Kirkeministeriet

Persondatapolitik

for

Kirkeministeriet

og

Den danske folkekirke

FOLKEKIRKEN

Maj 2018

Indholdsfortegnelse

DEFINITIONER

Behandling	Enhver aktivitet eller række af aktiviteter - med eller uden brug af automatisk behandling - som personoplysninger eller en samling af personoplysninger gøres til genstand for, f.eks. 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.
Dataansvarlig	Den myndighed eller institution, der alene eller sammen med andre afgør, til hvilke formål og med hvilke hjælpemidler der må foretages behandling af personoplysninger.
Databeskyttelsesrådgiver	En databeskyttelsesrådgiver udpeget af Kirkeministeriet i medfør af artikel 37 i Databeskyttelsesforordningen.
Personoplysninger	Enhver oplysning, der direkte eller indirekte kan henføres til en identificeret eller identificerbar fysisk person ("den registrerede person"). Ved identificerbar fysisk person forstås en fysisk person, der direkte eller indirekte kan identificeres, navnlig ved en identifikator, som f.eks. et navn, et identifikationsnummer, lokaliseringsdata, en onlineidentifikator eller et eller flere elementer, der er særlige for denne fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sociale identitet.
Sikkerhedsansvarlige	De personer (roller), som i medfør af cirkulære om informationssikkerhed, herunder sikkerhedsforanstaltninger i Kirkenettet autoriserer brugere til Kirkenettet herunder fører tilsyn med sikkerheden.
Systemejer	Den person (rolle) hos den dataansvarlige, som har det overordnede ansvar for en given behandling i et eller flere it-systemer.

1. FORMÅL

Beskyttelse af personoplysninger er et fokusområde for Kirkeministeriet og folkekirken.

Formålet med denne persondatapolitik for Kirkeministeriet og folkekirken er at bidrage at behandle personoplysninger forsvarligt og i overensstemmelse med den til enhver tid gældende databeskyttelseslovgivning og Kirkeministeriets regler om behandling af personoplysninger.

Persondatapolitikken henvender sig til folkevalgte, medarbejdere og frivillige m.fl. i Kirkeministeriet og folkekirken.

2. BAGGRUND

Databeskyttelsesloven og databeskyttelsesforordningen – under et: databeskyttelseslovgivningen – finder anvendelse fra den 25. maj 2018 og indebærer en række forpligtelser for Kirkeministeriet og folkekirken i forhold til beskyttelse af personoplysninger, i forhold til at kunne dokumentere, hvordan personoplysninger behandles, og hvordan man overholder reglerne.

Udgangspunktet er, at de enkelte myndigheder og institutioner inden for Kirkeministeriets ressort hver især er ansvarlige for overholdelse af databeskyttelseslovgivningen.

Kirkeministeriet har dog et særligt ansvar i forbindelse med myndighedernes og institutionernes anvendelse af de fælles systemer, som Kirkeministeriet stiller til rådighed. Dette ansvar er beskrevet i cirkulærer om fælles dataansvar vedrørende fælles systemer, som stilles til rådighed af Kirkeministeriet.

Kirkeministeriet udarbejder i tillæg hertil en række regler og procedurer på persondataområdet blandt andet med henblik på at sikre, at myndigheder og institutioner inden for Kirkeministeriets ressort har egnede og effektive risikostyringsprocedurer, og for at minimere de risici, der er forbundet med behandling af personoplysninger, både for Kirkeministeriet, for folkekirken og for de registrerede personer.

Denne persondatapolitik sammenfatter en række af de centrale forpligtelser for Kirkeministeriet og folkekirken i henhold til databeskyttelseslovgivningen samt Kirkeministeriets regler og procedurer vedrørende behandling af persondata. Politikken findes på Den digitale arbejdsplads (DAP) og opdateres løbende, herunder med aktuelle links til relevante regler og procedurer. Den senest opdaterede persondatapolitik er således altid den, der er gældende.

