DEN NORSKE KIRKE

Årsrapport 2019/2020 for personvernombudet i Den norske kirke

1. Felles personvernombud i trossamfunnet Den norske kirke

Siden 1. oktober 2019 har trossamfunnet Den norske kirke hatt et felles personvernombud.[1] Etter personvernforordningen (PVF) art 38 og 39 har personvernombudet to sentrale oppgaver:

1. gi råd til kirkens ledelse (Kirkerådet, de kirkelige fellesrådene og sognene) i spørsmål om personvern, herunder databeskyttelse og informasjonssikkerhet
2. være ombud for de registrerte (ansatte og medlemmer) i trossamfunnet Den norske kirke i spørsmål som gjelder personvern, databeskyttelse og informasjonssikkerhet

En stillingsbeskrivelse ble vedtatt av Kirkerådets direktør 1. oktober 2020[2]. Her fremgår det at personvernombudet skal

- arbeide risikobasert og gjøre en selvstendig vurdering av risikoene som er forbundet med behandlingen av personopplysninger, herunder behandlingens art, omfang, formål og sammenheng
- utføre sine oppgaver på en uavhengig måte og om nødvendig ha taushetsplikt for henvendelser fra de registrerte
- ha rett til å få den informasjon som er nødvendig fra alle organer og virksomheter som er en del av Den norske kirke
- på riktig måte og til rett tid, involveres i spørsmål som gjelder vern av personopplysninger

Perioden fra mars 2020 og frem til årsrapportens publisering har vært et unntaksår preget av pandemien med koronaviruset. Det har ikke vært mulig å gjennomføre en rekke fysiske besøk og deltakelse i informasjonsmøter og konferanser. Til gjengjeld har det vært gjennomført en rekke nettbaserte møter, samråd og kurser i tråd med at organisasjonens digitale modenhet har økt.

2. Personvern og informasjonssikkerhet

Sommeren 2018 fikk EØS-landene[3] en felles personvernlovgivning, personvernforordningen[4]. Lovgiveren ønsket at personvern og informasjonssikkerhet skulle ses i sammenheng, gjelde både offentlige og private virksomheter, og være et anliggende som havnet regelmessig på ledelsens bord i alle organisasjoner.

PVF art 24 fastsetter at ledelsen i en virksomhet skal «gjennomføre egnede tekniske og organisatoriske tiltak for å sikre og påvise at behandlingen utføres i samsvar med denne

[1] Ansatt i stillingen er cand. scient. pol. Nils G. Indahl
[2] https://kirken.no/globalassets/personvern/stillingsbeskrivelse_pvo.pdf
[3] De 27 medlemsstatene i Den europeiske union pluss Norge, Island og Liechtenstein
[4] https://lovdata.no/dokument/NL/lov/2018-06-15-38?q=personopplysningsloven

forordning. Nevnte tiltak skal gjennomgås på nytt og skal oppdateres ved behov». PVF art 32 fastsetter at den behandlingsansvarlige og databehandleren skal oppnå et sikkerhetsnivå som skal gi «evne til å sikre vedvarende konfidensialitet, integritet, tilgjengelighet og robusthet i behandlingssystemene og -tjenestene.»

Disse to bestemmelsene innebærer at et strømbrudd, vedvarende nedetid i et dataprogram, eller manglende ajourføring av et register (hvor det behandles personopplysninger) vil være et brudd på personvernforordningen. Etterlevelse krever derfor at en organisasjon systematisk ser personvern og informasjonssikkerhet som to sider av samme mynt.

I 2020 besluttet Kirkerådets ledelse å opprette en egen stilling som informasjonssikkerhets-ansvarlig (CISO[5]) i hele trossamfunnet. Fagpersonen rekrutteres våren 2021 og vil arbeide tett sammen med personvernombudet og sikkerhetsutvalget.

