



Årsrapport 2021 for personvernombudet i Den norske kirke

Hovedpunkter:

- Personvernombudet vurderer at integriteten i relasjonsopplysningene som ligger i kirkens medlemsregister, og som ble inntatt før 2018, er fallende og betyr gradvis svekket informasjonssikkerhet for de registrerte.
- I 2021 har personvernombudet gitt skriftlig råd i 192 henvendelser om personvern og informasjonssikkerhet fra ansatte og 26 henvendelser fra medlemmer eller medlemmers foresatte.
- I 2022 er det planlagt å danne et personvernnettverk med en representant fra hvert bispedømmeråd og de største kirkelige fellerådene. Medlemmene av nettverket vil fungere som en lokal ambassadør i aktuelle personvernspørsmål.
- På slutten av 2021 hadde 16 ansatte i Kirkerådet gjennomført fire kursmoduler i personvern og informasjonssikkerhet. I alt 534 brukere i hele trossamfunnet hadde tatt minst en kursmodul.
- Det er en prioritert oppgave å få på plass et ansatt- og organisasjonsregister for hele trossamfunnet. Det vil gjøre det mulig å ajourføre kontaktopplysninger om alle ansatte og ta i bruk et avvikssystem til arbeidsflyt og dokumentasjon.

1. Felles personvernombud i trossamfunnet Den norske kirke

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

1. gi råd til kirkens ledelse (Kirkerådet, de kirkelige fellerådene 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 fastsatt av Kirkerådets direktør 1. oktober 2020¹. 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

¹ https://kirken.no/globalassets/personvern/stillingsbeskrivelse_pvo.pdf



- 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

I 2020 besluttet Kirkerådets ledelse å opprette en egen stilling som informasjonssikkerhetsansvarlig (CISO). I 2021 ble stillingen besatt². Personvernombudet deltok i rekrutteringen og funksjonen har en nøkkelstilling i arbeidet med informasjonssikkerhet og personvern.

Også i 2021 har pandemien med koronaviruset begrenset møteformen i trossamfunnet. Det digitale dannelsesnivået er blitt høyere og det har vært mulig å gjennomføre en rekke nettbaserte møter, samråd og kurser. Som ledd i den årlige forvaltningsrevisjonen har det vært mulig å besøke Tunsberg og Møre bispedømmer fysisk. Dette har gitt merverdi både for personvernombudet, revisjonsgruppen og medarbeiderne.

2. Personvern og informasjonssikkerhet

Sommeren 2018 fikk EØS-landene en felles personvernlovgivning, personvernforordningen.³ 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. I en nylig personverndom (den såkalte *Legelistesaken*) uttaler Høyesterett⁴ at retten til personvern skal veies mot andre grunnleggende friheter som er sikret i Den europeiske unions pakt om grunnleggende rettigheter (2012/C 326/02).

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 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.»

I løpet av 2021 er det blitt klart at manglende integritet i trossamfunnets medlemsregister utgjør et økende problem. Siden 1. oktober 2018 har Den norske kirke ikke mottatt informasjon om relasjoner fra Folkeregisteret. Mens den lokale gravplassmyndigheten – hos det kirkelige fellesrådet - mottar tjenesten FREG fra Skatteetaten, har Skatteetaten ikke ønsket å gi trossamfunnet Den norske kirke denne tilgangspakken.

Tilbakemeldingen fra sogn og kirkelige fellesråd er at fordi informasjonen om relasjoner ikke kan ajourføres, svekkes informasjonssikkerheten gradvis. Eksempler er:

- Et medlem logger seg på Din side (Medlemsregisterets selvbetjeningsside) for å se barnets medlemsstatus. Uten relasjonsopplysninger kan den ikke verifiseres.
- I sitt medlemsregister har kirken en rekke døpte medlemmer som er avhengig av sine foreldre for å utøve sine rettigheter. De skal inviteres til fireårs-bok, seksårs-

² Elsa Aaquist Storeng er ansatt i stillingen

³ <https://lovdata.no/dokument/NL/lov/2018-06-15-38?q=personopplysningsloven>

⁴ Høyesteretts dom HR-2021-2403-A, (sak nr. 21-055809SIV-HRET) punkt 55



arrangement eller Lyvåken-arrangement for 11-åringer. Kirken ønsker å sende brev til forelderen, men har ikke dennes kontaktinformasjon fordi relasjonsdata mangler.

Personvernombudet vurderer at integriteten i relasjonsopplysningene som ligger i kirkens medlemsregister, og som ble inntatt før 2018, er fallende og betyr gradvis svekket informasjonssikkerhet for de registrerte. I *forskrift om den norske kirkes medlemsregister*⁵ og i personvernforordningen⁶ pålegges Den norske kirke å gjennomføre tiltak for å sikre integriteten i Medlemsregisteret.