3. ANVENDELSESOMRÅDE

Databeskyttelseslovgivningen finder anvendelse ved al behandling eller adgang til personoplysninger, som led i arbejde udført for Kirkeministeriet og folkekirkens myndigheder og institutioner.

3.1. GENERELLE FORPLIGTELSER

Alle behandlinger af personoplysninger i Kirkeministeriet og folkekirkens myndigheder og institutioner skal overholde databeskyttelseslovgivningen.

Alle, som får adgang til persondata, har pligt til at gøre sig bekendt med de til enhver tid gældende regelsæt på persondataområdet, herunder som sammenfattet i denne politik.

Kirkeministeriet og folkekirkens myndigheder og institutioner skal sikre, at enhver person, der udfører arbejde for Kirkeministeriet og folkekirken, og som får adgang til personoplysninger, kun behandler disse efter instruks, medmindre behandling kræves i henhold til anden lovgivning. Eksterne konsulenter skal ved indgåelse af konsulentaftale pålægges at efterleve relevante forpligtelser set i forhold til opgavens karakter.

3.2. NY ELLER ÆNDRET BEHANDLING

Før en ny behandling af personoplysninger iværksættes, eller når der ændres væsentligt i en allerede registreret behandling af personoplysninger, skal der tages de nødvendige skridt til at sikre, at behandlingen vil overholde databeskyttelseslovgivningen.

3.3. BEHANDLINGSPRINCIPPER

En række generelle behandlingsprincipper skal overholdes ved behandling af personoplysninger, og Kirkeministeriet og folkekirkens myndigheder og institutioner skal som dataansvarlige kunne dokumentere overholdelse heraf.

3.3.1. God databehandlingsskik

Enhver behandling af personoplysninger skal ske i overensstemmelse med god databehandlingsskik. Ved god databehandlingsskik forstås bl.a., at behandlingen er lovlig og rimelig, og at den registrerede får fyldestgørende oplysninger om, hvad de indsamlede data bliver anvendt til.

3.3.2. Formål med databehandlingen

Personoplysninger må alene behandles til varetagelse af et eller flere saglige formål, som skal være fastlagt på indsamlingstidspunktet. Personoplysningerne må som udgangspunkt alene benyttes til de formål, hvortil de blev indsamlet. Dog kan personoplysninger, der er indsamlet til ét formål, benyttes til et andet formål, der er foreneligt med det oprindelige formål, hvis behandlingen er tilladt i medfør af persondatalovgivningen eller anden lovgivning, eller der foreligger samtykke fra den registrerede.

3.3.3. Dataminimering

Personoplysninger skal være tilstrækkelige, relevante og begrænset til, hvad der er nødvendigt i forhold til de formål, hvortil oplysningerne behandles. Der må således ikke behandles oplysninger, som ikke er nødvendige eller proportionale.

3.3.4. Korrekthed

Personoplysninger skal være korrekte og om nødvendigt ajourførte. Kirkeministeriet og folkekirkens myndigheder og institutioner skal tage rimelige skridt for at sikre, at personoplysninger, der er urigtige i forhold til de formål, hvortil de behandles, slettes eller berigtiges.

3.3.5. Slettefrister

Personoplysninger skal slettes eller anonymiseres, når det ikke længere er nødvendigt at behandle dem af hensyn til de formål, hvortil oplysningerne blev indsamlet, eller af hensyn til eventuelt andre lovlige formål.

Kirkeministeriets vil udarbejde retningslinjer for en slettepolitik for de enkelte behandlingsområder.

3.3.6. Beskyttelse

Personoplysninger skal behandles på en måde, der under anvendelse af passende tekniske eller organisatoriske foranstaltninger, sikrer tilstrækkelig sikkerhed for beskyttelse af de pågældende personoplysninger, herunder beskyttelse mod uautoriseret eller ulovlig behandling og mod hændeligt tab, tilintetgørelse eller beskadigelse.