Trossamfunnet Den norske kirke består av en rekke rettssubjekter som på selvstendig grunnlag kan anskaffe informasjonssystemer og behandle personopplysninger. Eksempel på slike enheter er rettssubjektet Den norske kirke (som inkluderer Kirkerådet og bispedømmene), kirkelige fellesråd og sogn.

Kirkerådet og fellesrådene utøver et felles behandlingsansvar for kirkens medlemsregister og benytter noen felles informasjonssystemer også på andre områder. PVF art 26 bestemmer at de behandlingsansvarlige i slike tilfeller skal «på en åpen måte fastsette sitt respektive ansvar for å overholde forpliktelsene i denne forordning, særlig med hensyn til utøvelse av den registrertes rettigheter (...)». Sikkerhetsutvalget har behandlet et utkast til tilslutningsavtale mellom Kirkerådet og det enkelte kirkelige fellesråd på flere av sine møter og sendt disse utkastene til høring i alle deler av trossamfunnet.

Tilslutningsavtalen mellom Kirkerådet og de kirkelige fellesrådene er planlagt sendt ut våren 2021. Den fastsetter et felles behandlingsansvar for informasjonssystemer som defineres som felles. Tilslutningsavtalene gir grunnlaget for å etablere felles praksis, rutiner og godkjenning av systemer og gjør det mulig å ivareta personvernet og informasjonssikkerheten i hele trossamfunnet Den norske kirke.

3. Rådgivning og samhandling

PVF art 39 beskriver personvernombudets oppgaver. Den ene oppgaven er nevnt i PVF art 39 (1):

«Personvernombudet skal minst ha følgende oppgaver:

a) informere og gi råd til den behandlingsansvarlige eller databehandleren og de ansatte som utfører behandlingen, om de forpliktelsene de har i henhold til denne forordning (...)».

[5] CISO: Chief Information Security Officer

Den overveiende del av personvernombudets virksomhet består i å besvare henvendelser fra ansatte i kirken som ønsker råd om hvordan de kan behandle personopplysninger korrekt. Slike henvendelser er typisk:

- Hvordan registrerer/publiserer vi kirkelige handlinger?
- Hva må vi passe på når vi skriver kontrakt og databehandleravtale med en leverandør av informasjonssystem?
- Kan vi invitere medlemmer eller andre til kirkelige arrangementer, for eksempel allehelgengudstjeneste?
- Hvordan praktiserer vi tilgangsstyring og rolletildeling i våre informasjonssystemer?

Personvernombudet har gitt skriftlig råd i 44 henvendelser om personvern og informasjonssikkerhet. Disse er som hovedregel registrert i det elektroniske arkivet, Public 360.

Personvernombudet har deltatt i møtene i sikkerhetsutvalget og porteføljerådet, og stillingen er organisatorisk og fysisk plassert i seksjonen for digitalisering. Et slikt sentralt utsiktspunkt har vært avgjørende for å kunne planlegge og drive personvernarbeidet.

I 2020 ble modellen for felles digital satsing i Den norske kirke styrket. Kirkerådet vedtok i sitt møte 2. desember 2020 en digitaliseringsstrategi. En ny styringsmodell for digitalisering plasserer systemeieransvaret for trossamfunnets informasjonssystemer. Den fastslår at digitaliseringsstyret oppretter sikkerhetsutvalget og fastsetter mandat for dette. Digitaliseringsstyret består av Kirkerådets direktør, kirkevergene i Oslo, Trondheim, Bergen, Stavanger, leder av G-21 og en representant fra Norges kirkevergelag.

Personvernombudet har i perioden holdt orienteringer for og samtaler med Kirkerådets ledelse, utvidet ledergruppe, stiftsdirektørmøtet, digitaliseringsstyret, sikkerhetsutvalget, porteføljerådet og styret i Kirkevergelaget.

