkte behandling (dette betegnes som menighedsrådets oplysningspligt). Dette gøres i praksis via standardmeddelelser.

Når I modtager en mail på en af de officielle mailadresser, skal I sende et (auto)svar til opfyldelse af oplysningspligten ved den første henvendelse til menighedsrådet/sognet. Svaret skal enten indeholde jeres privatlivspolitik (se punkt 4.1) - eller indeholde et link til sognets hjemmeside der viser privatlivspolitikken (man skal lande direkte på privatlivspolitikken ved at klikke på linket). Hvis man ikke har egen hjemmeside, hvor privatlivspolitikken placeres og linkes til, så skal privatlivspolitikken sendes med.

[22] Se også Datatilsynets Vejledning om behandling af personoplysninger om hjemmesidebesøgende

Der findes her en skabelon til en standardmeddelelse, som menighedsrådet kan benytte. Skabelonen er også tilgængelig i grupperummet under "Registreredes rettigheder" (skabelonen er navngivet "Oplysningspligt").

De ansatte skal ikke benytte private mailadresser og en privat mailadresse skal ikke fremgå af jeres hjemmeside.

4.4 Nyhedsbreve

Hvis menighedsrådet tilbyder udsendelse af et nyhedsbrev, skal modtagere af nyhedsbrevet samtykke til den behandling af personoplysninger, som finder sted i forbindelse med registrering af modtagerens oplysninger.
Eksempel på den meddelelse, som skal fremgå ved tilmeldingen til modtagelse af et nyhedsbrev, kan ses i dette samtykke til nyhedsbrev.

Menighedsrådet skal sikre sig, at modtagere af nyhedsbreve aktivt har tilmeldt sig.

Menighedsrådet skal informere om, at modtagere af nyhedsbreve har ret til nemt og gratis at afmelde sig nyhedsbrevet. Det skal tydeligt fremgå af hvert eneste nyhedsbrev, at det er muligt at afmelde sig.

Ovenstående gælder uanset hvilket format nyhedsbrevet har, dvs. om det er mail, sms eller brevpost.

4.5 Offentliggørelse af billeder og videooptagelser

Offentliggørelse af billeder og videooptagelser på internettet af genkendelige personer betragtes som en behandling af personoplysninger. De databeskyttelsesretlige regler skal derfor være opfyldt, for at en sådan behandling (offentliggørelse af billedet og videooptagelsen) lovligt kan finde sted[23]. Det er afgørende, at de personer, der er på billedet, ikke med rimelighed kan føle sig udstillet, udnyttet eller krænket. Det indebærer bl.a., at menighedsrådet – inden menighedsrådet offentliggør billedet - skal have et grundlag for at offentliggøre billedet fx samtykke eller at det sker som led i samfundets interesse.

Der gælder de samme regler for offentliggørelse af billeder og videooptagelser, hvorfor de følgende afsnit gælder for begge dele.

Det er afgørende, at de personer, der er på billedet, ikke med rimelighed kan føle sig udstillet, udnyttet eller krænket, f.eks. i forbindelse med annoncering af arrangementer. Overvej derfor altid, hvilke eventuelle indvirkninger eller konsekvenser en offentliggørelse af billedet kan have for de personer, der er på billedet.

Børn og unge er ofte mindre bevidste om de risici og konsekvenser, som kan være forbundet med en behandling af personoplysninger. Hvis der derfor er tale om offentliggørelse af billeder med børn og unge, skal menighedsrådet – som en ekstra ting – tænke på, at denne gruppe af personer skal gives en særlig beskyttelse i forhold til, at de ikke kan føle sig udstillet, udnyttet eller krænket.

Tjekliste – læs mere i afsnittene nedenfor

- Er oplysningspligten opfyldt?
  - Skiltning
  - Oplysning fra fotograf, om at der tages billeder
  - Information om ret til indsigelse
- Kan vedkommende føle sig udstillet, udnyttet eller krænket?

[23] Se mere på Datatilsynets infoside om billeder på internettet

    - Særlig opmærksomhed på børn og unge
- Har menighedsrådet en samfundsmæssig interesse i at offentliggøre billedet?
- Kræver det samtykke at offentliggøre billedet?
    - Følsomme oplysninger – nadver, dåb, øvrige kirkelige handlinger
- Har medarbejdere og frivillige samtykket?

4.5.1 Offentliggørelse af billeder

Et billede kan offentliggøres, hvis det er nødvendigt, for at menighedsrådet kan udføre en opgave i samfundets interesse (se mere i punkt 2.3.2 om en opgave i samfundets interesse). Al sognepleje er at betragte som en opgave i samfundets interesse. Det er derfor i samfundets interesse at menighedsrådet kan fortælle om aktiviteter og arrangementer og reklamere for sine kommende arrangementer. Det gælder fx fællesspisninger, kor, gå-grupper mv.

Menighedsrådet må, uden samtykke, offentliggøre billeder af personer, der deltager i gudstjenester og kirkelige handlinger, da alle kan deltage i en offentlig gudstjeneste og deltagelsen i en gudstjeneste ikke umiddelbart fortæller noget om ens religiøse tilhørsforhold. Tilsvarende gælder for koncerter, foredrag og arrangementer, der foregår i kirkeligt regi.

Der skal være mulighed for og skiltet om at placere sig i områder, hvor der ikke tages billeder – se mere i punkt 4.5.3 om oplysningspligt og indsigelse.

Der gælder særlige regler om offentliggørelse af billeder fra nadver og religiøse handlinger – se næste punkt 4.5.2 om samtykke.

4.5.2 Samtykke

Menighedsrådet må ikke offentliggøre billeder af selve nadveren, dåben, konfirmationen, vielsen og begravelsen, medmindre menighedsrådet har samtykke dertil, da disse begivenheder netop kan sige noget om de pågældendes religiøse tilhørsforhold og derfor er følsomme oplysninger.