3.4. ANSVARLIGHED OG DOKUMENTATION

Kirkeministeriet fører tilsyn med, at Kirkeministeriet og folkekirkens myndigheder og institutioner opfylder de væsentligste kontrol- og dokumentationskrav med hensyn til hovedbehandlingsområderne for så vidt angår behandling af persondata inden for Kirkeministeriets ressort.

3.5. BEHANDLINGSHJEMMEL OG FORTEGNELSER

Lovlig behandling af personoplysninger kan i henhold databeskyttelsesforordningen blandt andet ske, når behandlingen er nødvendig af hensyn til 1) udførelse af en opgave i samfundets interesse, 2) offentlig myndighedsudøvelse, 3) opfyldelse af en kontrakt eller 4) for at overholde en retlig forpligtelse. Behandling kan også ske, når den registrerede har givet sit samtykke. Behandlingen skal i øvrigt foregå under iagttagelse af bestemmelserne i databeskyttelseslovgivningen.

Kirkeministeriet og folkekirkens behandlingshjemler er beskrevet i de centralt udarbejdede fortegnelser vedrørende brug af en række fælles systemer.

3.6. GENNEMSIGTIGHED OG REGISTREREDE PERSONERS RETTIGHEDER

3.6.1. Oplysningspligt

Når der indsamles personoplysninger, skal de registrerede modtage en række informationer, blandt andet om den påtænkte behandling. Dette gælder, uanset om oplysningerne indsamles hos den registrerede eller hos tredjepart. Dette gøres i praksis via standardmeddelelser, der kan basere sig på Datatilsynets skabelon.

Standardmeddelelsen kan efter omstændighederne indeholde links til uddybende omtale på de pågældende myndigheders og institutioners hjemmesider.

3.6.2. Henvendelser fra registrerede personer

De registrerede personer har en række rettigheder, når der behandles personoplysninger om dem, herunder en ret til – når visse betingelser er opfyldt – at få indsigt i, få rettet fejl i, få ajourført eller slettet oplysninger, samt til at få behandlingen af oplysningerne begrænset eller bragt til ophør efter indsigelse.

Kirkeministeriet fastlægger procedurer for behandling af registreredes begæring om udøvelse af heraf.

3.7. RISIKOVURDERING OG KONSEKVENSANALYSE

Inden en behandlingsaktivitet iværksættes eller ændres væsentligt, skal den dataansvarlige gennemføre en risikovurdering af den påtænkte behandlingsaktivitet. Kirkeministeriet har fastsat regler for denne risikovurdering.

Hvis risikovurderingen viser, at behandlingsaktiviteten indebærer høj risiko i forhold til de registrerede personers rettigheder og frihedsrettigheder, skal der i henhold til databeskyttelseslovgivningen gennemføres en konsekvensanalyse vedrørende databeskyttelse. Kirkeministeriet er ansvarlig for gennemførelse af konsekvensanalyse, når risikovurderingen viser, at behandlingsaktiviteter i nye fælles systemer kan være forbundet med en høj risiko for de registrerede.

Systemejeren er ansvarlig for, at revision af konsekvensanalysen iværksættes ved væsentlige senere ændringer i behandlingsaktiviteten. Kirkeministeriet har fastsat en standardprocedure for gennemførelse af konsekvensanalyser.

Såfremt en konsekvensanalyse viser, at behandlingsaktiviteten vil medføre høj risiko, som ikke kan afhjælpes ved kompenserende foranstaltninger, rådfører Kirkeministeriet sig med Datatilsynet, før behandlingen påbegyndes.

3.8. DATABESKYTTELSE VIA DESIGN OG STANDARDINDSTILLINGER

Ved anskaffelse og udvikling af nye fælles løsninger vil Kirkeministeriet gennemføre passende tekniske og organisatoriske foranstaltninger, som er designet med henblik på

effektiv implementering af databeskyttelsesprincipper og opfyldelse af kravene i databeskyttelsesforordningen og beskytte de registreredes rettigheder.