Den manglende tilgangen til relasjonsdata gjør det svært vanskelig å sikre integriteten i den grad kirken ønsker. I praksis fratar det, i en rekke tilfeller, medlemmene retten til å utøve sin religion eller tro gjennom gudstjeneste, undervisning, andakt og overholdelse av religiøse skikker.⁷

Kirkerådet og fellestrådene 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 (...)». Den norske kirke har gjort dette i form av en tilslutningsavtale, hvor de to behandlingsansvarlige avtaler sine respektive forpliktelser.

Ved årsskiftet 2021/22 hadde 300 kirkelige fellestråd underskrevet tilslutningsavtalen som regulerer hvordan Kirkerådet og det enkelte kirkelige fellestråd utøver sitt felles behandlingsansvar. Avtalen var resultatet av en omfattende høringsprosess i regi av sikkerhetsutvalget i Den norske kirke.⁸ Det arbeides på å få de resterende 18 fellestrådene med i ordningen. Skulle det ikke lykkes, vil de gjenværende fellestrådene måtte etablere og finansiere en egen lokal ordning med personvernombud og informasjonssikkerhetsansvarlig.

Tilslutningsavtalene gir grunnlaget for å etablere felles praksis, rutiner og godkjenning av systemer i hele trossamfunnet Den norske kirke. De gjør det også mulig å følge opp avvik og brudd på personopplysningsikkerheten på en systematisk måte.

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 <https://lovdata.no/forskrift/2021-11-14-3326/§12>

⁶ PVF art 32 (1) (b) <https://lovdata.no/lov/2018-06-15-38/gdpr/a32>

⁷ Charteret om grunnleggende rettigheter, artikkel 10

⁸ Sikkerhetsutvalget består av representanter for Kirkerådet, de større kirkelige fellestrådene og Arbeidsgiverorganisasjonen for kirkelige virksomheter. Personvernombudet og informasjonssikkerhetsansvarlig er også med i møtene.



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?
- Kan menigheten bruke Medlemsregisteret til å kontakte sine medlemmer?
- 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 192 henvendelser om personvern og informasjonssikkerhet fra ansatte og i 26 henvendelser fra medlemmer eller medlemmers foresatte.

Personvernombudet har deltatt i møtene i sikkerhetsutvalget og porteføljerådet, og stillingen er organisatorisk og fysisk plassert i seksjonen for digitalisering. Et slikt sentralt utsiktspunkt er 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, sikkerhetsutvalget, porteføljerådet, HR-forum, styret i Kirkevergelaget, årsmøtet i Nord-Hålogaland kirkevergelag og Møre bispedømmeråd. Dialogen med kirkevergelagets årsmøter fortsetter.

I 2022 er det planlagt å danne et personvernnettverk med en representant fra hvert bispedømmeråd og de største kirkelige fellesrådene. Medlemmene av nettverket vil fungere som en lokal ambassadør i aktuelle personvernspørsmål.

Tilslutningsavtalene gjør at et økende antall kirkeverger henvender seg til personvernombudet for å søke råd. Antallet henvendelser om å gjennomgå databehandleravtaler er økt kraftig både i Kirkerådet og i de kirkelige fellesrådene. Personvernombudet har gjennomgått og gjort vurderinger av 29 databehandleravtaler, noen i samarbeid med informasjonssikkerhetsansvarlig. Blant disse har vært anskaffelse av nytt elektronisk system for forhåndsvalg, oppgradering av nettpubliseringsplattform, og registeret *Veien til vigsling*.



Den norske kirke fortsetter å anbefale Det europeiske personvernrådets mal for databehandleravtale, som Den norske kirke har vært med å oversette til norsk.⁹ Malen har status som europeiske standardvilkår, er anbefalt av Datatilsynet, og bør fortsatt være standard når trossamfunnet inngår databehandleravtaler med sine leverandører.

Det foregår et arbeid for å oppdatere Kirkerådets eksisterende databehandleravtaler med viktige leverandører, med Personvernrådets mal som utgangspunkt. Det er inngått sentrale databehandleravtaler med Vitec Agrando AS og Kirkeidata AS og det arbeides med å utvikle felles standarder for informasjonssikkerhet og personvern sammen med disse leverandørene. Arbeidet med en databehandleravtale er tildels omfattende fordi det 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 takker for et godt samarbeid med internrevisor og juridisk avdeling i forbindelse med kontrollaktiviteter – og senere også med informasjonssikkerhetsansvarlig (CISO).

1. Tilsyn med Medlemsregisteret våren 2021

Det ble sammen med internrevisor og juridisk seksjon foretatt et tilsyn med to bispedømmer, Borg bispedømme og Nord-Hålogaland bispedømme, og til sammen 35 kirkelige fellesråd i de to bispedømmene. Tilsynet ble gjennomført ved spørreundersøkelser.