Hvis der tages billeder af deltagere i nadver, barnedåb mv. til brug for sognets udgivelser og kommunikationssteder på internettet, kræver det samtykke fra deltagerne. Samtykket skal kunne dokumenteres og det gøres bedst på skrift. Bemærk, at det er anderledes, hvis familien har aftalt med præsten, at familiemedlemmer eller fx dåbsgæster selv må tage billeder ved egen families dåb.

Se mere om krav til samtykke i punkt 2.3.3.

Offentliggørelse af billeder af medarbejdere – uanset situationen – kræver samtykke fra disse. Se mere under punkt 3.2.6.

4.5.3 Oplysningspligt og indsigelse

Når sognet har gudstjenester eller holder arrangementer, sangeftermiddage, kirkekaffe, fællesspisning, bibelkreds mv. kan der tages billeder, som benyttes på hjemmeside, nyhedsbreve og andet. Menighedsrådet skal sørge for, at den eller de personer, der er på billedet, er vidende om, at menighedsrådet har tænkt sig at offentliggøre billedet, så de har mulighed for at reagere, f.eks. gøre indsigelse imod det.

Deltagerne skal oplyses om, at der tages billeder til offentliggørelse og at de kan henvende sig til fotografen, hvis de ikke ønsker at medvirke på billeder. Der kan derudover suppleres med skilte ved indgangen til lokalet og i lokalet med hvor man kan placere sig, hvis man ikke ønsker at medvirke på billeder.

Hvis den person, der fremgår af billedet, er utilfreds med offentliggørelsen, har vedkommende ret til at gøre indsigelse. Det kan ske, før billedet er blevet offentliggjort eller på et senere tidspunkt. Personen skal i så fald oplyse, hvilket billede der ønskes slettet og hvorfor. Hvis den eller de personer, der er på billedet, ikke ønsker at have billedet liggende på internettet, bør I umiddelbart fjerne det.

5.0 Sikkerhed, sikkerhedsbrud og sletning

Regler og anbefalinger om sikkerhed følger ikke nødvendigvis af GDPR. Nogle anbefalinger er alment gældende om adgang til oplysninger mens andre er fastsat som krav særligt gældende i Folkekirken.

Landsforeningen har lavet en tekstskabelon til en sikkerheds- og slettepolitik, hvor også slettefrister for udvalgte emner fremgår. Hvis I behandler personoplysninger til andre formål end de angivne, skal I tage stilling til, hvilken slettefrist der gælder.

5.1 Sikkerhedsforanstaltninger

Menighedsrådet er ansvarligt for, at personoplysninger behandles sikkerhedsmæssigt forsvarligt. Det betyder, at menighedsrådet skal sikre, at ansatte, frivillige og menighedsrådsmedlemmer alle er bekendt med, hvordan oplysninger behandles sikkert. Oplysninger kan modtages på fx sms, mail el.lign., og det er menighedsrådets ansvar at sikre, at oplysningerne overføres til et sikkert opbevaringsmedie, fx på FIN.

5.1.1 Fysiske foranstaltninger

Fysiske foranstaltninger er ikke noget der reguleres af GDPR regler, men gælder alment om adgang til oplysninger.

Adgang til fysiske lokaliteter skal sikres mod uvedkommendes adgang. Lokaler, hvor der opbevares personoplysninger, skal være aflåst, når ingen medarbejdere er til stede. Hav derfor opmærksomhed på at kolleger, brugere og besøgende ved kirken ikke utilsigtet kan få adgang til personoplysninger. Indret fx kontoret så uvedkommende ikke utilsigtet kan få kiggeadgang til skærmen.

Fysiske dokumenter, der indeholder personoplysninger, skal opbevares på en måde, så de ikke er tilgængelige for uvedkommende, og så kun personer med et arbejdsbetinget behov kan anvende dem. Ved arbejdsdagens ophør må dokumenter med personoplysninger eller fortrolige oplysninger ikke ligge frit fremme på arbejdspladsen, herunder en eventuel hjemmearbejdsplads.

Fx skal det sikres, at kirketjener ikke kan få indsigt i de lønoplysninger kordegnen arbejder med. Eller graveren bruger en blok, hvor der noteres cpr-nr., før dette elektronisk indføres i Gravstedssystemet (elektronisk). Fortrolighed omkring papirblokken er ikke reguleret af GDPR-regler, men følger af almindelige principper om fortrolighed.

Menighedsrådet kan indføre fysiske foranstaltninger som

- Arbejdsmæssig adgang (lokaler, skabe mv.)
- Kontorets indretning (skærme)
- Opbevaring (lokaler, skabe mv.)
- Adgangskontrol (besøgende)
- Koder, alarm
- Bortskaffelse/makulering

5.1.2 Tekniske foranstaltninger

Vær opmærksom på, at Kirkeministeriet har ansvaret for sikkerheden på en Kirkenets PC og de systemer, som Kirkeministeriet stiller til rådighed. Når menighedsrådet anvender de it-systemer Kirkeministeriet stiller til rådighed fx FIN, GIAS, OneDrive mv., så *er* alle disse ting på plads, da menighedsrådet med jeres FIN-login har en sikret adgang.

Menighedsrådet har ansvaret for egne anskaffede pc'er og systemer i kirken fx til kirketjeneren eller graveren. Dvs. menighedsrådet er ansvarlig for antivirusprogram, adgangskoder mv.

Menighedsrådet kan indføre tekniske foranstaltninger som fx

- Arbejdsbetinget adgang
- Alene adgang til arbejdsstationer med individuelt brugernavn og adgangskode
- Brugeren skal logge af eller låse sin it-arbejdsstation hver gang den forlades
- Krav om at adgangskode er minimum X antal tegn (Adgangskode antal tegn/indeholde store, små bogstaver, tal, specialtegn, udskiftningsinterval)
- Der er installeret antivirusprogram – som også kan lave løbende automatisk viruscheck
- Der foretages kontrol med afviste adgangsforsøg, låsning efter x antal fejlslagne
- Automatisk timet logud ved inaktivitet
- Al forsendelse og opbevaring sker krypteret
- Mobilt udstyr skal være sikret med PIN- eller adgangskode
- Der benyttes VPN og kryptering ved hjemmearbejde
- Gæstenetværk

5.1.3 Organisatoriske foranstaltninger

Menighedsrådet er forpligtet til at lave fortegnelser over forskellige formål, data, herunder gruppering, risikovurderinger, slettefrister og kontrolforanstaltninger. (se punkt 7.0 Fortegnelser – og punkt 5.4 Sletning).