Kirkeministeriet har i den forbindelse fastsat regler for databeskyttelse via design og standardindstillinger i forbindelse med anskaffelse og udvikling af Kirkeministeriets og folkekirkens fælles systemer.

3.9. TREDJEPARTER

3.9.1. Databehandlere

Når Kirkeministeriet og folkekirken anvender en ekstern databehandler til behandling af personoplysninger, skal den dataansvarlige myndighed eller institution inden databehandleren får adgang til personoplysninger, sørge for at:

- Sikre at databehandleren kan etablere passende tekniske og organisatoriske foranstaltninger til beskyttelse af de personoplysninger, databehandleren skal behandle på vegne af myndigheden eller institutionen.
- Indgå en skriftlig databehandleraftale, som lever op til databeskyttelseslovgivningens krav hertil. Datatilsynet har udarbejdet en standarddatabehandleraftale, som eventuelt kan benyttes.

Myndigheder og institutioner skal føre det fornødne tilsyn med at databehandleren har etableret passende tekniske og organisatoriske foranstaltninger til beskyttelse af personoplysningerne, samt sikre, at databehandlerne gennemfører løbende kontrol med deres eventuelle underdatabehandlere.

Kirkeministeriet har indgået aftale med en række af folkekirkens mest anvendte eksterne databehandlere om anvendelse af Datatilsynets standarddatabehandleraftale. Når myndigheder og institutioner (typisk menighedsråd og provstiudvalg samt kirkegårde med selvstændig bestyrelse) indgår standarddatabehandleraftalen via DAP med disse leverandører, påtager Kirkeministeriet sig at føre dette tilsyn på vegne af de dataansvarlige. Kirkeministeriet fastsætter regler for dette tilsyn.

3.10. TREDJELANDSOVERFØRSLER

Dataansvarlige myndigheder eller institutioner, som har behov for, at overføre personoplysninger til tredjelande eller internationale organisationer, bør forinden kontakte Kirkeministeriets databeskyttelsesrådgiver herom.

3.11. IT-SIKKERHED

Kirkeministeriet og folkekirkens myndigheder og institutioner skal have passende tekniske og organisatoriske foranstaltninger og et sikkerhedsniveau for beskyttelse af personoplysninger, der, under hensyn til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål, modsvarer de risici, som en behandling udgør.

I øvrigt finder Cirkulære om informationssikkerhed, herunder sikkerhedsforanstaltninger i Kirkenettet også anvendelse for beskyttelse af personoplysninger, herunder krav til kryptering, adgangsstyring, logning mv.

3.12. DATASIKKERHEDSBRUD

3.12.1. Beredskabsplaner

Kirkeministeriet udarbejder beredskabsplaner og procedurer til håndtering af brud på datasikkerheden i de fælles systemer. Disse skal inddrage alle relevante medarbejdere, herunder Kirkeministeriets databeskyttelsesrådgiveren.

3.12.2. Brud på persondatasikkerheden

Et brud på persondatasikkerheden er enhver hændelse, som fører til hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse, adgang eller anden form for kompromittering af personoplysninger i de fælles systemer.

I tilfælde af brud på persondatasikkerheden skal den dataansvarlige myndighed eller institution hurtigst muligt og inden for 72 timer efter, at den dataansvarlige er blevet opmærksom på bruddet, informere Datatilsynet herom, medmindre den dataansvarlige kan vise, at det er usandsynligt, at bruddet vil medføre risiko for registrerede personers rettigheder eller friheder.

Hvis Datatilsynet ikke informeres inden for 72 timer, skal årsagen til forsinkelsen angives. Hvis det ikke er muligt at give informationen samlet, kan informationen meddeles trinvist.

Såfremt det er sandsynligt, at bruddet på datasikkerheden vil indebære en høj risiko for de registrerede personers rettigheder, skal den dataansvarlige ligeledes underrette de registrerede uden unødig forsinkelse, medmindre databeskyttelseslovgivningen hjemler undladelse heraf.