Etterhvert som personvernombudsordningen er blitt kjent i organisasjonen, er antallet henvendelser om å gjennomgå databehandleravtaler økt kraftig både i Kirkerådet og i de kirkelige fellesrådene. Personvernombudet har gjennomgått og gjort vurderinger av 25 databehandleravtaler, ofte i flere prosesser.

Den norske kirke har vært med og oversatt den danske malen for databehandleravtale til norsk (den finnes allerede på engelsk).[6] Denne malen har status som europeiske standardvilkår, er anbefalt av Datatilsynet, og bør være standard når trossamfunnet Den norske kirke inngår databehandleravtaler med sine leverandører.

Det foregår et arbeid for å oppdatere Kirkerådets eksisterende databehandleravtaler med viktige leverandører, med Datatilsynets mal som utgangspunkt. Blant annet er tre databehandleravtaler med Tieto EVRY inngått når det gjelder medlemsregisterets drift, datavask og forvaltning. Arbeidet med en databehandleravtale er tildels omfattende fordi det

[6] https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/databehandleravtale/databehandleravtale/hva-ma-en-databehandleravtale-inneholde/

berører ansvarsforhold, avvikshåndtering og informasjonssikkerhet, men er et viktig og nødvendig styringsdokument for den behandlingsansvarlige.

4. Kontrollvirksomhet

Personvernombudets annen oppgave er nevnt i PVF art 39 (1):

b) «kontrollere overholdelsen av denne forordning, av andre av Unionens eller medlemsstatenes personvernregler og den behandlingsansvarliges eller databehandlerens personvernretningslinjer, herunder fordeling av ansvar, holdningsskapende tiltak og opplæring av personellet som er involvert i behandlingsaktivitetene, og tilhørende revisjoner,».

Personvernombudet har samarbeidet med internrevisor om gjennomføringen av to kontrollaktiviteter:

1. *Tilsyn med medlemsregisteret våren 2020*

Det ble sammen med internrevisor og juridisk seksjon foretatt et tilsyn med to bispedømmer og fire fellesråd med medlemsregisteret (samtidig med en revisjon av gitte tilskudd til trosopplæring). Formålet var å se om reglene etterleves og om tilskudd benyttes etter formålet. Det ble gitt separate tilbakemeldinger til alle besøkte enheter og en overordnet tilbakemelding til seksjonsleder for digitalisering og Kirkerådets direktør. Tilbakemeldingene inneholdt også anbefalinger til videre tiltak som følges opp av den enkelte enhet.

For tilsynet var konklusjonen at «den lokale, årlige risikovurderingen varierer i omfang og kvalitet» og at «dokumentasjon av opplæring innen personvern og informasjonssikkerhet er ikke tilstrekkelig i forhold til lovkrav. Det gjenstår å utdanne ledere i felles ordning for personvern og informasjonssikkerhet.» I tillegg benytter mange fellesråd kommunen som databehandler (for eksempel til lønnsutbetaling) og trenger å inngå en databehandleravtale hvor kirkens sikkerhetskrav er ivaretatt.

2. *Forvaltningsrevisjon av personvern og informasjonssikkerhet høsten 2020*

På oppdrag fra kontrollutvalget ble det gjennomført en forvaltningsrevisjon av personvern og informasjonssikkerhet høsten 2020. Nord-Hålogaland bispedømme ble besøkt i Tromsø og Sør-Hålogaland bispedømme via videolink. I tillegg ble Kirkerådet besøkt dels på stedet og dels via videolink. Formålet var finne status på etterlevelsen av reglene og gi anbefalinger for å styrke etterlevelsen.

Det ble skrevet en revisjonsrapport basert på de tre besøkene, som ble lagt frem i kontrollutvalget i januar 2021. Konklusjonen var at «det er flere pågående prosesser i Kirkerådet som vil bedre etterlevelsen av PVF, men det er vesentlige mangler i etterlevelsen av kravene til databehandleravtaler, informasjonssikkerhet, medlemsregisterets integritet, samt rammeverk og risikostyring. Det er behov for å iverksette både noen umiddelbare tiltak og vesentlige strukturelle tiltak for sikre tilfredsstillende etterlevelse av kravene.»