Menighedsrådet kan indføre organisatoriske foranstaltninger som fx

- Formålsbeskrivelse og beskrivelse af hvilke oplysninger, der behandles
- Uddannelse/instruktion af medarbejdere/andre tilknyttede om opbevaring, sikkerhed, fortrolighed og omgang med data
- Forholdsregler, kommunikationsveje og -frister samt reaktion ved sikkerhedsbrud
- Egenkontrol af ovenstående
- Tilslutning til Adfærdskodeks (se punkt 8.0)

5.2 Informationssikkerhed

Kirkeministeriet har lavet et cirkulære[24], som udmønter de konkrete retningslinjer for informationssikkerhedspolitikken[25] for Kirkeministeriet og Den Danske Folkekirke. Cirkulæret indeholder regler for både menighedsråd, præster og folkekirkens IT. Det er et bredt cirkulære om bl.a. sikkerhedsorganisation, brug af udstyr, autorisering af brugere, kirkenettet – adgang og brug, beskyttelse af data, sikkerhedsansvarliges tilsyn og brud.

[24] https://www.retsinformation.dk/eli/retsinfo/2021/10009
[25] https://support.kirkenettet.dk/hc/da/articles/4412087703698-Informationssikkerhedspolitik-for-Kirkeministeriet-og-Den-danske-folkekirke

5.2.1 FIN-adgange

Folkekirkens IntraNet (FIN) er en lukket og sikker platform, hvor menighedsrådet kan dele oplysninger.

Menighedsrådet har automatisk to adgange til FIN via login med NemID/MitID, der som udgangspunkt gives til formanden og kontaktpersonen, medmindre formanden vælger andet. Derudover kan der tilkøbes adgange til de øvrige menighedsrådsmedlemmer. På FIN er der adgang til den almindelige fælles sognemail og tilhørende arkiv.

Arkivet kan fx bruges til dagsorden/bilag til menighedsrådsmøder.

Hvis et medlem har en enkeltmandspost fx kasserer, kontaktperson, kirkeværge mv. så fremgår dette af FIN, og vedkommende har adgang til relevante mapper på FIN. Fx har kontaktperson og formand automatisk adgang til fortrolig-postkassen, samt tilhørende arkiv, hvor der fx kan oprettes personalemapper. Formanden kan som sikkerhedsansvarlig vælge, om andre i rådet eller fx en ansat skal have adgang til fortrolig-postkassen. Adgange skal fornys hver 6. måned, ellers bortfalder de.

Hvis en medarbejder eller et menighedsrådsmedlem ikke længere har behov for adgangen, skal adgangen fratages omgående, fx hvis vedkommende fratræder.

Når adgang til FIN sker via en privat pc, skal der være særlig opmærksomhed på, at materiale der indeholder personoplysninger eller fortrolige oplysninger, ikke må gemmes på privat udstyr.

Det er menighedsrådets ansvar at sikre, at oplysninger, der modtages på fx sms, mail el.lign., overføres til et sikkert opbevaringsmedie, fx på FIN. Menighedsrådet må kun gemme personoplysninger hos internettjenester, som Kirkeministeriet administrerer eller som menighedsrådet har en databehandleraftale med. Det er fx FIN, GIAS, FLØS. Derudover kan menighedsrådet have aftaler med fx Brandsoft, Skovbo Data mv.

5.2.2 Mail og sms

Menighedsrådet er ansvarligt for, at personoplysninger sendes sikkert på mail.

Der må ikke anvendes sms til forsendelse af fortrolige eller følsomme personoplysninger.

5.2.2.1 Sikker mail

Datatilsynet anbefaler, at mail sendes med TLS-kryptering, altså at transporten er sikker. Når en oplysning sendes gennem internettet, så kan alle læse den. TLS er en ”nøgle” der dannes unikt hos afsender og modtager, og kun hvis begge parter har ”nøglen” sendes en mail med TLS-kryptering. Når der sendes med TLS, så sendes data afsted i små stykker, som samles i modtagerens indbakke. Når I sender mails via kirkenettet (@sogn.dk eller @km.dk), så er der tvungen TLS, dvs. en mail kan ikke afsendes, hvis ikke modtager har TLS.

Menighedsrådsmedlemmer kan sende fortrolige eller følsomme personoplysninger til *eksterne* via almindelig mail, så længe der sendes fra sogn.dk/km.dk og der er sikkerhed om modtagerens identitet. Hvis der er tvivl om identiteten, skal fortrolige og følsomme personoplysninger sendes via Digital Post. Det har kordegnen og præsten adgang til, idet de har en Kirkenets-pc.

1234@sogn.dk	alle menighedsrådsmedlemmer med FIN-licens har adgang
1234fortrolig@sogn.dk	formand og kontaktperson har adgang – formand kan give adgang til andre (via FIN)

Det er ikke tilladt at opsætte en generel regel om videresendelse af mail til en postkasse uden for Kirkenettet.

Eksempel: En fra menigheden har tilmeldt sig spisning, og har angivet, at vedkommende har fødevareallergi. Menighedsrådet/en medarbejder kan ved afsendelse fra en km/sogn.dk-mail skrive til vedkommendes gmail (som er ekstern), for at få bekræftet, at der er tale om glutenallergi og ikke nøddeallergi. Menighedsrådet kan *ikke* ved afsendelse fra en km/sogn.dk-mail skrive til en medarbejders gmail (som er intern), at deltageren har glutenallergi, fordi menighedsrådet har ansvaret for personoplysningerne i medarbejderens varetægt, og gmail ikke er sikker.