Kirkeministeriets databeskyttelsesrådgiver skal altid orienteres i tilfælde af brud på persondatasikkerheden og uvedkommende adgang. Kirkeministeriet fastsætter nærmere procedurer for håndtering af sikkerhedsbrister og uvedkommendes adgang, herunder involvering af databeskyttelsesrådgiveren.

3.13. VEJLEDNINGS- OG OPLYSNINGSMATERIALE

Kirkeministeriet offentliggør løbende på Den digitale Arbejdsplads (i grupperummet "databeskyttelsesforordningen") vejlednings- og oplysningsmateriale, der kan medvirke til, at alle, som får adgang til persondata, får et tilstrækkeligt kendskab til persondatalovgivningen, denne politik og Kirkeministeriets interne regelsæt for behandling af persondata.

3.14. ANSVAR OG GOVERNANCE

Kirkeministeriet er ansvarlig for at opdatere denne persondatapolitik.

De enkelte myndigheder og institutioner er ansvarlig for efterlevelsen af den til enhver tid gældende databeskyttelseslovgivning, herunder som sammenfattet i denne politik. De enkelte myndigheder og institutioner udarbejder i relevant omfang underliggende retningslinjer vedrørende behandling af persondata.

3.14.1. Databeskyttelsesrådgiveren

Kirkeministeriet udpeger en databeskyttelsesrådgiver. Databeskyttelsesrådgiverens opgaver består i at overvåge efterlevelsen af databeskyttelseslovgivningen samt Kirkeministeriets regler for behandling af personoplysninger.

Databeskyttelsesrådgiveren rådgiver og vejleder Kirkeministeriet samt folkekirkens myndigheder og institutioner. Databeskyttelsesrådgiveren rådgiver desuden i forbindelse med udførelsen af konsekvensanalyser og overvåger efterlevelsen af disse.

Databeskyttelsesrådgiveren er kontaktpunkt for og samarbejder med Datatilsynet.

Databeskyttelsesrådgiveren skal have et indgående kendskab til databeskyttelseslovgivningen samt til myndigheders og institutioners behandling af personoplysninger. Databeskyttelsesrådgiveren tildeles de nødvendige ressourcer til at varetage sine opgaver.

Databeskyttelsesrådgiveren må ikke udføre opgaver, der kan medføre en interessekonflikt i forhold til varetagelsen af de ovenfor beskrevne opgaver, og Databeskyttelsesrådgiveren må ikke modtage instrukser vedrørende udførelsen af opgaverne.

3.14.2. Kontrol og dokumentation

Databeskyttelsesrådgiveren gennemfører årligt en risikobaseret monitorering af henholdsvis behandlingen af persondata og ajourføring af behandlingsfortegnelserne ved indrapportering om nye eller ændrede persondatabehandlingsaktiviteter. I forbindelse med monitorering skal systemejeren bekræfte omfanget og indholdet af processerne, som denne er ansvarlig for.

3.14.3. Rapportering

Databeskyttelsesrådgiveren rapporterer halvårligt til Kirkeministeriets ledelsesgruppe om sine iagttagelser af og eventuelle bemærkninger til følgende:

- Udviklingen i Kirkeministeriets og folkekirkens behandling og beskyttelse af personoplysninger, herunder eventuelt forslag til ændringer i ledelsens risikovurdering, som omfatter forretningskritiske processer og systemer hvori persondata behandles
- Status vedrørende tidligere identificerede mangler
- Vurdering af, om Kirkeministeriets regler og kontrolprocedurer er tilstrækkelige til at sikre overholdelse af persondatalovgivningen
- Eventuelle forslag til ændringer i regler og kontrolprocedurer

- Eventuel kontakt med Datatilsynet, som der har været i løbet af den forgangne periode.
- Eventuelt andre områder, som databeskyttelsesrådgiveren skønner er relevante for Kirkeministeriets ledelse,

Kirkeministeriet den 25. maj 2018

Christian Dons Christensen
Departementschef