Formålet med tilsynet var å gi best mulig veiledning, støtte og føre kontroll med at reglene for personvern og informasjonssikkerhet følges i forvaltningen av Medlemsregisteret.

Det ble gitt separate tilbakemeldinger til besøkte bispedømmer og en felles tilbakemelding til fellesråd. En overordnet tilbakemelding ble gitt til seksjonsleder for digitalisering og Kirkerådet direktør. Tilbakemeldingene inneholdt også anbefalinger til videre tiltak og som følges opp av den enkelte enhet.

Konklusjonen for personvern og informasjonssikkerhet var at fellesråd har begynt å etablere rutiner og prosesser, men har behov for å avklare flere forhold knyttet til bl.a. behandlingsgrunnlag ved strømming av gudstjenester (inkludert gudstjenester med gravferd), å informere de registrerte, korrekt bruk av elektronisk arkiv, og veiledning om sikker kommunikasjon.

⁹ <https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/databehandleravtale/databehandleravtale/hva-ma-en-databehandleravtale-inneholde/>



2. Forvaltningsrevisjon av personvern og informasjonssikkerhet høsten 2021

På oppdrag av kontrollutvalget ble det gjennomført en forvaltningsrevisjon (fase 2) av personvern og informasjonssikkerhet høsten 2021. I revisjonsgruppen deltok – i tillegg til personvernombudet - internrevisor, CISO og en ekstern revisor fra KPMG. Tre bispedømmer ble besøkt; Møre bispedømme, Tunsberg bispedømme og Nidaros bispedømme (via møtelenke i Teams). Seks bispedømmer deltok i en spørreundersøkelse. Dette betyr at i 2021 og 2021 har alle bispedømmene deltatt i revisjon av personvern og informasjonssikkerhet.

Formålet var finne status på etterlevelsen av reglene og gi anbefalinger for å styrke fremtidig etterlevelse. Det ble skrevet en revisjonsrapport basert på de tre besøkene og spørreundersøkelsen. Rapporten ble presentert i kontrollutvalget 2. februar 2022.

Konklusjonen var at «Bispedømmene har etablert enkelte rutiner for håndtering av personvern og informasjonssikkerhet. Det mangler et helhetlig rammeverk for informasjonssikkerhet og behandling av personopplysninger med rutiner og retningslinjer tilpasset rettssubjektet. Det er gitt anbefalinger om opplæring av ansatte for å heve kompetansen innen personvern og informasjonssikkerhet og til etablering av nye rutiner og databehandleravtaler (...)»

Revisjonsrapporten inneholdt både anbefalinger om kortsiktige tiltak og langsiktige strukturtiltak. Tiltakene som ledelsen beslutter legges inn i den strategiske handlingsplanen for personvern og informasjonssikkerhet - som ble etablert i 2021 - følges opp av personvernombudet støttet av internrevisjonen.

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, bispemøtet og kommunikasjon, er det fastsatt delmål (fremtidig ønsket tilstand) for hvert halvår fra 2022 til 2023. Gjennomføring, tidsplan og ressurser er beskrevet for hver enhet. Det rapporteres status for gjennomføringen til kontrollutvalget hvert halvår.

5. Holdningsskapende tiltak

I mai 2021 ble det sendt ut en spørreundersøkelse om personvern til 5 300 e-postadresser i trossamfunnet Den norske kirke. 1 100 svarte på undersøkelsen. Disse ble senere invitert til å registrere seg i e-læringssystemet Motimate, hvor 4 kursmoduler ble gjort tilgjengelig:

1. Prinsippene for personvern
2. Personopplysninger i arbeidet
3. Medlemsregisteret
4. Avvikshåndtering

På slutten av 2021 hadde 16 ansatte i Kirkerådet gjennomført fire kursmoduler. I alt 534 brukere i hele trossamfunnet hadde tatt en eller flere kursmoduler i Motimate. Av disse ble 170 ansatte i rettssubjektet invitert med over i den nye læringsplattformen Educatia. Educatia gjør det mulig å tilby kurspakker til forskjellige ansattgrupper, og gjør at arbeidsledere kan invitere sine ansatte til å ta bestemte kurs. Når et ansatt- og



organisasjonsregister er på plass for hele trossamfunnet, vil alle ansatte kunne dra nytte av et omfattende kurstilbud i Educatia.

I desember 2021 ble ytterligere 3 kursmoduler gjort tilgjengelig på området personvern:

5. De registrertes rett til innsyn
6. Mobile enheter
7. Databehandleravtaler

Kursene vil være tilgjengelig på begge læringsplattformer inntil alle ansatte i trossamfunnet har tilgang til den nye læringsplattformen Educatia i løpet av 2022. Dermed vil det være mulig for alle ansatte i trossamfunnet å ta kurs i personvern også i utrullingsperioden.