5.2.2.2 "Egen" mail

Menighedsrådet kan have oprettet "egne" mailkonti udenfor kirkenettet fx formand@voreskirke.dk, kirketjener@voreskirke.dk. Menighedsrådet er selv ansvarlig for, at der kan sendes sikkert fra disse mailkonti samt at opbevaring sker sikkert. Menighedsrådet kan kontakte mailudbyder for oplysning og korrekt opsætning.

Hvis menighedsrådet selv har oprettet en voreskirke@gmail.com, NNkirkegård@hotmail.com er hverken forsendelse eller opbevaring sikker.

5.2.3 Den sikkerhedsansvarlige

I menighedsrådet er formanden sikkerhedsansvarlig. Menighedsrådet kan dog beslutte at tillægge rollen til et andet medlem af menighedsrådet eller til en sognepræst.

Den lokale sikkerhedsansvarlige har ansvaret for, at personoplysninger behandles sikkerhedsmæssigt forsvarligt. Det betyder, at den sikkerhedsansvarlige skal sikre, at ansatte, frivillige og menighedsrådsmedlemmer alle er bekendt med, hvordan oplysninger behandles sikkert og at der udvises sikker it-adfærd. Derudover skal der føres tilsyn med, at fysiske dokumenter med følsomme eller fortrolige personoplysninger håndteres hensigtsmæssigt, og reageres på uhensigtsmæssig adfærd eller andet, der udfordrer informationssikkerheden.

Når der vælges nye menighedsrådsmedlemmer eller ansættes nye medarbejdere, som har fået adgang til Kirkenettets systemer, så skal den sikkerhedsansvarlige udlevere informationssikkerhedspolitikken samt tilhørende cirkulære (se links i punkt 5.2), og de nye brugere skal læse dette.

Den sikkerhedsansvarlige skal administrere hvilke brugere, der har adgang til hvilke it-systemer. Hvert halve år skal den sikkerhedsansvarlige kontrollere, at de enkelte brugere kun er tildelt rettigheder på FIN, som brugeren arbejdsmæssigt har behov for. Den sikkerhedsansvarlige modtager en mail forud for genautorisering, hvor fremgangsmåde og frist er beskrevet. Hvis ikke fristen overholdes, så mister brugeren adgangen.

Sådan kan den sikkerhedsansvarlige gribe opgaven an:

1) Sæt dig ind i informationssikkerhedspolitikken og cirkulæret (links findes i punkt 5.2).
2) Dan dig et overblik over, hvilke it-systemer og kirkenet-udstyr, menighedsrådet råder over, og hvem der er brugere. Sæt dig også ind i, hvordan fysiske dokumenter med følsomme og fortrolige personoplysninger håndteres.
3) Instruér alle om god og sikker adfærd. Det kan f.eks. ske på et menighedsrådsmøde, det næste medarbejdermøde og det næste møde med eventuelle frivillige ved kirken. Tag udgangspunkt i cirkulæret, der blandt andet beskriver, hvordan I skal håndtere fysiske dokumenter, hvordan personfølsomme oplysninger kan sendes digitalt og hvad I gør ved sikkerhedsbrud.

5.3 Brud på datasikkerheden

Definition på sikkerhedsbrud[26]:
*"Hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til **personoplysninger**, der er transmitteret, opbevaret eller på anden måde behandlet."*

Et sikkerhedsbrud kan fx være en medarbejder, der ændrer eller sletter personoplysninger ved et uheld eller en medarbejder, der bevidst eller ubevidst videregiver personoplysninger om en kirkebruger til en anden kirkebruger – eller måske ligefrem flere uvedkommende personer (fx maillister, hvor der sendes cc til alle på maillisten, så alle modtagere kan se, hvem der er sendt til – i stedet for bcc). Det kan også være en medarbejders/menighedsrådsmedlems pc der er blevet hacket.

Hvis sikkerhedsbruddet medfører risiko for personers rettigheder, skal der ske anmeldelse til Datatilsynet.

Hvis sikkerhedsbruddet medfører høj risiko for personers rettigheder, skal der ud over anmeldelse til Datatilsynet også ske underretning til den registrerede.

"En risiko for fysiske personers rettigheder og frihedsrettigheder omfatter bl.a. diskrimination, identitetstyveri eller -svindel, økonomisk tab, skade på omdømme, tab af fortrolighed af data underlagt tavshedspligt eller enhver anden væsentlig økonomisk eller social ulempe for den registrerede."

5.3.1 Anmeldelse til Datatilsynet

For at vurdere om der er sket et brud, som kræver anmeldelse til Datatilsynet, skal flere elementer indgå.

Menighedsrådet skal indledningsvist vurdere om bruddet medfører en risiko for personers rettigheder eller frihedsrettigheder.

"En risiko for fysiske personers rettigheder og frihedsrettigheder omfatter bl.a. diskrimination, identitetstyveri eller -svindel, økonomisk tab, skade på omdømme, tab af fortrolighed af data underlagt tavshedspligt eller enhver anden væsentlig økonomisk eller social ulempe for den registrerede."

Det har betydning hvilket omfang bruddet har. Er der tale om mange oplysninger eller få oplysninger? Vedrører det mange eller få personer? Hvad er den tidsmæssige udstrækning? Hvilken type oplysninger er der tale om? Hvis der fx er tale om følsomme oplysninger, så kan selv én oplysning være nok til at der skal ske anmeldelse.

Dernæst skal der ses på alvorligheden af konsekvenser for de berørte personer. Hvis der er tale om følsomme eller fortrolige oplysninger, kan konsekvenserne af et brud for den registrerede være alvorligere. Fx hvis bruddet involverer oplysninger om helbred, cpr.nr., økonomi mv. Der kan også være særlige forhold hos den registrerede, som skærper vurderingen. Fx hvis der er tale om børn eller sårbare (demente, handicappede mv.), der ikke selv kan tage vare på at beskytte sig.

