

DEN NORSKE KIRKE

Færder kirkelige fellesråd

Dato:	09.08.2018	
Arkivsak	18/00044	
Dokumentnummer:	18/00044-001	
Arkivkode:	046	
Saksbehandler:	Merete Allum	

Saksnr	Sak	Møtedato
019/18	Ny personvernforordning - General Data Protection Regulation «GDPR»	04.09.2018

Saksvedlegg

Saksfremstilling

EUs nye personvernforordning (GDPR – General Data Protection Regulation) ble vedtatt i april 2016. Forordningen ble, sammen med nasjonale tillegg, til ny personopplysningslov i Norge og trådte i kraft 1. juli 2018. Hovedformålet med forordningen og den nye personopplysningsloven, er å ivareta personvernet til den enkelte ved elektronisk behandling av personopplysninger.

Personopplysninger er informasjon eller vurderinger som kan knyttes til deg som enkeltperson. For eksempel navn, adresse, telefonnummer, epost, bilnummer, fingeravtrykk, fødselsnummer mv. I tillegg er det sensitive personopplysninger som etnisk bakgrunn, straffemessige forhold, politisk – filosofisk eller religiøs oppfatning, seksuell legning og medlemskap i fagforeninger.

Personvernforordningens formål og grunnprinsipper er i betydelig grad en videreføring av det foregående personopplysningsregelverket.

Noen gjeldende krav er skjerpet mens andre krav er nye. Her nevnes spesielt:

- Styrking av den registrertes rettigheter med tanke på innsyn, korrigering, sletting mm. Den enkelte skal i størst mulig grad bestemme over egne personopplysninger og få innsyn i alt som er lagret elektronisk om en selv. Krav om sletting eller endring kan dog ikke settes over arkivloven.
- Flere plikter for databehandleransvarlig og databehandler. Behandlingsansvarlig for Den norske kirkes medlemsregister er Kirkerådet v/ daglig leder hos direktør. Kirkevergen er behandlingsansvarlig for de personopplysningene som behandles i fellesrådet. Databehandler er ulike ansatte som registrerer, behandler og sletter personopplysninger. I flere plikter ligger bl.a. strengere krav til oversikt av personopplysninger, sikre informasjonssikkerhet med tanke på konfidensialitet, integritet og tilgjengelighet, og at personopplysningene ikke lagres lenger enn det som er nødvendig for å gjennomføre formålet med behandlingen.
- For å behandle personopplysninger må den de gjelder ha samtykket hvis det ikke er hjemlet i lov eller man kan legge «berettiget interesse» til grunn. Forskrift til medlemsregisteret gir samtykke til å bruke medlemsregisteret bl.a. til tilbud om opplæring eller diakonale tiltak, i prestens arbeid, innsamlingsarbeid mm. Kirkeloven og gravferdsloven gir også samtykke til å innhente noen opplysninger (for eksempel om fester for gravsted). Behandlingsgrunnlaget

DEN NORSKE KIRKE

Færder kirkelige fellesråd

«berettiget interesse» kan benyttes for de fleste normale kirkelige aktiviteter. Dette innebærer for eksempel at vi ikke behøver å be om samtykke for å lage medlemslister etter påmelding til en aktivitet.

Dersom det skal innhentes samtykke (for eksempel ved behandling av sensitive personopplysninger), skal det være frivillig, uttrykkelig, informert og utvetydig.

Inaktivitet/passivitet er ikke lovlig samtykke og samtykkeskjema må være klart og konsist.

Tilbaketrekking av samtykke skal være like enkelt som å avgi samtykke.

- Personopplysninger kan bare behandles for de formål det er innsamlet for. Dersom man ønsker å benytte opplysningene til annet formål må det enten bes om samtykke eller så må opplysningene innhentes på nytt.
- Krav om risikovurdering først og fremst med tanke på brudd på konfidensialitet og risiko for tap av essensielle personopplysninger. Det må gjøres en vurdering på hvem som skal ha tilgang og hva som evt skal krypteres.
- Det er blitt skjerpede krav til avvikshåndtering. Virksomheten har plikt til å melde alle brudd på datasikkerhet til Datatilsynet innen 72 timer. En slik hendelse kan være feilsending av epost, at en minnepinne blir borte, datainnbrudd mm.
- Det kan gis betydelige bøter for ikke å følge den nye forordningen

Hvordan har Færder kirkelige fellesråd jobbet med dette?

Risikoanalyse:

I oppstartsfasen ble det gjennomført en risikoanalyse med ulike tema. Eksempel fra fokusområde i denne analysen er blant annet: rutiner for varsling av gravferd, informasjon på avveie (mest fokus på telefoner og epost), at lovkrav ikke oppfylles, at man får for lite informasjon. Sannsynlighet for at en uønsket hendelse kan skje ble vurdert opp mot mulige konsekvenser. Konsekvenser kan for eksempel være bøter, at omdømmet svekkes og at vi får manglende tillit hos befolkningen.

Det er utført en kartlegging (se under) blant ansatte relatert til informasjonssikkerhet. På bakgrunn av dette vil risikoanalysen bli utvidet med fokus på flere temaer i høst. Blant annet: tilgangsstyring for dokumenter lagret på felles områder og Medarbeider, sikker utskrift fra kopimaskiner, e-post til eksterne som inneholder personinformasjon, sletterrutiner, dataangrep.

Kartlegging:

I mai/ juni ble det gjennomført en grundig kartlegging av ansattes bevissthet om informasjonssikkerhet, hva slags personopplysninger som lagres digitalt og hvordan disse håndteres.

Denne kartleggingen har gitt oss et godt utgangspunkt for videre arbeid med å etablere nye rutiner og opplæring av de ansatte, samt at vi har fått en oversikt over alle personopplysninger som lagres digitalt i fellesrådet.

Det første som skal utarbeides i høst er en personvernerklæring. Her må det gis opplysninger om at personopplysninger behandles, hvilke dette er og hva som er behandlingsgrunnlaget. Det må stå noe om lagringstid (også ift arkivloven), rett til innsyn/endring/sletting og formål. Denne personvernerklæringen legges på hjemmesiden vår og skal være et aktivt dokument hver gang vi

DEN NORSKE KIRKE

Færder kirkelige fellesråd

etterspør personinformasjon. Kirkelig arbeidsgiverorganisasjon (KA) har utarbeidet et forslag på en personvernerklæring som vi kommer til å benytte som et utgangspunkt.

Kartleggingen viste at vi har relativt stor grad av informasjonssikkerhet i fellesrådet, men at de ansatte ikke har stor nok bevissthet knyttet til dette og til ny forordning. Det er ikke tillatt å lagre personopplysninger på privat PC og minnepinne benyttes i liten grad. Man benytter fagprogram og lagringsområder på server (etter innlogging/ to-trinns autentisering). Enkelte benytter privat telefon og Dropbox for lagring av navn, telefonnummer og epost, men ikke for lagring av sensitiv informasjon.

Endringer til rutiner

Flere rutiner er endret relatert til ny forordning. Dette gjelder særlig personinformasjon knyttet til gravferdshandlinger og endringer til nettsiden. På bakgrunn av utvidet risikoanalyse og kartlegging utarbeides en handlingsplan som inneholder rutiner og retningslinjer samt en opplæringsplan for de ansatte.

Forslag til vedtak

Færder kirkelige fellesråd tar informasjon til orientering.

Møtebehandling

Vedtak