6. Håndtering av avvik

På sikkerhetsutvalgets fire møter i 2021 har status fra personvernombudet vært en fast orienteringspost på dagsordenen. Punktet har inkludert avvikssaker som personvernombudet har blitt forelagt. De fleste avvik er meldt til Datatilsynet i henhold til PVF art 33, fulgt opp og lukket. Blant avvikene kan nevnes:

- En oppdatering av fagsystemet Medarbeideren førte til at interne notater i en kalender ble publisert på internett i 14 kirkelige fellesråd (avviket ble meldt av Bærum kirkelige fellesråd)
- Ved elektronisk påmelding til konfirmasjon i fagsystemet fra Kirkeidata ble alle opplysningene i påmeldingen – inkludert helseopplysninger – sendt i e-post til foreldrene
- Kommentarfeltet i Medlemsregisteret har vært brukt å notere helseopplysninger om medlemmer, hvilket kirken ikke har behandlingsgrunnlag for
- 12 707 kirkelige handlinger er ikke korrekt registrert i Medlemsregisteret med fødselsnummer (tallet kan inkludere dobbelregistreringer)
- Elektronisk arkiv (P360) har i enkelte tilfeller vært brukt til å arkivere vandelsattest

Andre temaer som har vært behandlet i sikkerhetsutvalget er:

- Oppsett og tilgang til personalmapper i Public 360. Her har søknader vært overført fra Webcruiter til elektronisk arkiv uten behandlingsgrunnlag.
- Arbeid med databehandleravtaler og råd om dette til fellesrådene.

I tillegg til avviket som er nevnt i det første kulepunktet over, har ett fellesråd meldt et brudd på personopplysningssikkerheten i 2021, som er meldt til Datatilsynet. Det er grunn til å tro at det er en underrapportering av avvik i trossamfunnet, noe som kan endre seg når det etableres en felles rapportering og oppfølging av avvik i et elektronisk avvikssystem.

7. Prioriteringer fremover

Ledelsen har - i dialog med Kontrollutvalget - besluttet å iverksette en strategisk handlingsplan for personvern og informasjonssikkerhet for perioden 2021 - 23. Blant tiltakene som skal gjøres i 2022 er å:



- Fullføre arbeidet med behandlingsprotokoller i trossamfunnet i henhold til PVF art 30
- Gjennomføre en risikovurdering av Bispemøtets register *Veien til vigsling*
- Gjennomføre en DPIA for kameraovervåking og adgangskontroll i Kirkens Hus, hos bispedømmene, samt for det elektroniske arkivet Public 360
- Sørge for at databehandleravtaler er på plass på bispedømmekontorene for databehandlere som leverer tilgangskontroll og kameraovervåking av bygninger
- Gjennomføre kontrolltiltak for å se at reglene for strømming av gudstjenester etterleves

Som oppfølging av forvaltningsrevisjonen 2021 (innen personvern og informasjonssikkerhet) foreslår personvernombudet at følgende tiltak tas inn i den strategiske handlingsplanen:

- Etablere et ledelsessystem (styringssystem) for informasjonssikkerhet i trossamfunnet Den norske kirke basert på internasjonale standarder
- Innføre rutiner som gjør det mulig å respondere raskt på digitale hendelser i kirkens informasjonssystemer, og innføre strakstiltak
- Få arbeidsledere til å invitere og følge opp sine ansatte slik at de gjennomgår e-læringsmodulene i personvern og informasjonssikkerhet som er tilgjengelige i læringsportalen Educatia

For øvrig, 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:

- Gi fullmakter, retningslinjer og ressurser som gjør det mulig for sikkerhetsutvalget å følge opp tilslutningsavtalene. Gjøre sikkerhetsutvalget i stand til å innføre langsiktige tiltak som bedrer informasjonssikkerheten og datakvaliteten i trossamfunnets medlemsregister, samt i lokale fagsystemer hos fellesråd og sogn.
- Få på plass et ansatt- og organisasjonsregister for hele trossamfunnet som gjør det mulig å få kontaktopplysninger til alle ansatte. Dermed blir det mulig å ta i bruk avvikssystemet DraftIt til arbeidsflyt og dokumentasjon av avvik.
- Rulle ut *Kirkens lokale skrivebord* – Microsofts sikkerhetsløsning med Intune og andre komponenter – for å øke sikkerheten i trossamfunnets Microsoft 365-løsning.
- Fortsette arbeidet med å oppdatere og fornye databehandleravtaler med viktige databehandlere, i særdeleshet Kirkepartner AS.



DEN NORSKE KIRKE

- Revidere databehandleravtaler og fortsette dialogen med tredjepartsleverandører av fagsystemer for å sikre bedre kontroll på personopplysninger og fagsystemer som leverer data til Medlemsregisteret.

Oslo, 1. mars 2022

Nils G. Indahl