Det er således det samlede *aktuelle* risikobillede, der er afgørende for, om der skal ske anmeldelse af et brud på persondatasikkerheden til Datatilsynet.

Hvis der er tvivl om anmeldelse er nødvendigt, så anmeld – hellere en anmeldelse for meget end en for lidt.

[26] Databeskyttelsesforordningen artikel 4, nr. 12
Se også Datatilsynets Vejledning om håndtering af brud på persondatasikkerheden

5.3.1.4 Procedure og frist

Anmeldelse skal ske uden unødig forsinkelse og senest 72 timer efter bruddet opdages. Der tages ikke hensyn til weekend, helligdage, ferier mv. Overskrides de 72 timer, skal den dataansvarlige være i stand til at redegøre for de særlige grunde, der umuliggjorde anmeldelse til Datatilsynet inden for fristen.

Anmeldelse kan ske trinvis og kan senere suppleres. At den dataansvarlige ikke er i stand til at afgive alle de oplysninger, der som minimum skal med i anmeldelsen, inden for tidsfristen på de 72 timer, kan ikke udgøre en begrundelse for at fravige det overordnede krav om, at anmeldelse af bruddet skal ske til Datatilsynet inden for 72 timer. Den dataansvarlige må i stedet afgive oplysninger trinvist til Datatilsynet uden yderligere forsinkelse.

Anmeldelse sker via det offentlige indberetningssystem www.virk.dk og kræver at anmelderen har sognets brugeradgang til www.virk.dk. Oftest har en kordegn brugeradgang til www.virk.dk for at kunne indberette sygedagpengerefusion mv. Vær opmærksom på, at det derfor kan være en fordel at et menighedsrådsmedlem også har brugeradgang, så indberetning af brud kan ske rettidigt også selv om kordegnen er fraværende.

I www.virk.dk bliver anmelderen ledt igennem en formular med alle de oplysninger, der kan oplyses om databruddet. Formularen indsendes, også selv om der kun kan laves en delvis anmeldelse, der senere suppleres. En række minimumskrav til indholdet af anmeldelsen (udfyldes i formularen):

- Karakteren af bruddet på persondatasikkerheden mv.
- Navn på og kontaktoplysninger for databeskyttelsesrådgiveren eller et andet kontaktpunkt, hvor yderligere oplysninger kan indhentes
- De sandsynlige konsekvenser af bruddet på persondatasikkerheden
- De foranstaltninger, som den dataansvarlige har truffet eller foreslår truffet for at håndtere bruddet på persondatasikkerheden, herunder, hvis det er relevant, foranstaltninger for at begrænse dets mulige skadevirkninger

5.3.2 Underretning af den registrerede

Menighedsrådet skal lave en risikovurdering for at afgøre om der skal ske underretning. Alle de mulige konsekvenser og negative virkninger for den registrerede bør tages i betragtning.

Underretning skal ske, hvis bruddet indebærer en **høj risiko** for fysiske personers rettigheder og frihedsrettigheder. Der findes i databeskyttelsesforordningen ikke en definition af begrebet "høj risiko". Det må ved en vurdering af risikoens omfang, lægges til grund, at jo mere alvorlige konsekvenser bruddet kan medføre, jo større vil risikoen være for de berørte personer. Eksempler på brud, hvor man vurderer, at der er høj risiko for den registrerede, kan være læk af cpr.nr. (risiko for identitetstyveri) eller hemmelig adresse (risiko for at "blive fundet").

Underretning skal ske til den enkelte registrerede uden unødig forsinkelse.

Underretningen, der skal gives i et klart og forståeligt sprog, skal beskrive karakteren af bruddet og mindst indeholde oplysninger om:

- Navn på og kontaktoplysninger for databeskyttelsesrådgiveren eller et andet kontaktpunkt, hvor yderligere oplysninger kan indhentes
- De sandsynlige konsekvenser af bruddet på persondatasikkerheden

- De foranstaltninger, som den dataansvarlige har truffet eller foreslår truffet for at håndtere bruddet på persondatasikkerheden, herunder, hvis det er relevant, foranstaltninger for at begrænse dets mulige skadevirkninger

Det er ikke nødvendigt at underrette den registrerede, hvis en af følgende betingelser er opfyldt:

- Den dataansvarlige har gennemført passende tekniske og organisatoriske beskyttelsesforanstaltninger.
  Fx En kirketjener har haft mulighed for at "kigge med" på kirkekulturmedarbejders deltagerliste med spisning og allergier. Den datatansvarlige tager fat i kirketjener og gør opmærksom på tavshedspligten.
- Den dataansvarlige har truffet efterfølgende foranstaltninger, der sikrer, at den høje risiko for de registrerede ikke længere er reel.
- Det vil kræve en uforholdsmæssig indsats – i så fald skal der i stedet foretages en offentlig meddelelse eller tilsvarende foranstaltning, hvorved de registrerede underrettes på en tilsvarende effektiv måde.

5.3.3 Pligt til at logge hændelser

Log/registrer alle sikkerhedshændelser. Menighedsrådet skal dokumentere alle brud, herunder hændelser, der ikke indberettes som brud. Menighedsrådet skal beskrive de faktiske omstændigheder, konsekvenser og trufne afhjælpende foranstaltninger og om der er sket anmeldelse til Datatilsynet.