Revisjonsrapporten inneholdt både anbefalinger om kortsiktige tiltak og langsiktige strukturtiltak. På basis av revisjonsrapporten bestemte ledelsen av det skulle lages en strategisk handlingsplan for personvern og informasjonssikkerhet. Den inneholder mål for oppfyllelse av revisjonsrapportens anmerkninger. Handlingsplanen ble lagt frem for, og tatt til etterretning av, kontrollutvalget 11. mars 2021.

Den strategiske handlingsplanen vil være et sentralt dokument i arbeidet med personvern og informasjonssikkerhet frem til utgangen av 2023. For forvaltningen/informasjons-sikkerhetsansvarlig og enhetene HR, digitalisering og bispemøtet er det fastsatt delmål (fremtidig ønsket tilstand) for hvert halvår fra 2021 til 2023. Gjennomføring, tidsplan og ressurser er beskrevet for hver enhet. Det rapporteres status for gjennomføringen til kontrollutvalget hvert halvår.

5. Håndtering av avvik

På sikkerhetsutvalgets seks møter i 2019 og 2020 har status fra personvernombudet vært en fast orienteringspost på dagsordenen. Punktet har inkludert avvikssaker som personvernombudet har blir forelagt.

- Ett avvik i ID-porten ble rapportert til Datatilsynet i henhold til PVF art 33, fulgt opp og lukket.
- Et avvik i Telias sentralbordløsning ble rapportert av databehandleren i henhold til PVF art 33 – og er likeledes fulgt opp og lukket.

Tre av henvendelsene fra de registrerte har resultert i at et kirkelig fellesråd har meldt et avvik til Datatilsynet etter råd fra personvernombudet.

Andre temaer som har vært behandlet i sikkerhetsutvalget er:

- Oppsett og tilgang til personalmapper i Public 360. Her har det forekommet feil tilganger.
- Kirkerådet og KA har laget en felles veiledning om personvern og sikkerhet i forbindelse med strømming av gudstjenester. Et møte med Datatilsynet om dette ble holdt 29. januar 2020.
- Arbeid med databehandleravtaler og råd om dette til fellesrådene.

Intet fellesråd har på eget initiativ foreslått å melde et avvik til sikkerhetsutvalget eller til Datatilsynet. Det er grunn til å tro at det er en underrapportering av avvik, noe som kan endre seg når det etableres en felles rapportering og oppfølging av avvik i systemet DraftIt.

6. Prioriteringer fremover

Ut fra de henvendelsene personvernombudet har mottatt og de observasjonene som er gjort, ønsker personvernombudet å gi et råd til ledelsen om hvilke områder som bør prioriteres i arbeidet med personvern og informasjonssikkerhet. I vurderingen er det tatt hensyn til behandlingens art, omfang, formål og sammenheng. Anbefaling:

- Sikre at de kirkelige fellesrådene skriver under tilslutningsavtalen, slik at en felles ordning for personvern og informasjonssikkerhet etableres i trossamfunnet

- Etablere stillingen som informasjonssikkerhetsansvarlig (CISO) i organisasjonen

- Gjennomføre arbeidet med å registrere behandlingsprotokoller som grunnlag for felles praksis

- Ta i bruk DraftIt som dokumentasjonsverktøy og for å håndtere og følge opp avvik (arbeidsflyt)

- Implementere e-læringsmoduler slik at alle ansatte får et tilbud om opplæring innen personvern og informasjonssikkerhet

- Revidere databehandleravtaler og intensivere dialogen med tredjepartsleverandører av fagsystemer

- Fortsette arbeidet med å oppdatere og fornye databehandleravtaler med viktige databehandlere, i særdeleshet Kirkepartner AS

Oslo, 12. mars 2021

Nils G. Indahl