5.3.4 Eksempler

Eksempel	**Anmeldelse til Datatilsynet**	**Underretning af den registrerede**
Kirkesangers pc stjæles, indeholdende korlister med navn, adresse, mailadr., tlf.nr. PC er ikke krypteret.	Ja, idet bruddet indebærer en risiko for den registrerede.	Nej. Medmindre en registreret har hemmelig adresse – her kan underretning være nødvendig.
Et menighedsrådsmedlems private pc hackes. Ansøgninger til julehjælp ligger lokalt på pc'en i strid med menighedsrådets instruks.	Ja, idet bruddet indebærer en risiko for den registrerede.	Ja, da oplysninger i ansøgning om julehjælp ofte indeholder oplysninger af fortrolig karakter fx om økonomi.
Et menighedsrådsmedlems private pc hackes. Ansøgninger til julehjælp ligger på FIN, som kræver login.	Nej, idet bruddet ikke indebærer en risiko for den registrerede.	Nej
Kordegn sender deltagerliste til fællesspisning, med oplysning om allergener, til et forkert menighedsrådsmedlem. Modtageren sletter listen.	Ikke nødvendigvis, hvis menighedsrådet vurderer, at bruddet ikke indebærer en risiko for den registrerede.	Nej

5.4 Sletning

Menighedsrådene er forpligtet til at slette personoplysninger, når der ikke længere er behov for eller hjemmel til at opbevare dem[27]. Menighedsrådene kan behandle personoplysninger ud fra forskellige formål og dermed kan der også være forskellige hjemler for behandlingen.

Sletning betyder, at materiale slettes uigenkaldeligt og ikke kan gendannes eller anonymiseres, så det ikke er muligt at finde tilbage til den registrerede. Det betyder også, at de pågældende oplysninger skal slettes fra jeres backup, hvis det er teknisk muligt. Hvis I får brug for genetablering af data fra jeres backup, skal I fjerne de data fra backup'en, der i mellemtiden er slettet. Der skal derfor være viden om hvilket materiale der slettes, så samme materiale kan blive slettet i en gendannet backup (fx via en slettelog).

Vær opmærksom på, at en slettet mail, også skal slettes fra "Slettet post" ligesom en slettet deltagerliste i Word/Excel også skal slettes fra papirkurven.

Også fysisk materiale, som opbevares i et kartotek i et arkivskab, skal makuleres, når det ikke længere er relevant.

Menighedsrådet skal fastsætte en politik for, hvornår og hvordan personoplysninger slettes – se link til tekstskabelon for sikkerheds- og slettepolitik i punkt 5.0.

Menighedsrådet kan fx fastsætte slettefrister for behandling af oplysninger om stillingsansøgere, ansatte, sagsbehandling, julehjælp, brug af kirkebil mv.

6.0 Deling eller videregivelse af personoplysninger

Når Menighedsrådet deler eller videregiver personoplysninger, er det vigtigt at være opmærksom på, hvilken rolle rådet har i forbindelse med behandlingen – enten dataansvarlig eller databehandler, fordi kravene og forpligtelserne til dataansvarlige og databehandlere er forskellige. I udgangspunktet er det nemlig den dataansvarlige, som har ansvaret for, at en behandling af personoplysninger lever op til reglerne i databeskyttelsesforordningen.

***Dataansvarlig**: alene eller sammen med andre afgør, til hvilke formål og med hvilke hjælpemidler der må foretages behandling af personoplysninger*

***Fælles dataansvar**: flere myndigheder/parter har begge ansvaret for den persondata, som behandles.*

***Databehandler**: behandler personoplysninger på den dataansvarliges vegne. Den dataansvarlige har eneansvaret for den persondata, som behandles af en anden part og den dataansvarlige instruerer databehandleren.*

***Videregivelse**: personoplysninger videregives til en selvstændig dataansvarlig*

Et tip til at afklare, hvem der er dataansvarlig og hvem der er databehandler, er, at man skal lægge vægt på, hvem der træffer afgørelse om formål og hjælpemidler for behandlingen af personoplysningerne.

Hvis begge parter har lige stor indflydelse på formål, hjælpemidler mv., vil der være fælles dataansvar (se punkt 6.1).

Når et menighedsråd bestemmer formålet og hvordan personoplysningerne må behandles, så er menighedsrådet alene dataansvarlig og den anden part er databehandler (se punkt 6.2). Menighedsrådet

[27] Databeskyttelsesforordningen art. 17, stk. 1

bevarer retten til alene at bestemme formålet og de væsentligste behandlingsskridt, herunder indsamling, sletning, videregivelse og brug af eventuelle underdatabehandlere.

Hvis data deles med andre[28] skal der foreligge en skriftlig aftale om enten fælles dataansvar eller en databehandleraftale. Aftalen fastlægger, hvem der har ansvaret som hhv. dataansvarlig og databehandler – samt nærmere krav til hvordan databehandleren skal passe på de delte data.

6.1 Fælles dataansvar

I tilfælde, hvor 2 parter har lige indflydelse på at fastlægge formål og behandlingsmidler vedrørende indhentede personoplysninger er der fælles dataansvar. Det betyder, at begge parter har en fælles forpligtelse til at opfylde forpligtelserne som dataansvarlig på en gennemsigtig måde.

Se tekstskabelon til en aftale om fælles dataansvar.

6.1.1 Fælles dataansvar med Kirkeministeriet

Menighedsrådet deler oplysninger med Kirkeministeriet ved brug af fx GIAS, FIN og Sogn.dk - og her er allerede fastlagt fælles dataansvar. Dette gælder ved Kirkeministeriets fælles it-systemer vedrørende økonomi-, betalings-, administrations-, HR- og lønområdet.

Menighedsrådet har fælles dataansvar med Kirkeministeriet, når menighedsrådene benytter de it-løsninger, der stilles til rådighed af Kirkeministeriet.

Det gælder de fælles systemer vedrørende økonomi-, betalings-, administrations-, HR- og lønområdet.

- FIN
- Økonomiportalen
- FLØS
- GIAS

Det fælles dataansvar er reguleret i Kirkeministeriets cirkulære om fælles dataansvar, så menighedsrådet skal ikke foretage sig yderligere i henhold til benyttelse af disse systemer.

6.1.2 Fælles dataansvar med øvrige

Hvis menighedsrådet har fælles dataansvar med andre parter, fx et andet menighedsråd, skal der oprettes en aftale om fælles dataansvar. Se tekstskabelon i punkt 6.1.

Der kan fx være fælles dataansvar hvis flere menighedsråd deler hjemmeside som fx indsamler cookies eller bruges til at offentliggøre billeder af personer fra arrangementer. Eller der i kraft at samarbejdsaftaler deles oplysninger om fx medarbejdere. I disse samarbejder bør der afklares, hvilke oplysninger der deles, formål, behandlinger, varighed, fortrolighed, opbevaring, registreredes rettigheder mv.

Hav opmærksomhed på, at det fremgår i privatlivspolitik og fortegnelse, hvis der er fælles dataansvar.

6.2 Databehandleraftaler

Der skal være en databehandleraftale, hvis en aftale eller en del af en aftale mellem menighedsrådet og en anden part (en databehandler) går ud på, at denne anden part skal *behandle* (f.eks. indsamle, registrere, opbevare, videregive eller slette) personoplysninger efter instruks fra menighedsrådet som dataansvarlig.

En databehandleraftale skal være skriftlig og skal foreligge elektronisk.

[28] Databeskyttelsesforordningen art. 26 og art. 28

Datatilsynet har udarbejdet en skabelon til databehandleraftaler, som I kan finde på vores hjemmeside. Klik her for tekstskabelon til en databehandleraftale. Der er en væsentlig fordel forbundet med brugen af Datatilsynets skabelon, som består i den sikkerhed, der ligger i aftalens juridisk bindende status, der som nævnt betyder, at Datatilsynet fx i forbindelse med et tilsynsbesøg, ikke vil efterprøve det allerede fastlagte indhold.

En databehandleraftale **skal** fastsætte:

- Genstanden for behandling – hvilke oplysninger, der deles; det kan være navne, adresser (udsendelse af kirkeblad ved trykkeri) – eller navn og emailadresser (nyhedsbreve)
- Varigheden af behandlingen
- Behandlingens karakter og formål
- Typen af personoplysninger
- Kategorierne af registrerede
- Den dataansvarliges forpligtelser og rettigheder

Herunder skal der også være oplysninger om:

- Instruks fra den dataansvarlige – hvilken opgave der skal løses – formål
- Fortroligheds- og tavshedsforpligtelse
- Krav om behandlingssikkerhed fx opbevaring, adgangskoder, kryptering mv.
- Krav om brugen af underdatabehandlere – fx forbud mod at benytte underdatabehandlere – eller at det kun kan ske mod dataansvarliges godkendelse
- Forpligtelse til bistand ved besvarelse af anmodninger om udøvelse af de registreredes rettigheder om fx indsigt, berigtigelse, sletning mv.
- Krav om bistand til den dataansvarlige
- Forpligtelse til at slette og tilbagelevere data
- Forpligtelse til at stille alle nødvendige oplysninger til rådighed fx også slettelogs, som bevis på at databehandler har handlet på en instruks om sletning.

6.2.1 Eksterne it-systemer, som menighedsrådet kan tilslutte sig via FIN

Et menighedsråd kan benytte systemer, hvor databehandleraftalerne stilles til rådighed via Kirkeministeriet/Folkekirkens IT.

For disse systemer er der allerede udarbejdet databehandleraftaler og menighedsrådet er i denne relation dataansvarlig, mens systemleverandørerne er databehandlere. Menighedsrådet behøver derfor ikke selv udforme databehandleraftaler og lave instrukser til databehandlerne, men kan tilslutte sig aftalerne på FIN. Databehandleraftalerne kan ses på FIN på Kirkeportalen → "Adfærdskodeks og aftaler".

Det omfatter følgende systemer:

- DKM, Danmarks Kirkelige Mediecenter
- EG Brandsoft
- Skovbo Data
- Kirkeadministration

Menighedsrådene skal kun tilslutte sig de aftaler for de softwareløsninger, der benyttes.

6.2.2. Eksterne it-systemer, som menighedsrådet selv indgår databehandleraftaler med

Et menighedsråd kan selv anskaffe sig softwareløsninger, hvor der deles persondata med firmaer, der herved bliver databehandlere, fx hjemmesideudbydere, pladsbookingsystemer, kalendersystemer. Her har menighedsrådet ansvar for, at der laves en databehandleraftale.

Vær opmærksom på, at nogle softwareleverandører har nogle standardforretningsbetingelser, der er konstrueret således, at man ved accept af handelsbetingelserne også accepterer en indbygget databehandleraftale/aftale om fælles dataansvar. Der er eksempler på, at sådanne standardbetingelser fastlægger, at der er fælles dataansvar og at softwareleverandøren bliver "medejer" til data i systemet. Dette er fx set ved bookingsystemer.

I nogle situationer kan menighedsrådet i stedet for at tiltræde standardbetingelserne vælge at erstatte disse af en egen databehandleraftale. Se punkt 6.2.

Eksempel: Hvis menighedsrådet har en aftale med et trykkeri om fremstilling af kirkeblade, vil der være tale om levering af en ydelse, der ikke kræver en databehandleraftale. Hvis trykkeriet også skal uddele bladet til navngivne personer, vil der skulle laves en databehandleraftale. Hvis trykkeriet vælger at bruge et eksternt distributionsfirma til uddeling af kirkebladet, vil det skulle fremgå af jeres databehandleraftale, at der benyttes underdatabehandlere.

6.3 Videregivelse af oplysninger

Ved videregivelse er "modtagerparten" selvstændig dataansvarlig for behandling af de personoplysninger vedkommende modtager. Menighedsrådet skal have hjemmel til at videregive oplysninger fx i lov, overenskomster, samfundsmæssig interesse, kontrakt mv.

Der skal *ikke* indgås en aftale om fælles dataansvar eller en databehandleraftale når menighedsrådet udelukkende videregiver en oplysning, idet der netop ifølge lov, overenskomst, samfundsmæssig interesse, kontrakt mv. allerede er hjemmel til videregivelsen.

Hvis menighedsrådet tilbyder kirkebilskørsel, er en videregivet oplysning om fx navn og adresse på en kirkebilsbruger en praktisk nødvendighed for at kunne modtage kørselsydelsen fra vognmanden. Hjemlen til videregivelse er i dette tilfælde udførelse af en opgave i samfundets interesse.

Hvis en personalesag ikke kan løses lokalt, kan menighedsrådet videregive personoplysninger om overenskomstansatte til stifterne/ Kirkeministeriet. Det er indbygget i hovedaftaler, organisationsaftaler mv. at det er stifterne/Kirkeministeriet, der har forhandlingsretten ved fagretlig behandling. Det samme gælder for tjenestemænd, tjenestemandslignende og cirkulæreansatte, hvor kompetencen ligger hos stifterne/Kirkeministeriet.

7.0 Fortegnelser

Et menighedsråd har pligt til at lave fortegnelser over sine behandlingsaktiviteter[29]. Formålet med fortegnelsen er at dokumentere de overvejelser, som menighedsrådet alligevel skal foretage sig, idet:

1. den dataansvarlige (og databehandleren) har ansvaret for, at forordningens regler efterleves, og

[29] Databeskyttelsesforordningens art. 30
Se også Datatilsynets vejledning om Fortegnelser fra August 2018

2. den dataansvarlige skal også kunne påvise, at de behandlinger denne har ansvaret for lever op til forordningens regler.

Fortegnelser skal foreligge skriftligt og elektronisk. Det betyder, at du ikke udelukkende må føre fortegnelsen i et fysisk dokument eller efter hukommelsen. Der stilles ikke herudover krav til fortegnelsens format. Du vil således kunne føre fortegnelsen i et skema eller i et almindeligt tekstbehandlingsdokument. Klik her for tekstskabelon til en fortegnelse.

Fortegnelser er et internt dokument, og skal kun efter anmodning udleveres til Datatilsynet.

7.1 Indhold i en fortegnelse

Fortegnelser skal omfatte al behandlingsaktivitet uanset personoplysningernes karakter. En fortegnelse skal som minimum indeholde:

- Menighedsrådets **navn og kontaktoplysninger**, herunder andre aktører, hvis der fx er fælles dataansvar.
- **Samtlige formål** med behandlingsaktiviteter under menighedsrådets ansvar. Flere behandlingsaktiviteter kan samles i én fortegnelse, hvis der fx er tale om den samme opgave eller det samme lovgrundlag for behandlingerne. Menighedsrådene kan fx samle oplysninger om sognepleje, personaleadministration, kontraktsforhold eller gravstedsadministration i hver sin fortegnelse. Se mere i punkt 7.2 om fortegnelser på FIN.
  Det skal fremgå hvilke udtrykkeligt angivne og saglige formål en behandling af personoplysninger sker efter.
- **Kategorier af registrerede** afhænger af hvilken fortegnelse, der er tale om. Hvis det fx er fortegnelsen for personaleadministration, så kan registrerede fx være: ansøgere, nuværende og tidligere ansatte, pårørende, børn og unge under 18 år.
- **Kategorier af personoplysninger** kræver, at menighedsrådet som minimum kan anføre om der fx er tale om en almindelig oplysning eller en følsom oplysning (se punkt 2.2 Typer af personoplysninger). Hvis der behandles følsomme oplysninger, skal det specificeres nærmere hvilke oplysninger der behandles.
- Kategorier af **modtagere ved videregivelse samt hvilke oplysninger**, der gives til hvilke modtagere. Det kan fx være SKAT (identifikationsoplysninger, løn, personnummer), PBS (identifikationsoplysninger, personnummer) eller pensionskasser (identifikationsoplysninger, stilling og tjenestested, pensionsforhold, lønforhold).
- Overførsler til tredjelande og internationale organisationer – kan fx være hvis menighedsrådet bruger MailChimp til udsendelse af nyhedsbreve
- Hvis det er muligt, skal **slettefrister** fremgå (se punkt 5.4 Sletning)
- Tekniske og organisatoriske foranstaltninger skal beskrives generelt (se punkt 5.1 Sikkerhedsforanstaltninger)

7.2 Fortegnelser på FIN

Der er udarbejdet flere fortegnelser for menighedsrådene, som er tilgængelige på FIN (se Grupperum → Databeskyttelse → Fortegnelser). Der er bl.a. fortegnelser for personaleadministration, lønadministration, sagsbehandling, kommunikation mv.

Undersøg derfor først, om der allerede er en fortegnelse som dækker menighedsrådets behandling, inden menighedsrådet udarbejder egen fortegnelse.

8.0 Adfærdskodeks

Menighedsrådet kan vælge at tilslutte sig "Adfærdskodeks for menighedsråds behandling af personoplysninger som led i sognepleje". Kodeksen består af en række retningslinjer, der kan medvirke til korrekt anvendelse af databeskyttelseslovens regler. Den beskriver, hvordan menighedsrådet skal behandle personoplysninger som led i sogneplejen fx tilmeldinger til arrangementer, brug af kirkebil, brug af sociale medier mv.

Samtidig forpligter menighedsrådet sig også til at anvende intranetløsningen og arkivsystemet på Folkekirkens IntraNet (FIN) til al elektronisk sagsbehandling, administrative opgaver samt intern og ekstern kommunikation via menighedsrådets officielle mail-postkasser. Der er pligt til årligt at følge op på at menighedsrådet overholder Adfærdskodeksen.

Tilslutning sker ved, at menighedsrådet på et menighedsrådsmøde beslutter at ville tilslutte sig. Samtidig udvælger menighedsrådet et menighedsrådsmedlem, der kan foretage tilslutningen via en webløsning, som Kirkeministeriet stiller til rådighed.

Uanset om menighedsrådet vælger at tilslutte sig eller ej, indeholder kodeksen svar på mange af de praktiske udfordringer, som opstår i forbindelse med sognepleje.

Se adfærdskodeksen her samt på vores GDPR-side.